

コマンドリファレンス

Rev.4.07.04

索引

A

administrator	300	analog extension dial prefix	239
administrator password	4	analog extension log	235
alarm connection analog	311	analog extension machine-id	234
alarm connection data	311	analog extension machine-id delete	235
alarm entire	312	analog extension master	232
alarm intrusion	312	analog extension mode	230
analog arrive incoming-signal	224	analog extension sip address	238
analog arrive incoming-signal delete	224	analog extension sip address delete	238
analog arrive modem signal type	216	analog extension slave permit	233
analog arrive number display	215	analog hooking inhibit timer	219
analog arrive prior-port	212	analog hooking timer	218
analog arrive restrict	209	analog l-mail-service	227
analog arrive restrict list add	210	analog local address	207
analog arrive restrict list delete	211	analog pad receive	221
analog arrive ringer-type list add	213	analog pad send	220
analog arrive ringer-type list delete	214	analog pause timer	228
analog arrive without-calling-number	226	analog rapid call	208
analog disc-signal	222	analog sip arrive myaddress	241
analog dtmf level	223	analog sip arrive myaddress delete	242
analog extension address refer	231	analog sip call myname	243
analog extension address refer pp	231	analog sip use arrive	240
		analog sip use call	244
		analog use	206

analog wait dial timer	217	dhcp client client-identifier pool	149
C		dhcp client client-identifier pp	149
clear analog account	307	dhcp client client-identifier type	151
clear arp	304	dhcp client hostname lan_if primary	152
clear dns cache	307	dhcp client hostname lan_if secondary	152
clear ip dynamic routing	304	dhcp client hostname pool	152
clear ipv6 dynamic routing	304	dhcp client hostname pp	152
clear ipv6 neighbor cache	305	dhcp delete scope	139
clear log	306	dhcp relay select	147
clear nat descriptor dynamic	305	dhcp relay server	146
clear nat descriptor interface dynamic	306	dhcp relay threshold	148
cold start	303	dhcp scope	138
connect	316	dhcp scope bind	140
console character	10	dhcp scope unbind	144
console columns	10	dhcp server duplicate check	145
console info	12	dhcp server rfc2131 compliant	136
console lines	11	dhcp service	135
console prompt	12	disconnect	317
D		disconnect ip connection	41
date	7	disconnect ipv6 connection	98
dhcp client client-identifier lan_if primary ...	149	dns domain	188
dhcp client client-identifier lan_if secondary ...	149	dns notice order	191
		dns private address spoof	189
		dns private name	190
		dns server	182
		dns server dhcp	184

dns server pp	183	ip filter dynamic	37
dns server select	185	ip filter dynamic comment	43
dns server select delete	185	ip filter dynamic comment delete	44
dns service	187	ip filter dynamic delete	39
dns static	193	ip filter dynamic timer	40
dns static delete	195	ip filter source-route	35
dns syslog resolv	192	ip host	193
		ip host delete	195
		ip icmp echo-reply send	153
E		ip icmp log	157
exit	301	ip icmp mask-reply send	154
		ip icmp parameter-problem send	154
H		ip icmp redirect receive	155
help	3	ip icmp redirect send	155
httpd frame use	277	ip icmp time-exceeded send	156
httpd host	276	ip icmp timestamp-reply send	156
httpd listen	275	ip icmp unreachable send	157
httpd service	274	ip lan_if address	45
		ip lan_if broadcast	50
I		ip lan_if dhcp lease time	48
ip filter	30	ip lan_if dhcp retry	49
ip filter comment	36	ip lan_if intrusion detection	42
ip filter comment delete	36	ip lan_if mtu	57
ip filter delete	34	ip lan_if nat descriptor	165
ip filter directed-broadcast	35	ip lan_if netmask	58
		ip lan_if proxyarp	55

ip lan_if rip auth key	54	ip pp secure filter	76
ip lan_if rip auth type	53	ip route	27
ip lan_if rip filter	51	ip route delete	29
ip lan_if rip listen	52	ip routing	25
ip lan_if routing protocol	59	ip routing cache	26
ip lan_if secondary address	47	ip simple-service	23
ip lan_if secure filter	56	ip stealth	158
ip pp hide static route	77	ip tunnel nat descriptor	167
ip pp hold routing	71	ip tunnel secure filter	78
ip pp intrusion detection	42	ipv6 filter	94
ip pp local address	60	ipv6 filter delete	95
ip pp mtu	77	ipv6 filter dynamic	96
ip pp nat descriptor	166	ipv6 filter dynamic delete	98
ip pp netmask	67	ipv6 icmp echo-reply send	159
ip pp remote address	63	ipv6 icmp log	162
ip pp remote address pool	66	ipv6 icmp packet-too-big send	162
ip pp rip auth key	75	ipv6 icmp parameter-problem send	159
ip pp rip auth type	74	ipv6 icmp redirect receive	160
ip pp rip connect interval	69	ipv6 icmp redirect send	160
ip pp rip connect send	69	ipv6 icmp time-exceeded send	161
ip pp rip disconnect interval	70	ipv6 icmp unreachable send	161
ip pp rip disconnect send	70	ipv6 interface address	81
ip pp rip filter	72	ipv6 interface address delete	81
ip pp rip hop	73	ipv6 interface mtu	80
ip pp rip listen	73	ipv6 interface prefix	82
ip pp routing protocol	68	ipv6 interface prefix delete	82

ipv6 interface rip filter	91
ipv6 interface rip receive	88
ipv6 interface rip send	88
ipv6 interface rip trust gateway	89
ipv6 interface rtadv send	85
ipv6 interface secure filter	95
ipv6 pp rip connect interval	92
ipv6 pp rip connect send	91
ipv6 pp rip disconnect interval	93
ipv6 pp rip disconnect send	92
ipv6 pp rip hold routing	93
ipv6 pp rip hop	90
ipv6 prefix	83
ipv6 rip use	87
ipv6 route	86
ipv6 route delete	86
ipv6 routing	79
ipv6 stealth	163

L

lan1 type auto-crossover	21
lan2 type	20
lan_if transmit timeout	22
less config	327
less config pp	327

less log	360
login password	4
login timer	6

M

mail-check go	248
mail-check led	249
mail-check prohibit	248
mail-check server	247
mail-check timeout	250
mail-notify charset	260
mail-notify intrusion	261
mail-notify intrusion go	262
mail-notify intrusion subject	262
mail-transfer filter	258
mail-transfer go	254
mail-transfer prohibit	259
mail-transfer receive from	253
mail-transfer receive maxlength	253
mail-transfer receive restrict	257
mail-transfer send maxlength	256
mail-transfer send to	252
mail-transfer server	251
mail-transfer timeout	255

N

nat descriptor address inner	170
nat descriptor address outer	169
nat descriptor delete	175
nat descriptor ftp port	179
nat descriptor log	179
nat descriptor masquerade incoming	178
nat descriptor masquerade port range	177
nat descriptor masquerade rlogin	172
nat descriptor masquerade static	173
nat descriptor masquerade static delete ...	176
nat descriptor masquerade ttl hold	174
nat descriptor masquerade unconvertible port	
180	
nat descriptor static	171
nat descriptor static delete	176
nat descriptor timer	175
nat descriptor type	168
netvolante-dns delete go	290
netvolante-dns delete go pp	290
netvolante-dns get hostname list	291
netvolante-dns get hostname list pp	291
netvolante-dns go	289
netvolante-dns go pp	289
netvolante-dns hostname host	292

netvolante-dns hostname host pp	292
netvolante-dns port	294
netvolante-dns server	295
netvolante-dns sip use	293
netvolante-dns sip use pp	293
netvolante-dns timeout	294
netvolante-dns timeout pp	294
netvolante-dns use	288
netvolante-dns use pp	288
ntpdate	9

