

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

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

1. コマンドリファレンスの見方	15
1.1 対応するプログラムのリビジョン	15
1.2 コマンドリファレンスの見方	15
2. ヘルプ	17
2.1 コンソールに対する簡易説明の表示	17
2.2 コマンド一覧の表示	17
3. 機器の設定	19
3.1 ログインパスワードの設定	19
3.2 管理パスワードの設定	19
3.3 セキュリティクラスの設定	19
3.4 ログインタイマの設定	19
3.5 タイムゾーンの設定	20
3.6 現在の日付けの設定	20
3.7 現在の時刻の設定	20
3.7.1 リモートホストによる時計の設定	20
3.7.2 NTP による時計の設定	20
3.8 コンソールの言語とコードの設定	20
3.9 コンソールの表示文字数の設定	21
3.10 コンソールの表示行数の設定	21
3.11 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	21
3.12 コンソールのプロンプト表示の設定	21
3.13 SYSLOG を受けるホストの IP アドレスの設定	21
3.14 SYSLOG ファシリティの設定	21
3.15 NOTICE タイプの SYSLOG を出力するか否かの設定	22
3.16 INFO タイプの SYSLOG を出力するか否かの設定	22
3.17 DEBUG タイプの SYSLOG を出力するか否かの設定	22
3.18 LAN インタフェースパケットのダンプを SYSLOG へ出力するか否かの設定	22
3.19 PP インタフェースパケットのダンプを SYSLOG へ出力するか否かの設定	22
3.20 TFTP によりアクセスできるホストの IP アドレスの設定	23
4. ISDN 関連の設定	25
4.1 自分側の設定	25
4.1.1 PP 側の回線の種類の指定	25
4.1.2 自分の ISDN 番号の設定	25
4.1.3 i・ナンバーサービスのポート番号の設定	25
4.1.4 課金額による発信制限の設定	25
4.1.5 PIAFS の発信を許可するか否かの設定	26
4.1.6 PIAFS の着信を許可するか否かの設定	26
4.1.7 PIAFS 接続時の起動側の指定	26
4.1.8 G4 FAX の着信を拒否するとき使用する理由表示情報の設定	27

4.2	相手毎の設定	27
4.2.1	相手 ISDN 番号の設定	27
4.2.2	相手への発信順序の設定	27
4.2.3	自動接続の設定	27
4.2.4	自動切断の設定	28
4.2.5	相手にコールバック要求を行うか否かの設定	28
4.2.6	相手からのコールバック要求に応じるか否かの設定	28
4.2.7	着信許可の設定	28
4.2.8	発信許可の設定	28
4.2.9	エラー切断後の再発信禁止タイマの設定	29
4.2.10	再発信抑制タイマの設定	29
4.2.11	コールバック要求タイプの設定	29
4.2.12	コールバック受け入れタイプの設定	29
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	29
4.2.14	コールバックタイマの設定	30
4.2.15	コールバック待機タイマの設定	30
4.2.16	ISDN 回線を切断するタイマ方式の指定	30
4.2.17	切断タイマの設定 (ノーマル)	30
4.2.18	入力切断タイマの設定 (ノーマル)	30
4.2.19	出力切断タイマの設定 (ノーマル)	31
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	31
4.2.21	切断タイマの設定 (ファスト)	31
4.2.22	切断タイマの設定 (強制)	32
4.2.23	同じ相手に対して連続して認証に失敗できる回数の設定	32
4.2.24	相手先毎の課金額による発信制限の設定	32
4.2.25	相手先毎の累積接続時間による発信制限の設定	32
4.2.26	相手先毎の累積接続回数による発信制限の設定	32
5.	フレームリレー関連の設定	33
5.1	PP 側でのカプセル化の種類の設定	34
5.2	PP 側フレームリレーでの DLCI の設定	34
5.3	PP 側フレームリレーでの PVC 状態確認手順の設定	34
5.4	PP 側フレームリレーでの InARP 使用の設定	34
5.5	FR 圧縮機能の設定	35
5.6	回線に対する送信順序方式の設定	35
5.7	指定パケットに DE ビットを立てるか否かの設定	35
6.	IP の設定	37
6.1	LAN、PP 共通の設定	37
6.1.1	IP パケットを扱うか否かの設定	37
6.1.2	IP の静的経路情報の追加	37
6.1.3	IP の静的経路情報の削除	38
6.1.4	IP パケットのフィルタの設定	38
6.1.5	IP パケットのフィルタの削除	39
6.1.6	Source-route オプション付き IP パケットをフィルタアウトするか否かの設定	40
6.1.7	Directed-Broadcast パケットをフィルタアウトするか否かの設定	40
6.2	LAN 側の設定	40
6.2.1	IP アドレスの設定	40
6.2.2	LAN 側のセカンダリ IP アドレスの設定	40
6.2.3	ブロードキャストアドレスの設定	41
6.2.4	RIP のフィルタリングの設定	41
6.2.5	RIP に関して信用できるゲートウェイの設定	41
6.2.6	LAN 側 RIP2 での認証の設定	41
6.2.7	LAN 側 RIP2 での認証キーの設定	42
6.2.8	Proxy ARP の設定	42
6.2.9	LAN 側でのフィルタリングによるセキュリティの設定	42
6.2.10	LAN インタフェースの MTU の設定	42

6.3	PP 側相手毎の IP の設定	43
6.3.1	自分の PP 側 IP アドレスの設定	43
6.3.2	相手の PP 側 IP アドレスの設定	44
6.3.3	リモート IP アドレスプールの設定	44
6.3.4	PP 側のネットマスクの設定	44
6.3.5	PP 側の動的経路制御の設定	45
6.3.6	回線接続時の PP 側の RIP の動作の設定	45
6.3.7	回線接続時の PP 側の RIP 送出の時間間隔の設定	45
6.3.8	回線切断時の PP 側の RIP の動作の設定	45
6.3.9	回線切断時の PP 側の RIP 送出の時間間隔の設定	45
6.3.10	回線切断時の動的経路制御情報の保持	46
6.3.11	RIP のフィルタリングの設定	46
6.3.12	RIP ホップ加算数の設定	46
6.3.13	RIP に関して信用できるゲートウェイの設定	46
6.3.14	PP 側 RIP2 での認証の設定	46
6.3.15	PP 側 RIP2 での認証キーの設定	47
6.3.16	PP 側でのフィルタリングによるセキュリティの設定	47
6.3.17	PP インタフェースの MTU の設定	47
7.	IPsec の設定	49
7.1	事前共有鍵の登録	50
7.2	相手側セキュリティ・ゲートウェイの IP アドレス設定	50
7.3	相手側のセキュリティゲートウェイの名前設定	50
7.4	自分側セキュリティ・ゲートウェイの IP アドレス設定	50
7.5	自分側のセキュリティゲートウェイの名前の設定	51
7.6	鍵交換の再送回数と間隔の設定	51
7.7	IKE が用いる暗号アルゴリズムの設定	51
7.8	IKE が用いるグループの設定	51
7.9	IKE が用いるハッシュアルゴリズムの設定	52
7.10	自分側の ID の設定	52
7.11	IKE のログの種類の設定	52
7.12	ペイロードのタイプの設定	52
7.13	PFS を用いるか否かの設定	53
7.14	相手側の ID の設定	53
7.15	IKE の情報ペイロードを送信するか否かの設定	53
7.16	SA 関連の設定	53
7.16.1	SA のポリシーの定義	53
7.16.2	SA のポリシーの削除	54
7.16.3	IPsec SA の寿命の設定	54
7.16.4	ISAKMP SA の寿命の設定	54
7.16.5	SA の削除	54
7.16.6	SA の手動更新	54
7.16.7	SA を自動更新するか否かの設定	54
7.17	トンネルインタフェース関連の設定	55
7.17.1	使用する SA のポリシーの設定	55
7.18	IPComp 機能の設定コマンド	55
7.18.1	トンネルインタフェースに対するフィルタリングの設定	55
7.19	トランスポートモード関連の設定	56
7.19.1	トランスポートモードの定義	56
7.19.2	トランスポートモードの削除	56
8.	PPP の設定	57
8.1	相手の名前とパスワードの設定	57
8.2	相手の名前の削除	57
8.3	要求する認証タイプの設定	57
8.4	受け入れる認証タイプの設定	58
8.5	自分の名前とパスワードの設定	58
8.6	自分の名前の消去	58
8.7	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	58

8.8	LCP 関連の設定	58
8.8.1	Address & Control Field Compression オプション使用の設定	58
8.8.2	Magic Number オプション使用の設定	59
8.8.3	Maximum Receive Unit オプション使用の設定	59
8.8.4	Protocol Field Compression オプション使用の設定	59
8.8.5	パラメータ lcp-restart の設定	59
8.8.6	パラメータ lcp-max-terminate の設定	59
8.8.7	パラメータ lcp-max-configure の設定	60
8.8.8	パラメータ lcp-max-failure の設定	60
8.8.9	専用線キープアライブを使用するか否かの設定	60
8.8.10	専用線キープアライブのログをとるか否かの設定	60
8.8.11	専用線キープアライブの時間間隔の設定	60
8.8.12	専用線ダウン検出時の動作の設定	60
8.9	PAP 関連の設定	61
8.9.1	パラメータ pap-restart の設定	61
8.9.2	パラメータ pap-max-authreq の設定	61
8.10	CHAP 関連の設定	61
8.10.1	パラメータ chap-restart の設定	61
8.10.2	パラメータ chap-max-challenge の設定	61
8.11	IPCP 関連の設定	61
8.11.1	Van Jacobson Compressed TCP/IP 使用の設定	61
8.11.2	PP 側 IP アドレスのネゴシエーションの設定	61
8.11.3	パラメータ ipcp-restart の設定	62
8.11.4	パラメータ ipcp-max-terminate の設定	62
8.11.5	パラメータ ipcp-max-configure の設定	62
8.11.6	パラメータ ipcp-max-failure の設定	62
8.11.7	IPCP の MS 拡張オプションを使うか否かの設定	62
8.11.8	WINS サーバの IP アドレスの設定	62
8.12	MSCBCP 関連の設定	63
8.12.1	パラメータ msbcpc-restart の設定	63
8.12.2	パラメータ msbcpc-maxretry の設定	63
8.13	CCP 関連の設定	63
8.13.1	全パケットの圧縮タイプの設定	63
8.13.2	パラメータ ccp-restart の設定	63
8.13.3	パラメータ ccp-max-terminate の設定	63
8.13.4	パラメータ ccp-max-configure の設定	63
8.13.5	パラメータ ccp-max-failure の設定	63
8.14	MP 関連の設定	64
8.14.1	MP を使用するか否かの設定	64
8.14.2	MP の制御方法の設定	64
8.14.3	MP のための負荷閾値の設定	64
8.14.4	MP の最大リンク数の設定	64
8.14.5	MP の最小リンク数の設定	64
8.14.6	MP のための負荷計測間隔の設定	65
8.14.7	MP のパケットを分割するか否かの設定	65
8.15	BACP 関連の設定	65
8.15.1	パラメータ bacp-restart の設定	65
8.15.2	パラメータ bacp-max-terminate の設定	65
8.15.3	パラメータ bacp-max-configure の設定	65
8.15.4	パラメータ bacp-max-failure の設定	65
8.15.5	BAP/BACP 手順の設定	66
8.15.6	パラメータ bap-restart の設定	66
8.15.7	パラメータ bap-max-retry の設定	66
9.	DHCP の設定	67
9.1	DHCP の動作の設定	67
9.2	RFC2131 対応動作設定	68
9.3	DHCP スコープの定義	69
9.4	DHCP スコープの削除	69
9.5	DHCP 予約アドレスの設定	70
9.6	DHCP 予約アドレスの解除	71
9.7	重複チェック動作	71
9.8	DHCP サーバの指定の設定	72

9.9	DHCP サーバの選択方法の設定	72
9.10	DHCP BOOTREQUEST パケットの中継基準の設定	72
10.	SNMP の設定	73
10.1	読み出し専用のコミュニティ名の設定	73
10.2	読み書き可能なコミュニティ名の設定	73
10.3	認証失敗時 (authenticationFailure) にトラップを送信するか否かの設定	73
10.4	SNMP によるアクセスを許可するホストの設定	73
10.5	sysContact の設定	73
10.6	sysLocation の設定	73
10.7	sysName の設定	74
10.8	送信トラップのコミュニティ名の設定	74
10.9	トラップの受信ホストの設定	74
11.	ICMP の設定	75
11.1	ICMP Echo Reply を送信するか否かの設定	75
11.2	ICMP Mask Reply を送信するか否かの設定	75
11.3	ICMP Parameter Problem を送信するか否かの設定	75
11.4	ICMP Redirect を送信するか否かの設定	75
11.5	ICMP Redirect 受信時の処理の設定	75
11.6	ICMP Time Exceeded を送信するか否かの設定	75
11.7	ICMP Timestamp Reply を送信するか否かの設定	76
11.8	ICMP Destination Unreachable を送信するか否かの設定	76
11.9	受信した ICMP のログを記録するか否かの設定	76
12.	RADIUS の設定	77
12.1	RADIUS サーバの指定	77
12.2	RADIUS 認証サーバの指定	77
12.3	RADIUS 認証サーバの UDP ポートの設定	77
12.4	RADIUS アカウントサーバの指定	77
12.5	RADIUS アカウントサーバの UDP ポートの設定	77
12.6	RADIUS シークレットの設定	77
12.7	RADIUS 再送信パラメータの設定	78
12.8	RADIUS による認証を使用するか否かの設定	78
12.9	RADIUS によるアカウントを使用するか否かの設定	78
13.	NAT 機能	79
13.1	LAN 側インタフェースに NAT ディスクリプタを適用する設定	79
13.2	PP 側インタフェースに NAT ディスクリプタを適用する設定	79
13.3	トンネルインタフェースへの NAT ディスクリプタ適用の設定	79
13.4	NAT ディスクリプタの動作タイプを指定する	80
13.5	NAT 処理の外側 IP アドレスの設定	80
13.6	NAT 処理の内側 IP アドレスの設定	80
13.7	静的 NAT エントリの設定	81
13.8	IP マスカレード使用時の rlogin,rcp,ssh の使用許可設定	81
13.9	静的 IP マスカレードエントリの設定	81
13.10	NAT の IP アドレスマップの消去タイマの設定	81
13.11	NAT ディスクリプタの削除	81
13.12	静的 NAT エントリの削除	82
13.13	静的 IP マスカレードエントリの削除	82
13.14	設定した NAT ディスクリプタの設定状態表示	82
13.15	動作中の NAT ディスクリプタのアドレスマップの表示	82
13.16	動作中の NAT ディスクリプタの適用リストの表示	82
13.17	各インタフェース毎に NAT のアドレスマップを表示	82
13.18	NAT アドレステーブルのクリア	83
13.19	各インタフェースの NAT アドレステーブルのクリア	83
13.20	NAT でのアドレス割当の記録	83

14. DNS の設定	85
14.1 DNS サーバの IP アドレスの設定.....	85
14.2 DNS サーバを通知してもらう相手先情報番号の設定.....	85
14.3 DNS 問い合わせの内容に応じた DNS サーバの選択.....	86
14.4 DNS ドメイン名の設定.....	86
14.5 プライベートアドレスに対する問い合わせを処理するか否かの設定.....	87
14.6 DHCP/IPCP MS 拡張で DNS サーバを通知する順序の設定.....	87
14.7 SYSLOG 表示で DNS により名前解決するか否かの設定.....	87
14.8 静的 DNS レコードの登録.....	88
14.9 静的 DNS レコードの削除.....	88
14.10 静的 DNS レコードの表示.....	88
15. アナログ通信機能の設定	89
15.1 キー操作とコンソールコマンドの対応.....	90
15.2 アナログポートを使うか否かの設定.....	91
15.3 アナログポートの ISDN 番号の設定.....	91
15.4 アナログポートに接続する機器の指定.....	91
15.5 アナログポートの発信者番号を通知するか否かの設定.....	92
15.6 相手先番号による即時発信を許可するか否かの設定.....	92
15.7 ダイヤル完了ボタンの設定.....	92
15.8 グローバル着信を許可するか否かの設定.....	93
15.9 アナログポートでの識別着信をするか否かの設定.....	93
15.10 識別着信リストの登録.....	93
15.11 識別着信リストの削除.....	93
15.12 サブアドレス無し着信を許可するか否かの設定.....	94
15.13 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.....	94
15.14 話中着信を許可するか否かの設定.....	94
15.15 優先着信機能の設定.....	95
15.16 着信ベルリストの登録.....	95
15.17 着信ベルリストの削除.....	95
15.18 ナンバー・ディスプレイ設定.....	96
15.19 ナンバー・ディスプレイ信号の設定.....	96
15.20 ダイヤル桁間タイマの設定.....	96
15.21 フッキングを判定する時間の設定.....	96
15.22 フッキング後にキー操作を受け入れる時間の設定.....	97
15.23 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.....	97
15.24 アナログポートの再呼出時間設定.....	97
15.25 フレックスホン機能の使用パターンの設定.....	98
15.26 着信転送先アドレスの設定.....	98
15.27 着信転送トーキの設定.....	98
15.28 着信転送を起動するタイミングの設定.....	99
15.29 着信転送が拒否された時の動作の設定.....	99
15.30 送話 PAD の設定.....	99
15.31 受話 PAD の設定.....	100
15.32 MP 時に電話発着信のために 1B チャネルに落とすか否かの設定.....	100
15.33 TEL ポートへの切断信号の送出の設定.....	100
15.34 DTMF 検出レベルの設定.....	101
15.35 i・ナンバーサービスのポート番号の設定.....	101
15.36 アナログダイヤルインと無鳴動着信機能の設定.....	102
15.37 発番号情報なし着信機能と擬似ナンバー・リクエスト機能の設定.....	102
16. 操作	103
16.1 相手先情報番号の選択.....	103
16.2 トンネルインタフェース番号の選択.....	103

16.3	設定に関する操作	103
16.3.1	管理ユーザへの移行	103
16.3.2	設定内容の保存	103
16.3.3	終了	103
16.3.4	相手先の初期化	104
16.3.5	トンネルインタフェースの初期化	104
16.3.6	相手先毎の設定の複写	104
16.3.7	設定の初期化	104
16.3.8	遠隔地のルータの設定	104
16.3.9	遠隔地のルータからの設定に対する制限	104
16.4	動的情報のクリア操作	105
16.4.1	ARP テーブルのクリア	105
16.4.2	IP の動的経路情報のクリア	105
16.4.3	ログのクリア	105
16.4.4	アカウントのクリア	105
16.4.5	相手先毎のアカウントの消去	105
16.4.6	アナログポートに関するアカウントのクリア	105
16.4.7	DNS キャッシュのクリア	105
16.5	スケジュール	106
16.5.1	スケジュールの設定	106
16.5.2	スケジュールの削除	107
16.5.3	スケジュールの確認	107
16.6	本体に関する設定	107
16.6.1	CONN/DISC ボタンにより接続するか否かの設定	107
16.6.2	CONN/DISC ボタンにより切断するか否かの設定	107
16.6.3	アナログポート通信の接続・切断時のアラーム音の設定	107
16.6.4	データ通信の接続・切断・異常切断時のアラーム音の設定	107
16.6.5	ボタンや電話機からの操作時のクリック音の設定	108
16.6.6	MP データ通信時にリンク数変化でアラーム音を鳴らすか否かの設定	108
16.6.7	アラーム音の制御	108
16.6.8	バックライトの点灯パターンの指定	108
16.7	キューの設定	109
16.7.1	キューイングアルゴリズムタイプの選択	109
16.7.2	クラス毎のキュー長の設定	109
16.7.3	インタフェース毎のキューの表示	109
16.8	その他の操作	109
16.8.1	相手先の使用許可の設定	109
16.8.2	トンネルインタフェースの使用許可の設定	110
16.8.3	トンネルインタフェースの使用不許可の設定	110
16.8.4	相手先の使用不許可の設定	110
16.8.5	再起動	110
16.8.6	発信	110
16.8.7	切断	110
16.8.8	ping	111
16.8.9	traceroute	111
16.8.10	telnet	111
16.8.11	telnet サーバ機能の ON/OFF の設定	112
16.8.12	telnet サーバ機能の listen ポートの設定	112
16.8.13	telnet サーバへアクセスできるホストの IP アドレスの設定	112
17.	設定の表示	113
17.1	機器設定の表示	113
17.1.1	機器設定の表示	113
17.1.2	SYSLOG 関連の表示	113
17.1.3	TFTP 関連の表示	113
17.1.4	すべての設定内容の表示	113
17.1.5	指定した PP の設定内容の表示	113
17.1.6	PP 毎の設定内容の表示	114
17.2	相手先一覧の表示	114
17.2.1	相手先一覧の表示	114
17.3	ISDN 関連の表示	114
17.3.1	自分側設定の表示	114
17.3.2	相手側設定の表示	114

17.4	フレームリレー関連の表示	115
17.4.1	PP 側フレームリレー設定の表示	115
17.4.2	DLCI の表示	115
17.5	IP 関連の表示	115
17.5.1	IP パケットのフィルタの一覧表示	115
17.5.2	IP パケットのフィルタの表示	115
17.5.3	LAN 側 IP 設定の表示	115
17.5.4	PP 側 IP 設定の表示	116
17.6	PPP の設定の表示	116
17.6.1	認証関連の設定の表示	116
17.6.2	LCP 関連の設定の表示	117
17.6.3	PAP 関連の設定の表示	117
17.6.4	CHAP 関連の設定の表示	117
17.6.5	IPCP 関連の設定の表示	118
17.6.6	MSCBCP 関連の設定の表示	118
17.6.7	BACP 関連の設定の表示	118
17.6.8	CCP 関連の設定の表示	118
17.6.9	MP 関連の設定の表示	119
17.7	DHCP スコープの表示	119
17.8	DHCP サーバの状態の表示	119
17.9	SNMP 関連の設定の表示	120
17.10	ICMP 関連の設定の表示	120
17.11	RADIUS 関連の設定の表示	120
17.12	DNS 関連の設定の表示	120
17.13	WINS 関連の設定の表示	120
17.14	アナログ関係の設定の表示	121
18.	状態の表示	123
18.1	ARP テーブルの表示	123
18.2	LAN 側の状態の表示	123
18.3	PP 側の状態の表示	123
18.4	各相手先の状態の表示	123
18.5	IP の経路情報テーブルの表示	124
18.6	アナログ関係の状態の表示	124
18.7	IPsec の SA の状態の表示	124
19.	ロギング	125
19.1	ログの表示	125
19.2	アカウントの表示	125
19.3	相手先毎のアカウントの表示	125
19.4	アナログ関係のアカウントの表示	125

コマンド索引

A

account threshold	25
administrator	103
administrator password	19
alarm click	108
alarm connection analog	107
alarm connection data	107
alarm entire	108
alarm mp	108
analog arrive another-device permit	94
analog arrive global permit	93
analog arrive incomming-signal	102
analog arrive inumber-port	101
analog arrive modem signal type	96
analog arrive number display	96
analog arrive prior-port	95
analog arrive restrict	93
analog arrive restrict list add	93
analog arrive restrict list delete	93
analog arrive ringer-type list add	95
analog arrive ringer-type list delete	95
analog arrive ring-while-talking permit	94
analog arrive without-calling-number	102
analog arrive without-subaddress permit	94
analog device type	91
analog disc-signal	100
analog dtmf level	101
analog end-of-dialing-code	92
analog hooking inhibit timer	97
analog hooking timer	96
analog hooking wait timer	97
analog local address	91
analog local address notice	92
analog mp prior	100
analog pad receive	100
analog pad send	99
analog rapid call	92
analog re-ringing-timer	97
analog supplementary-service	98
analog supplementary-service call-deflection address ..	98
analog supplementary-service call-deflection reject ..99	
analog supplementary-service call-deflection ringer ..99	
analog supplementary-service call-deflection talkie ..98	
analog use	91
analog wait dial timer	96

C

clear account	105
clear analog account	105
clear arp	105
clear dns cache	105
clear ip dynamic routing	105
clear log	105
clear nat descriptor dynamic	83
clear nat descriptor interface dynamic lan	83
clear nat descriptor interface dynamic pp	83
clear nat descriptor interface dynamic tunnel	83
clear pp account	105
cold start	104
connect	110
console character	20

console columns	21
console info	21
console lines	21
console prompt	21

D

date	20
dhcp delete scope	69
dhcp relay select	72
dhcp relay server	72
dhcp relay threshold time	72
dhcp scope	69
dhcp scope bind	70
dhcp scope unbind	71
dhcp server duplicate check	71
dhcp server rfc2131 compliant	68
dhcp service	67
disconnect	110
display backlight	108
dns domain	86
dns notice order	87
dns private address spoof	87
dns server	85
dns server pp	85
dns server select	86
dns server select delete	86
dns static	88
dns static delete	88
dns syslog resolv	87

E

exit	103
exit save	103

F

fr compression use	35
fr de	35
fr dlci	34
fr inarp	34
fr lmi	34
fr pp dequeue type	35

H

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

I

ip filter	38
ip filter delete	39
ip filter directed-broadcast	40
ip filter source-route	40
ip host	88
ip host delete	88
ip icmp echo-reply send	75
ip icmp log	76
ip icmp mask-reply send	75
ip icmp parameter-problem send	75
ip icmp redirect receive	75
ip icmp redirect send	75
ip icmp time-exceeded send	75
ip icmp timestamp-reply send	76
ip icmp unreachable send	76
ip lan address	40
ip lan broadcast	41
ip lan mtu	42
ip lan nat descriptor	79

ip lan proxyarp	42
ip lan rip auth key	42
ip lan rip auth type	41
ip lan rip filter	41
ip lan rip listen	41
ip lan secondary address	40
ip lan secure filter	42
ip pp hold routing	46
ip pp local address	43
ip pp mtu	47
ip pp nat descriptor	79
ip pp netmask	44
ip pp remote address	44
ip pp remote address pool	44
ip pp rip auth key	47
ip pp rip auth type	46
ip pp rip connect interval	45
ip pp rip connect send	45
ip pp rip disconnect interval	45
ip pp rip disconnect send	45
ip pp rip filter	46
ip pp rip hop	46
ip pp rip listen	46
ip pp routing protocol	45
ip pp secure filter	47
ip route	37
ip route delete	38
ip routing	37
ip tunnel nat descriptor	79
ip tunnel secure filter	55
ipsec auto refresh	54
ipsec ike duration ipsec-sa	54
ipsec ike duration isakmp-sa	54
ipsec ike encryption	51
ipsec ike group	51
ipsec ike hash	52
ipsec ike local address	50
ipsec ike local id	52
ipsec ike local name	51
ipsec ike log	52
ipsec ike payload type	52
ipsec ike pfs	53
ipsec ike pre-shared-key	50
ipsec ike remote address	50
ipsec ike remote id	53
ipsec ike remote name	50
ipsec ike retry	51
ipsec ike send info	53
ipsec ipcomp type	55
ipsec refresh sa	54
ipsec sa delete	54
ipsec sa policy	53
ipsec sa policy delete	54
ipsec transport	56
ipsec transport delete	56
ipsec tunnel	55
isdn arrive g4-fax reject cause	27
isdn arrive inumber-port	25
isdn arrive permit	28
isdn auto connect	27
isdn auto disconnect	28
isdn call block time	29
isdn call permit	28
isdn call prohibit auth-error count	32
isdn call prohibit time	29

isdn callback mscbcpc user-specify	29
isdn callback permit	28
isdn callback permit type	29
isdn callback request	28
isdn callback request type	29
isdn callback wait time	30
isdn disconnect input time	30
isdn disconnect interval time	31
isdn disconnect output time	31
isdn disconnect policy	30
isdn disconnect time	30
isdn fast disconnect time	31
isdn forced disconnect time	32
isdn local address	25
isdn piafs arrive	26
isdn piafs call	26
isdn piafs control	26
isdn remote address	27
isdn remote address call	27
isdn remote call order	27

L

lan queue length	109
lan queue type	109
leased keepalive down	60
leased keepalive interval	60
leased keepalive log	60
leased keepalive use	60
less config	113
less config pp	113
less log	125
login password	19
login timer	19

N

nat descriptor address inner	80
nat descriptor address outer	80
nat descriptor delete	81
nat descriptor log	83
nat descriptor masquerade rlogin	81
nat descriptor masquerade static	81
nat descriptor masquerade static delete	82
nat descriptor static	81
nat descriptor static delete	82
nat descriptor timer	81
nat descriptor type	80
ntpdate	20

O

operation connect	107
operation disconnect	107

P

packetdump lan	22
packetdump pp	22
ping	111
pp account threshold	32
pp auth accept	58
pp auth clear myname	58
pp auth delete username	57
pp auth multi connect prohibit	58
pp auth myname	58
pp auth request	57
pp auth username	57
pp connect count threshold	32

pp connect time threshold32
 pp copy104
 pp default104
 pp disable110
 pp enable109
 pp encapsulation34
 pp line25
 pp queue length109
 pp queue type109
 pp select103
 ppp bacp maxconfigure65
 ppp bacp maxfailure65
 ppp bacp maxterminate65
 ppp bacp restart65
 ppp bacp use66
 ppp bap maxretry66
 ppp bap restart66
 ppp ccp maxconfigure63
 ppp ccp maxfailure63
 ppp ccp maxterminate63
 ppp ccp restart63
 ppp ccp type63
 ppp chap maxchallenge61
 ppp chap restart61
 ppp ipcp ipaddress61
 ppp ipcp maxconfigure62
 ppp ipcp maxfailure62
 ppp ipcp maxterminate62
 ppp ipcp msex62
 ppp ipcp restart62
 ppp ipcp vjc61
 ppp lcp acfc58
 ppp lcp magicnumber59
 ppp lcp maxconfigure60
 ppp lcp maxfailure60
 ppp lcp maxterminate59
 ppp lcp mru59
 ppp lcp pfc59
 ppp lcp restart59
 ppp mp control64
 ppp mp divide65
 ppp mp load threshold64
 ppp mp maxlink64
 ppp mp minlink64
 ppp mp timer65
 ppp mp use64
 ppp msbcp maxretry63
 ppp msbcp restart63
 ppp pap maxauthreq61
 ppp pap restart61

Q

quit103

R

radius account78
 radius account port77
 radius account server77
 radius auth78
 radius auth port77
 radius auth server77
 radius retry78
 radius secret77
 radius server77
 rdate20

remote setup104
 remote setup accept104
 restart110

S

save103
 schedule at106
 schedule delete107
 security class19
 show account125
 show analog account125
 show analog config121
 show arp123
 show auth116
 show command17
 show config113
 show config pp113
 show dhcp119
 show dhcp status119
 show dlci115
 show dns120
 show dns static88
 show environment113
 show fr115
 show ip filter115
 show ip filter list115
 show ip host88
 show ip icmp120
 show ip lan115
 show ip pp116
 show ip route124
 show ipsec sa124
 show isdn local114
 show isdn remote114
 show lan queue109
 show log125
 show nat descriptor address82
 show nat descriptor config82
 show nat descriptor interface address lan82
 show nat descriptor interface address pp82
 show nat descriptor interface address tunnel82
 show nat descriptor interface bind82
 show pp account125
 show pp config114
 show pp queue109
 show ppp bacp118
 show ppp ccp118
 show ppp chap117
 show ppp ipcp118
 show ppp lcp117
 show ppp mp119
 show ppp msbcp118
 show ppp pap117
 show radius120
 show remote list114
 show schedule107
 show snmp120
 show status analog124
 show status bri123
 show status lan123
 show status pp123
 show syslog113
 show tftp113
 show wins120
 snmp community read-only73

snmp community read-write	73
snmp enableauthentraps	73
snmp host	73
snmp syscontact	73
snmp syslocation	73
snmp sysname	74
snmp trap community	74
snmp trap host	74
syslog debug	22
syslog facility	21
syslog host	21
syslog info	22
syslog notice	22

T

telnet	111
telnetd host	112
telnetd listen	112
telnetd service	112
tftp host	23
time	20
timezone	20
traceroute host	111
tunnel default	104
tunnel disable	110
tunnel enable	110
tunnel select	103

W

wins server	62
-------------------	----

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 RT52pro プログラムの **Rev.4.02.04** に対応しています。
 このコマンドリファレンス作成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 URL の WWW サーバにある情報を参照してください。

- <http://www.rtpro.yamaha.co.jp/>

1.2 コマンドリファレンスの見方

このコマンドリファレンスは、ルータのコンソールから入力するコマンドを説明しています。

1つ1つのコマンドは次の項目の組合せで説明します。

項目	説明
[入力形式]	コマンドの入力形式を説明します。キー入力時には大文字と小文字のどちらを使用しても構いません。本書の文中では小文字に統一してあります。コマンドの名称部分は太字 (Bold face) で、パラメータ部分は斜体 (<i>italic face</i>) で、キーワード部分は標準書体 (Normal face) で表します。
[パラメータ]	括弧 ([]) で囲まれたパラメータは省略可能部分であることを表します。
[説明]	コマンドのパラメータの種類とその意味を説明します。
[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です。
[デフォルト値]	このコマンドのデフォルト値を示します。
[設定例]	このコマンドの具体例を示します。

2. ヘルプ

2.1 コンソールに対する簡易説明の表示

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

2.2 コマンド一覧の表示

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

3. 機器の設定

3.1 ログインパスワードの設定

- [入力形式] **login password**
 [パラメータ] なし
 [説明] 一般ユーザとしてログインするためのパスワードを設定する。コマンド入力後、パスワードを問い合わせる。

3.2 管理パスワードの設定

- [入力形式] **administrator password**
 [パラメータ] なし
 [説明] 管理ユーザとしてルータの設定を変更する為の管理パスワードを8文字以内で設定する。コマンド入力後、パスワードを問い合わせる。

3.3 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.IXlma (ダブリュー、カンマ、エル、エックス、エル、エム、エー) でもログインでき、設定の変更も可能になる。ただしシリアル経由のみ
 • off.....パスワードを入力しないとログインできない
 • *telnet*
 • on.....TELNET クライアントとして **telnet** コマンドが使用できる
 • off..... **telnet** コマンドは使用できない
 [説明] セキュリティクラスを設定する。
 [ノート] **remote setup accept** コマンドにより、遠隔地のルータらのログイン (remote setup) を細かくアクセス制限することができる。
 [デフォルト値] *level* = 1
 forget = on
 telnet = off

3.4 ログインタイマの設定

- [入力形式] **login timer time**
 [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

3.5 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

3.6 現在の日付けの設定

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

3.7 現在の時刻の設定

- [入力形式] **time** *time*
- [パラメータ] • *time* hh:mm:ss
- [説明] 現在の時刻を設定する。

3.7.1 リモートホストによる時計の設定

- [入力形式] **rdate** *host* [syslog]
- [パラメータ] • *host*
- リモートホストの IP アドレス (xxx.xxx.xxx.xxx (xxx は 10 進数))
 - ホストの名称
- syslog
- 出力結果を SYSLOG へ出力することを表すキーワード
- [説明] ルータの時計を、パラメータで指定したホストの時間に合わせる。
- [ノート] RT52pro 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。

3.7.2 NTP による時計の設定

- [入力形式] **ntpdate** *ntp_server* [syslog]
- [パラメータ] • *ntp_server*
- NTP サーバの IP アドレス (xxx.xxx.xxx.xxx (xxx は 10 進数))
 - NTP サーバの名称
- syslog
- 出力結果を SYSLOG へ出力することを表すキーワード
- [説明] NTP を利用してルータの時計を設定する。
- [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。RT52pro 自身は NTP サーバとはなれない。
- syslog キーワードを指定した場合には、コマンドの出力結果を INFO レベルの SYSLOG へ出力する。

3.8 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

3.9 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

3.10 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

3.11 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*

3.12 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

3.13 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*
- 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。
 syslog debug コマンドが *on* に設定されている場合、大量のデバッグメッセージが送信されるので、このコマンドで設定するホストには十分なディスク領域を確保しておくことが望ましい。
- [デフォルト値] *clear*

3.14 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*

3.15 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

3.16 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

3.17 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ため、syslog host に設定するホスト側には十分なディスク領域を確保しておき、必要なデータが得られたらすぐに off にする。
- [デフォルト値] off

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

- [入力形式] **packetdump lan [count]**
- [パラメータ] • *count*
- パケット数 (1..21474836)
 - off.....出力しない
 - infinity off にするまで出力する
- [説明] LAN インタフェースを入出力するパケットのダンプ情報を DEBUG タイプの SYSLOG で出力するか否か設定する。
- [デフォルト値] 100

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

- [入力形式] **packetdump pp [peer_number] [count]**
- [パラメータ] • *peer_number*...省略時は、選択されている相手について表示する
- 相手先情報番号
 - anonymous
 - leased
- *count*
- パケット数 (1..21474836)
 - off.....出力しない
 - infinity off にするまで出力する
- [説明] 選択されている相手について、PP インタフェースを入出力するパケットのダンプ情報を DEBUG タイプの SYSLOG で出力するか否か設定する。
- [デフォルト値] 100

3.20 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 アドレス TFTP によりアクセスできるホストの IP アドレス
- any すべてのホストから TFTP によりアクセスできる
- none すべてのホストから TFTP によりアクセスできない

[説明] TFTP によりアクセスできるホストの IP アドレスを設定する。

[ノート] セキュリティの観点から、プログラムのリビジョンアップや設定ファイルの読み書きが終了したらすぐに none にすること。

[デフォルト値] none

4. ISDN 関連の設定

4.1 自分側の設定

4.1.1 PP 側の回線の種類の指定

- [入力形式] **pp line line [channels]**
- [パラメータ] • *line*
- *isdn* ISDN 回線交換
 - *164* デジタル専用線 64kbit/s
 - *1128* デジタル専用線 128kbit/s
- *channels*
- *1b* B チャンネルは 1 チャンネルだけ使用
 - *2b* B チャンネルは 2 チャンネルとも使用
- [説明] PP 側の回線を指定する。デフォルト以外に設定した場合には、必ず再起動すること。
- [ノート] 別の通信機器の発着信のために 1B チャンネルを確保したい時は *channels* を *1b* にする。
- [デフォルト値] *line* = *isdn*
channels = *2b*

4.1.2 自分の ISDN 番号の設定

- [入力形式] **isdn local address isdn_number/sub_address**
isdn local address isdn_number
isdn local address /sub_address
isdn local address /
- [パラメータ] • *isdn_number* ISDN 番号
- *sub_address* ISDN サブアドレス (0x21 から 0xe の ASCII 文字)
- [説明] 自分の ISDN 番号とサブアドレスを設定する。ISDN 番号、サブアドレスとも完全に設定して運用することが推奨される。また、ISDN 番号は市外局番も含めて設定した方がよい。

4.1.3 i・ナンバーサービスのポート番号の設定

- [入力形式] **isdn arrive inumber-port inum_port [inum_port..]**
- [パラメータ] • *inum_port* i・ナンバーサービスのポート番号
- *1* ポート番号 1 で着信する
 - *2* ポート番号 2 で着信する
 - *3* ポート番号 3 で着信する
 - *all* 全てのポート番号で着信する
 - *none* 着信しない
- [説明] ルータで着信する i・ナンバーサービスのポート番号を選択する。
- [デフォルト値] *all*

4.1.4 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場合に、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よい。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** を実行するようしておく、毎月一定額以内に課金を抑えるといったことが自動で可能。
- [ノート] 課金額は通信の切断時に NTT から ISDN で通知される料金情報に基づくため、割引サービスなどを利用している場合には、最終的に NTT から請求される料金とは異なる場合がある。また、NTT 以外の通信事業者を利用して通信した場合には料金情報は通知されない。
- [デフォルト値] *off*

4.1.5 PIAFS の発信を許可するか否かの設定

[入力形式] **isdn piafs call** *sw* [*64kmode*]

- [パラメータ]
- *sw*
 - off発信を同期 PPP とする
 - 32k発信を PIAFS 32k とする
 - 64k発信を PIAFS 64k とする
 - *64kmode*
 - *guarantee* PIAFS 64k の発信ではギャランティー方式を使用する
 - *best-effort* PIAFS 64k の発信ではベストエフォート方式を使用する

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

[デフォルト値] off

[ノート] PIAFS 64k では特別なサブアドレスが用いられ、ユーザが設定したサブアドレスは無視される。

4.1.6 PIAFS の着信を許可するか否かの設定

[入力形式] **isdn piafs arrive** *arrive*

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

[説明] PIAFS の着信を許可するか否かを設定する。
 [ノート] PHS 端末側で発信者番号を通知する設定になっている必要がある。
 [デフォルト値] on

4.1.7 PIAFS 接続時の起動側の指定

[入力形式] **isdn piafs control** *sw*

- [パラメータ]
- *sw* スイッチ
 - call自分が発信側の時に PIAFS の起動側となる
 - both自分が発信側いづれの場合でも PIAFS の起動側となる
 - arrive自分が着信側の時に PIAFS の起動側となる

[説明] PIAFS を制御する側を選択する。

[設定例]

```
# pp select N
# isdn piafs control call
# pp enable N
(※ N は相手先情報番号)
```

[ノート] 本コマンドの設定と、発信 / 着信の組み合わせにより、起動側となるか被起動側となるかが以下のように決定される。

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

なお both は、本コマンド実装前の動作と同じである。

[デフォルト値] call

4.2.4 自動切断の設定

[入力形式] **isdn auto disconnect auto**

[パラメータ] • *auto*
 ◦ on.....自動切断する
 ◦ off.....自動切断しない

[説明] 選択されている相手について自動切断するか否かを設定する。
 各種切断タイマの設定を変更せずに、自動切断を無効にしたい場合に使用する。

[ノート] **schedule at** コマンドと併用して、テレホーダイ時間中に自動切断しないようにしたい場合等に有効。
 anonymous に対して使用する事はできない。

[デフォルト値] on

4.2.5 相手にコールバック要求を行うか否かの設定

[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うか否かを設定する。

[デフォルト値] off

4.2.6 相手からのコールバック要求に応じるか否かの設定

[入力形式] **isdn callback permit callback_permit**

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

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

[デフォルト値] off

4.2.7 着信許可の設定

[入力形式] **isdn arrive permit arrive**

[パラメータ] • *arrive*
 ◦ on.....許可する
 ◦ off.....許可しない

[説明] 選択されている相手からの着信を許可するか否かを設定する。

[ノート] **isdn arrive permit**、**isdn call permit** とも off を設定した時は通信できない。

[デフォルト値] on

4.2.8 発信許可の設定

[入力形式] **isdn call permit permit**

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

[説明] 選択されている相手への発信を許可するか否かを設定する。

[ノート] **isdn arrive permit**、**isdn call permit** とも off に設定した時は通信できない。

[デフォルト値] on

4.2.9 エラー切断後の再発信禁止タイマの設定

- [入力形式] **isdn call prohibit time** *time*
- [パラメータ] • *time*秒数 (60..21474836)
- [説明] 選択されている相手に発信しようとして失敗した時に、同じ相手に対し再度発信するのを禁止する時間を設定する。秒数は 0.1 秒単位で設定できる。
isdn call block time コマンドによるタイマは切断後に常に適用されるが、このコマンドによるタイマはエラー切断にのみ適用される点が異なる。
- [デフォルト値] 60

4.2.10 再発信抑制タイマの設定

- [入力形式] **isdn call block time** *time*
- [パラメータ] • *time*秒数 (0..15)
- [説明] 選択されている相手との通信が切断された後、同じ相手に対し再度発信するのを禁止する時間を設定する。秒数は 0.1 秒単位で設定できる。
isdn call prohibit time コマンドによるタイマはエラーで切断された時だけに適用されるが、このコマンドによるタイマは正常切断でも適用される点が異なる。
- [ノート] 切断後すぐに発信ということを繰り返す状況では適当な値を設定すべきである。
isdn forced disconnect time コマンドと併用するとよい。
- [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 1 つでもあればそれに対してのみコールバックする。しかし、Anonymous への着信で、発信者番号通知がなく、コールバックのために使用でき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** *type time*
- [パラメータ] • *type*
- 1b1B でコールバックする場合
 - 2b2B もしくは any でコールバックする場合
- *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] 5 秒

4.2.15 コールバック待機タイマの設定

- [入力形式] **isdn callback wait time** *time*
- [パラメータ] • *time*.....秒数 (1..60)
- [説明] 選択されている相手にコールバックを要求し、それが受け入れられていったん回線が切断されてから、このタイマがタイムアウトするまで相手からのコールバックによる着信を受け取れなかった場合には接続失敗とする。秒数は 0.1 秒単位で設定できる。
- [デフォルト値] 60

4.2.16 ISDN 回線を切断するタイマ方式の指定

- [入力形式] **isdn disconnect policy** *type*
- [パラメータ] • *type*
- 1単純トラフィック監視方式
 - 2課金単位時間方式
- [説明] 単純トラフィック監視方式は従来型の方式であり、**isdn disconnect time**、**isdn disconnect input time**、**isdn disconnect output time** の 3 つのタイマコマンドでトラフィックを監視し、一定時間パケットが流れなくなった時点で回線を切断する。
- 課金単位時間方式では、課金単位時間と監視時間を **isdn disconnect interval time** コマンドで設定し、監視時間中にパケットが流れなければ課金単位時間の倍数の時間で回線を切断する。通信料金を減らす効果が期待できる。
- [デフォルト値] 1

4.2.17 切断タイマの設定 (ノーマル)