P

packetdump lan_if	17
packetdump pp	18
password reenter	24
ping	318
ping6	101
pp always-on	313
pp auth accept	105
pp auth clear myname	106
pp auth delete username	103
pp auth multi connect prohibit	107
pp auth myname	106
pp auth request	104
pp auth username	103

pp bind tunnel	281	ppp lcp maxconfigure	113
pp copy	303	ppp lcp maxfailure	113
pp default	302	ppp lcp maxterminate	112
pp disable	315	ppp lcp mru	110
pp enable	315	ppp lcp pfc	111
pp keepalive interval	314	ppp lcp restart	112
pp name	265	ppp mscbcx maxretry	123
pp select	299	ppp mscbcx restart	123
ppp ccp maxconfigure	126	ppp pap maxauthreq	114
ppp ccp maxfailure	126	ppp pap restart	114
ppp ccp maxterminate	125	pppoe	132
ppp ccp no-encryption	287	pppoe access concentrator	128
ppp ccp restart	125	pppoe auto connect	128
ppp ccp type	124	pppoe auto disconnect	129
ppp chap maxchallenge	115	pppoe disconnect time	131
ppp chap restart	115	pppoe padi maxretry	129
ppp ipcp ipaddress	117	pppoe padi restart	130
ppp ipcp maxconfigure	118	pppoe padr maxretry	130
ppp ipcp maxfailure	119	pppoe padr restart	131
ppp ipcp maxterminate	118	pppoe service-name	132
ppp ipcp msextr	120	pppoe tcp mss limit	132
ppp ipcp restart	117	pppoe use	127
ppp ipcp vjc	116	pptp call-id mode	283
ppp ipv6cp use	121	pptp clear hostname	282
ppp lcp acfc	108	pptp hostname	282
ppp lcp magicnumber	109	pptp keepalive interval	286

pptp keepalive log	286
pptp keepalive use	285
pptp service type	281
pptp tunnel disconnect time	284
pptp window size	283
provider dns server	268
provider dns server pp	269
provider filter routing	270
provider ipv6 connect pp	278
provider lan_if dns server	279
provider lan_if name	271
provider netvolante-dns hostname sip	278
provider ntp server	272
provider ntpdate	273
provider select	267
provider set off	266
provider set on	266
provider type	264
pstn dial type	199
pstn disable	204
pstn enable	205
pstn hooking timer	202
pstn number display	200
pstn pad receive	203
pstn pad send	204
pstn pause timer	201

pstn supplementary-service	201
----------------------------------	-----

Q

quit	301
------------	-----

R

rdate	8
restart	316

S

save	301
schedule at	308
schedule delete	310
security class	5
show analog account	361
show analog config	348
show analog extension	349
show analog extension config	350
show arp	351
show auth	335
show command	3
show config	327
show config pp	327
show dhcp	342

show dhcp status	343	show pp config	328
show dhcpc status	344	show pp connect time	361
show dns	347	show pp queue	328
show dns static	334	show ppp ccp	341
show environment	325	show ppp chap	338
show history	362	show ppp ipcp	339
show ip connection	330	show ppp lcp	336
show ip filter	329	show ppp mscbcpc	340
show ip filter list	329	show ppp pap	337
show ip host	334	show schedule	310
show ip icmp	347	show status analog	357
show ip intrusion detection	331	show status lan_if	352
show ip lan_if	332	show status netvolante-dns	357
show ip pp	333	show status netvolante-dns pp	357
show ip route	354	show status pp	353
show ipv6 address	354	show status rtp	358
show ipv6 connection	356	show status sip presence	359
show ipv6 neighbor cache	355	show syslog	326
show ipv6 rip table	355	show tftp	326
show ipv6 route	354	show wins	348
show log	360	sip ip protocol	237
show mail-check status	249	sip netvolante dial domain	245
show nat descriptor address	345	sip use	236
show nat descriptor config	345	syslog debug	16
show nat descriptor interface address	346	syslog facility	14
show nat descriptor interface bind	346	syslog host	13

syslog info	15
syslog notice	14

upnp use	296
----------------	-----

T

telnet	320
telnetd host	324
telnetd listen	323
telnetd service	322
tftp host	19
time	8
timezone	7
traceroute	319
traceroute6	102
tunnel default	302
tunnel disable	100
tunnel enable	100
tunnel encapsulation	280
tunnel endpoint address	99
tunnel endpoint clear name	285
tunnel endpoint name	284
tunnel select	300

W

wins server	122
-------------------	-----

U

upnp external address refer	297
upnp external address refer pp	297

1. はじめに

1.1 対応するプログラムのリビジョンについて

本書は、RT56v のファームウェア、Rev.4.07.04 に対応しています。

本書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 NetVolante シリーズのホームページにある情報を参照してください。

- <http://NetVolante.jp/>

1.2 コマンドリファレンスの見方

本書は、ルータのコンソールから入力するコマンドについて説明しています。
各コマンドについて、以下に示した項目の組合せで説明しています。

項目	説明
----	----

〔書式〕 コマンドの入力書式を説明します。

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 (*italic face*) で、キーワード部分は標準書体 (Normal face) で示します。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示します。

〔設定値〕 コマンドの設定値の種類と、その意味を示します。

〔説明〕 コマンドの説明部分を示します。

〔ノート〕 本コマンドを使用する場合に特に注意すべき事柄を示します。

〔初期値〕 本コマンドの初期値を示します。

〔設定例〕 本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

〔書式〕 **help**

〔設定値〕 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

〔書式〕 **show command**

〔設定値〕 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

〔書式〕 **login password**

〔設定値〕 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

〔書式〕 **administrator password**

〔設定値〕 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

〔書式〕 **security class level telnet**

〔設定値〕 ◦ *level*

- 1 TELNET でログインできる
- 3 TELNET でログインできない

◦ *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。

〔初期値〕 *level* = 1, *telnet* = off

3.4 ログインタイマの設定

[書式] **login timer** *time*
login timer clear

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

[説明] キー入力がない場合に自動的にログアウトするまでの時間を設定する。

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

[初期値] 300

3.5 タイムゾーンの設定

〔書式〕 **timezone** *timezone*

〔設定値〕 ◦ *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。

〔初期値〕 jst

3.6 現在の日付けの設定

〔書式〕 **date** *date*

〔設定値〕 ◦ *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

[書式] **time** *time*

[設定値] ◦ *time*hh:mm:ss

[説明] 現在の時刻を設定する。

3.8 リモートホストによる時計の設定

[書式] **rdate** *host* [syslog]

[設定値] ◦ *host*

- リモートホストの IP アドレス (xxx.xxx.xxx.xxx (xxx は 10 進数))
- ホストの名称

◦ **syslog**

- 出力結果を SYSLOG へ出力することを表すキーワード

[説明] ルータの時計を、パラメータで指定したホストの時間に合わせる。
このコマンドが実行されるとホストの TCP の 37 番ポートに接続する。

[ノート] 本機、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。

3.9 NTP による時計の設定

[書式] **ntpdate** *ntp_server* [syslog]

[設定値] ◦ *ntp_server*

- NTP サーバの IP アドレス (**xxx.xxx.xxx.xxx** (xxx は 10 進数))
- NTP サーバの名称

◦ **syslog**出力結果を SYSLOG へ出力することを表すキーワード

[説明] NTP を利用してルータの時計を設定する。

このコマンドが実行されるとホストの UDP の 123 番ポートに接続する。

[ノート] インターネットに接続している場合には、**rdate** コマンドを使用した場合よりも精密な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。本機自身は NTP サーバとはなれない。

syslog キーワードを指定した場合には、コマンドの出力結果を INFO レベルの SYSLOG へ出力する。

3.10 コンソールの言語とコードの設定

[書式] **console character code**

[設定値] ◦ *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。
本コマンドは一般ユーザでも実行できる。

[初期値] *sjis*

3.11 コンソールの表示文字数の設定

[書式] **console columns col**

[設定値] ◦ *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。
本コマンドは一般ユーザでも実行できる。

[初期値] 80

3.12 コンソールの表示行数の設定

[書式] **console lines** *lines*

[設定値] ◦ *lines*

- 整数 (10..100)
- **infinity**.....スクロールを止めない

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

[初期値] 24

3.13 コンソールにシステムメッセージを表示するか否かの設定

[書式] **console info** *info*

[設定値] ◦ *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。

[初期値] off

3.14 コンソールのプロンプト表示の設定

[書式] **console prompt** *prompt*

[設定値] ◦ *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。

[初期値] 空文字列

3.15 SYSLOG を受けるホストの IP アドレスの設定

[書式] **syslog host** *host*
syslog host clear

[設定値] ◦ *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、本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。

[初期値] clear

3.16 SYSLOG ファシリティの設定

[書式] **syslog facility** *facility*

[設定値] ◦*facility*

- 0..23
- user 1
- local0..local7 16..23

[説明] SYSLOG のファシリティを設定する。

[初期値] user

3.17 NOTICE タイプの SYSLOG を出力するか否かの設定

[書式] **syslog notice** *notice*

[設定値] ◦*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。

[初期値] off

3.18 INFO タイプの SYSLOG を出力するか否かの設定

[書式] **syslog info** *info*

[設定値] ◦ *info*

- on.....出力する
- off出力しない

[説明] 呼制御情報等を SYSLOG で出力するか否か設定する。

[初期値] on

3.19 DEBUG タイプの SYSLOG を出力するか否かの設定

[書式] **syslog debug** *switch*

[設定値] ◦ *switch*

- **on**.....出力する
- **off**出力しない

[説明] 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。

[初期値] **off**

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

[書式] **packetdump** *lan_if* [*count*]

[設定値] ◦ *lan_if*

- *lan1* LAN インタフェース
- *lan2* WAN インタフェース

◦ *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
- 省略時は 100

[説明] 有線 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。

[初期値] *off*

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

[書式] **packetdump pp** *peer_num* [*count*]

[設定値] ◦ *peer_num*

- 相手先情報番号 (1..30)
- **anonymous**

◦ *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
- 省略時は 100

[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。

[初期値] off

3.22 TFTP によりアクセスできるホストの IP アドレスの設定

【書式】 **tftp host** *host*

【設定値】 ◦ *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。

【初期値】 none

3.23 有線 LAN インタフェースの速度タイプの設定

[書式] **lan2 type** *type*

[設定値] ◦ *type*

- **auto** 速度自動設定
- **100-fdx** 100BASE-TX 全二重
- **100-hdx** 100BASE-TX 半二重
- **10-fdx** 10BASE-T 全二重
- **10-hdx** 10BASE-T 半二重

[説明] LAN インタフェースの速度タイプを設定する。

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

[ノート] LAN インターフェースの速度タイプは本体上部の DIP スイッチにより速度自動設定 (auto) と 10BASE-T 半二重 (10-hdx) の間で切り替えることができる。

[初期値] **auto**

3.24 クロス・ストレータケーブル自動判別機能の設定

[書式] **lan1 type auto-crossover switch**

[設定値] ◦ *switch*

- on.....自動判別機能を使用する
- off自動判別機能を使用しない

[説明] クロス・ストレータケーブル自動判別機能を使用するか否かを設定する。

ポート毎の指定はできず、全てのポートに共通の設定。

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

[初期値] on

3.25 LAN 送信タイムアウトの時間の設定

[書式] ***lan_if transmit timeout time***

[設定値] ◦ *lan_if*

- *lan1* LAN インタフェース
- *lan2* WAN インタフェース

◦ *time* ミリ秒 (30..1000)

[説明] LAN の送信タイムアウトの値を設定する。パケット送出後、この時間が経過しても送信完了状態とならない場合、何らかのエラーが発生したものとみなして LAN コントローラのリセットを行う。送信タイムアウトが頻発してスループットが低下する場合など、この値を調整することでスループットが改善される場合がある。送信タイムアウトの発生は DEBUG レベルのログで確認できる。

[初期値] 500

3.26 TCP/UDP の各種サービスの動作の設定

[書式] **ip simple-service** *switch*

[設定値] ◦ *switch* TCP/UDP の各種サービス

- **on** 動作させる
- **off** 停止させる

[説明] TCP/UDP の echo(7)、discard(9)、time(37) の各種サービスを動作させるかどうかを設定する。

[初期値] **on**

3.27 パスワード再入力機能の設定

[書式] **password reenter** *reenter*

[設定値] ◦ *reenter*

- **enable**.....パスワード再入力可能
- **disable**.....パスワード再入力不可能

[説明] 本体ディップスイッチ 6 を **off** にした時、起動後 10 分間はパスワードを再入力可能にするか否かを設定する。
再入力可能な 10 分間は、telnet でもパスワードなしでログインが可能となる。

[初期値] **enable**

4. IP の設定

4.1 LAN 側、PP 側共通の設定

4.1.1 IP パケットを扱うか否かの設定

[書式] **ip routing** *route*

[設定値] ◦*route*

- **on**.....IP パケットを処理対象として扱う
- **off**IP パケットを処理対象として扱わない

[説明] IP パケットをルーティングするかどうかを設定する。本スイッチを **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。

[初期値] **on**

4.1.2 IP 経路制御キャッシュのサイズの設定

[書式] **ip routing cache size**

[設定値] ◦ *size*.....サイズ (0..255)

[説明] IP 経路制御キャッシュのサイズを設定します。

[初期値] 16

4.1.3 IP の静的経路情報の追加

[書式] **ip route** *ip_address*[/*masklen*] *gateway gateway* [*parameter*] [*gateway gateway* [*parameter*]]

- [設定値]
- *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 *peer_num*
 - *peer_num*
 - 相手先情報番号 (1..30)
 - anonymous
 - pp anonymous name=*name*
 - *name* PAP/CHAP による名前
 - dhcp *lan_if*.. DHCP クライアントとして動作している LAN インタフェース
 - *parameter*.....以下のパラメータを空白で区切り複数設定可能
 - filter *number* [*number*...] フィルタ型経路の指定
 - *number* フィルタの番号 (1..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、**hide** キーワードが指定されているゲートウェイは、回線が接続している場合のみ有効で、回線が接続していない場合には評価されない。

4.1.4 IP の静的経路情報の削除

[書式] **ip route delete** *ip_address*[/*masklen*]

- [設定値]
- *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。

4.1.5 IP パケットのフィルタの設定

[書式] **ip filter** *filter_num* *pass_reject* *src_addr*[/*mask*][*dest_addr*[/*mask*]][*protocol* [*src_port_list* [*dest_port_list*]]]

- [設定値]
- *filter_num*..... 静的フィルタ番号 (1..2147483647)
 - *pass_reject*
 - *pass-log*..... 一致すれば通す (ログに記録する)
 - *pass-nolog*..... 一致すれば通す (ログに記録しない)
 - *reject-log*..... 一致すれば破棄する (ログに記録する)
 - *reject-nolog*..... 一致すれば破棄する (ログに記録しない)
 - *restrict-log*..... 回線が接続されていれば通し、切断されていれば破棄する (ログに記録する)
 - *restrict-nolog*..... 回線が接続されていれば通し、切断されていれば破棄する (ログに記録しない)
 - *src_addr*..... IP パケットの始点 IP アドレス
 - **XXX.XXX.XXX.XXX** (XXX は 10 進数)
 - * (ネットマスクの対応するビットが 8 ビットとも 0 と同じ)
 - 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する
 - * (すべての IP アドレスに対応)
 - *dest_addr*..... IP パケットの終点 IP アドレス (*src_addr* と同じ形式)

省略時は 1 個の * と同じ
 - *mask*..... IP アドレスのビットマスク、省略時は **0xffffffff** と同じ

src_addr 及び *dest_addr* がネットワークアドレスの場合にのみ指定可

- **xxx.xxx.xxx.xxx** (xxx は 10 進数)
 - **0x** に続く 16 進数
 - マスクビット数
- *protocol* フィルタリングするパケットの種類
- プロトコルを表す 10 進数 (0..255)
 - プロトコルを表すニーモニック

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

- 上項目のカンマで区切った並び (5 個以内)
- * (すべてのプロトコル)
- **tcpflag=flag_value/flag_mask**
- **tcpflag!=flag_value/flag_mask**
 - *flag_value* TCP フラグの値
 - header length (offset) ~ code bits の 2byte
 - 0x に続く 16 進数 (0x0000..0xffff)