- [入力形式] **isdn disconnect time** *time*
- [パラメータ] • *time*
- 秒数(1..21474836)
 - off.....タイマを設定しない
- [説明] 選択されている相手について PP 側のデータ送受信がない時の切断までの時間を設定する。秒数は 0.1 秒単位で設定できる。
- [ノート] 本コマンドの設定値を X 秒、**isdn disconnect input time** コマンドの設定値を IN 秒、**isdn disconnect output time** コマンドの設定値を OUT 秒とする。
- X>IN または X>OUT のように設定した場合、パケットの入出力が観測されないと X 秒で切断される。
- [デフォルト値] 60

4.2.18 入力切断タイマの設定 (ノーマル)

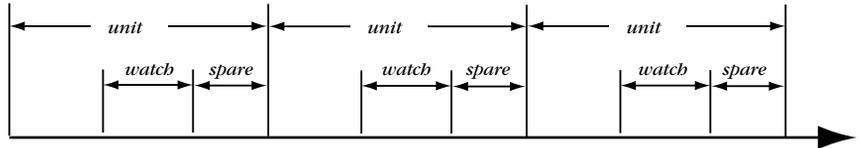
- [入力形式] **isdn disconnect input time** *time*
- [パラメータ] • *time*
- 秒数(1..21474836)
 - off.....タイマを設定しない
- [説明] 選択されている相手について PP 側からデータ受信がない時の切断までの時間を設定する。秒数は 0.1 秒単位で設定できる。
- [ノート] 例えば、UDP パケットを定期的に出すようなプログラムが暴走したような時、このタイマを設定しておくことにより回線を切断することができる。
- 30 ページの切断タイマの設定 (ノーマル) のノート参照。
- [デフォルト値] 120

4.2.19 出力切断タイマの設定 (ノーマル)

- [入力形式] **isdn disconnect output time time**
- [パラメータ] • *time*
- 秒数.....(1..21474836)
 - off タイマを設定しない
- [説明] 選択されている相手について PP 側へのデータ送信がない時の切断までの時間を設定する。秒数は 0.1 秒単位で設定できる。
- [ノート] 例えば、UDP パケットを定期的に出すようなプログラムが暴走したような場合、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。
- 30 ページの切断タイマの設定 (ノーマル) のノート参照。
- [デフォルト値] 120

4.2.20 課金単位時間方式での課金単位時間と監視時間の設定

- [入力形式] **isdn disconnect interval time unit watch spare**
- [パラメータ] • *unit*.....課金単位時間
- 秒数 (1..21474836)
 - off
- *watch*.....監視時間
- 秒数 (1..21474836)
 - off
- *spare*.....切断余裕時間
- 秒数 (1..21474836)
 - off
- [説明] 課金単位時間方式で使われる、課金単位時間と監視時間を設定する。秒数は 0.1 秒単位で設定できる。それぞれの意味は下図のとおり：



watch で示した間だけトラフィックを監視し、この間にパケットが流れなければ回線を切断する。*spare* は切断処理に時間がかかりすぎて、実際の切断が単位時間を越えないように余裕を持たせるために使う。

回線を接続している時間が *unit* の倍数になるので、単純トラフィック監視方式よりも通信料金を減らす効果が期待できる。

- [デフォルト値] *nunit* = 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場合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** コマンドで off 設定時には、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。

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 同じ相手に対して連続して認証に失敗できる回数の設定

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

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

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

pp auth accept / pp auth request / pp auth myname / pp auth username / pp auth clear myname / pp auth delete username

[デフォルト値] 5

4.2.24 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。

off

4.2.25 相手先毎の累積接続時間による発信制限の設定

[入力形式] **pp connect time threshold time**

[パラメータ] • *time*
◦ 秒数 (1..21474836)
◦ off累積接続時間による発信制限機能を使わない

[説明] 選択された相手先に対する累計接続時間の閾値を設定する。なお、発信時の接続時間の累計を累積接続時間として使用する。

[デフォルト値] off

4.2.26 相手先毎の累積接続回数による発信制限の設定

[入力形式] **pp connect count threshold count**

[パラメータ] • *count*
◦ 回数 (1..21474836)
◦ off.....累積接続回数による発信制限機能を使わない

[説明] 選択された相手先に対する累計接続回数の閾値を設定する。なお、発信時の接続回数の累計を累積接続回数として使用する。累積接続回数は **clear pp account** コマンドにより 0 に設定される。

[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 HDLC¹ フレームを使用して通信しますが、PPP とフレームリレーでは HDLC フレーム内のフォーマットが異なるため、フレームリレーで運用を開始する前にはカプセル化プロトコルを指定する必要があります。カプセル化の指定は **pp encapsulation** コマンドで設定します。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。

DLCI² 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** コマンドで行います。

自動取得の場合には、PVC³ 状態確認手順の LMI⁴ により行われます。YAMAHA リモートルータは、JT-Q933 と ANSI の 2 種類の LMI をサポートしており、**fr lmi** コマンドを使用していずれかを指定します。手動設定の場合、DLCI は最大 96 個まで設定できます。ルータに設定されている DLCI は **show dlci** コマンドで確認することができます。

一般に、フレームリレーでのルーティングは 1 つの相手先情報番号に複数の相手先 (DLCI) が接続するために PP 側は **numbered** となります。相手の PP 側の IP アドレスと DLCI の対応を解決するプロトコルが InARP⁵ です。InARP を使用するかどうかは **fr inarp** コマンドで設定します。

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

データ圧縮機能によってフレームリレー回線上での通信負荷を最大 1/5 程度まで軽減することが可能です。本機能の実装は Frame Relay Forum の FRF.9 に基づいており、特に、FRF.9 のモード 1 に対応しています。データの圧縮と伸長アルゴリズムは Stac LZS を使用します。

このデータ圧縮機能を使用するか否かは **fr compression use** コマンドで設定します。

なお、このデータ圧縮機能が適用できる対地の最大数は 16 であり、これを超える数の対地に対して本機能を適用することはできません。

同じフレームリレー回線にインタフェースを複数バインドする場合、**leased** インタフェースが代表となります。

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

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

1. High level Data Link Control procedure
 2. Data Link Connection Identifier
 3. Permanent Virtual Circuit
 4. Local Management Interface
 5. Inverse Address Resolution Protocol; RFC2390

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*
- pppPPP 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。
- [デフォルト値] ppp

5.2 PP 側フレームリレーでの DLCI の設定

- [入力形式] **fr dlci dlci_num**
- [パラメータ] • *dlci_num*
- auto.....DLCI を自動取得する
 - DLCI 値 (16..991) を空白で区切って並べたもの (96 個以内)
- [説明] 選択されている相手で使用する DLCI を自動設定するか、または手動設定する。
auto の場合は PVC 状態確認手順により DLCI を自動取得する。
- [ノート] fr lmi off ではない場合に、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う
 - ansi.....ANSI T1.617 Annex D に基づいて状態確認を行う
 - offPVC 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 に設定してなければ、回線ダウンとみなされる。
- [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
- 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。
- ip pp local address** コマンドを参照。
- [デフォルト値] on

5.5 FR 圧縮機能の設定

- [入力形式] **fr compression use dlci=dlci_num type**
- [パラメータ]
- *dlci_num*
 - DLCI 値 (16..991)
 - * (すべてのデータリンク)
 - *type*
 - *stac* Stac LZS 方式を用いてデータを圧縮する
 - *cstac* cstac 方式を用いてデータを圧縮する
 - *none* データを圧縮しない
- [説明] FR のデータ圧縮機能の方式を設定する。
dlci_num パラメータには、対象となるリンクに付された自分側の DLCI 値を指定する。
 なお、このコマンドを設定している場合でも、交渉に失敗した場合には圧縮機能は働かない。
- [デフォルト値] *type* = none

5.6 回線に対する送信順序方式の設定

- [入力形式] **fr pp dequeue type type**
- [パラメータ]
- *type*
 - *serial* 順次サーチ方式
 - *round-robin* ラウンドロビン方式
- [説明] 同じフレームリレー回線に複数のインタフェースがバインドされている時の送信順序方式を設定する。
serial の場合には、同じフレームリレー回線にバインドされたインタフェースに対して順位を与え、順位の高いインタフェースから優先してパケットを送信する。
round-robin の場合には、優先順位を設定せずに全てのインタフェースから均等にパケットを送信する。
- [ノート] 相手先情報番号の若いインタフェースがより高い順位を持つものと定義する。RT52pro では、これに加えて、LEASED が最も高い順位を持つものと定義する。
- [デフォルト値] *round-robin*

5.7 指定パケットに DE ビットを立てるか否かの設定

- [入力形式] **fr de protocol filter dlci=dlci_num filter_number_list**
fr de protocol filter dlci=dlci_num clear
- [パラメータ]
- *protocol*
 - *ip* IP パケット
 - *ipx* IPX パケット
 - *bridge* ブリッジするパケット
 - *filter* 固定のキーワード
 - *dlci_num*
 - DLCI 値 (16..991)
 - * (すべてのデータリンク)
 - *filter_number_list* フィルタの番号 (1..100)
 - *clear* 設定を削除
- [説明] 指定パケットに DE ビットを立てるか否かを設定する。
filter_number_list で指定したフィルタを順番にパケットに対して適用し、マッチしたところでそのフィルタが *pass-log*、*pass-nolog*、*restrict-log*、*restrict-nolog* のいずれかであれば DE ビットを立てる。*reject-log* または *reject-nolog* である場合は DE ビットを立てない。
 フィルタ列の最後までマッチしなかった時には DE ビットを立てない。
- [デフォルト値] *clear*

6. 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
 - offIP 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。
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 の静的経路情報の追加

- [入力形式] **ip route** *ip_address[/masklen]* gateway *gateway* [*parameter*] [*gateway gateway* [*parameter*]]
- [パラメータ] • *ip_address..*送り先のホスト / ネットワーク IP アドレス
- xxx.xxx.xxx.xxx (xxx は 10 進数)
 - default
- *masklen* マスクビット数 (省略時は 32)
- *gateway*
- IP アドレス ..xxx.xxx.xxx.xxx (xxx は 10 進数)
 - pp *pp_num* [dldci=DLCI]
 - *pp_num*
 - PP 番号 (1..30)
 - leased
 - anonymous
 - キーワード *dldci=DLCI* が指定された場合は、フレームリレーの DLCI への経路
 - pp *anonymous name=name*
 - *name*PAP/CHAP による名前
 - tunnel *tunnel_num* トンネルインタフェースへの経路
 - *tunnel_num...* トンネル番号
- *parameter..* 以下のパラメータを空白で区切り複数設定可能
- filter *N* [*N..*]... フィルタ型経路の指定
 - *N* フィルタの番号 (1..100) (空白で区切り複数設定可能)
 - metric *metric* メトリックの指定
 - *metric*.....メトリック値 (1..15) (省略時は 1)
 - hide..... 出力インタフェースが PP インタフェースの場合のみ有効なオプションで、回線が接続されている場合だけ経路が有効になることを意味する
- [説明] IP の静的経路情報を追加する。
- gateway* のパラメータとしてフィルタ型経路を指定した場合には、記述されている順にフィルタを適用していき、適合したゲートウェイが選択される。
適合するゲートウェイが存在しない場合や、フィルタ型経路が指定されているゲートウェイが 1 つも記述されていない場合には、フィルタ型経路が指定されていないゲートウェイが選択される。
フィルタ型経路が指定されていないゲートウェイも存在しない場合には、その経路は存在しないものとして処理が継続される。
フィルタ型経路が指定されていないゲートウェイが複数記述された場合の経路の選択は、それらの経路を使用する時点でラウンドロビンにより決定される。
いずれの場合でも、キーワード *hide* が指定されているゲートウェイは、回線が接続している場合のみ有効で、回線が接続していない場合には評価されない。

6.1.3 IP の静的経路情報の削除

- [入力形式] **ip route delete** *ip_address[/masklen]*
- [パラメータ] • *ip_address..* 送り先のホスト / ネットワーク IP アドレス
- xxx.xxx.xxx.xxx (xxx は 10 進数)
 - default
- *masklen* マスクビット数
- [説明] IP の静的経路情報を削除する。

6.1.4 IP パケットのフィルタの設定

- [入力形式] **ip filter** *filter_num pass_reject src_addr[/mask][dest_addr[/mask]][proto [src_port_list [dest_port_list]]]*
- [パラメータ] • *filter_num ..* フィルタの番号 (1..100)
- *pass_reject*
 - *pass-log.....* 一致すれば通す (ログに記録する)
 - *pass-nolog* 一致すれば通す (ログに記録しない)
 - *reject-log* 一致すれば破棄する (ログに記録する)
 - *reject-nolog ..* 一致すれば破棄する (ログに記録しない)
 - *restrict-log* 回線が接続されていれば通し、切断されていれば破棄する (ログに記録する)
 - *restrict-nolog* 回線が接続されていれば通し、切断されていれば破棄する (ログに記録しない)
 - *src_addr* IP パケットの始点 IP アドレス
 - xxx.xxx.xxx.xxx xxx は
 - 10 進数
 - * (ネットマスクの対応するビットが 8 ビットとも 0 と同じ)
 - 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。
 - * (すべての IP アドレスに対応)
 - *dest_addr ...* IP パケットの終点 IP アドレス (*src_addr* と同じ形式)。省略した時は 1 個の * と同じ。
 - *mask* IP アドレスのビットマスク、省略した時は 0xffffffff と同じ。
src_addr 及び *dest_addr* がネットワークアドレスの場合にのみ指定可。
 - xxx.xxx.xxx.xxx (xxx は 10 進数)
 - 0x に続く 16 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 10 進数
 - プロトコルを表すニーモニック

icmp	1
tcp	6
udp	17

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

省略時は * と同じ。

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

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

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

省略した時は * と同じ。

- *dest_port_list*.....UDP、TCP のデスティネーションポート番号

[説明] IP パケットのフィルタを設定する。このコマンドで設定されたフィルタは **ip lan secure filter** コマンド、**ip pp secure filter** コマンド、**ip lan rip filter** コマンド、及び **ip pp rip filter** コマンドで用いられる。

[ノート] **restrict-log** 及び **restrict-nolog** を使ったフィルタは、回線が接続されている時だけ通せば十分で、そのために回線に発信するまでもないようなパケットに対して有効。例えば、時計をあわせる NTP パケット。

"ip filter pass ** icmp,tcp telnet" などのように、TCP/UDP 以外のプロトコルとポート番号の両方が指定されている場合、TCP/UDP 以外のパケットに関しては、ポート番号の指定をチェックしない。

"ip filter pass *** telnet" などのように、TCP/UDP と明記せずにポート番号を指定していた場合、TCP/UDP 以外もフィルタに該当する。

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

6.1.5 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。

6.1.6 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

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

- [入力形式] **ip filter directed-broadcast filter_out**
- [パラメータ] • *filter_out*
- on.....フィルタアウトする
 - off.....フィルタアウトしない
- [説明] 終点 IP アドレスが Directed-Broadcast アドレス宛になっている IP パケットをルータが接続されているネットワークにブロードキャストするか否かを設定する。
いわゆる smurf 攻撃を防止するためには on にしておく。
- [デフォルト値] off

6.2 LAN 側の設定

6.2.1 IP アドレスの設定

- [入力形式] **ip lan address ip_address/netmask**
ip lan address clear
- [パラメータ] • *ip_address*...xxx.xxx.xxx.xxx (xxx は 10 進数)
- *netmask*
 - xxx.xxx.xxx.xxx (xxx は 10 進数)
 - 0x に続く 16 進数
 - マスクビット数
 - clearRARP により IP アドレスを決定する
- [説明] LAN の IP アドレスとネットマスクを設定する。
ip_address を設定した場合には、その IP アドレスが固定的に使用される。
clear を指定した場合、パワーオン時に RARP により IP アドレスを取得しに行く。
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なしとして扱う。また、一度 clear を設定すると、次に *netmask* パラメータが指定されるまでネットマスクは IP アドレスのクラスのネットマスクに設定される。
- [デフォルト値] clear

6.2.2 LAN 側のセカンダリ IP アドレスの設定

- [入力形式] **ip lan secondary address ip_address/netmask**
ip lan secondary address clear
- [パラメータ] • *ip_address*...xxx.xxx.xxx.xxx (xxx は 10 進数)
- *netmask*
 - xxx.xxx.xxx.xxx (xxx は 10 進数)
 - 0x に続く 16 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 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。受信に関しては全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

6.2.4 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 とともに clear

6.2.5 RIP に関して信用できるゲートウェイの設定

- [入力形式] **ip 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

6.2.6 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

6.2.7 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*
- 16 進数列 RIP2 での認証キーを設定する
 - clearRIP2 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

6.2.8 Proxy ARP の設定

- [入力形式] **ip lan proxyarp** *proxyarp*
- [パラメータ] • *proxyarp*
- on.....Proxy ARP を使用する
 - off.....Proxy ARP を使用しない
- [説明] Proxy ARP を使用するか否かを設定する。
- [デフォルト値] off

6.2.9 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*
- inLAN 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、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

## 6.2.10 LAN インタフェースの MTU の設定

---

- [ 入力形式 ]     **ip lan mtu** *mtu*
- [ パラメータ ]   • *mtu* .....MTU の値 (64..1500)
- [ 説明 ]           各インタフェースの MTU の値を設定する。
- [ デフォルト値 ] 1500

## 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] **ip pp local address ip\_address[/netmask]**  
**ip pp local address clear**

- [パラメータ]
- *ip\_address*..xxx.xxx.xxx.xxx (xxx は 10 進数)
  - *netmask*
    - xxx.xxx.xxx.xxx (xxx は 10 進数)
    - 0x に続く 16 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。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。

| local 側の PP 側<br>IP アドレスの解決 |                                                 | local 側設定                                    |                                                |                                      |                                                |
|-----------------------------|-------------------------------------------------|----------------------------------------------|------------------------------------------------|--------------------------------------|------------------------------------------------|
|                             |                                                 | ppp ipcp ipaddress<br>↓<br>on                |                                                | ppp ipcp ipaddress<br>↓<br>off       |                                                |
|                             |                                                 | ip pp local<br>address<br>↓<br>clear         | ip pp local<br>address<br>↓<br>xxx.xxx.xxx.xxx | ip pp local<br>address<br>↓<br>clear | ip pp local<br>address<br>↓<br>xxx.xxx.xxx.xxx |
| remote 側設定                  | ip pp remote<br>address<br>↓<br>clear           | Unnumberd                                    | Numberd<br>(xxx.xxx.xxx.xxx)                   | Unnumberd                            | Numberd<br>(xxx.xxx.xxx.xxx)                   |
|                             | ip pp remote<br>address<br>↓<br>yyy.yyy.yyy.yyy | yyy.yyy.yyy.yyy<br>端末型接続の<br>IP アドレス<br>割り当て | Numberd<br>(xxx.xxx.xxx.xxx)<br>または<br>接続不可    | Unnumberd                            | Numberd<br>(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** 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 10 進数)
  - dhcp.....DHCP スコープから利用できるアドレスを渡す
  - 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。  
 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。

| remote 側の PP 側<br>IP アドレスの解決 |                                                 | remote 側設定                                   |                                                |                                      |                                                |
|------------------------------|-------------------------------------------------|----------------------------------------------|------------------------------------------------|--------------------------------------|------------------------------------------------|
|                              |                                                 | ppp ipcp ipaddress<br>↓<br>on                |                                                | ppp ipcp ipaddress<br>↓<br>off       |                                                |
|                              |                                                 | ip pp local<br>address<br>↓<br>clear         | ip pp local<br>address<br>↓<br>xxx.xxx.xxx.xxx | ip pp local<br>address<br>↓<br>clear | ip pp local<br>address<br>↓<br>xxx.xxx.xxx.xxx |
| local 側設定                    | ip pp remote<br>address<br>↓<br>clear           | Unnumberd                                    | Numberd<br>(xxx.xxx.xxx.xxx)                   | Unnumberd                            | Numberd<br>(xxx.xxx.xxx.xxx)                   |
|                              | ip pp remote<br>address<br>↓<br>yyy.yyy.yyy.yyy | yyy.yyy.yyy.yyy<br>端末型接続の<br>IP アドレス<br>割り当て | Numberd<br>(xxx.xxx.xxx.xxx)                   | Unnumberd                            | Numberd<br>(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.. anonymous のためにプールする IP アドレス
  - dhcp.....DHCP スコープから利用できるアドレスを渡す
  - 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。  
 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 10 進数)
  - 0x に続く 16 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 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

### 6.3.6 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

### 6.3.7 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

### 6.3.8 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

### 6.3.9 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

### 6.3.10 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 bold**
- [ パラメータ ]   • *bold*
- 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

### 6.3.11 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*

### 6.3.12 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

### 6.3.13 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

### 6.3.14 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

### 6.3.15 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*
- 16 進数列 .....RIP2 での認証キーを設定する
  - clear ..... RIP2 での認証キーを削除する
  - text ..... テキスト型の認証キーを設定する
- [説明]           選択されている相手について PP 側で RIP2 を使用する時の認証キーを設定する。  
clear の場合は認証なし。  
text の時は text の後ろに文字列で入力する。
- [デフォルト値] clear
- [設定例]       # ip pp rip auth key text testing123  
                  # ip pp rip auth key text "hello world"  
                  # ip pp rip auth key 01 02 ff 35 8e 49 a8 3a 5e 9d

### 6.3.16 PP 側でのフィルタリングによるセキュリティの設定

- [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、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

### 6.3.17 PP インタフェースの MTU の設定

- [入力形式]     **ip pp mtu mtu**
- [パラメータ]   • *mtu* .....MTU の値 (64..1500)
- [説明]           選択されている相手について、PP インタフェースの MTU の値を設定する。
- [デフォルト値] 1500



## 7. IPsec の設定

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

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

**ipsec ike duration ipsec-sa**、**ipsec ike duration isakmp-sa** コマンドで寿命を設定します。

SA の削除は **ipsec sa delete** コマンドで、SA の初期化は **ipsec refresh sa** コマンドで行います。

**ipsec auto refresh** コマンドにより、SA を自動更新させることも可能です。

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

トンネルモードは VPN (Virtual Private Network) のように利用するためのモードです。ルータがセキュリティ・ゲートウェイとなり、LAN 上に流れる IP パケットデータを暗号化して WAN 回線に流し、ルータが IPsec に必要な処理をすべて行なうので、LAN 上の始点や終点となるホストには特別な設定を必要としません。

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

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

トランスポートモードは特殊なモードであり、ルータ自身が始点または終点になる通信に対してセキュリティを保証するモードです。ルータからリモートのルータへ telnet に入るなどの特殊な場合に利用できます。トランスポートモードを使用するには **ipsec transport** コマンドで定義を行い、使用をやめるには **ipsec transport delete** コマンドで定義を削除します。

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

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

| バージョン系列     | IPsec リリース 1 | IPsec リリース 2      | IPsec リリース 3     |
|-------------|--------------|-------------------|------------------|
| 3.00        | 3.00.09 ~ 11 | -                 | -                |
| 3.01        | 3.01.07      | 3.01.11 ~         | -                |
| 4.00        | -            | 4.00.02 ~ 4.00.14 | 4.00.18 ~        |
| <b>4.02</b> | -            | -                 | <b>4.02.04 ~</b> |
| 6.00        | -            | -                 | 6.00.01 ~        |

## 7.1 事前共有鍵の登録

---

- [ 入力形式 ]     **ipsec ike pre-shared-key gateway\_id key**  
**ipsec ike pre-shared-key gateway\_id text text**  
**ipsec ike pre-shared-key gateway\_id clear**
- [ パラメータ ]   • *gateway\_id*. .....セキュリティ・ゲートウェイの識別子 (1..10)  
 • *key*..... 鍵となる 0x ではじまる 16 進数列 (最大 32 バイト)  
 • *text*..... 鍵をテキストで入力することを示すキーワード  
 • *text*..... ASCII 文字列で表した鍵 (最大 32 文字)  
 • *clear* ..... 指定したセキュリティ・ゲートウェイに対する鍵をクリアする
- [ 説明 ]           鍵交換に必要な事前共有鍵を登録する。これが設定されていない場合、鍵交換は行われ  
 ない。鍵交換を行なう相手ルータには同じ事前共有鍵が設定されている必要がある。  
 最大 10 個まで登録できる。
- [ ノート ]         登録状況は **show config** コマンドで確認する。
- [ デフォルト値 ] *clear*
- [ 設定例 ]         # ipsec ike pre-shared-key 1 text himitsu  
 # ipsec ike pre-shared-key 1 0xCDEEDC0CEDCD

## 7.2 相手側セキュリティ・ゲートウェイの IP アドレス設定

---

- [ 入力形式 ]     **ipsec ike remote address gateway\_id ip\_address**
- [ パラメータ ]   • *gateway\_id*. .....セキュリティ・ゲートウェイの識別子 (1..10)  
 • *ip\_address*  
   ◦ IP アドレス  
   ◦ *clear* .....IP アドレスをクリア  
   ◦ *any* .....自動選択
- [ 設定例 ]         相手側セキュリティ・ゲートウェイの IP アドレスを設定する。相手側セキュリティ・ゲ  
 トウェイ 1 つに対して 1 つ設定可能。
- [ デフォルト値 ] *clear*

## 7.3 相手側のセキュリティゲートウェイの名前設定

---

- [ 入力形式 ]     **ipsec ike remote name gateway\_id name**
- [ パラメータ ]   • *gateway\_id*. .....セキュリティ・ゲートウェイの識別子 (1..10)  
 • *name*  
   ◦ 名前 (最大 32 文字)  
   ◦ *clear* .....名前をクリア
- [ 説明 ]           相手側のセキュリティゲートウェイの名前を設定する。
- [ デフォルト値 ] *clear*

## 7.4 自分側セキュリティ・ゲートウェイの IP アドレス設定

---

- [ 入力形式 ]     **ipsec ike local address gateway\_id ip\_address**
- [ パラメータ ]   • *gateway\_id*. .....セキュリティ・ゲートウェイの識別子 (1..10)  
 • *ip\_address*  
   ◦ IP アドレス  
   ◦ *clear* .....IP アドレスをクリア
- [ 説明 ]           自分側セキュリティ・ゲートウェイの IP アドレスを設定する。  
*clear* を設定したときには、相手側のセキュリティ・ゲートウェイに近いインタフェースの  
 IP アドレスを用いて IKE を起動する。
- [ デフォルト値 ] *clear*

## 7.5 自分側のセキュリティゲートウェイの名前の設定

---

- [入力形式]     **ipsec ike local name gateway name**
- [パラメータ]   • *gateway\_id*. ....セキュリティ・ゲートウェイの識別子 (1..10)
- *name*
- 名前 (最大 32 文字)
- *clear* ..... 名前をクリア
- [説明]           自分側のセキュリティゲートウェイの名前を設定する。
- [デフォルト値] *clear*

## 7.6 鍵交換の再送回数と間隔の設定

---

- [入力形式]     **ipsec ike retry count interval**
- [パラメータ]   • *count* .....再送回数 (1..50)
- *interval*. ....再送間隔の秒数 (1..100)
- [説明]           鍵交換が失敗した時に鍵交換を繰り返す回数とその時間間隔を設定します。
- [デフォルト値] *count* = 10
- interval* = 5

## 7.7 IKE が用いる暗号アルゴリズムの設定

---

- [入力形式]     **ipsec ike encryption gateway\_id algorithm**
- [パラメータ]   • *gateway\_id*. ....セキュリティ・ゲートウェイの識別子 (1..10)
- *algorithm*.....暗号アルゴリズム
- *3des-cbc* .. 3DES - CBC
- *des-cbc* .... DES - CBC
- [説明]           IKE が用いる暗号アルゴリズムを設定する。
- [ノート]         IKE で始動側として働くときには、このコマンドで設定されたアルゴリズムを提案する。応答側として働くときはこのコマンドの設定に関係なく、DES-CBC と 3DES-CBC を用いることができる。
- [デフォルト値] *des-cbc*

## 7.8 IKE が用いるグループの設定

---

- [入力形式]     **ipsec ike group gateway\_id group [group]**
- [パラメータ]   • *gateway\_id*. ....セキュリティ・ゲートウェイの識別子 (1..10)
- *group* .....グループ識別子
- *modp768*
- *modp1024*
- [説明]           IKE で用いるグループを設定する。
- [ノート]         IKE で始動側として働くときにはこのコマンドで設定されたグループを提案する。応答側として働くときはこのコマンドの設定に関係なく、MODP768 と MODP1024 を用いることができる。
- 2 種類のグループを設定したときには、1 番目がフェーズ 1 で、2 番目がフェーズ 2 で提案される。グループを 1 種類しか設定しないときは、フェーズ 1 とフェーズ 2 の両方で、設定したグループが提案される。
- [デフォルト値] *modp768*

## 7.9 IKE が用いるハッシュアルゴリズムの設定

---

- [ 入力形式 ]     **ipsec ike hash gateway\_id algorithm**
- [ パラメータ ]   • *gateway\_id*.....セキュリティ・ゲートウェイの識別子 (1..10)
- *algorithm* ...ハッシュアルゴリズム
- md5..... MD5
- sha ..... SHA
- [ 説明 ]           IKE が用いるハッシュアルゴリズムを設定する。
- [ ノート ]        IKE で始動側として働くときには、このコマンドで設定されたアルゴリズムを提案する。応答側として働くときはこのコマンドの設定に関係なく、MD5 と SHA を用いることができる。
- [ デフォルト値 ] md5

## 7.10 自分側の ID の設定

---

- [ 入力形式 ]     **ipsec ike local id gateway\_id ip\_address[/mask]**  
**ipsec ike local id gateway\_id clear**
- [ パラメータ ]   • *gateway\_id*.....セキュリティ・ゲートウェイの識別子 (1..10)
- *ip\_address*.....IP アドレス
- *mask* ..... ネットマスク
- *clear* .....IP アドレスをクリア
- [ 説明 ]           IKE のフェーズ 2 で用いる自分側の ID を設定する。
- [ ノート ]        *clear* を設定したときには、ID を送信しない。*mask* パラメータを省略したときは、タイプ 1 が送信される。また、*mask* パラメータを指定したときは、タイプ 4 の ID が送信される。
- [ デフォルト値 ] clear

## 7.11 IKE のログの種類の設定

---

- [ 入力形式 ]     **ipsec ike log gateway\_id type [type...]**  
**ipsec ike log gateway\_id clear**
- [ パラメータ ]   • *gateway\_id*.....セキュリティ・ゲートウェイの識別子 (1..10)
- *type* ..... 出力するログの種類
- message-info.....IKE メッセージの内容
- payload-info.. ペイロードの処理内容
- key-info... .. 鍵計算の処理内容
- *clear* ..... ログの種類を設定しない
- [ 説明 ]           出力するログの種類を設定する。ログはすべて、syslog の debug レベルで出力される。
- [ ノート ]        *clear* を設定したときには、最小限のログしか出力しない。複数の *type* パラメータを設定することもできる。
- [ デフォルト値 ] clear

## 7.12 ペイロードのタイプの設定

---

- [ 入力形式 ]     **ipsec ike payload type gateway\_id type**
- [ パラメータ ]   • *gateway\_id*.....セキュリティ・ゲートウェイの識別子 (1..10)
- *type* ..... ペイロードのタイプ
- 1 .....IPsec リリース 2 以前
- 2 .....IPsec リリース 3
- [ 説明 ]           IKE ペイロードのタイプを設定する。YAMAHA リモートルータの古いリビジョンと接続する場合には、タイプを 1 に設定する必要がある。
- [ デフォルト値 ] 2

## 7.13 PFS を用いるか否かの設定

- [入力形式]     **ipsec ike pfs gateway\_id pfs**
- [パラメータ]   • *gateway\_id*.....セキュリティ・ゲートウェイの識別子 (1..10)
- *pfs*
- on.....用いる
- off.....用いない
- [説明]           IKE で PFS を用いるか否かを設定する。
- [ノート]         相手側のセキュリティ・ゲートウェイと同じように設定する必要がある。
- [デフォルト値] off

## 7.14 相手側の ID の設定

- [入力形式]     **ipsec ike remote id gateway\_id ip\_address[/mask]**  
**ipsec ike remote id gateway\_id clear**
- [パラメータ]   • *gateway\_id*.....セキュリティ・ゲートウェイの識別子 (1..10)
- *ip\_address*.....IP アドレス
- *mask*.....ネットマスク
- *clear*.....IP アドレスをクリア
- [説明]           IKE のフェーズ 2 で用いる相手側の ID を設定する。
- [ノート]         *clear* を設定したときには ID を送信しない。
- mask* パラメータを省略したときは、タイプ 1 の ID が送信される。また、*mask* パラメータを指定したときは、タイプ 4 の ID が送信される。
- [デフォルト値] clear

## 7.15 IKE の情報ペイロードを送信するか否かの設定

- [入力形式]     **ipsec ike send info gateway\_id info**
- [パラメータ]   • *gateway\_id*.....セキュリティ・ゲートウェイの識別子 (1..10)
- *info*
- on.....送信する
- off.....送信しない
- [説明]           IKE の情報ペイロードを送信するか否かを設定する。受信に関しては、この設定に関わらず、すべての情報ペイロードを解釈する。
- [ノート]         このコマンドは、接続性の検証などの特別な目的で使用される。定常の運用時は **on** に設定する必要がある。
- [デフォルト値] on

## 7.16 SA 関連の設定

再起動されるとすべての SA がクリアされることに注意。

### 7.16.1 SA のポリシーの定義

- [入力形式]     **ipsec sa policy policy-id gateway\_id protocol algorithm [algorithm]**
- [パラメータ]   • *policy-id*.....ポリシー ID (1..255)
- *gateway\_id*.
- セキュリティ・ゲートウェイの識別子 (1..10)
- *protocol*
- *ah*..... 認証ヘッダ (Authentication Header)
- *esp*..... 暗号ペイロード (Encapsulating Security Payload)
- *algorithm*
- *md5-hmac*.....HMAC - MD5
- *sha-hmac*.....HMAC - SHA
- *3des-cbc*.....3DES-CBC
- *des-cbc*.....DES-CBC
- [説明]           SA のポリシーを定義する。
- この定義はトンネルモード及びトランスポートモードの設定に必要である。この定義は複数のトンネルモード及びトランスポートモードで使用可能。

### 7.16.2 SA のポリシーの削除

---

- [ 入力形式 ]     **ipsec sa policy delete** *policy-id*
- [ パラメータ ]   • *policy-id* ..... ポリシー ID (1..255)
- [ 説明 ]           指定したポリシー ID のポリシーを削除する。

### 7.16.3 IPsec SA の寿命の設定

---

- [ 入力形式 ]     **ipsec ike duration ipsec-sa gateway\_id second** [*kbytes*]
- [ パラメータ ]   • *gateway\_id* .....セキュリティ・ゲートウェイの識別子 (1..10)
- *second* ..秒数 (300..691200)
- *kbytes* ...キロ単位のバイト数 (100..100000)
- [ 説明 ]           IKE で提案する IPsec SA の寿命を設定する。  
*kbytes* パラメータを指定した場合には、*second* パラメータで指定した時間を経過するか指定したバイト数のデータが処理された後に SA は消滅する。
- [ デフォルト値 ] 28800

### 7.16.4 ISAKMP SA の寿命の設定

---

- [ 入力形式 ]     **ipsec ike duration isakmp-sa gateway\_id second** [*kbytes*]
- [ パラメータ ]   • *gateway\_id* .....セキュリティ・ゲートウェイの識別子 (1..10)
- *second* ..秒数 (300..691200)
- *kbytes* ...キロ単位のバイト数 (100..100000)
- [ 説明 ]           IKE で提案する ISAKMP SA の寿命を設定する。  
*kbytes* パラメータを指定した場合には、*second* パラメータで指定した時間を経過するか指定したバイト数のデータが処理された後に SA は消滅する。
- [ デフォルト値 ] 28800

### 7.16.5 SA の削除

---

- [ 入力形式 ]     **ipsec sa delete** *id*
- [ パラメータ ]   • *id*
- SA の ID (1..128)
- all .....すべての SA
- [ 説明 ]           指定した SA を削除する。  
SA の ID は自動的に付与されるので、**show ipsec sa** コマンドで確認すること。

### 7.16.6 SA の手動更新

---

- [ 入力形式 ]     **ipsec refresh sa**
- [ パラメータ ]   なし
- [ 説明 ]           SA を手動で更新する。
- [ ノート ]         管理されている SA をすべて削除して、IKE の状態を初期化する。

### 7.16.7 SA を自動更新するか否かの設定

---

- [ 入力形式 ]     **ipsec auto refresh** *refresh*
- [ パラメータ ]   • *refresh*
- on.....自動更新する
- off.....自動更新しない
- [ 説明 ]           SA を自動更新するか否かを設定する。
- [ ノート ]         古い SA を削除せずに新しい SA を生成する。
- [ デフォルト値 ] off

## 7.17 トンネルインタフェース関連の設定

### 7.17.1 使用する SA のポリシーの設定

- [入力形式]     **ipsec tunnel policy-id**
- [パラメータ]   • *policy-id*
- ポリシー ID(1..255)
  - clear ..... ポリシーをクリアする
- [説明]            選択されているトンネルインタフェースで使用する SA のポリシーを設定する。
- [デフォルト値] clear

## 7.18 IPComp 機能の設定コマンド

- [入力形式]     **ipsec ipcomp type type**
- [パラメータ]   • *type* ..... 圧縮アルゴリズム
- deflate ..... 圧縮アルゴリズムとして deflate を使用する
  - none ..... 圧縮をしない
- [説明]            IPComp でデータ圧縮を行うかどうかを設定する。サポートしているアルゴリズムは deflate のみである。
- 受信した IPComp パケットを展開するためには、特別な設定を必要としない。すなわち、サポートしているアルゴリズムで圧縮された IPComp パケットを受信したときには、設定に関係なく展開する。
- 必ずしもセキュリティ・ゲートウェイの両方にこのコマンドを設定する必要はない。片側のみ設定した場合には、そのセキュリティ・ゲートウェイから送信される IP パケットのみが圧縮される。
- トランスポートモードのみを使用する場合には、IPComp を使用することはできない。
- [ノート]          データ圧縮には、PPP で使われる CCP や、フレームリレーで使われる FRF.9 もある。圧縮アルゴリズムとして、IPComp で使われる deflate と、CCP/FRF.9 で使われる Stac-LZS との間に基本的な違いはない。しかし、CCP/FRF.9 でのデータ圧縮は IPsec による暗号化の後に行われる。このため、暗号化でランダムになったデータを圧縮しようとすることになり、ほとんど効果がない。一方、IPComp は IPsec による暗号化の前にデータ圧縮が行われるため、一定の効果が得られる。また、CCP/FRF.9 とは異なり、対向のセキュリティ・ゲートウェイまでの全経路で圧縮されたままのデータが流れるため、例えば本機の出力行インタフェースが LAN であってもデータ圧縮効果を期待できる。
- [デフォルト値] none

### 7.18.1 トンネルインタフェースに対するフィルタリングの設定

- [入力形式]     **ip tunnel secure filter direction filter\_list [filter\_list..]**
- [パラメータ]   • *direction*
- in ..... トンネル側から入ってくるパケットのフィルタリング
  - out ..... トンネル側に出ていくパケットのフィルタリング
- *filter\_list*
- 空白で区切られた *filter\_number* の並び (100 個以内)
  - clear (フィルタリングしない)
- [説明]            **ip filter** コマンドによるパケットのフィルタを組み合わせ、トンネルインタフェースを通るパケットの種類の制限を設定する。
- [デフォルト値] clear

## 7.19 トランスポートモード関連の設定

### 7.19.1 トランスポートモードの定義

---

- [ 入力形式 ]     **ipsec transport *id* *policy\_id* [*proto* [*src\_port\_list* [*dst\_port\_list*]]]**
- [ パラメータ ]   • *id* ..... トランスポート ID(1..255)
- *policy\_id* .... ポリシー ID(1..255)
- *proto* ..... プロトコル
- *src\_port\_list* .....UDP、TCP のソースポート番号列
- ポート番号を表す 10 進数
- ポート番号を表すニーモニック
- \* (すべてのポート)
- *dst\_port\_list* .....UDP、TCP のデスティネーションポート番号列
- ポート番号を表す 10 進数
- ポート番号を表すニーモニック
- \* (すべてのポート)
- [ 説明 ]           トランスポートモードを定義する。
- 定義後、*proto*、*src\_port\_list*、*dst\_port\_list* パラメータに合致する IP パケットに対してトランスポートモードでの通信を開始する。
- [ 設定例 ]       192.168.112.25 のルータへの telnet のデータをトランスポートモードで通信。
- # ipsec ike remote address 1 192.168.112.25
- # ipsec sa policy 102 1 esp des-cbc sha-hmac
- # ipsec transport 1 102 tcp \* telnet

### 7.19.2 トランスポートモードの削除

---

- [ 入力形式 ]     **ipsec transport delete *id***
- [ パラメータ ]   • *id* ..... トランスポート ID (1..255)
- [ 説明 ]           定義してあるトランスポートモードを削除する。

## 8. PPP の設定

### 8.1 相手の名前とパスワードの設定

- [入力形式]     **pp auth username username password [isdn1] [clid [isdn2]] [mscbcp] [ip\_address]**
- [パラメータ]   • *username*... 名前 (64 文字以内)
- *password*.... パスワード (64 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** コマンドに対応)
- [説明]           相手の名前とパスワードを設定する。複数設定可。オプションで ISDN 番号が設定でき、名前と結びついたルーティングやリモート IP アドレスに対しての発信を可能にする。*isdn1* は発信用の ISDN アドレスである。*isdn1* を省略すると、この相手には発信しなくなる。名前に "\*" を与えた時にはワイルドカードとして扱い、他の名前とマッチしなかった相手に対してその設定を使用する。
- キーワード *clid* は発番号認証を利用することを指示する。このキーワードがない場合は発番号認証は行われない。発番号認証は *isdn2* があれば *isdn2* を用い、または *isdn2* がなければ *isdn1* を用い、一致したら認証は成功したとみなす。
- キーワード *mscbcp* は MS コールバックを許可することを指示する。このユーザからの着信に対しては、同時に *isdn callback permit on* に設定してあれば MS コールバックの動作を行う。

### 8.2 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 (64 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。

### 8.3 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
- *arrive-only*... .. 着信時にのみ PPP による認証を要求
- [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。
- キーワード *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*

## 8.4 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。PP 毎の  
コマンドである。
- [デフォルト値] none

## 8.5 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。

## 8.6 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。

## 8.7 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。  
anonymous が選択された時のみ有効である。
- [デフォルト値] off

## 8.8 LCP 関連の設定

### 8.8.1 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

### 8.8.2 Magic Number オプション使用の設定

- [入力形式]     **ppp lcp magicnumber** *magic\_number*
- [パラメータ]   • *magic\_number*
- 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

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

- [入力形式]     **ppp lcp mru** *mru* [*length*]
- [パラメータ]   • *mru*
- on.....用いる
  - off .....用いない
- *length*
- 1500.....1500bytes
  - 1792.....1792bytes
- [説明]            選択されている相手について [PPP,LCP] の Maximum Receive Unit オプションを用いるか否かと、MRU の長さを設定する。
- [ノート]          on を設定していても相手に拒否された時は用いない。一般には on でよいが、このオプションをつけると接続できないルータに接続する時には off にする。  
データが圧縮されている時には、*length* パラメータの設定は常に 1792 として動作する。
- [デフォルト値]  *mru* = on  
                  *length* = 1792

### 8.8.4 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

### 8.8.5 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

### 8.8.6 パラメータ lcp-max-terminate の設定

- [入力形式]     **ppp lcp maxterminate** *count*
- [パラメータ]   • *count* .....回数 (1..10)
- [説明]            選択されている相手について [PPP,LCP] の terminate-request の送信回数を設定する。
- [デフォルト値]  2



## 8.9 PAP 関連の設定

### 8.9.1 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

### 8.9.2 パラメータ pap-max-authreq の設定

---

- [入力形式]     **ppp pap maxauthreq count**  
 [パラメータ]   • *count* ..... 回数 (1..10)  
 [説明]         選択されている相手について [PPP,PAP] authenticate-request の送信回数を設定する。  
 [デフォルト値] 10

## 8.10 CHAP 関連の設定

### 8.10.1 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

### 8.10.2 パラメータ chap-max-challenge の設定

---

- [入力形式]     **ppp chap maxchallenge count**  
 [パラメータ]   • *count* ..... 回数 (1..10)  
 [説明]         選択されている相手について [PPP,CHAP] challenge の送信回数を設定する。  
 [デフォルト値] 10

## 8.11 IPCP 関連の設定

### 8.11.1 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

### 8.11.2 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 アドレスの設定コマンド、6.3.2 相手の PP 側 IP アドレスの設定コマンドを参照。  
 [デフォルト値] off

### 8.11.3 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

### 8.11.4 パラメータ ipcp-max-terminate の設定

---

- [ 入力形式 ]     **ppp ipcp maxterminate count**  
 [ パラメータ ]   • *count* .... 回数 (1..10)  
 [ 説明 ]         選択されている相手について [PPP,IPCP] の terminate-request の送信回数を設定する。  
 [ デフォルト値 ] 2

### 8.11.5 パラメータ ipcp-max-configure の設定

---

- [ 入力形式 ]     **ppp ipcp maxconfigure count**  
 [ パラメータ ]   • *count* .... 回数 (1..10)  
 [ 説明 ]         選択されている相手について [PPP,IPCP] の configure-request の送信回数を設定する。  
 [ デフォルト値 ] 10