▪ *flag_mask*..... TCP フラグのビットマスク

- 0xに続く 16 進数 (0x0000..0xffff)

tcpflag	意味
0x0020	URG
0x0010	ACK
0x0008	PSH
0x0004	RST
0x0002	SYN
0x0001	FIN

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

- 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。

- 上項目のカンマで区切った並び (10 個以内)
 - * (すべてのポート)
- 省略時は * と同じ。
- *dest_port_list* ...UDP、TCP のデスティネーションポート番号

[説明] IP パケットのフィルタを設定する。本コマンドで設定されたフィルタは **ip lan_if secure filter**、**ip pp secure filter**、**ip lan_if rip filter**、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場合だけ通せば十分で、そのために回線に発信するまでもないようなパケットに対して有効。例えば、時計をあわせる NTP パケット。

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

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

"ip filter pass ** tcpflag=*flag_value/flag_mask*" は、TCP のフラグと *flag_mask* の論理積が *flag_value* と一致すればフィルタに該当する。

"ip filter pass ** tcpflag!=*flag_value/flag_mask*" はTCPのフラグと*flag_mask*の論理積が *flag_value* と一致しなければフィルタに該当する。

"ip filter pass * * tcpfin" は "ip filter pass * * tcpflag=0x0001/0x0001" と同じである。

"ip filter pass * * tcprst" は "ip filter psss * * tcpflag=0x0004/0x0004" と同じである。

[設定例] # ip filter 3 pass-nolog 172.20.10.* 172.21.192.0/18 tcp ftp

「サーバを公開するとき、公開サーバへの TCP 接続は許可するが、公開サーバからインターネット向けの通信は拒否したい。」というポリシー。

```
# ip filter 1 reject server_ip * tcpflag=0x0002/0x00ff server_port *
```

```
# ip filter 100 pass * * * * *
```

```
# pp select n
```

```
# ip pp secure filter out 1 100
```

4.1.6 IP パケットのフィルタの削除

[書式] **ip filter delete** *filter_num*

[設定値] ◦*filter_num*.....静的フィルタ番号 (1..2147483647)

[説明] 指定した番号の IP のフィルタを削除する。

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

[書式] **ip filter source-route** *filter_out*

[設定値] ◦*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。

[初期値] off

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

[書式] **ip filter directed-broadcast** *filter_out*

[設定値] ◦*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。

[初期値] off

4.1.9 静的フィルタの定義のコメントの設定

[書式] **ip filter comment** *filter_num comment*

- [設定値] ◦ *filter_num*..... フィルタ番号 (1..2147483647)
◦ *comment* コメント文字列

[説明] かんたん設定専用コマンド。
個々のフィルタ定義のコメントを記録する。

[ノート] コンソールなどから手動設定した場合の動作は保証されない。

4.1.10 静的フィルタの定義のコメントの削除

[書式] **ip filter comment delete** *filter_num*

- [設定値] ◦ *filter_num*..... フィルタ番号 (1..2147483647)

[説明] かんたん設定専用コマンド。
個々のフィルタ定義のコメントを削除する。

[ノート] コンソールなどから手動設定した場合の動作は保証されない。

4.1.11 動的フィルタの定義

[書式] **ip filter dynamic** *dyn_filter_num srcaddr dstaddr protocol* [*option ...*]
ip filter dynamic *dyn_filter_num srcaddr dstaddr filter filter_list* [*in filter_list*]
[*out filter_list*] [*option ...*]

- [設定値]
- *dyn_filter_num*.....動的フィルタ番号 (1..2147483647)
 - *srcaddr*.....始点 IP アドレス
 - *dstaddr* 終点 IP アドレス
 - *protocol* プロトコル
 - tcp
 - udp
 - ftp
 - tftp
 - domain
 - www
 - smtp
 - pop3
 - telnet
 - *filter_list* **ip filter** コマンドで登録されたフィルタ番号の並び
 - *option*
 - *syslog=switch*
 - **on** コネクションの通信履歴を syslog に残す

- **off** コネクションの通信履歴を syslog に残さない
- **timeout=time**
 - **time** データが流れなくなったときにコネクション情報を解放するまでの時間 (秒)

[説明] 動的フィルタを定義する。1つ目の書式では、あらかじめルータに登録されているアプリケーション名を指定する。2つ目の書式では、ユーザがアクセス制御のルールを記述する。キーワードの **filter**、**in**、**out** の後には、**ip filter** コマンドで定義されたフィルタ番号を設定する。

filter キーワードの後に記述されたフィルタに該当するコネクション (トリガ) を検出したら、それ以降 **in** キーワードと **out** キーワードの後に記述されたフィルタに該当するコネクションを通過させる。**in** キーワードはトリガの方向に対して逆方向のアクセスを制御し、**out** キーワードは動的フィルタと同じ方向のアクセスを制御する。なお、**ip filter** コマンドの IP アドレスは無視される。**pass/reject** の引数も同様に無視される。ここに記載されていないアプリケーションについては、**filter** キーワードを使って定義することで扱える可能性がある。特に snmp のように動的にポート番号が変化しないプロトコルに扱いは容易である。

tcp か **udp** を設定することで扱える可能性がある。特に、telnet のように動的にポート番号が変化しないプロトコルは **tcp** を指定することで扱うことができる。

[初期値] **syslog = on**
timeout = 60

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

4.1.12 動的フィルタの削除

[書式] **ip filter dynamic delete** *dyn_filter_num*

[設定値] ◦ *dyn_filter_num*.....動的フィルタ番号

[説明] 指定した動的フィルタの定義を削除する。

4.1.13 動的フィルタのタイムアウトの設定

[書式] **ip filter dynamic timer** [*option=timeout* [*option...*]]

[設定値] ◦ *option*..... オプション名

- **tcp-syn-timeout** SYN を受けてから設定された時間内にコネクションが確立しなければセッションを切断する
- **tcp-fin-timeout** FIN を受けてから設定された時間が経てばコネクションを強制的に解放する
- **tcp-idle-time** 設定された時間内に TCP コネクションのデータが流れなければコネクションを切断する
- **udp-idle-time** 設定された時間内に UDP コネクションのデータが流れなければコネクションを切断する
- **dns-timeout** DNS の要求を受けてから設定された時間内に応答を受けなければコネクションを切断する

◦ *timeout*..... 待ち時間 (秒)

[説明] 動的フィルタのタイムアウトを設定する。

[ノート] 本設定はすべての検査において共通に使用される。

[初期値] **tcp-syn-timeout** = 30

tcp-fin-timeout = 5

tcp-idle-time = 3600

udp-idle-time = 30

dns-timeout=5

4.1.14 動的フィルタのコネクション管理情報の削除

[書式] **disconnect ip connection** *session_id* [*channel_id*]

- [設定値]
- *session_id*セッションの識別子
 - *channel_id*チャネルの識別子

[説明] 指定したセッションに属する特定のチャネルを削除する。チャネルを指定しないときには、そのセッションに属するすべてのチャネルを削除する。

4.1.15 侵入検知機能の動作の設定

[書式] **ip lan_if intrusion detection direction switch** [option]
ip pp intrusion detection direction switch [option]

- [設定値]
- *lan_if*
 - *lan1* LAN インタフェース
 - *lan2* WAN インタフェース
 - *direction* 観察するパケットの方向
 - *in* インタフェース側から内側へ
 - *out* インタフェース側から外側へ
 - *switch* 動作
 - *on* 実行する
 - *off* 実行しない
 - *option* オプション
 - *reject=rjt*
 - *on* 不正なパケットを破棄する
 - *off* 不正なパケットを破棄しない

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

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

[初期値] *switch* = off
reject = off

4.1.16 動的フィルタ定義のコメントを記録

[書式] **ip filter dynamic comment** *dyn_filter_num comment*

[設定値] ◦ *dyn_filter_num*.....動的フィルタ番号 (1..2147483647)
◦ *comment* コメント文字列

[説明] *かんたん*設定専用のコマンド。
個々のフィルタ定義のコメントを記録する。

[ノート] コンソールなどから手動設定した場合の動作は保証されない。

4.1.17 動的フィルタ定義のコメントを削除

〔書式〕 **ip filter dynamic comment delete** *dyn_filter_num*

〔設定値〕 ◦ *dyn_filter_num*.....動的フィルタ番号 (1..2147483647)