### 8.11.6 パラメータ ipcp-max-failure の設定

---

- [ 入力形式 ]     **ppp ipcp maxfailure count**  
 [ パラメータ ]   • *count* .... 回数 (1..10)  
 [ 説明 ]         選択されている相手について [PPP,IPCP] の configure-nak の送信回数を設定する。  
 [ デフォルト値 ] 10

### 8.11.7 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 msextr msextr**  
 [ パラメータ ]   • *msextr*  
                   • on.....使用する  
                   • off.....使用しない  
 [ 説明 ]         選択されている相手について、[PPP,IPCP] の MS 拡張オプションを使うか否かを設定する。IPCP の Microsoft 拡張オプションを使うように設定すると、DNS サーバの IP アドレスと WINS(Windows Internet Name Service) サーバの IP アドレスを、接続した相手である Windows マシンに渡すことができる。渡すための DNS サーバや WINS サーバの IP アドレスはそれぞれ、**dns server** コマンドおよび **wins server** コマンドで設定する。  
 [ デフォルト値 ] off

### 8.11.8 WINS サーバの IP アドレスの設定

---

- [ 入力形式 ]     **wins server server1 [server2]**  
                   **wins server clear**  
 [ パラメータ ]   • *server1, server2*  
                   • IP アドレス (xxx.xxx.xxx.xxx(xxx は 10 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。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

## 8.12 MSCBCP 関連の設定

### 8.12.1 パラメータ `mscbcpr-start` の設定

---

- [入力形式]     **ppp mscbcpr start time**  
 [パラメータ]   • *time* ..... ミリ秒 (20..10000)  
 [説明]         選択されている相手について [PPP, MSCBCP] の request/Response の再送時間を設定する。  
 [デフォルト値] 1000

### 8.12.2 パラメータ `mscbcpr-maxretr` の設定

---

- [入力形式]     **ppp mscbcpr maxretr count**  
 [パラメータ]   • *count* ..... 回数 (1..30)  
 [説明]         選択されている相手について [PPP, MSCBCP] の request/Response の再送回数を設定する。  
 [デフォルト値] 30

## 8.13 CCP 関連の設定

### 8.13.1 全パケットの圧縮タイプの設定

---

- [入力形式]     **ppp ccp type type**  
 [パラメータ]   • *type*  
                 • *stac* ..... Stac LZS で圧縮する  
                 • *costac* ..... Stac LZS で圧縮する (接続相手が Cisco ルータの場合)  
                 • *3stac* ..... Stac LZS で圧縮する (一部機器)  
                 • *none* ..... 圧縮しない  
 [説明]         選択されている相手について [PPP, CCP] 圧縮方式を選択する。  
                 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、Stac LZS を使用して動作しない場合に *costac* を選択することにより動作する場合がある。  
 [デフォルト値] *stac*

### 8.13.2 パラメータ `ccpr-start` 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

### 8.13.3 パラメータ `ccpr-max-terminat` の設定

---

- [入力形式]     **ppp ccp maxterminate count**  
 [パラメータ]   • *count* ..... 回数 (1..10)  
 [説明]         選択されている相手について [PPP, CCP] の terminate-request の送信回数を設定する。  
 [デフォルト値] 2

### 8.13.4 パラメータ `ccpr-max-configure` の設定

---

- [入力形式]     **ppp ccp maxconfigure count**  
 [パラメータ]   • *count* ..... 回数 (1..10)  
 [説明]         選択されている相手について [PPP, CCP] の configure-request の送信回数を設定する。  
 [デフォルト値] 10

### 8.13.5 パラメータ `ccpr-max-failure` の設定

---

- [入力形式]     **ppp ccp maxfailure count**  
 [パラメータ]   • *count* ..... 回数 (1..10)  
 [説明]         選択されている相手について [PPP, CCP] の configure-nak の送信回数を設定する。  
 [デフォルト値] 10

## 8.14 MP関連の設定

### 8.14.1 MPを使用するか否かの設定

- [入力形式] **ppp mp use use**
- [パラメータ] • *use*
- *on*.....使用する
  - *off*.....使用しない
- [説明] 選択されている相手についてMPを使用するか否かを選択する。  
*on*に設定していても、LCPの段階で相手とのネゴシエーションが成立しなければMPを使わずに通信する。
- [デフォルト値] *off*

### 8.14.2 MPの制御方法の設定

- [入力形式] **ppp mp control type**
- [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*

### 8.14.3 MPのための負荷閾値の設定

- [入力形式] **ppp mp load threshold call\_load call\_count disc\_load disc\_count**
- [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目の発信を行う。逆に*disc\_load* を下回る負荷が*disc\_count* 回繰り返されたら2B目を切断する。
- [デフォルト値] *call\_load* = 70  
*call\_count* = 1  
*disc\_load* = 30  
*disc\_count* = 2

### 8.14.4 MPの最大リンク数の設定

- [入力形式] **ppp mp maxlink number**
- [パラメータ] • *number* ....リンク数 (1..2)
- [説明] 選択されている相手について [PPP,MP] の最大リンク数を設定する。  
 リンク数の最大値は、使用モデルのBRI回線数の2倍までとなる。
- [デフォルト値] 2

### 8.14.5 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..2)
- [説明] 選択されている相手について [PPP,MP] の最小リンク数を設定する。
- [デフォルト値] 1

### 8.14.6 MP のための負荷計測間隔の設定

---

- [入力形式]     **ppp mp timer time**  
 [パラメータ]   • *time* .....秒数 (1..21474836)  
 [説明]            選択されている相手について [PPP,MP] のための負荷計測間隔を設定する。  
                   単位は秒。負荷計測だけでなく、すべての MP の動作はこのコマンドで設定した間隔で行  
                   われる。  
 [デフォルト値] 10

### 8.14.7 MP のパケットを分割するか否かの設定

---

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

## 8.15 BACP 関連の設定

### 8.15.1 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

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

---

- [入力形式]     **ppp bacp maxterminate count**  
 [パラメータ]   • *count* .....回数 (1..10)  
 [説明]            選択されている相手について [PPP,BACP] の terminate-request の送信回数を設定する。  
 [デフォルト値] 2

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

---

- [入力形式]     **ppp bacp maxconfigure count**  
 [パラメータ]   • *count* .....回数 (1..10)  
 [説明]            選択されている相手について [PPP,BACP] の configure-request の送信回数を設定する。  
 [デフォルト値] 10

### 8.15.4 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

### 8.15.5 BAP/BACP 手順の設定

---

- [ 入力形式 ]     **ppp bap use** *sw*
- [ パラメータ ]   • *sw*
- on.....MP 接続時に BAP/BACP 手順を使用する
  - off.....MP 接続時に BAP/BACP 手順を使用しない
- [ 説明 ]           MP 接続時に BACP を使用するか否か設定する。
- [ デフォルト値 ] off

### 8.15.6 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

### 8.15.7 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

## 9. DHCP の設定

RT52pro は DHCP<sup>1</sup> 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, 98 や Windows NT 等で実装されており、これらと RT52pro 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。

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

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

DHCP リレーエージェント機能は、ローカルセグメントの DHCP クライアントからの要求を、予め設定されたリモートのネットワークセグメントにある DHCP サーバへ転送します。リモートセグメントの DHCP サーバは **dhcp relay server** コマンドで設定します。DHCP サーバが複数ある場合には、**dhcp relay select** コマンドにより選択方式を指定することができます。

### 9.1 DHCP の動作の設定

[ 入力形式 ]      **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

[ 説明 ]            DHCP に関する機能を設定する。

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

[ デフォルト値 ] off

1. Dynamic Host Configuration Protocol; RFC1541  
URL 参照 : <http://rfc.rtp.yamaha.co.jp/rfc/rfc1541.txt>

## 9.2 RFC2131 対応動作設定

[ 入力形式 ]

**dhcp server rfc2131 compliant comp**  
**dhcp server rfc2131 compliant** [except] *function* [*function*..]

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

[ 説明 ]

DHCP サーバの動作を指定する。on の場合には RFC2131 準拠となる。off の場合には、RFC1541 準拠の動作となる。

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

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

[ デフォルト値 ] on

## 9.3 DHCP スコープの定義

- [入力形式]     **dhcp scope** *N ip\_address-ip\_address/netmask* [except *ex\_ip ...*] [*gateway gw\_ip*][*expire time*]  
[max*expire time*]
- [パラメータ]   • *N* .....スコープ番号 (1..65535)  
                  • *ip\_address-ip\_address* .....対象となるサブネットで割り当てる IP アドレスの範囲  
                  • *netmask* .... ネットマスク  
                    ◦ xxx.xxx.xxx.xxx (xxx は 10 進数)  
                    ◦ 0x に続く 16 進数  
                    ◦ マスクビット数  
                  • *ex\_ip* .....IP アドレス指定範囲の中で除外する IP アドレス (空白で区切って複数指定可能)  
                  • *gw\_ip* .....IP アドレス対象ネットワークのゲートウェイの IP アドレス  
                  • *time* .....時間  
                    ◦ 分 (1..21474836)  
                    ◦ 時間:分  
                    ◦ **infinity** .....無期限リース
- [説明]           DHCP サーバとして割り当てる IP アドレスのスコープを設定する。  
                   除外 IP アドレスは複数指定できる。リース期間としては無期限を指定できるほか、DHCP  
                   クライアントから要求があった場合の許容最大リース期間を指定できる。
- [ノート]         ひとつのネットワークについて複数の DHCP スコープを設定することはできない。複数の  
                   DHCP スコープで同一の IP アドレスを含めることはできない。IP アドレス範囲にネット  
                   ワークアドレス、ブロードキャストアドレスを含む場合、割り当て可能アドレスから除外  
                   される。  
                   DHCP リレーエージェントを経由しない DHCP クライアントに対して **gateway** キーワード  
                   による設定パラメータが省略されている場合にはルータ自身の IP アドレスを通知する。  
                   DHCP スコープを上書きした場合、以前のリース情報および予約情報は消去される。
- [デフォルト値] **expire time = 72:00**  
**maxexpire time = 72:00**

## 9.4 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。

## 9.5 DHCP 予約アドレスの設定

- [ 入力形式 ]     **dhcp scope bind** *scope\_num ip\_address [type] id*  
**dhcp scope bind** *scope\_num ip\_address mac\_address*  
**dhcp scope bind** *scope\_num ip\_address ipcp*
- [ パラメータ ]   • *scope\_num*.....スコープ番号 (1..65535)  
• *ip\_address*.....予約する IP アドレス  
• *type* ..... Client-Identifier オプションの *type* フィールドを決定する  
  ◦ *text* ..... 0x00  
  ◦ *ethernet*.....0x01  
• *id*  
  ◦ *type* が *ethernet* の場合 ....MAC アドレス  
  ◦ *type* が *text* の場合..... 文字列  
  ◦ *type* が省略された場合.....2桁 16進数の列で先頭は *type* フィールド  
• *mac\_address* ... xx:xx:xx:xx:xx:xx (xx は 16 進数) 予約 DHCP クライアントの MAC アドレス  
• *ipcp*.....IPCP でリモート側に与えることを示す
- [ 説明 ]           IP アドレスをリースする DHCP クライアントを固定的に設定する。  
[ ノート ]           IP アドレスは、*scope\_num* パラメータで指定された DHCP スコープ範囲内でなければならない。1つの DHCP スコープ内では、1つの MAC アドレスに複数の IP アドレスを設定することはできない。他の DHCP クライアントにリース中の IP アドレスを予約設定した場合、リース終了後にその IP アドレスの割り当てが行われる。

**dhcp scope** コマンド、あるいは **dhcp delete scope** コマンドを実行した場合、関連する予約はすべて消去される。  
*ipcp* の指定は、同時に接続できる B チャンネルの数に限られる。また、*ipcp* で与えるアドレスや擬似 LAN に与えるアドレスは、LAN 側のスコープから選択される。

コマンドの第 1 の書式を使う場合は、あらかじめ **dhcp server rfc2131 compliant on** あるいは **use-clientid** 機能を使用するよう設定されていなければならない。また **dhcp server rfc2131 compliant off** あるいは **use-clientid** 機能が使用されないよう設定された時点で、コマンドの第 1 の書式による予約は消去される。

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

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

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

- [ 設定例 ]       A. # **dhcp scope bind** *scope\_num ip\_address ethernet* 00:a0:de:01:23:45  
B. # **dhcp scope bind** *scope\_num ip\_address text* client01  
C. # **dhcp scope bind** *scope\_num ip\_address* 01 00 a0 de 01 23 45 01 01 01  
D. # **dhcp scope bind** *scope\_num ip\_address* 00:a0:de:01:23:45

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

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

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

**dhcp server rfc2131 compliant on** あるいは **use-clientid** 機能ありでアドレスをリースする場合、

DHCP サーバは `chaddr` に優先して `Client-Identifier` オプションを使用する。そのため、この場合の `show status dhcp` コマンド実行でクライアントの識別子を確認することで、クライアントが `Client-Identifier` オプションを使っているか否かを判別することも可能である。

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

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

| <b>dhcp scope bind</b> での指定方法 | A.     | (※ 2) |
|-------------------------------|--------|-------|
| クライアントの識別に用いる情報               | chaddr | (※ 3) |

※ 2 他の方法での指定は出来ない

※ 3 `Client-Identifier` オプションは無視される

なお、クライアントとの相互作用に関して下記の留意点がある。

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

## 9.6 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。

## 9.7 重複チェック動作

[入力形式] **dhcp server duplicate check check1 check2**

[パラメータ] • *check1*

- on.....LAN 内を対象とするチェックを行う
- off.....LAN 内を対象とするチェックを行わない

• *check2*

- on.....LAN 外 (DHCP リレーエージェント経由) を対象とするチェックを行う
- off.....LAN 外 (DHCP リレーエージェント経由) を対象とするチェックを行わない

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

[デフォルト値] *check1*=on

*check2*=on

[ノート] LAN 内の *scope* に対しては arp を、DHCP リレーエージェント経由の *scope* に対しては ping を使ってチェックする。

## 9.8 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*
- 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。

## 9.9 DHCP サーバの選択方法の設定

---

- [ 入力形式 ]     **dhcp relay select** *type*
- [ パラメータ ]   • *type*
- hash .....Hash 関数を利用して一つだけサーバを選択する
  - all .....すべてのサーバを選択する
- [ 説明 ]           **dhcp relay server** コマンドで設定された複数のサーバの取り扱いを設定する。  
*hash* が指定された時は、Hash 関数を利用して一つだけサーバが選択されてパケットが中継される。この Hash 関数は、DHCP メッセージの *chaddr* フィールドを引数とするので、同一の DHCP クライアントに対しては常に同じサーバが選択されるはずである。*all* が指定された時は、パケットはすべてのサーバに対し複写中継される。
- [ デフォルト値 ] *hash*

## 9.10 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

## 10. SNMP の設定

### 10.1 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

### 10.2 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

### 10.3 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

### 10.4 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*  
 ◦ 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

### 10.5 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

### 10.6 sysLocation の設定

---

- [入力形式] **snmp syslocation name**  
 [パラメータ] • *name* .....sysLocation として登録する名称  
 [説明] YAMAHA リモートルータの設置場所を表す MIB 変数 sysLocation を設定する。  
 名称は 255 文字以内。空文字列可。  
 [デフォルト値] 空文字列

## 10.7 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。
- [ デフォルト値 ] 空文字列

## 10.8 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

## 10.9 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*
- 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**

## 11. ICMP の設定

### 11.1 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

### 11.2 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

### 11.3 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

### 11.4 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

### 11.5 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。  
 [デフォルト値] off

### 11.6 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

### 11.7 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

### 11.8 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

### 11.9 受信した ICMP のログを記録するか否かの設定

---

- [ 入力形式 ]     **ip icmp log log**
- [ パラメータ ]   • *log*
- on.....受信した ICMP をログに記録する
  - off.....受信した ICMP をログに記録しない
- [ 説明 ]           受信した ICMP を debug タイプのログに記録するか否かを設定する。
- [ デフォルト値 ] off

## 12. RADIUS の設定

### 12.1 RADIUS サーバの指定

---

- [入力形式]     **radius server ip\_1 [ip\_2]**
- [パラメータ]   • *ip\_1*.....RADIUS サーバ(正)の IP アドレス  
                  • *ip\_2*.....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。

### 12.2 RADIUS 認証サーバの指定

---

- [入力形式]     **radius auth server ip\_1 [ip\_2]**  
                  **radius auth server clear**
- [パラメータ]   • *ip\_1*.....RADIUS 認証サーバ(正)の IP アドレス  
                  • *ip\_2*.....RADIUS 認証サーバ(副)の IP アドレス  
                  • *clear*.....設定の消去
- [説明]           RADIUS 認証サーバを設定する。2つまで指定でき、最初のサーバから返事をもらえない場合は、2番目のサーバに問い合わせを行う。
- [ノート]         このコマンドで RADIUS 認証サーバの IP アドレスが指定されていない時は、**radius server** コマンドで指定した IP アドレスを認証サーバとして用いる。

### 12.3 RADIUS 認証サーバの UDP ポートの設定

---

- [入力形式]     **radius auth port port\_number**
- [パラメータ]   • *port\_number*...ポート番号
- [説明]           RADIUS 認証サーバの UDP ポート番号を設定する。
- [ノート]         新しい RFC ではポート番号として 1812 を使うことになっている。
- [デフォルト値] 1645

### 12.4 RADIUS アカウントサーバの指定

---

- [入力形式]     **radius account server IP1 [IP2]**  
                  **radius account server clear**
- [パラメータ]   • *IP1* .....RADIUS 認証サーバ(正)の IP アドレス  
                  • *IP2* .....RADIUS 認証サーバ(副)の IP アドレス  
                  • *clear*.....設定の消去
- [説明]           RADIUS アカウントサーバを設定する。2つまで指定でき、最初のサーバから返事をもらえないときは、2番目のサーバに問い合わせを行う。
- [ノート]         このコマンドで RADIUS アカウントサーバの IP アドレスが指定されていない場合は、**radius server** コマンドで指定した IP アドレスを認証サーバとして用いる。

### 12.5 RADIUS アカウントサーバの UDP ポートの設定

---

- [入力形式]     **radius account port port\_number**
- [パラメータ]   • *port\_number*..ポート番号
- [説明]           RADIUS アカウントサーバの UDP ポート番号を設定する。
- [ノート]         新しい RFC ではポート番号として 1813 を使うことになっている。
- [デフォルト値] 1646

### 12.6 RADIUS シークレットの設定

---

- [入力形式]     **radius secret secret**
- [パラメータ]   • *secret* .....シークレット文字列
- [説明]           RADIUS シークレットを設定する。  
                  空文字列を設定するときにはパラメータ部分に " " を入力する。

## 12.7 RADIUS 再送信パラメータの設定

---

- [ 入力形式 ]     **radius retry count time**
- [ パラメータ ]   • *count* .... 再送回数 (1..10)  
                 • *time*..... ミリ秒 (20..10000)
- [ 説明 ]           RADIUS パケットの再送回数とその時間間隔を設定する。
- [ デフォルト値 ] *count* = 4  
                  *time* = 3000

## 12.8 RADIUS による認証を使用するか否かの設定

---

- [ 入力形式 ]     **radius auth auth**
- [ パラメータ ]   • *auth*  
                 ◦ *on*.....使用する  
                 ◦ *off*.....使用しない
- [ 説明 ]           anonymous に対して何らかの認証を要求する設定の時に、相手から受け取ったユーザネーム (PAP であれば UserID、CHAP であれば NAME) が、自分で持つユーザネーム (**pp auth username** コマンドで指定) の中に含まれていない場合には RADIUS サーバに問い合わせるか否かを設定する。
- 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 re-mote 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*

## 12.9 RADIUS によるアカウントを使用するか否かの設定

---

- [ 入力形式 ]     **radius account account**
- [ パラメータ ]   • *account*  
                 ◦ *on*.....使用する  
                 ◦ *off*.....使用しない
- [ 説明 ]           RADIUS によるアカウントを使用するか否かを設定する。
- STOP 時に次のアトリビュートを送信する。  
                  ACCT SESSION TIME、ACCT INPUT PACKETS、ACCT INPUT OCTETS、ACCT OUTPUT PACKETS、ACCT OUTPUT OCTETS
- それぞれの値は **show status pp** コマンドで表示されるものとは必ずしも一致していない可能性がある。
- RADIUS による認証と RADIUS によるアカウントは独立して使用できる。
- [ デフォルト値 ] *off*

## 13. NAT 機能

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

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

RT52pro では、始点/終点 IP アドレスの変換だけを行うことを NAT と呼び、TCP/UDP のポート番号の変換を伴うものを IP マスカレードと呼んでいます。

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

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

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

### 13.1 LAN 側インタフェースに NAT ディスクリプタを適用する設定

- [入力形式] **ip lan nat descriptor nat\_descriptor\_list**
- [パラメータ] • **nat\_descriptor\_list**
- 空白で区切られた NAT ディスクリプタの識別番号 (1..21474836) の並び (16 個以内)
  - **clear**.....NAT ディスクリプタを適用しない
- [説明] 適用された LAN インタフェースを通過するパケットに対して、リストに定義された順番で NAT ディスクリプタによって定義された NAT 変換を順番に処理する。
- [ノート] LAN 側に設定された NAT ディスクリプタの OUTER アドレスに関しては、同一 LAN の ARP 要求に対して ARP 応答する。
- [デフォルト値] **clear**

### 13.2 PP 側インタフェースに NAT ディスクリプタを適用する設定

- [入力形式] **ip pp nat descriptor nat\_descriptor\_list**
- [パラメータ] • **nat\_descriptor\_list**
- 空白で区切られた NAT ディスクリプタの識別番号 (1..21474836) の並び (16 個以内)
  - **clear**.....NAT ディスクリプタを適用しない
- [説明] 適用された PP インタフェースを通過するパケットに対して、リストに定義された順番で NAT ディスクリプタによって定義された NAT 変換を順番に処理する。
- [デフォルト値] **clear**

### 13.3 トンネルインタフェースへの NAT ディスクリプタ適用の設定

- [入力形式] **ip tunnel nat descriptor nat\_descriptor\_list**
- [パラメータ] • **nat\_descriptor\_list**
- 空白で区切られた NAT ディスクリプタ番号 (1..21474836) の並び (16 個以内)
  - **clear**.....NAT ディスクリプタを適用しない
- [説明] 適用されたトンネルインタフェースを通過するパケットに対して、リストに定義された順番で NAT ディスクリプタによって定義された NAT 変換を順番に処理する。
- [デフォルト値] **clear**