〔説明〕 かんたん設定専用のコマンド。
個々のフィルタ定義のコメントを削除する。

〔ノート〕 コンソールなどから手動設定した場合の動作は保証されない。

4.2 LAN 側の設定

4.2.1 IP アドレスの設定

[書式] **ip lan_if address ip_address [/netmask]**
ip lan_if address dhcp
ip lan_if address clear

- [設定値]
- *lan_if*
 - lan1 LAN インタフェース
 - lan2 WAN インタフェース
 - *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
 - *dhcp* DHCP クライアントとして IP アドレスを取得
 - *clear* IP アドレスをクリア

[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。
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。
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。

dhcp を設定した場合には、コマンド実行後に DHCP クライアントとして IP アドレスを取得しに行く。DHCP で IP アドレスを取得できなかった場合、または **clear** を設定した場合、LAN に対して IP の動作を行わない。

[初期値] 192.168.0.1/24 (lan1 の場合)

clear (lan2 の場合)

4.2.2 LAN 側のセカンダリ IP アドレスの設定

[書式] **ip lan_if secondary address ip_address [/netmask]**
ip lan_if secondary address dhcp
ip lan_if secondary address clear

- [設定値]
- *lan_if*
 - lan1 LAN インタフェース
 - lan2 WAN インタフェース
 - *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
 - *dhcp* DHCP クライアントとして IP アドレスを取得
 - *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。

[初期値] clear

4.2.3 DHCP クライアントが要求する IP アドレスのリース期間の設定

[書式] **ip lan_if dhcp lease time time**
ip lan_if dhcp lease time clear

- [設定値]
- *lan_if*
 - lan1 LAN インタフェース
 - lan2 WAN インタフェース
 - *time* リース期間
 - 分 (1..21474836)
 - 時間:分
 - *clear* リース期間の要求をしない

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

[ノート] リース期間の要求をしてもその要求が通らない場合がある。その場合、及びリース期間の要求をしない場合には、DHCP サーバから与えられるリース期間を利用する。

[初期値] clear

4.2.4 IP アドレス取得の再送回数と間隔の設定

[書式] **ip lan_if dhcp retry count interval**

[設定値] ◦ *lan_if*

- *lan1* LAN インタフェース
- *lan2* WAN インタフェース

◦ *count*

- 再送回数 (1..100)
- *infinity*..... 無制限

◦ *interval*..... 間隔

- 秒数 (1..100)

[説明] IP アドレスの取得を失敗した場合に、再度取得を試みる回数と、その時間間隔を設定する。

[初期値] *count* = *infinity*

interval = 5

4.2.5 ブロードキャストアドレスの設定

[書式] **ip lan_if broadcast broadcast_address**

[設定値] ◦ *lan_if*

- **lan1** LAN インタフェース
- **lan2** WAN インタフェース

◦ *broadcast_address*

- **0** 0.0.0.0 を用いる
- **1** 255.255.255.255 を用いる
- **2** ネットワークアドレス + オール 0 を用いる
- **3** ネットワークアドレス + オール 1 を用いる

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

[初期値] 1

4.2.6 RIP のフィルタリングの設定

〔書式〕 **ip lan_if rip filter** *direction filter_list*

〔設定値〕 ◦ *lan_if*

- **lan1** LAN インタフェース
- **lan2** WAN インタフェース

◦ *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*

- 空白で区切られた静的フィルタ番号の並び (1..2147483647)
- **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 側へ送出する 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。

〔初期値〕 clear

4.2.7 RIP に関して信用できるゲートウェイの設定

〔書式〕 **ip lan_if rip listen gateway_list**

〔設定値〕 ◦ *lan_if*

- **lan1** LAN インタフェース
- **lan2** WAN インタフェース

◦ *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。

〔初期値〕 none

4.2.8 LAN 側 RIP2 での認証の設定

[書式] **ip lan_if rip auth type type**

[設定値] ◦ *lan_if*

- **lan1** LAN インタフェース
- **lan2** WAN インタフェース

◦ *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 を使用する場合の認証の設定をする。
none の場合は認証なし。
text の場合はテキスト型の認証を行う。

[初期値] none

4.2.9 LAN 側 RIP2 での認証キーの設定

[書式] **ip lan_if rip auth key key**

[設定値] ○lan_if

- lan1 LAN インタフェース
- lan2 WAN インタフェース

○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] LAN 側で RIP2 を使用する場合は認証キーを設定する。
clear の場合は認証なし。
text の場合は 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

4.2.10 Proxy ARP の設定

[書式] **ip lan_if proxyarp proxyarp**

[設定値] ◦ *lan_if*

- **lan1** LAN インタフェース
- **lan2** WAN インタフェース

◦ *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。

[初期値] off

4.2.11 LAN 側でのフィルタリングによるセキュリティの設定

[書式] **ip lan_if secure filter** *direction* [*filter_list...*] [*dynamic filter_list...*]

[設定値] ◦ *lan_if*

- **lan1** LAN インタフェース
- **lan2** WAN インタフェース

◦ *direction*

- **in** LAN 側から入ってくるパケットのフィルタリング
- **out** LAN 側に出ていくパケットのフィルタリング

◦ *filter_list*

- 空白で区切られたフィルタ番号の並び
- **clear** フィルタリングしない

◦ **dynamic** キーワード後に動的フィルタの番号を記述する

[説明] **ip filter** コマンドによるパケットのフィルタを組み合わせ、インタフェースに静的フィルタと動的フィルタを適用し、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場合は破棄になる。

[初期値] clear

4.2.12 LAN インタフェースの MTU の設定

[書式] **ip *lan_if* mtu *mtu***

[設定値] ◦ *lan_if*

- **lan1** LAN インタフェース
- **lan2** WAN インタフェース
- **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。

[初期値] 1500

4.2.13 ネットマスクの設定

[書式] **ip lan_if netmask netmask**

[設定値] ◦ *lan_if*

- **lan1** LAN インタフェース
- **lan2** WAN インタフェース

◦ *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 を解釈して自動設定する

[説明] LAN 側のネットマスクを設定する。

[初期値] class

4.2.14 動的経路情報の設定

[書式] **ip lan_if routing protocol routing-protocol**

[設定値] ◦ *lan_if*

- *lan1* LAN インタフェース
- *lan2* WAN インタフェース

◦ *routing-protocol*

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

[説明] LAN 側の動的経路制御を設定する。

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

[初期値] *none*

4.3 PP 側相手毎の IP の設定

4.3.1 自分の PP 側 IP アドレスの設定

[書式] **ip pp local address** *ip_address* [/netmask]
ip pp local address clear

- [設定値]
- *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 側設定				
		ppp ipcp ipaddress ↓ on		ppp ipcp ipaddress ↓ off		
local 側の PP 側 IPアドレスの解決 ダイヤルアップサーバから IPアドレスを付与される ダイヤルアップ接続端末の立場		ip pp local address ↓ clear	ip pp local address ↓ XXX.XXX.XX X.XXX	ip pp local address ↓ clear	ip pp local address ↓ XXX.XXX.XX X.XXX	
		remote 側設定	ip pp remote address ↓ clear	Unnum- berd	Numberd (XXX.XXX.XX X.XXX)	Unnum- berd
		ip pp remote address ↓ yyy.yyy.y yy.yyy	yyy.yyy.yy y.yyy 端末型接続の IP アドレス 割り当て	Numberd (XXX.XXX.XX X.XXX) または 接続不可	Unnum- berd	Numberd (XXX.XXX.X XX.XXX)