### 13.4 NAT ディスクリプタの動作タイプを指定する

- [ 入力形式 ]     **nat descriptor type** *nat\_descriptor type*
- [ パラメータ ]   • *nat\_descriptor* .. ...NAT ディスクリプタの識別番号 (1..21474836)
- *type* .....NAT ディスクリプタの動作タイプ
- none.....NAT 変換機能を利用しない
- nat .....動的 NAT 変換と静的 NAT 変換が利用できる
- masquerade .. 静的 NAT 変換と IP マスカレード変換
- nat-masquerade.. .... 動的 NAT 変換と静的 NAT 変換と IP マスカレード変換
- [ 説明 ]           NAT 変換の動作タイプを指定する。
- [ デフォルト値 ] *type=none*

### 13.5 NAT 処理の外側 IP アドレスの設定

- [ 入力形式 ]     **nat descriptor address outer** *nat\_descriptor outer\_ipaddress\_list*
- [ パラメータ ]   • *nat\_descriptor* ....NAT ディスクリプタの識別番号 (1..21474836)
- *outer\_ipaddress\_list* ..NAT 対象の外側 IP アドレス範囲のリストまたはニーモニック
- 1 個の IP アドレスまたは間に-をはさんだ IP アドレス ( 範囲指定 )、及びこれらを任意に並べたもの
- *ipcp* ..... PPP の IPCP の IP-Address オプションにより接続先から通知される IP アドレス
- *primary*... **ip lan address** コマンドで設定されている IP アドレス
- *secondary*..**ip lan secondary address** コマンドで設定されている IP アドレス
- [ 説明 ]           動的 NAT 処理の対象である外側の IP アドレスの範囲を指定する。IP マスカレードでは、先頭の 1 個の外側の IP アドレスが使用される。
- [ ノート ]        ニーモニックをリストにすることはできない。  
適用されるインタフェースにより以下の表のように意味が異なる。

|                  | 適用インタフェース |    |      |
|------------------|-----------|----|------|
|                  | LAN       | PP | トンネル |
| <i>ipcp</i>      | ×         |    | ×    |
| <i>primary</i>   |           | ×  | ×    |
| <i>secondary</i> |           | ×  | ×    |
| IP アドレス          |           |    |      |

- [ デフォルト値 ] *ipcp*

### 13.6 NAT 処理の内側 IP アドレスの設定

- [ 入力形式 ]     **nat descriptor address inner** *nat\_descriptor inner\_ipaddress\_list*
- [ パラメータ ]   • *nat\_descriptor* ....NAT ディスクリプタの識別番号 (1..21474836)
- *inner\_ipaddress\_list* ..NAT 対象の内側 IP アドレス範囲のリストまたはニーモニックらを任意に並べたもの
- 1 個の IP アドレスまたは間に-をはさんだ IP アドレス ( 範囲指定 )、及びこれらを任意に並べたもの
- *auto*.....全て
- [ 説明 ]           NAT/IP マスカレード処理の対象である内側の IP アドレスの範囲を指定する。  
適用されるインタフェースにより以下の表のように意味が異なる。
- [ デフォルト値 ] *auto*

## 13.7 静的 NAT エントリの設定

- [入力形式]     **nat descriptor static nat\_descriptor id outer\_ip=inner\_ip [count]**
- [パラメータ]   • *nat\_descriptor*. ....NAT ディスクリプタの識別番号 (1..21474836)
- *id*.....静的 NAT エントリの識別情報 (1 以上の数値)
- *outer\_ip* ....外側 IP アドレス
- *inner\_ip* ....内側 IP アドレス
- *count* ... 連続設定する個数 (省略時は 1)
- [説明]           NAT 変換で固定割り付けする IP アドレスの組み合わせを指定する。  
個数数を同時に指定すると指定されたアドレスと始点とした範囲指定とする。
- [ノート]         外側アドレスが NAT 処理対象として設定されているアドレスである必要は無い。  
静的 NAT のみを使用する場合には、**nat descriptor address outer** コマンドと **nat descriptor address inner** コマンドの設定に注意する必要がある。デフォルト値がそれぞれ *ipcp* と *auto* であるので、例えば何らかの IP アドレスをダミーで設定しておくことで動的動作しないようにする。

## 13.8 IP マスカレード使用時の rlogin,rcp,ssh の使用許可設定

- [入力形式]     **nat descriptor masquerade rlogin nat\_descriptor use**
- [パラメータ]   • *nat\_descriptor*. .... NAT ディスクリプタの識別番号 (1..21474836)
- *use*
- *on*.....使用する
- *off*.....使用しない
- [説明]           IP マスカレード使用時の *rlogin*、*rcp*、*ssh* の使用を許可する
- [ノート]         *use* を *on* にすると、*rlogin*、*rcp* と *ssh* のトラフィックに対して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*

## 13.9 静的 IP マスカレードエントリの設定

- [入力形式]     **nat descriptor masquerade static nat\_descriptor id inner\_ip protocol port**
- [パラメータ]   • *nat\_descriptor*. ....NAT ディスクリプタの識別番号 (1..21474836)
- *id*.....静的 IP マスカレードエントリの識別情報 (1..21474836)
- *inner\_ip* ....内側 IP アドレス
- *protocol* ....対象プロトコル
- *tcp* .....tcp プロトコル
- *udp* .....udp プロトコル
- プロトコル番号 IANA で割り当てられている *protocol numbers*
- *port*.....固定するポート番号、または、範囲指定
- ポート番号、または、ポート番号のニーモニック
- [説明]           IP マスカレードによる通信でポート番号変換を行わないようにポートを固定する。

## 13.10 NAT の IP アドレスマップの消去タイマの設定

- [入力形式]     **nat descriptor timer nat\_descriptor time**
- [パラメータ]   • *nat\_descriptor*. .... NAT ディスクリプタの識別番号 (1..21474836)
- *time* .....消去タイマの秒数設定 (30..21474836)
- [説明]           動的に生成された NAT 管理テーブルから自動的に消去されるまでの時間を設定する。
- [デフォルト値] 900

## 13.11 NAT ディスクリプタの削除

- [入力形式]     **nat descriptor delete nat\_descriptor**
- [パラメータ]   • *nat\_descriptor*. .... NAT ディスクリプタの識別番号 (1..21474836)
- [説明]           指定された NAT ディスクリプタ番号の設定を削除 (初期化) する。

### 13.12 静的 NAT エントリの削除

---

- [ 入力形式 ]     **nat descriptor static delete** *nat\_descriptor id*
- [ パラメータ ]   • *nat\_descriptor* ..... NAT ディスクリプタの識別番号 (1..21474836)
- *id* ..... 静的 NAT エントリの識別情報 (1..21474836)
- [ 説明 ]           静的 NAT エントリを削除する。

### 13.13 静的 IP マスカレードエントリの削除

---

- [ 入力形式 ]     **nat descriptor masquerade static delete** *nat\_descriptor id*
- [ パラメータ ]   • *nat\_descriptor* ..... NAT ディスクリプタの識別番号 (1..21474836)
- *id* ..... 静的 NAT エントリの識別情報 (1..21474836)
- [ 説明 ]           静的 IP マスカレードエントリを削除する。

### 13.14 設定した NAT ディスクリプタの設定状態表示

---

- [ 入力形式 ]     **show nat descriptor config** *nat\_descriptor*
- [ パラメータ ]   • *nat\_descriptor* ..... NAT ディスクリプタの識別番号 (1..21474836)
- [ 説明 ]           NAT ディスクリプタの設定状態を書式に従って表示する。

### 13.15 動作中の NAT ディスクリプタのアドレスマップの表示

---

- [ 入力形式 ]     **show nat descriptor address** [*nat\_descriptor*]
- [ パラメータ ]   • *nat\_descriptor*
- NAT ディスクリプタの識別番号 (1..21474836)
- all .....有効な NAT ディスクリプタのすべて
- [ 説明 ]           NAT ディスクリプタのアドレスマップを表示する。
- [ デフォルト値 ] all

### 13.16 動作中の NAT ディスクリプタの適用リストの表示

---

- [ 入力形式 ]     **show nat descriptor interface bind**
- [ パラメータ ]   なし
- [ 説明 ]           NAT ディスクリプタと適用インタフェースのリストを表示する。

### 13.17 各インタフェース毎に NAT のアドレスマップを表示

---

- [ 入力形式 ]     **show nat descriptor interface address pp** *peer\_number*
- show nat descriptor interface address lan**
- show nat descriptor interface address tunnel** *tunnel\_interface*
- [ パラメータ ]   • *peer\_number*
- 相手先情報番号
- anonymous
- leased
- *tunnel\_interface*
- トンネルインタフェース番号 (1..10)
- [ 説明 ]           各インタフェースに適用されている NAT ディスクリプタのアドレスマップを表示する。

### 13.18 NAT アドレステーブルのクリア

---

- [入力形式]     **clear nat descriptor dynamic** *nat\_descriptor*
- [パラメータ]   • *nat\_descriptor*
- NAT ディスクリプタの識別番号 (1..21474836)
  - all ..... 有効な NAT ディスクリプタのすべて
- [説明]           指定された NAT ディスクリプタの NAT アドレステーブルをクリアする。
- [ノート]         通信中にアドレス管理テーブルをクリアした場合、通信が一時的に不安定になる可能性がある。
- [デフォルト値] all

### 13.19 各インタフェースの NAT アドレステーブルのクリア

---

- [入力形式]     **clear nat descriptor interface dynamic lan**  
**clear nat descriptor interface dynamic pp** *peer\_number*  
**clear nat descriptor interface dynamic tunnel** *tunnel\_interface*
- [パラメータ]   • *peer\_number*...PP 番号
- 相手先情報番号
  - anonymous ...ISDN 番号が不明である相手の設定
  - leased..... .....専用線使用時の設定
- [パラメータ]   • *tunnel\_interface*
- トンネルインタフェース番号 (1..10)
- [説明]           各インタフェースに適用されている NAT ディスクリプタのアドレステーブルをクリアする。

### 13.20 NAT でのアドレス割当の記録

---

- [入力形式]     **nat descriptor log** *sw*
- [パラメータ]   • *sw*.....スイッチ
- on..... 記録をとる
  - off ..... 記録をとらない
- [説明]           NAT/IP Masquerade 機能で、動的なアドレスの割当をログに記録する機能。  
**nat descriptor log** コマンドの設定を on にすると、アドレスの割当と解放のタイミングで info レベルの syslog が出力される。
- [デフォルト値] off



## 14. DNS の設定

RT52pro は、DNS(Domain Name Service)機能として名前解決、リカーシブサーバ機能、上位 DNS サーバの選択機能、簡易 DNS サーバ機能(静的 DNS レコードの登録)を持ちます。

名前解決の機能としては、**ping** や **tracert**、**rdns**、**ntpdns**、**telnet** コマンドなどの IP アドレスパラメータの代わりに名前を指定したり、SYSLOG などの表示機能において IP アドレスを名前解決したりします。

リカーシブサーバ機能は、RT52pro 宛に届いた DNS 問い合わせパケットを **dns server** コマンドで設定された DNS ネームサーバに中継します。最大 256 件のキャッシュを持ちます。

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

### 14.1 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

### 14.2 DNS サーバを通知してもらう相手先情報番号の設定

- 
- [入力形式]     **dns server pp peer\_number**
- [パラメータ]   • *peer\_number*
- DNS サーバを通知してもらう相手先情報番号
  - none
- [説明]           DNS サーバを通知してもらう相手先情報番号を設定する。このコマンドで相手先情報番号が設定されていると、DNS での名前解決を行うときに、まずこの相手先に発信して、そこで PPP の IPCP MS 拡張機能で通知された DNS サーバに対して問い合わせを行う。  
相手先に接続できなかったり、接続できても DNS サーバの通知がなかった場合には名前解決は行われない。  
**dns server** コマンドで DNS サーバが明示的に指定されている場合には、そちらの設定が優先される。**dns server** コマンドに指定したサーバから返事がない場合には、相手先への接続と DNS サーバの通知取得が行われる。
- [ノート]        この機能を使用する場合には、**dns server pp** コマンドで指定された相手先情報に、**ppp ipcp msxmt on** の設定が必要である。
- [デフォルト値] none

### 14.3 DNS 問い合わせの内容に応じた DNS サーバの選択

- [ 入力形式 ]     **dns server select id server [type] query [original-sender][restrict pp connection-pp]**  
**dns server select id pp pp\_num [default-server] [type] query [original-sender]**  
**dns server select delete id**
- [ パラメータ ]
- *id* .....DNS サーバ選択テーブルの番号
  - *server* ...DNS サーバの IP アドレス
  - *type*.....DNS レコードタイプ (省略時は a)
    - *a* .....ホストの IP アドレス
    - *ptr*.....IP アドレスの逆引き用のポインタ
    - *mx* ..... メールサーバ
    - *ns* ..... ネームサーバ
    - *cname* .... 別名
    - *any*..... すべてのタイプにマッチする
  - *query*..... DNS 問い合わせの内容
    - *type* が *a*、*mx*、*ns*、*cname* の場合  
*query* はドメイン名を表す文字列であり、後方一致とする。例えば、  
"yamaha.co.jp" であれば、*comm.yamaha.co.jp*、*rtpro.yamaha.co.jp* などにマッ  
チする。
    - *type* が *ptr* の場合  
*query* は IP アドレス (*ip\_address[/masklen]*) であり、*masklen* を省略したとき  
は IP アドレスにのみマッチし、*masklen* を指定したときはネットワークア  
ドレスに含まれるすべての IP アドレスにマッチする。DNS 問い合わせに含ま  
れる *.in-addr.arpa* ドメインで記述された FQDN は、IP アドレスへ変換され  
た後に比較される。
  - *original-sender* .....DNS 問い合わせの送信元の IP アドレスの範囲
  - *connection-pp*.....DNS サーバを選択する場合、接続状態を確認する接続相手先番号
  - *pp\_num* .....IPCPにより接続相手から通知される DNS サーバを使う場合の接続相手先番号
  - *default-server*.....パラメータ *pp\_num* で指定した接続相手から DNS サーバを獲得できな  
かったときに使う DNS サーバの IP アドレス
- [ 説明 ]     DNS 問い合わせの解決を依頼する DNS サーバとして、DNS 問い合わせの内容および DNS  
問い合わせの送信元および回線の接続状態を確認する接続相手先番号と DNS サーバとの組  
合せを複数登録しておき、DNS 問い合わせに応じてその組合せから適切な DNS サーバを選  
択できるようにする。テーブルは小さい番号から検索され、DNS 問い合わせの内容に  
*query* がマッチしたら、その DNS サーバを用いて DNS 問い合わせを解決しようとする。一度  
マッチしたら、それ以降のテーブルは検索しない。すべてのテーブルを検索してマッチする  
ものがない場合には、**dns server** コマンドで指定された DNS サーバを用いる。

### 14.4 DNS ドメイン名の設定

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

## 14.5 プライベートアドレスに対する問い合わせを処理するか否かの設定

- [入力形式]     **dns private address spoof spoof**
- [パラメータ]   • *spoof*
- on..... 処理する
  - off ..... 処理しない
- [説明]           on の場合、DNS リカーシブサーバ機能で、プライベートアドレスの PTR レコードに対する問い合わせに対し、上位サーバに問い合わせを転送することなく、自分でその問い合わせに対し "NXDomain"、すなわち「そのようなレコードはない」というエラーを返す。
- [デフォルト値] off

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

- [入力形式]     **dns notice order protocol server [server]**
- [パラメータ]   • *protocol*
- dhcp ..... DHCP による通知
  - msex ..... IPCP MS 拡張による通知
- *server*
- none ..... 一切通知しない
  - me ..... RT52pro 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 RT52pro 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  
msex me server

## 14.7 SYSLOG 表示で DNS により名前解決するか否かの設定

- [入力形式]     **dns syslog resolv resolv**
- [パラメータ]   • *resolv*
- on..... 解決する
  - off ..... 解決しない
- [説明]           SYSLOG 表示で DNS により名前解決するか否かを設定する。
- [デフォルト値] off

## 14.8 静的 DNS レコードの登録

---

[ 入力形式 ] **ip host** *fqdn value*

**dns static** *type name value*

- [ パラメータ ]
- *type* ..... 名前のタイプ
    - *a* ..... ホストの IP アドレス
    - *ptr* ..... IP アドレスの逆引き用のポインタ
    - *mx* ..... メールサーバ
    - *ns* ..... ネームサーバ
    - *cname* ..... 別名
  - *name, value* ..... *type* パラメータによって以下のように意味が異なる

| <i>type</i>  | <i>name</i> | <i>value</i> |
|--------------|-------------|--------------|
| <i>a</i>     | FQDN        | IP アドレス      |
| <i>ptr</i>   | IP アドレス     | FQDN         |
| <i>mx</i>    | FQDN        | FQDN         |
| <i>ns</i>    | FQDN        | FQDN         |
| <i>cname</i> | FQDN        | FQDN         |

- [ 説明 ]
- *fqdn* ..... 完全修飾ドメイン名 (Fully Qualified Domain Name の略)
- 静的な DNS レコードを定義する。  
**ip host** コマンドは、**dns static** コマンドで *a* と *ptr* を両方設定することを簡略化したものである。
- [ ノート ]
- 問い合わせに対して返される DNS レコードは以下のような特徴を持つ。
    - TTL フィールドには 1 がセットされる
    - Answer セクションに回答となる DNS レコードが 1 つセットされるだけで、Authority/Additional セクションには DNS レコードがセットされない
    - MX レコードの preference フィールドは 0 にセットされる
- [ 設定例 ]
- ```
# ip host pc1.rtrpro.yamaha.co.jp 133.176.200.1
# dns static ptr 133.176.200.2 pc2.yamaha.co.jp
# dns static cname mail.yamaha.co.jp mail2.yamaha.co.jp
```

14.9 静的 DNS レコードの削除

[入力形式] **ip host delete** *fqdn*

dns static delete *type name*

- [パラメータ]
- *fqdn* 完全修飾ドメイン名 (Fully Qualified Domain Name の略)
 - *type* 名前のタイプ
 - *a* ホストの IP アドレス
 - *ptr* IP アドレスの逆引き用のポインタ
 - *mx* メールサーバ
 - *ns* ネームサーバ
 - *cname* 別名
 - *name* *type* パラメータによって以下のように意味が異なる

<i>type</i>	<i>name</i>
<i>a</i>	FQDN
<i>ptr</i>	IP アドレス
<i>mx</i>	FQDN
<i>ns</i>	FQDN
<i>cname</i>	FQDN

- [説明]
- 静的な DNS レコードを削除定義する。

14.10 静的 DNS レコードの表示

[入力形式] **show ip host**

show dns static

[パラメータ] なし

[説明] 静的な DNS レコードを表示する。

15. アナログ通信機能の設定

RT52pro のアナログ通信機能の設定は、アナログポートに接続した PB 電話機のキー操作でも可能ですが、ここではコンソールからのコマンドについてだけ述べます。キー操作による設定手順は取扱説明書を参照してください。キー操作とコンソールコマンドの対応表は次ページに示します。

アナログ通信機能は、RT52pro が ISDN 回線に接続されている場合にだけ利用できます。高速デジタル専用線に接続した場合には、アナログポートに接続したアナログ通信機器は内線通話以外は使用できません。

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

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

RT52pro のアナログポートへの着信ベル音は 2 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。

RT52pro はフレックスホン機能¹と、その一部機能を擬似的に行う擬似フレックスホンをサポートします。フレックスホン機能は NTT の交換機側で提供される機能であり、擬似フレックスホン機能はそれと同様な機能を RT52pro のソフトウェアでシミュレーションします。これらの機能を使用するためには **analog supplementary service** コマンドで NTT との契約形態を設定します。このコマンドで設定された機能だけが使用可能となります。

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

RT52pro 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、モデムや FAX 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調節し、最適な状態にします。

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。

1. NTT との契約が必要な有料サービス。

15.1 キー操作とコンソールコマンドの対応

機能	機能番号	対応するコンソールコマンド
TEL ポートのダイヤル番号設定	11	analog local address
TEL ポートのサブアドレス設定	12	analog local address
通信機器の種類設定	13	analog device type
アナログポート使用制限の設定	14	analog use
発信者番号通知	21	analog local address notice
即時発信	22	analog rapid call
グローバル着信	31	analog arrive global permit
識別着信	32	analog arrive restrict
識別着信の番号登録	33	analog arrive restrict list add
サブアドレスなしの着信	34	analog arrive without-subaddress permit
通信機器種別指定の着信	35	analog arrive another-device permit
話中着信	36	analog arrive ring-while-talking permit
優先着信ポート	37	analog arrive prior-port
着信ベル設定	38	analog arrive ringer-type list add
ナンバー・ディスプレイ機能	39	analog arrive number display
ダイヤル桁の間隔設定 (秒)	41	analog wait dial timer
フッキング判定時間 (1/10 秒)	42	analog hooking timer
フッキング後の操作有効時間 (秒)	43	analog hooking wait timer
フッキング、オンフック無効時間 (秒)	44	analog hooking inhibit timer
擬似切断信号の設定	45	analog disc-signal
ナンバー・ディスプレイ信号の設定	46	analog arrive modem signal type
INS キャッチホン機能 (コールウェイトニング)	52	analog supplementary-service
通信中転送機能	53	analog supplementary-service
三者通話機能	54	analog supplementary-service
着信転送機能	55	analog supplementary-service
着信転送先番号登録	56	analog supplementary-service call-deflection address
着信転送トーン設定	57	analog supplementary-service call-deflection talkie
着信転送起動タイミング設定	58	analog supplementary-service call-deflection ringer
着信転送失敗時の動作設定	59	analog supplementary-service call-deflection reject
送話 PAD の音量設定	61	analog pad send
受話 PAD の音量設定	62	analog pad receive
DTMF 検出レベルの設定	63	analog dtmf level
LAN 側のルータ IP アドレス設定	71	ip lan address
LAN 側のネットマスク設定	72	ip lan netmask
BOD の設定	73	analog mp prior
i・ナンバーの設定	81	analog arrive inumber-port
着信時サービス設定	82	analog arrive incomming-signal
擬似ナンバー・リクエストの設定	83	analog arrive without-calling-number
ダイヤル完了ボタンの設定	84	analog end-of-dialing-code
アナログポートの再呼出時間設定	85	analog re-ringing-timer
アナログポート設定の消去	91	-
識別着信の番号削除	92	analog arrive restrict list delete
着信ベルの番号削除	93	analog arrive ringer-type list delete
料金情報の消去	94	clear analog account
アナログポート設定の全消去	99	-
パスワードの設定	00	login password, administrator password

15.2 アナログポートを使うか否かの設定

- [入力形式] **analog use port use**
- [パラメータ]
- **port**.....アナログポート
 - 1..... TEL1 ポート
 - 2..... TEL2 ポート
 - 3..... TEL3 ポート
 - **use**
 - on..... 発着信可能として使用する
 - off..... 使用しない
 - call-only... 発信専用として使用
 - arrive-only..... 着信専用として使用
- [説明] アナログポートを使用するか否かを設定する。off 以外にしないとアナログ通信機能は一切使用できない。
- [デフォルト値] on