【初期値】 clear

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

4.3.2 相手の PP 側 IP アドレスの設定

[書式] **ip pp remote address** *ip_address*
ip pp remote address clear

[設定値] ◦ *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
- **dhcpc lan**
 - **dhcpc**DHCP クライアントを利用することを示すキーワード
 - **lan_if**DHCP クライアントとして動作する LAN インタフェース
 - **lan1**LAN インタフェース (*lan_if* 省略時)
 - **lan2**WAN インタフェース
- **clear**.....相手の PP 側 IP アドレスを設定しない

[説明] 選択されている相手の PP 側の IP アドレスを設定する。

dhcp を設定した場合は、自分自身が DHCP サーバとして動作している必要がある。自分で管理している DHCP スコープの中から、IP アドレスを割り当てる。

dhcpc を設定した場合は、**lan** パラメータで設定した LAN インタフェースが DHCP クライアントとして IP アドレスを取得し、そのアドレスを pp 側に割り当てる。取得できなかった場合は、0.0.0.0 を割り当てる。

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 側設定			
		ppp ipcp ipaddress		ppp ipcp ipaddress	
		↓ on		↓ off	
remote 側の PP 側 IP アドレスの解決 ダイヤルアップ接続端末に IP アドレスを付与する ダイヤルアップサーバの立場		ip pp local address	ip pp local address	ip pp local address	ip pp local address
		↓ clear	↓ XXX.XXX.XXX. XXX	↓ clear	↓ XXX.XXX.XX X.XXX
local 側設定	ip pp remote address	Unnum- berd	Numberd (XXX.XXX.XXX. XXX)	Unnum- berd	Numberd (XXX.XXX.X XX.XXX)
	↓ clear				
	ip pp remote address	yyy.yyy.yy y.yyy	Numberd (XXX.XXX.XXX. XXX)	Unnum- berd	Numberd (XXX.XXX.X XX.XXX)
	↓ yyy.yyy.y yy.yyy	端末型接続の IP アドレス 割り当て			

【初期値】 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` になることを意味する。

4.3.3 リモート IP アドレスプールの設定

[書式] **ip pp remote address pool ip_address**
ip pp remote address pool clear

[設定値] ◦ *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
- *dhcpc lan_if*
 - *dhcpc* DHCP クライアントを利用することを示すキーワード
 - *lan_if* DHCP クライアントとして動作する LAN インタフェース
 - ◻ *lan1* LAN インタフェース (*lan_if* 省略時)
 - ◻ *lan2* WAN インタフェース
- *clear* プールした IP アドレスをクリアする

[説明] *anonymous* で相手に割り当てるための IP アドレスプールを設定する。
dhcp を設定した場合は、自分自身が DHCP サーバとして動作している必要がある。自分で管理している DHCP スコープの中から、IP アドレスを割り当てる。
dhcpc を設定した場合は、*lan* パラメータで設定した LAN インタフェースが DHCP クライアントとして IP アドレスを取得し、そのアドレスを割り当てる。取得できなかった場合は、0.0.0.0 を割り当てる。
本機では、6 個まで設定及び DHCP クライアントによる取得ができる。
PP として *anonymous* が選択された時のみ有効である。

4.3.4 PP 側のネットマスクの設定

[書式] **ip pp netmask** *netmask*

[設定値] ◦ *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。

[初期値] **class**

4.3.5 PP 側の動的経路制御の設定

[書式] **ip pp routing protocol** *routing_protocol*

[設定値] ◦ *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。

[初期値] none

4.3.6 回線接続時の PP 側の RIP の動作の設定

[書式] **ip pp rip connect send** *rip_action*

[設定値] ◦ *rip_action*

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

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

[初期値] update

4.3.7 回線接続時の PP 側の RIP 送出の時間間隔の設定

[書式] **ip pp rip connect interval** *time*

[設定値] ◦ *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 の場合に有効である。

[初期値] 30

4.3.8 回線切断時の PP 側の RIP の動作の設定

[書式] **ip pp rip disconnect send** *rip_action*

[設定値] ◦ *rip_action*

- none.....回線切断時に RIP を送出不しい
- interval..... **ip pp rip disconnect interval** コマンドで設定された時間間隔で RIP を送出的る
- update.....経路情報が変わった場合にのみ RIP を送出的る

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

[初期値] none

4.3.9 回線切断時の PP 側の RIP 送出的時間間隔の設定

[書式] **ip pp rip disconnect interval** *time*

[設定値] ◦ *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 を送出的る時間間隔を設定する。

ip pp routing protocol コマンドで rip、**ip pp rip disconnect send** コマンドで interval に設定されている場合に有効である。

[初期値] 3600

4.3.10 回線切断時の動的経路制御情報の保持

〔書式〕 **ip pp hold routing** *hold*

〔設定値〕 ◦ *hold*

- on..... 保持する
- off 保持しない

〔説明〕 選択されている相手について回線接続中に変更された動的経路情報を回線切断後も保持するか否かを設定する。

〔初期値〕 off

4.3.11 RIP のフィルタリングの設定

[書式] **ip pp rip filter** *direction filter_list*

[設定値] ◦ *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*

- 空白で区切られた静的フィルタ番号の並び (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 側へ送出する 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。

[初期値] in, out とともに clear

4.3.12 RIP ホップ加算数の設定

[書式] **ip pp rip hop** *direction hop_count*

[設定値] ◦ *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。

[初期値] in, out とも 0

4.3.13 RIP に関して信用できるゲートウェイの設定

[書式] **ip pp rip listen** *listen*

[設定値] ◦ *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。

[初期値] on

4.3.14 PP 側 RIP2 での認証の設定

[書式] **ip pp rip auth type** *type*

[設定値] ◦ *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 を使用する場合の認証の設定をする。
none の場合は認証なし。
text の場合はテキスト型の認証を行う。

[初期値] **none**

4.3.15 PP 側 RIP2 での認証キーの設定

[書式] **ip pp rip auth key** *key*

[設定値] ◦ *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 を使用する場合は認証キーを設定する。
clear の場合は認証なし。
text の場合は **text** の後ろに文字列で入力する。

[初期値] **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

4.3.16 PP 側でのフィルタリングによるセキュリティの設定

[書式] **ip pp secure filter** *direction* [*filter_list...*] [*dynamic filter_list...*]

[設定値] ◦ *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*

- 空白で区切られたフィルタ番号の並び (1..2147483647)
- **clear** フィルタリングしない

◦ **dynamic** キーワード後に動的フィルタの番号を記述する

[説明] **ip filter** コマンドによるパケットのフィルタを組み合わせ、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場合は破棄になる。

[初期値] **clear**

4.3.17 PP インタフェースの MTU の設定

[書式] **ip pp mtu mtu**

[設定値] ◦ *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。

[初期値] 1500

4.3.18 回線切断中に静的経路情報を RIP で広告するか否かの設定

[書式] **ip pp hide static route hide**

[設定値] ◦ hide

- on.....広告する
- off広告しない

[説明] 選択されている相手について、回線切断中に静的経路情報を RIP で広告するか否かを設定する。

[初期値] off

4.4 トンネルインタフェースの設定

4.4.1 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

[書式] **ip tunnel secure filter** *direction filter_list*

[設定値] ◦ *direction*

- **in**..... TUNNEL 側から入ってきたパケットのフィルタリング
- **out**..... TUNNEL 側へ出ていくパケットのフィルタリング

◦ *filter_list*

- 空白で区切られたフィルタ番号の並び (1..2147483647)、100 個以内
- **clear**..... フィルタリングしない

[説明] このコマンドは **ip filter** コマンドと併せて利用する。

設定の際には予め対象となるトンネルインタフェースを **tunnel select** コマンドによって選択しておく必要がある。

[初期値] clear

5. IPv6 の設定

5.1 共通の設定

5.1.1 IPv6 パケットを扱うか否かの設定

[書式] **ipv6 routing route**

[設定値] ◦ *route*

- **on**..... 処理対象として扱う
- **off** 処理対象として扱わない

[説明] IPv6 パケットをルーティングするかどうかを設定する。本スイッチを **on** にしないと PP 側の IPv6 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。

[初期値] on

5.1.2 IPv6 インタフェースのリンク MTU の設定

[書式] **ipv6 interface mtu mtu**

[設定値] ◦ *interface*

- lan1 LAN インタフェース
- lan2 WAN インタフェース
- pp PP インタフェース
- *mtu*..... MTU の値 (1280..1500)

[説明] IPv6 インタフェースのリンク MTU を設定する。

[初期値] 1500

5.2 IPv6 アドレスの管理

5.2.1 インタフェースの IPv6 アドレスの設定

[書式] **ipv6 interface address** *ipv6_address/prefix_len*
ipv6 interface address delete *ipv6_address/prefix_len*

- [設定値] ◦ *interface* インタフェース名 (lan1、lan2、pp、tunnel)
◦ *ipv6_address* ... IPv6 アドレス
◦ *prefix_len* プレフィックス長

[説明] インタフェースに IPv6 アドレスを付与する。

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

5.2.2 インタフェースの IPv6 アドレスの設定

[書式] **ipv6 interface prefix** *ipv6_address/prefix_len*
ipv6 interface prefix delete *ipv6_address/prefix_len*

[設定値] ◦ *interface* インタフェース名 (lan1、lan2、pp、tunnel)
◦ *ipv6_address* ... IPv6 アドレス
◦ *prefix_len* プレフィックス長

[説明] インタフェースに IPv6 プレフィックスを付与する。

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

5.3 近隣探索

5.3.1 ルータ広告で配布するプレフィックスの定義

[書式] **ipv6 prefix** *prefix_id prefix/prefix_len* [valid_lifetime=*time*]
[preferred_lifetime=*time*] [l_flag=*switch*] [a_flag=*switch*]
ipv6 prefix *prefix_id* clear

- [設定値]
- *prefix_id* プレフィックス番号
 - *prefix* プレフィックス
 - *prefix_len* プレフィックス長
 - *valid_lifetime* プレフィックスの有効寿命 (60..15552000)
 - *preferred_lifetime* プレフィックスの推奨寿命 (60..15552000)
 - *time* 時間設定
 - **YYYY-MM-DD,bb:mm[:ss]**
 - **YYYY** 年 (1980..2079)
 - **MM** 月 (01..12)
 - **DD** 日 (01..31)
 - **bb** 時 (00..23)
 - **mm** 分 (00..59)
 - **ss** 秒 (00..59、省略時は 00)
 - *l_flag* on-link フラグ

- **a_flag**..... autonomous address configuration フラグ
- **switch**
 - on
 - off

[説明] ルータ広告で配布するプレフィックスを定義する。実際に広告するためには、**ipv6 interface rtadv prefix** コマンドの設定が必要である。

time では寿命を秒数または寿命が尽きる時刻のいずれかを設定できる。**time** として数値 (60 以上 15552000 以下) を設定すると、その秒数を寿命として広告する。**time** として時刻を設定すると、その時刻に寿命が尽きるものとして寿命を計算し、広告する。時刻を設定する場合は、上記のフォーマットに従う。最終有効期間とはアドレスが無効になるまでの時間であり、推奨有効期間とはアドレスを新たな接続での使用が不可となる時間である。また、on-link フラグはプレフィックスがそのデータリンクに固有である時に **on** とする。autonomous address configuration フラグはプレフィックスを自律アドレス設定で使うことができる場合に **on** とする。

[ノート] リンクローカルのプレフィックスを設定することはできない。

[初期値] **valid_lifetime = 2592000**
preferred_lifetime = 604800
l_frag = on
a_flag = on

5.3.2 ルータ広告の送信の制御

[書式] **ipv6 interface rtadv send** *prefix_id* [*prefix_id...*] [*m_flag=switch*]
[*o_flag=switch*]
ipv6 interface rtadv send off

- [設定値]
- *interface* インタフェース (lan1、lan2、pp)
 - *prefix_id* プレフィックス番号
 - *m_flag* managed address configuration フラグ
 - *o_flag* other stateful configuration フラグ
 - *switch*
 - on
 - off

[説明] インタフェースごとにルータ広告の送信を制御する。送信されるプレフィックスとして、**ipv6 prefix** コマンドで設定されたものが用いられる。managed address configuration フラグを **off** とすることで、ネットワークに接続されているホストのステートレス自動設定が許され、ホスト自身でアドレス設定がなされる。また other stateful configuration フラグを **off** とすることで、ホストはオプションとして格納されているプレフィックスリストを調べることになる。

[初期値] *m_flag* = off
o_flag = off

5.4 IPv6 の経路情報の追加

[書式] **ipv6 route** *network gateway gateway* [*parameter*] [*gateway gateway* [*parameter*]]

ipv6 route delete *network*

[設定値] ◦network

- IP アドレスIPv6 アドレス / プレフィックス長
- **default** デフォルト経路

◦*gateway*ゲートウェイ

- IP アドレス % スコープ識別子
- **pp peer_num** [*dldci=dldci*].. PP インタフェースへの経路
 "*dldci=dldci*" が指定された場合は、フレームリレーの DLCI への経路

▪*peer_num*

- 相手先情報番号 (1..30)
- anonymous**

• **pp anonymous name=name**

▪*name* PAP/CHAP による名前

• **tunnel tunnel_num ...** Tunnel インタフェースへの経路

• **filter_num** フィルタ番号 (1..100)

◦*parameter*.....以下のパラメータを空白で区切り複数設定可能

• **filter number** [*number*..]..... フィルタ型経路の指定

▪*number* フィルタの番号 (1..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] IPv6 の経路情報を追加する。LAN インタフェースが複数ある機種ではスコープ識別子でインタフェースを指定する必要がある。インタフェースに対応するスコープ識別子は **show ipv6 address** コマンドで表示される。LAN インタフェースがひとつである機種に関しては、スコープ識別子が省略されると LAN1 が指定されたものとして扱う。

5.5 RIPng の設定

[書式] **ipv6 rip use use**

[設定値] ◦ *use*

- *on*RIPng を使う
- *off*RIPng を使わない

[説明] RIPng を使うかどうかを設定する。

[初期値] *off*

5.5.1 インタフェースにおける RIPng の送信ポリシーの設定

[書式] **ipv6 interface rip send switch**

- [設定値] ◦ *interface* インタフェース名 (lan1、lan2、pp、tunnel)
◦ *switch*
- **on**..... RIPng を送信する
 - **off** RIPng を送信しない

[説明] RIPng の送信ポリシーを設定する。

[初期値] off

5.5.2 インタフェースにおける RIPng の受信ポリシーの設定

[書式] **ipv6 interface rip receive switch**

- [設定値] ◦ *interface* インタフェース名 (lan1、lan2、pp、tunnel)
◦ *switch*
- **on**..... 受信した RIPng パケットを処理する
 - **off** 受信した RIPng パケットを無視する

[説明] RIPng の受信ポリシーを設定する。

[初期値] on

5.5.3 インタフェースにおける信頼できる RIPng ゲートウェイの設定

[書式] **ipv6 interface rip trust gateway** [except] *gateway* [*gateway* ...]