15.3 アナログポートの ISDN 番号の設定

- [入力形式] **analog local address port isdn_number/sub_address [isdn_number_list]**
analog local address port isdn_number [isdn_number_list]
analog local address port /sub_address [isdn_number_list]
analog local address port clear
- [パラメータ]
- **port**.....アナログポート
 - 1..... TEL1 ポート
 - 2..... TEL2 ポート
 - 3..... TEL3 ポート
 - **isdn_number**...ISDN 番号
 - **sub_address**.....ISDN サブアドレス (0x21 から 0x7e の ASCII 文字)
 - **isdn_number_list**.ISDN 番号とサブアドレス、ISDN 番号のみ、またはサブアドレスのみの ISDN 番号を空白で区切った並び (最大 5 つ)
 - **clear**.....全ての ISDN 番号をクリア
- [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よい。
- [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。

15.4 アナログポートに接続する機器の指定

- [入力形式] **analog device type port type**
- [パラメータ]
- **port**.....アナログポート
 - 1..... TEL1 ポート
 - 2..... TEL2 ポート
 - 3..... TEL3 ポート
 - **type**.....接続する機器の種類
 - any..... 通信機器の指定無し
 - tel..... 電話
 - fax..... G2/G3 FAX
- [説明] アナログポートに接続する機器を指定する。
 これを設定すると、**type** パラメータが **any** の場合には HLC をつけずに、それ以外では指定した HLC をつけて発信する。また **analog arrive another-device permit** コマンドとの組み合わせにより、着信時に **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**

15.5 アナログポートの発信者番号を通知するか否かの設定[入力形式] **analog local address notice port notice**

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

[説明] アナログポートに設定した発信者番号を相手に通知するか否かを設定する。相手に通知される番号は **analog local address** コマンドで設定されたものである。**analog local address** コマンドで複数の番号が設定されている場合は、最初に設定した番号が通知される。

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

[デフォルト値] off

15.6 相手先番号による即時発信を許可するか否かの設定[入力形式] **analog rapid call port rapid**

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

[説明] 相手先番号による即時発信を許可するか否かを設定する。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

15.7 ダイヤル完了ボタンの設定[入力形式] **analog end-of-dialing-code port sw**

- [パラメータ]
- **port** アナログポート
 - 1 TEL1 ポート
 - 2 TEL2 ポート
 - 3 TEL3 ポート
 - **sw**
 - on '#' ボタンをダイヤル完了ボタンとして使用する
 - off '#' ボタンをダイヤル完了ボタンとして使用しない

[説明] '#' ボタンをダイヤル完了ボタンとして使用するか否かを選択する。off を指定している場合には、'#' ボタンは回線番号として網に通知される。

[デフォルト値] on

15.8 グローバル着信を許可するか否かの設定

- [入力形式] **analog arrive global permit port permit**
- [パラメータ] • *port*.....アナログポート
- 1..... TEL1 ポート
 - 2..... TEL2 ポート
 - 3..... TEL3 ポート
- *permit*
- on..... 許可する
 - off..... 拒否する
- [説明] グローバル着信を許可するか否かを設定する。
グローバル着信の場合、着信時に着番号情報要素が着いてこない。グローバル着信を使用するためには、ダイヤルイン契約の際に利用指定が必要。
- [デフォルト値] on

15.9 アナログポートでの識別着信をするか否かの設定

- [入力形式] **analog arrive restrict port restrict**
- [パラメータ] • *port*.....アナログポート
- 1..... TEL1 ポート
 - 2..... TEL2 ポート
 - 3..... TEL3 ポート
- *restrict*
- permit..... 着信許可
 - reject 着信拒否
 - none 識別着信しない
- [説明] アナログポートで識別着信をするか否かを設定する。
analog arrive restrict list add コマンドで登録された識別着信リストに対しての着信動作を決定する。permit の場合には、発番号が登録リストに含まれれば着信許可となり、それ以外は着信拒否となる。reject の場合には、発番号が登録リストに含まれれば着信拒否となり、それ以外は着信許可となる。none の場合には、全ての発番号に対して着信許可となる。
- [デフォルト値] reject

15.10 識別着信リストの登録

- [入力形式] **analog arrive restrict list add port isdn_number/[sub_address]**
- [パラメータ] • *port*.....アナログポート
- 1..... TEL1 ポート
 - 2..... TEL2 ポート
 - 3..... TEL3 ポート
- *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。
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。

15.11 識別着信リストの削除

- [入力形式] **analog arrive restrict list delete port number**
- [パラメータ] • *port*.....アナログポート
- 1..... TEL1 ポート
 - 2..... TEL2 ポート
 - 3..... TEL3 ポート
- *number*..... 識別着信用の登録番号
- [説明] パラメータで指定された登録番号を識別着信リストから削除する。

15.12 サブアドレス無し着信を許可するか否かの設定

- [入力形式] **analog arrive without-subaddress permit port permit**
- [パラメータ] • *port* アナログポート
- 1 TEL1 ポート
 - 2 TEL2 ポート
 - 3 TEL3 ポート
- *permit*
- on 許可する
 - off 拒否する
- [説明] サブアドレス情報要素の無い着信を許可するか否かを設定する。
- analog local address** コマンドを使用してポート毎に異なるサブアドレスを設定しておく
と、ポートを区別して着信することが可能になる。
- 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

15.13 異なる種類の通信機器からの着信を許可するか否かの設定

- [入力形式] **analog arrive another-device permit port permit**
- [パラメータ] • *port* アナログポート
- 1 TEL1 ポート
 - 2 TEL2 ポート
 - 3 TEL3 ポート
- *permit*
- on 許可する
 - off 許可しない
- [説明] 異なる種類の通信機器からの着信を許可するか否かを設定する。
- [ノート] 着信時の HLC 情報要素と **analog device type** コマンドにより設定された機器を比較して、
着信整合性を調べる。
- [デフォルト値] on

15.14 話中着信を許可するか否かの設定

- [入力形式] **analog arrive ring-while-talking permit port permit**
- [パラメータ] • *port* アナログポート
- 1 TEL1 ポート
 - 2 TEL2 ポート
 - 3 TEL3 ポート
- *permit*
- on 許可する
 - off 許可しない
- [説明] 話中着信を許可するか否かを設定する。
- [ノート] この設定が **on** になっていないと、フレックスホンの **INS** キャッチホン (コールウェイ
ティング) も擬似キャッチホン (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] off

15.15 優先着信機能の設定

- [入力形式] **analog arrive prior-port port priority**
- [パラメータ] • *port*.....アナログポート
- 1..... TEL1 ポート
 - 2..... TEL2 ポート
 - 3..... TEL3 ポート
- *priority*
- 1..... 優先順位 1 位
 - 2..... 優先順位 2 位
 - 3..... 優先順位 3 位
- [説明] どのポートを優先的に呼び出すかを設定する。
- [ノート] TEL ポート間で優先順位の重複があっても構わない。すべての TEL ポートと同一優先順位に設定した場合、優先着信は行われずにすべての TEL ポートが呼び出される。
- [デフォルト値] *priority* = 2

15.16 着信ベルリストの登録

- [入力形式] **analog arrive ringer-type list add port type number isdn_number/[sub_address]**
- [パラメータ] • *port*.....アナログポート
- 1..... TEL1 ポート
 - 2..... TEL2 ポート
 - 3..... TEL3 ポート
- *type*.....着信時のベル音の種類 (1,2)
- *number*.....リスト番号
- *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。

15.17 着信ベルリストの削除

- [入力形式] **analog arrive ringer-type list delete port type number**
- [パラメータ] • *port*.....アナログポート
- 1..... TEL1 ポート
 - 2..... TEL2 ポート
 - 3..... TEL3 ポート
- *type*.....着信時のベル音の種類 (1,2)
- *number*.....リスト番号
- [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。

15.18 ナンバー・ディスプレイ設定

- [入力形式] **analog arrive number display port mode**
- [パラメータ] • *port* アナログポート
- 1 TEL1 ポート
 - 2 TEL2 ポート
 - 3 TEL3 ポート
- *mode*
- *off* ナンバー・ディスプレイ、キャッチホン・ディスプレイを使用しない
 - *on* ナンバー・ディスプレイを使用する
 - *with-catch-phone* ナンバー・ディスプレイとキャッチホン・ディスプレイの両方を使用する
- [説明] 指定したアナログポートでナンバーディスプレイを使用可能にする。
with-catch-phone は、話中着信設定が *on* であればナンバー・ディスプレイに加えてキャッチホン・ディスプレイも使用可能にすることができる。
- [ノート] キャッチホン・ディスプレイを使用する場合、話中着信設定で話中着信を許可する設定にしてください。
- [デフォルト値] *off*

15.19 ナンバー・ディスプレイ信号の設定

- [入力形式] **analog arrive modem signal type port type**
- [パラメータ] • *port* アナログポート
- 1 TEL1 ポート
 - 2 TEL2 ポート
 - 3 TEL3 ポート
- *type* 信号の設定
- 1 ストップビット信号長がボーレートの整数倍
 - 2 ストップビット信号長がボーレートの 1 ~ 2 倍 (従来方式)
- [説明] 指定したアナログポートから送出するナンバー・ディスプレイ信号を選択する。
- [デフォルト値] 1

15.20 ダイヤル桁間タイマの設定

- [入力形式] **analog wait dial timer port time**
- [パラメータ] • *port* アナログポート
- 1 TEL1 ポート
 - 2 TEL2 ポート
 - 3 TEL3 ポート
- *time* 秒数 (1..59)
- [説明] ダイヤル桁間タイマ値を設定する。
ダイヤル中にこのタイマ値を越えてキー操作が無いと発信動作を開始する。秒数は 1 秒単位で設定できる。
- [デフォルト値] 4

15.21 フッキングを判定する時間の設定

- [入力形式] **analog hooking timer port time**
- [パラメータ] • *port* アナログポート
- 1 TEL1 ポート
 - 2 TEL2 ポート
 - 3 TEL3 ポート
- *time* 秒数 (0.5..2)
- [説明] フッキングとして判断する最大の時間を設定する。
この時間を越えてアナログポートに接続された通信機器のフックスイッチを押し続けた場合はオンフックとみなして切断処理される。秒数は 0.1 秒単位で設定できる。
- [デフォルト値] 1

15.22 フッキング後にキー操作を受け入れる時間の設定

- [入力形式] **analog hooking wait timer** *port time*
- [パラメータ] • *port*.....アナログポート
- 1.....TEL1 ポート
 - 2.....TEL2 ポート
 - 3.....TEL3 ポート
- *time*
- 秒数 (1..9)
- [説明] フッキング後にキー操作を受け入れる時間を設定する。
フレックスホン機能を利用するためのフック操作を行った後、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

15.23 フッキング及びオンフック検出を無効と判断する時間の設定

- [入力形式] **analog hooking inhibit timer** *port time*
- [パラメータ] • *port*.....アナログポート
- 1.....TEL1 ポート
 - 2.....TEL2 ポート
 - 3.....TEL3 ポート
- *time*
- 秒数 (1..3)
 - off.....0秒
- [説明] オフフック後から、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] オフフック後の数秒間、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

15.24 アナログポートの再呼出時間設定

- [入力形式] **analog re-ringing-timer** *port time*
- [パラメータ] • *port*.....アナログポート
- 1.....TEL1 ポート
 - 2.....TEL2 ポート
 - 3.....TEL3 ポート
- *time*再呼出時間の秒数 (10..180)
- [説明] 指定したアナログポートの再呼出時間を設定します。
- [デフォルト値] 30

15.25 フレックスホン機能の使用パターンの設定

- [入力形式] **analog supplementary-service** [network] *func1* [*func2...func6*]
analog supplementary-service pseudo *func1* [*func2...func6*]
analog supplementary-service clear
- [パラメータ]
- network 網提供のフレックスホンを示すキーワード
 - *func1, func2, func3, func4, func5, func6*
 - call-waiting... INS キャッチホン (コールウェイティング) 機能使用を示すキーワード
 - call-transfer... 通信中転送機能使用を示すキーワード
 - add-on..... 三者通話機能使用を示すキーワード
 - call-deflection 1. TEL1 ポートでの着信転送機能使用を示すキーワード
 - call-deflection 2. TEL2 ポートでの着信転送機能使用を示すキーワード
 - call-deflection 3. TEL3 ポートでの着信転送機能使用を示すキーワード
 - pseudo.. 擬似機能使用を示すキーワード
 - clear 全ての機能を使用しない
- [説明] フレックスホン機能の使用パターンを設定する。
- [ノート] 着信転送機能を実際に動作させるためには、着信転送先アドレスの設定 (**analog supplementary-service call-deflection address** コマンド)が必要。
- [デフォルト値] clear

15.26 着信転送先アドレスの設定

- [入力形式] **analog supplementary-service call-deflection address** *port isdn_number* [*sub_address*]
- [パラメータ]
- *port* アナログポート
 - 1 TEL1 ポート
 - 2 TEL2 ポート
 - 3 TEL3 ポート
 - *isdn_number*... ISDN 番号
 - *sub_address* サブアドレス (0x21 から 0x7e の ASCII 文字)
- [説明] 着信転送先アドレスを登録する。
- [ノート] 網提供のフレックスホンによる着信転送では、サブアドレスの指定は無効となる。

15.27 着信転送トーキの設定

- [入力形式] **analog supplementary-service call-deflection talkie** *port transfer originator*
- [パラメータ]
- *port* アナログポート
 - 1 TEL1 ポート
 - 2 TEL2 ポート
 - 3 TEL3 ポート
 - *transfer.* 転送トーキ
 - on..... あり
 - off..... なし
 - *originator.* 転送元トーキ
 - on..... あり
 - off..... なし
- [説明] 着信転送におけるトーキのありなしを設定する。
- [ノート] 転送トーキは、網提供の着信転送使用時に、転送される相手側で聞こえる音声ガイドであり、転送元トーキは、転送先の相手に聞こえる音声ガイドのこと。
なお、擬似機能による着信転送使用時には転送トーキは無い。
- [デフォルト値] *transfer* = off
originator = off

15.28 着信転送を起動するタイミングの設定

- [入力形式] **analog supplementary-service call-deflection ringer port count**
- [パラメータ] • *port*.....アナログポート
- 1..... TEL1 ポート
 - 2..... TEL2 ポート
 - 3..... TEL3 ポート
- *count*
- 回数 (1..10)指定回数着信ベルを鳴らした後に起動する
 - off.....着信ベルを鳴らさずにすぐに起動開始する
- [説明] 着信転送を起動するタイミングを設定する。
タイミングは3秒周期のリズムを1回とカウントする。
- [デフォルト値] off

15.29 着信転送が拒否された時の動作の設定

- [入力形式] **analog supplementary-service call-deflection reject port action**
- [パラメータ] • *port*.....アナログポート
- 1..... TEL1 ポート
 - 2..... TEL2 ポート
 - 3..... TEL3 ポート
- *action*
- busy.....着信に対し、ビジートーン(話中)を返す
 - alert.....着信に対して応答する
- [説明] 着信転送を行おうとして、網からそれを拒否された時の動作を設定する。busyの場合には、着信に対しビジー(話中)を返すので、電話をかけてきた方にはビジートーンが返り、通話はできない。alertの場合には、呼出を返すと同時に手元の電話機のベルを鳴らすので、ここで受話器をとれば通話できる。
- [デフォルト値] alert

15.30 送話 PAD の設定

- [入力形式] **analog pad send port pad**
- [パラメータ] • *port*.....アナログポート
- 1..... TEL1 ポート
 - 2..... TEL2 ポート
 - 3..... TEL3 ポート
- *pad*
- -3dB..... -3dB PAD 挿入
 - -6dB..... -6dB PAD 挿入
 - -9dB..... -9dB PAD 挿入
 - -12dB..... -12dB PAD 挿入
 - -15dB..... -15dB PAD 挿入
 - -18dB..... -18dB PAD 挿入
 - -21dB..... -21dB PAD 挿入
 - off.....PAD なし
- [説明] 送話 PAD を設定する。
- [デフォルト値] off

15.31 受話 PAD の設定

- [入力形式] **analog pad receive port pad**
- [パラメータ] • *port* アナログポート
- 1TEL1 ポート
 - 2TEL2 ポート
 - 3TEL3 ポート
- *pad*
- -3dB..... -3dB PAD 挿入
 - -6dB..... -6dB PAD 挿入
 - -9dB..... -9dB PAD 挿入
 - -12dB..... -12dB PAD 挿入
 - -15dB..... -15dB PAD 挿入
 - -18dB..... -18dB PAD 挿入
 - -21dB..... -21dB PAD 挿入
 - off.....PAD なし
- [説明] 受話 PAD を設定する。
- [デフォルト値] off

15.32 MP 時に電話発着信のために 1B チャンネルに落とすか否かの設定

- [入力形式] **analog mp prior port down**
- [パラメータ] • *port* アナログポート
- 1TEL1 ポート
 - 2TEL2 ポート
 - 3TEL3 ポート
- *down*
- on.....落とす
 - off.....落とさない
- [説明] MP 時に 2B チャンネルでデータ通信中、電話の発着信を行うためにデータ通信のチャンネル数を 1B に落とすか否かを設定する。
- [デフォルト値] on

15.33 TEL ポートへの切断信号の送出の設定

- [入力形式] **analog disc-signal port use**
- [パラメータ] • *port* アナログポート
- 1TEL1 ポート
 - 2TEL2 ポート
 - 3TEL3 ポート
- *use*
- on.....使用する
 - off.....使用しない
- [説明] 指定したアナログポートで TEL ポートへの切断信号を送出するか否かを設定する。
on に設定すると、発信側が先に通信を切断した場合に、極性反転して擬似的な切断信号をその TEL ポートへ送出する。
- [デフォルト値] on

15.34 DTMF 検出レベルの設定

- [入力形式] **analog dtmf level** *port level*
- [パラメータ] • *port*.....アナログポート
- 1.....TEL1 ポート
 - 2.....TEL2 ポート
 - 3.....TEL3 ポート
- *level*.....検出レベル dB(-30..0)
- [説明] アナログポートの DTMF 信号検出レベルを設定する。
- [デフォルト値] -18

15.35 i・ナンバーサービスのポート番号の設定

- [入力形式] **analog arrive inumber-port** *port [inum_port...]*
analog arrive inumber-port *port all*
analog arrive inumber-port *port none*
- [パラメータ] • *port*.....アナログポート
- 1.....TEL1 ポート
 - 2.....TEL2 ポート
 - 3.....TEL3 ポート
- *inum_port*.....i・ナンバーサービスのポート番号 (1, 2, 3)
- *all*.....i・ナンバーサービスのポート番号 1, 2, 3 全てに対応する
- *none*.....i・ナンバーサービスのポート番号に対応させない
- [説明] i・ナンバーサービスで網から送られるポート番号を、RT52proのアナログポートに対応させる。対応させたポート番号が送られてきたら、そのアナログポートが着信を受ける。
*all*を設定したときには、どのポート番号が送られてきても着信を受ける。
*none*を設定したときには、どのポート番号が送られてきても着信を受けない。
- [デフォルト値] i・ナンバーサービスのポート番号と同じ番号のアナログポートが着信を受ける。

15.36 アナログダイヤルインと無鳴動着信機能の設定

[入力形式] **analog arrive incomming-signal** port number address type signal dial_in-number

analog arrive incomming-signal delete port number

[パラメータ]

- port アナログポート
 - 1 TEL1 ポート
 - 2 TEL2 ポート
 - 3 TEL3 ポート
- number 登録番号 (1..)
- address アドレス
 - global グローバル着信を登録
 - local1 1 番目のローカルアドレスを登録
 - local2 2 番目のローカルアドレスを登録
 - local3 3 番目のローカルアドレスを登録
 - local4 4 番目のローカルアドレスを登録
 - local5 5 番目のローカルアドレスを登録
 - inumber1 i・ナンバーのポート番号 1 を登録
 - inumber2 i・ナンバーのポート番号 2 を登録
 - inumber3 i・ナンバーのポート番号 3 を登録
- type HLC 種別
 - tel HLC が電話
 - fax HLC が FAX
 - none HLC がない
 - all 全ての HLC
- signal
 - modem モデムダイヤルイン
 - pb PB ダイヤルイン
 - no-ringing-fax 無鳴動着信
- dial_in-number ... アナログ機器に送出するダイヤルイン番号
(signal で modem と pb を指定したときのみ有効)

[説明]

指定した port に対して、address と type の一致する着信があったときに、signal に相当した着信処理を行う。アナログダイヤルインのときには、dial_in-number で設定されたダイヤルイン信号を出す。

15.37 発番号情報なし着信機能と擬似ナンバー・リクエスト機能の設定

[入力形式] **analog arrive without-calling-number** port type [option]

[パラメータ]

- port アナログポート
 - 1 TEL1 ポート
 - 2 TEL2 ポート
 - 3 TEL3 ポート
- type タイプ
 - permit 発番号情報なし着信を許可する
 - reject 発番号情報なし着信を拒否する
 - calling-number-request 発番号情報なし着信を擬似ナンバー・リクエストで拒否する
- option
 - all すべての着信を対象にする (オプション省略時)
 - public-telephone この設定を公衆電話からの着信に限定する
 - rejected-by-user. この設定をユーザによる通知拒否の着信に限定する
 - service-unavailable .. この設定を表示圏外からの着信に限定する

[説明]

指定したアナログポートの発番号情報なしの着信を、指定した非通知理由により許可するか否か、または擬似ナンバー・リクエストで拒否するか否かを選択する。

[デフォルト値]

type = permit

option = all

16. 操作

16.1 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。

16.2 トンネルインタフェース番号の選択

- [入力形式] **tunnel select tunnel_number**
- [パラメータ] • *tunnel_number*
- トンネルインタフェース番号 (1..10)
 - none トンネル先を指定しない
- [説明] トンネルモードの設定や表示の対象となるトンネルインタフェース番号を選択する。以降プロンプトには、**console prompt** コマンドで設定した文字列とトンネルインタフェース番号が続けて表示される。**none** を指定すると、プロンプトにトンネルインタフェース番号を表示しない。
- [ノート] この操作コマンドは一般ユーザでも実行できる。
プロンプトが **tunnel** のときに PP 関係のコマンド入力はできない。

16.3 設定に関する操作

16.3.1 管理ユーザへの移行

- [入力形式] **administrator**
- [パラメータ] なし
- [説明] このコマンドを発行してからでなければ、ルータの設定を変更できない。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。

16.3.2 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。

16.3.3 終了

- [入力形式] **quit** [*save*]
exit [*save*]
- [パラメータ] • *save* 管理ユーザから抜ける時に **save** を指定すると、設定内容を不揮発性メモリに保存して終了する
- [説明] ルータへのログインを終了、または管理ユーザから抜ける。
設定を変更して保存せずに管理ユーザから抜けようとする、新しい設定内容を保存するか否かを問い合わせる。

16.3.4 相手先の初期化

- [入力形式] **pp default peer_number**
- [パラメータ] • *peer_number*
- 相手先情報番号
 - *anonymous*
 - *leased*
- [説明] 指定した相手先の設定をデフォルト値に戻す。

16.3.5 トンネルインタフェースの初期化

- [入力形式] **tunnel default tunnel_number**
- [パラメータ] • *tunnel_number*
- トンネルインタフェース番号 (1..10)
 - *all*全てのトンネルインタフェース
- [説明] 指定したトンネル先の設定をデフォルトに戻す。

16.3.6 相手先毎の設定の複写

- [入力形式] **pp copy peer_number1 peer_number2**
- [パラメータ] • *peer_number1, peer_number2*
- 相手先情報番号
 - *anonymous*
- [説明] *peer_number1* の設定内容を *peer_number2* の設定に複写する。経路情報テーブルの内容は複写されない。

16.3.7 設定の初期化

- [入力形式] **cold start**
- [パラメータ] なし
- [説明] 工場出荷時の設定に戻し、設定を保存した後再起動する。
コマンド実行時に管理パスワードを問い合わせる。

16.3.8 遠隔地のルータの設定

- [入力形式] **remote setup isdn_number/sub_address**
remote setup dlci=dlci_num
- [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
- [説明] 遠隔地のルータの設定をする。
- [ノート] 専用線の場合には *isdn_number* 及び *sub_address* パラメータは不要である。

16.3.9 遠隔地のルータからの設定に対する制限

- [入力形式] **remote setup accept isdn_number/sub_address**
remote setup accept isdn_number [isdn_number_list]
remote setup accept any
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* 全ての遠隔地のルータからの設定を許可する
• *none* 全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、1 または 2 番目の形式で設定する。
- [デフォルト値] *any*

16.4 動的情報のクリア操作

16.4.1 ARP テーブルのクリア

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

16.4.2 IP の動的経路情報のクリア

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

16.4.3 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。

16.4.4 アカウントのクリア

- [入力形式] **clear account**
 [パラメータ] なし
 [説明] データ通信に関する合計アカウントと、全てのアナログポートのアカウントをクリアする。
 相手先情報番号ごとのアカウントはクリアされない。

16.4.5 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。
 [ノート] このコマンドにより各 PP ごとの累積情報に関する発信制限が解除される。

16.4.6 アナログポートに関するアカウントのクリア

- [入力形式] **clear analog account** [*port*]
 [パラメータ] • *port*.....アナログポート
 ◦ 1.....TEL1 ポート
 ◦ 2.....TEL2 ポート
 ◦ 3.....TEL3 ポート
 [説明] 選択されているかまたは指定したアナログポートに関するアカウントをクリアする。
port パラメータを省略した場合には、全てのアナログポートのアカウントがクリアされる。

16.4.7 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。

16.5 スケジュール

16.5.1 スケジュールの設定

[入力形式] **schedule at [date] time peer_number command**

- [パラメータ]
- **date**..... 日付省略可
 - 月/日
 - 省略した時は */* とみなす

月の指定例	意味
1,2	1月と2月
2-	2月から12月まで
2-7	2月から7月まで
-7	1月から7月まで
*	毎月
日の指定例	意味
1	1日のみ
1,2	1日と2日
2-	2日から月末まで
2-7	2日から7日まで
-7	1日から7日まで
mon	月曜日のみ
sat,sun	土曜日と日曜日
mon-fri	月曜日から金曜日
-fri	日曜日から金曜日
*	毎日

- **time**..... 時刻
 - 時 (0..23 または *): 分 (0..59 または *)
 - **startup**起動時
- **peer_number**
 - 相手先情報番号
 - anonymous
 - leased
 - **peer_number** を省略した時は相手先情報番号を指定しないという意味になる
 - * (実行するコマンドが **peer_number** を指定する必要が無い場合)
- **command** ..実行するコマンド制限あり

[説明] **time** で指定した時刻に **peer_number** で指定した相手先に **command** を実行する。
schedule at コマンドは複数指定でき、同じ時刻に指定されたものはコマンドを設定した順番に実行される。実行順は **show schedule** コマンドで確認する。
 以下のコマンドは指定できない。

administrator, administrator password, cold start, console で始まるコマンド, **date, help, login password, login timer, ping, pp copy, pp default, pp line, quit, remote setup, save, show** で始まるコマンド, **time, timezone, traceroute**

[ノート] 入力時、**command** パラメータに対して TAB キーによるコマンド補完は行いが、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
```

16.5.2 スケジュールの削除

- [入力形式] **schedule delete** *schedule_number*
- [パラメータ] • *schedule_number..*....スケジュール番号
- [説明] スケジュール番号で示されるスケジュールを削除する。
スケジュール番号は **show schedule** コマンドで表示される番号。

16.5.3 スケジュールの確認

- [入力形式] **show schedule**
- [パラメータ] なし
- [説明] スケジュールをスケジュール番号とともに表示する。

16.6 本体に関する設定

16.6.1 CONN/DISC ボタンにより接続するか否かの設定

- [入力形式] **operation connect** *peer_number*
operation connect none
- [パラメータ] • *peer_number..*.....ボタンにより接続する相手先番号 (1..30)
• none.....ボタンによる接続をしない
- [説明] CONN/DISC ボタンにより接続するか否かを設定する。
- [デフォルト値] none

16.6.2 CONN/DISC ボタンにより切断するか否かの設定

- [入力形式] **operation disconnect** *peer_number*
operation disconnect all
operation disconnect none
- [パラメータ] • *peer_number..*.....ボタンにより切断する相手先番号 (1..30)
• allボタンにより全ての相手先を切断する
• none.....ボタンによる切断をしない
- [説明] CONN/DISC ボタンにより切断するか否かを設定する。
- [ノート] アナログ機能による接続には関係ない。
- [デフォルト値] all

16.6.3 アナログポート通信の接続・切断時のアラーム音の設定

- [入力形式] **alarm connection analog** *switch*
- [パラメータ] • *switch*
 ◦ on.....鳴らす
 ◦ off鳴らさない
- [説明] アナログポート通信の接続、切断時にアラーム音を鳴らすか否かを設定する。
- [デフォルト値] on

16.6.4 データ通信の接続・切断・異常切断時のアラーム音の設定

- [入力形式] **alarm connection data** *switch*
- [パラメータ] • *switch*
 ◦ on.....鳴らす
 ◦ off鳴らさない
- [説明] データ通信の接続、切断時にアラーム音を鳴らすか否かを設定する。
- [デフォルト値] on

16.6.5 ボタンや電話機からの操作時のクリック音の設定[入力形式] **alarm click switch**[パラメータ] • *switch*

- on.....鳴らす
- off.....鳴らさない

[説明] ボタンや電話機からの操作、設定処理時にクリック音を鳴らすか否かを設定する。

[デフォルト値] on

16.6.6 MP データ通信時にリンク数変化でアラーム音を鳴らすか否かの設定[入力形式] **alarm mp switch**[パラメータ] • *switch*

- on.....鳴らす
- off.....鳴らさない

[説明] データ通信時に MP の 2B 目の UP/DOWN 時にアラーム音を鳴らすか否かを設定する。

[デフォルト値] on

16.6.7 アラーム音の制御[入力形式] **alarm entire switch**[パラメータ] • *switch*

- on.....有効な設定に対して鳴らす
- off.....まったく鳴らさない

[説明] **alarm connection analog**、**alarm connection data**、**alarm click**、**alarm mp** コマンドによるアラーム音の有効な設定に対して鳴らすか、まったく鳴らさないかを設定する。

[デフォルト値] on

16.6.8 バックライトの点灯パターンの指定[入力形式] **display backlight mode**[パラメータ] • *mode*

- while表示変更時に一定時間 (10 秒) 点灯
- online.....表示変更時に一定時間 (10 秒) 点灯。回線使用中は常に点灯。
- always常に点灯
- disable常に消灯

[説明] バックライトの点灯パターンを指定する。

[デフォルト値] while

16.7 キューの設定

16.7.1 キューイングアルゴリズムタイプの選択

- [入力形式] **lan queue type** *type*
 pp queue type *type*
 • *type*
- *fifo* First In, First Out 形式のキューイング
 - *wfq* Weighted Fair Queue 形式のキューイング
- [説明] 指定したインタフェースに対して、キューイングアルゴリズムタイプを選択する。
fifo は最も基本的なキューである。*fifo* の場合、パケットは必ず先にルータに到着したの
 から送信される。パケットの順番が入れ替わることは無い。*fifo* キューにたまったパケット
 の数が **lan/pp queue type** コマンドで指定した値を越えた場合、キューの再後尾、つまり
 最も最後に到着したパケットが破棄される。
wfq は、送信待ちのパケットを始点・終点 IP アドレスやプロトコル、ポート番号でフロー
 としてグループ分けして、それぞれのフローで使用する帯域のバランスが取れるようにす
 るキューイングアルゴリズムである。*wfq* を使用すると、TELNET のような、帯域はあまり
 必要としないが速い応答時間を必要とするプロトコルと、FTP のような応答時間よりも
 広い帯域を必要とするプロトコルを同時に利用した場合に、TELNET の応答時間の落ち込
 みを *fifo* に比べて軽減することができる。
wfq のもう一つの特徴は、設定がいら無いということである。設定するところがないため、
 優先制御や帯域制御に比べて細かい調整はできないが、簡単にフロー間での帯域のバラン
 スを図ることができる。
- [デフォルト値] *fifo*

16.7.2 クラス毎のキュー長の設定

- [入力形式] **lan queue length** *len0* [*len1*..*len15*]
 pp queue length *len0* [*len1*..*len15*]
- [パラメータ] • *len0*..*len15*.....クラス 0 からクラス 15 のキュー長
- [説明] インタフェースに対して、指定したクラスのキューに入ることのできるパケットの個数を
 指定する。設定を省略したクラスに関しては、最後に指定されたキュー長が残りのクラス
 にも適用される。
- [デフォルト値] 40 (LAN インタフェース)
 20 (PP インタフェース)

16.7.3 インタフェース毎のキューの表示

- [入力形式] **show lan queue**
 show pp queue [*peer_number*]
- [パラメータ] • *peer_number*
- 相手先情報番号
 - *anonymous*
 - *leased*
- [説明] LAN インタフェースまたは選択されている PP に対して、キューの設定及び状態を表示する。

16.8 その他の操作

16.8.1 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。

16.8.2 トンネルインタフェースの使用許可の設定

[入力形式] **tunnel enable** *tunnel_number*

[パラメータ] • *tunnel_number*

- トンネルインタフェース番号 (1..10)
- allすべてのトンネルインタフェース

[説明] トンネルインタフェースを使用できる状態にする。
工場出荷時、すべてのトンネルインタフェースは使用不許可状態であり、使用する場合には本コマンドで許可状態に設定する必要がある。

16.8.3 トンネルインタフェースの使用不許可の設定

[入力形式] **tunnel disable** *tunnel_number*

[パラメータ] • *tunnel_number*

- トンネルインタフェース番号 (1..10)
- allすべてのトンネルインタフェース

[説明] トンネルインタフェースを使用できない状態にする。
トンネル先の設定を行う場合は、不許可状態であることが望ましい。

16.8.4 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。
相手先の設定を行う時は **disable** 状態であることが望ましい。

16.8.5 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った場合には再起動が必要となる。

16.8.6 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。

16.8.7 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。

16.8.8 ping

- [入力形式] **ping** *bost* [*count*]
- [パラメータ] • *bost*
- ping をかけるホストの IP アドレス (xxx.xxx.xxx.xxx (xxx は 10 進数))
 - ping をかけるホストの名称
- *count*
- 実行回数 (1..21474836)
 - infinity...Ctrl+C を入力するまで繰り返す
- [説明] ICMP ECHO 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。

16.8.9 traceroute

- [入力形式] **traceroute** *bost* [*noresolv*]
- [パラメータ] • *bost*
- traceroute をかけるホストの IP アドレス (xxx.xxx.xxx.xxx (xxx は 10 進数))
 - traceroute をかけるホストの名称
- [説明] 指定したホストまでの経路を調べて表示する。キーワード *noresolv* を指定した場合には、DNS による解決を行わない。

16.8.10 telnet

- [入力形式] **telnet** *bost* [*port* [*mode* [*negotiation* [*abort*]]]]
- [パラメータ] • *bost*TELNET をかける相手のホスト名、もしくは IP アドレス
- *port*使用するポート番号
 - 10 進数
 - ポート番号のニーモニック
 - 省略時は 23(TELNET)
 - *mode*telnet 通信 (送信) の動作モード
 - *character*文字単位で通信する
 - *line*行単位で通信する
 - *auto**port* パラメータの設定値により *character/line* を選択
 - 省略時は *auto*
 - *negotiation* telnet オプションのネゴシエーションの選択
 - *on*ネゴシエーションする
 - *off*ネゴシエーションしない
 - *auto**port* パラメータの設定値により *on/off* を選択
 - 省略時は *auto*
 - *abort*TELNET クライアントを強制的に終了させるためのアボートキー
 - 10 進数の ASCII コード
 - 省略時は 29(^)
- [説明] TELNET クライアントを実行する。
- [ノート] *character* モードは、通常の TELNET サーバなどへの接続のための透過的な通信を行う。
line モードは、入力行を編集して行単位の通信を行う。行編集の終了は、改行コード (CR:0x0d または LF:0x0a) の入力で判断する。
- ポート番号による機能自動選択について
1. telnet 通信の動作モードの自動選択
port 番号が 23 の場合は文字単位モードとなり、そうでない場合は行単位モードとなる。
 2. telnet オプションのネゴシエーションの自動選択
port 番号が 23 の場合はネゴシエーションし、そうでない場合はネゴシエーションしない。
- [デフォルト値] *port* = 23
mode = *auto*
negotiation = *auto*
abort = 29(^)

16.8.11 telnet サーバ機能の ON/OFF の設定

- [入力形式] **telnetd service service**
- [パラメータ] • *service*
- on.....telnet サーバ機能を有効にする
 - off.....telnet サーバ機能を停止させるする
- [説明] telnet サーバ機能の利用を選択する。
- [ノート] 設定は再起動後有効になる。
telnet サーバが停止している時、telnet サーバはアクセス要求に一切応答しない。
- [デフォルト値] on

16.8.12 telnet サーバ機能の listen ポートの設定

- [入力形式] **telnetd listen port**
- [パラメータ] • *port*
- telnet サーバ機能の待ち受け (listen) ポート番号 (1..65535)
- [説明] telnet サーバ機能の listen ポートを選択する。
- [ノート] 設定は再起動後有効になる。
telnetd は、TCP の 23 番ポートで待ち受けしているが、このコマンドにより待ち受けポートを変更することができる。
ただし、待ち受けポートを変更した場合には、ポート番号が変更されても、telnet オプションのネゴシエーションが行える telnet クライアントを用いる必要がある。
- [デフォルト値] 23

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

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

17. 設定の表示

17.1 機器設定の表示

17.1.1 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。 <ul style="list-style-type: none"> ▫ システムのリビジョン ▫ MAC アドレス ▫ メモリの使用量 (%) ▫ date, time, timezone ▫ sysname ▫ security class ▫ remote setup accept ▫ login timer ▫ console character ▫ console columns ▫ console lines ▫ console info ▫ account threshold

17.1.2 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。 <ul style="list-style-type: none"> ▫ syslog host ▫ syslog facility ▫ 出力する SYSLOG のタイプ

17.1.3 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。 <ul style="list-style-type: none"> ▫ tftp host

17.1.4 すべての設定内容の表示

[入力形式]	show config less config
[パラメータ]	なし
[説明]	システムのリビジョンと MAC 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。

17.1.5 指定した PP の設定内容の表示

[入力形式]	show config pp <i>[peer_number]</i> less config pp <i>[peer_number]</i>
[パラメータ]	<ul style="list-style-type: none"> • <i>peer_number</i> (省略時は選択されている相手について表示) <ul style="list-style-type: none"> ▫ 相手先情報番号 ▫ anonymous ▫ leased
[説明]	show config 、 less config コマンドの表示の中から、指定した相手先情報番号に関するものだけを表示する。

17.1.6 PP 毎の設定内容の表示

- [入力形式] **show pp config** [*peer_number*]
- [パラメータ] • *peer_number* (省略時は選択されている相手について表示)
- 相手先情報番号
 - anonymous
 - leased
- [説明] 以下の項目が表示される。
- pp account threshold
 - pp encapsulation

17.2 相手先一覧の表示

17.2.1 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。

17.3 ISDN 関連の表示

17.3.1 自分側設定の表示

- [入力形式] **show isdn local**
- [パラメータ] なし
- [説明] 以下の項目が表示される。
- pp line
 - isdn local address

17.3.2 相手側設定の表示

- [入力形式] **show isdn remote** [*peer_number*]
- [パラメータ] • *peer_number* (省略時は選択されている相手について表示)
- 相手先情報番号
 - anonymous
 - leased
- [説明] 以下の項目が表示される。
- isdn remote address
 - isdn bulk

以下の項目の内、有効なものリスト。

- 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

17.4 フレームリレー関連の表示

17.4.1 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* (省略時は選択されている相手について表示)
 ◦ 相手先情報番号
 ◦ anonymous
 ◦ leased
 [説明] フレームリレー関連の設定内容を表示する。

17.4.2 DLCI の表示

- [入力形式] **show dcli** [*peer_number*]
 [パラメータ] • *peer_number* (省略時は選択されている相手について表示)
 ◦ 相手先情報番号
 ◦ anonymous
 ◦ leased
 [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。

17.5 IP 関連の表示

17.5.1 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。

17.5.2 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。

17.5.3 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

17.5.4 PP 側 IP 設定の表示

[入力形式] **show ip pp** [*peer_number*]

[パラメータ] • *peer_number* (省略時は選択されている相手について表示)
 ◦ 相手先情報番号
 ◦ anonymous
 ◦ leased

[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

[説明] 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。

17.6 PPP の設定の表示

17.6.1 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* (省略時は選択されている相手について表示)
 ◦ 相手先情報番号
 ◦ anonymous
 ◦ leased

[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。

17.6.2 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* (省略時は選択されている相手について表示)
- 相手先情報番号
 - anonymous
 - leased
- [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

17.6.3 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* (省略時は選択されている相手について表示)
- 相手先情報番号
 - anonymous
 - leased
- [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。

17.6.4 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* (省略時は選択されている相手について表示)
- 相手先情報番号
 - anonymous
 - leased
- [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。

17.6.5 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* (省略時は選択されている相手について表示)
- 相手先情報番号
 - anonymous
 - leased
- [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

17.6.6 MSCBCP 関連の設定の表示

- [入力形式] **show ppp mscbc**p [*peer_number*]
- [パラメータ] • *peer_number* (省略時は選択されている相手について表示)
- 相手先情報番号
 - anonymous
 - leased
- [説明] 以下の項目が表示される。
- ppp mscbc restart
 - ppp mscbc maxretry
 - ppp bacp use

17.6.7 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* (省略時は選択されている相手について表示)
- 相手先情報番号
 - anonymous
 - leased
- [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 bacp use
 - ppp bap restart
 - ppp bap maxretry

17.6.8 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* (省略時は選択されている相手について表示)
- 相手先情報番号
 - anonymous
 - leased
- [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

17.6.9 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* (省略時は選択されている相手について表示する)
- 相手先情報番号
 - anonymous
 - leased
- [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

17.7 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

17.8 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、またはクライアント ID
 - 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)

17.9 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

17.10 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

17.11 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

17.12 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。

17.13 WINS 関連の設定の表示

- [入力形式] **show wins**
- [パラメータ] なし
- [説明] WINS 関連の設定を表示する。

17.14 アナログ関係の設定の表示

- [入力形式] **show analog config** [*port*]
- [パラメータ] • *port*.....アナログポート
- 1.....TEL1 ポート
 - 2.....TEL2 ポート
 - 3.....TEL3 ポート
- [説明] アナログ関係の設定を表示する。

18. 状態の表示

18.1 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。

18.2 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。
 - MAC 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
 - 内部で処理できなかったパケットの発生数

18.3 PP 側の状態の表示

- [入力形式] **show status bri**
 [パラメータ] なし
 [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

18.4 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* (省略時は選択されている相手について表示)
 - 相手先情報番号
 - anonymous
 - leased
 [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

18.5 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* (省略した時は経路情報テーブル全体を表示)
- 相手先 IP アドレス
- [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。

18.6 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 (省略時は全てのアナログポートを表示)
- 1 TEL1 ポート
 - 2 TEL2 ポート
 - 3 TEL3 ポート
- [説明] アナログ関係の状態を表示する。

18.7 IPsec の SA の状態の表示

- [入力形式] **show ipsec sa**
- [パラメータ] なし
- [説明] IPsec の SA の状態を表示する。

19. ログイン

19.1 ログの表示

- [入力形式] **show log**
less log
- [パラメータ] なし
- [説明] パワーオンからのログを表示する。
- パワーオンの日時
 - 不揮発性メモリに設定を保存した日時
 - 設定のためのログインの記録
 - 接続した日時、発着
 - 回線の種類
 - 接続失敗の原因
 - 切断した日時、接続時間、ISDN 料金

19.2 アカウントの表示

- [入力形式] **show account bri**
- [パラメータ] • *bri*
- BRI 番号
 - all.....全ての BRI 番号
- [説明] 以下の項目が表示される。
- 発信回数
 - 着信回数
 - ISDN 料金の総計
- [ノート] 課金額は通信の切断時に NTT から ISDN で通知される料金情報に基づくため、割引サービスなどを利用している場合には、最終的に NTT から請求される料金とは異なる場合がある。また、NTT 以外の通信事業者を利用して通信した場合には料金情報は通知されない。

19.3 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* (省略した時は選択されている相手について表示)
- 相手先情報番号
 - anonymous
 - leased
- [説明] 選択されている相手のアカウントを表示する。
- [ノート] 課金額は通信の切断時に NTT から ISDN で通知される料金情報に基づくため、割引サービスなどを利用している場合には、最終的に NTT から請求される料金とは異なる場合がある。また、NTT 以外の通信事業者を利用して通信した場合には料金情報は通知されない。

19.4 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 (省略時はアナログポートの合計を表示)
- 1.....TEL1 ポート
 - 2.....TEL2 ポート
 - 3.....TEL3 ポート
- [説明] アナログ関係のアカウントを表示する。
- [ノート] 課金額は通信の切断時に NTT から ISDN で通知される料金情報に基づくため、割引サービスなどを利用している場合には、最終的に NTT から請求される料金とは異なる場合がある。また、NTT 以外の通信事業者を利用して通信した場合には料金情報は通知されない。