- [設定値] ◦ *interface* インタフェース名 (lan1、lan2、pp)
◦ *gateway* IPv6 アドレス

[説明] 信頼できる RIPng ゲートウェイを設定する。

except キーワードを指定していない場合には、列挙したゲートウェイを信用できるゲートウェイとし、それらからの RIP だけを受信する。

except キーワードを指定した場合は、列挙したゲートウェイを信用できないゲートウェイとし、それらを除いた他のゲートウェイからの RIP だけを受信する。

5.5.4 RIPng の加算ホップ数の設定

[書式] **ipv6 pp rip hop** *direction hop*

[設定値] ◦ *direction*

- **in**.....受信時に加算する
- **out**.....送信時に加算する
- *hop*加算ホップ数 (0..15)

[説明] PP インタフェースで送受信する RIPng のメトリックに対して加算するホップ数を設定する。

[初期値] 0

5.5.5 RIPng で送受信する経路に対するフィルタリングの設定

[書式] **ipv6 interface rip filter** *direction filter_list* [*filter_list...*]

- [設定値] ◦ *interface* インタフェース名 (lan1、lan2、pp、tunnel)
- *direction*
- **in** 内向きのパケットを対象にする
 - **out** 外向きのパケットを対象にする
- *filter_list* フィルタ番号の並び

[説明] PP インタフェースで送受信する RIPng パケットに対して適用するフィルタを設定する。

[初期値] clear

5.5.6 回線接続時の PP 側の RIPng の動作の設定

[書式] **ipv6 pp rip connect send** *action*

- [設定値] ◦ *action*
- **interval** 一定の間隔で RIPng を送信する
 - **update** 経路情報が変化したときのみ RIPng を送信する

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

[初期値] update

5.5.7 回線接続時の PP 側の RIPng 送出の時間間隔の設定

[書式] **ipv6 pp rip connect interval time**

[設定値] ◦ *time* 送出間隔 [秒] (30..21474836)

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

[初期値] 30

5.5.8 回線切断時の PP 側の RIPng の動作の設定

[書式] **ipv6 pp rip disconnect send action**

[設定値] ◦ *action*

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

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

[初期値] none

5.5.9 回線切断時の PP 側の RIPng 送出手間間隔の設定

[書式] **ipv6 pp rip disconnect interval** *time*

[設定値] ◦ *time*送出間隔 [秒] (30..21474836)

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

[初期値] 3600

5.5.10 RIPng による経路を回線切断時に保持するか否かの設定

[書式] **ipv6 pp rip hold routing** *bold*

[設定値] ◦ *bold*

- *on* 保持する
- *off* 保持しない

[説明] PP インタフェースから RIPng で得られた経路を、回線が切断されたときに保持するか否かを設定する。

[初期値] *off*

5.6 フィルタの設定

5.6.1 IPv6 フィルタの定義

[書式] **ipv6 filter** *filter_num* *pass_reject* *src_address*[/*prefix_len*] [*dst_address*[/*prefix_len*]
[*protocol* [*src_port_list* [*dst_port_list*]]]

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

[説明] IPv6 のフィルタを定義する。

5.6.2 IPv6 フィルタの削除

[書式] **ipv6 filter delete** *filter_num*

[設定値] ◦ *filter_num*..... フィルタ番号 (1..100)

[説明] IPv6 のフィルタを削除する。

5.6.3 IPv6 フィルタの適用

[書式] **ipv6 interface secure filter** *direction filter_list* [*filter_list...*]

[設定値] ◦ *interface* インタフェース名 (lan1、lan2、pp、tunnel)

◦ *direction*..... 方向

• **in**..... 内向きのパケットを対象にする

• **out**..... 外向きのパケットを対象にする

◦ *filter_list* 静的フィルタ番号の並び

[説明] IPv6 フィルタをインタフェースに適用する。

5.6.4 IPv6 動的フィルタの定義

[書式] **ipv6 filter dynamic** *dyn_filter_num srcaddr dstaddr protocol* [*option ...*]
ipv6 filter dynamic *dyn_filter_num srcaddr dstaddr filter filter_list* [*in filter_list*] [*out filter_list*] [*option ...*]

- [設定値]
- *dyn_filter_num*.....動的フィルタ番号 (1..2147483647)
 - *srcaddr*.....始点 IPv6 アドレス
 - *dstaddr*.....終点 IPv6 アドレス
 - *protocol*プロトコル
 - tcp
 - udp
 - ftp
 - tftp
 - domain
 - www
 - smtp
 - pop3
 - telnet
 - *filter_list* **ipv6 filter** コマンドで登録されたフィルタ番号のリスト
 - *option*
 - *syslog=switch*
 - **on** コネクションの通信履歴を syslog に残す

- **off** コネクションの通信履歴を syslog に残さない
- **timeout=time**
 - **time** データが流れなくなったときにコネクション情報を解放するまでの時間 (秒)

[説明] IPv6 の動的フィルタを定義する。1 つ目の書式では、あらかじめルータに登録されているアプリケーション名を指定する。2 つ目の書式では、ユーザがアクセス制御のルールを記述する。キーワードの **filter**、**in**、**out** の後には、**ipv6 filter** コマンドで定義されたフィルタ番号を設定する。

filter キーワードの後に記述されたフィルタに該当するコネクション (トリガ) を検出したら、それ以降 **in** キーワードと **out** キーワードの後に記述されたフィルタに該当するコネクションを通過させる。**in** キーワードはトリガの方向に対して逆方向のアクセスを制御し、**out** キーワードは動的フィルタと同じ方向のアクセスを制御する。なお、**ipv6 filter** コマンドの IP アドレスは無視される。**pass/reject** の引数も同様に無視される。ここに記載されていないアプリケーションについては、**filter** キーワードを使って定義することで扱える可能性がある。特に snmp のように動的にポート番号が変化しないプロトコルに扱いは容易である。

tcp か **udp** を設定することで扱える可能性がある。特に、telnet のように動的にポート番号が変化しないプロトコルは **tcp** を指定することで扱うことができる。

[初期値] **syslog = on**
timeout = 60

5.6.5 IPv6 動的フィルタの削除

[書式] **ipv6 filter dynamic delete** *dyn_filter_num*

[設定値] ◦ *dyn_filter_num*.....動的フィルタ番号

[説明] id で指定された動的フィルタの定義を削除する。

5.6.6 IPv6 動的フィルタのコネクション管理情報の削除

[書式] **disconnect ipv6 connection** *session_id* [*channel_id*]

[設定値] ◦ *session_id*セッションの識別子

◦ *channel_id*チャネルの識別子

[説明] 指定したセッションに属する特定のチャネルを削除する。チャネルを指定しないときには、そのセッションに属するすべてのチャネルを削除する。

5.7 トンネリング

5.7.1 トンネルインタフェース端点の IP アドレスの設定

[書式] **tunnel endpoint address** [*local*] *remote*
tunnel endpoint address clear

- [設定値] ◦ *local*自分側のトンネルインタフェース端点の IP アドレス
◦ *remote*相手側のトンネルインタフェース端点の IP アドレス

[説明] トンネルインタフェース端点の IP アドレスを設定する。IP アドレスは IPv4/IPv6 いずれのアドレスも設定できるが、*local* パラメータと *remote* パラメータの IPv4/IPv6 の種別を揃える必要がある。トンネルインタフェース端点として IPv4 アドレスを設定した場合には、IPv4 over IPv4 トンネルと IPv6 over IPv4 トンネルが、IPv6 アドレスを設定した場合には IPv4 over IPv6 トンネルと IPv6 over IPv4 トンネルが利用できる。

local パラメータを省略した場合は、適当なインタフェースの IP アドレスが利用される。

5.7.2 トンネルインタフェースの使用許可の設定

[書式] **tunnel enable** *tunnel_num*

[設定値] ◦ *tunnel_num*

- トンネルインタフェース番号 (1..4)
- all すべてのトンネルインタフェース

[説明] トンネルインタフェースを使用できる状態にする。
工場出荷時は、すべてのトンネルインタフェースは disable 状態であり、使用する場合は本コマンドにより、インタフェースを有効にしなければならない。

5.7.3 トンネルインタフェースの使用不許可の設定

[書式] **tunnel disable** *tunnel_num*

[設定値] ◦ *tunnel_num*

- トンネルインタフェース番号 (1..4)
- all すべてのトンネルインタフェース

[説明] トンネルインタフェースを使用できない状態にする。
トンネル先の設定を行う場合は、disable 状態で行うのが望ましい。

5.8 管理ツール

5.8.1 ping の実行

[書式] **ping6** *destination* [*count*]
ping6 *destination scope_id* [*count*]
ping6 *destination interface* [*count*]
ping6 *destination pp peer_num* [*count*]

- [設定値]
- *destination*送信する宛先の IPv6 アドレス
 - *scope_id*スコープ ID
 - *interface*LAN インタフェース
 - *peer_num*相手先情報番号 (1..30)
 - *count*送信回数 (1..21474836)

[説明] 指定した宛先に対して ICMPv6 Echo Request を送信する。
スコープ ID は、**show ipv6 address** コマンドで表示できる。

5.8.2 traceroute の実行

[書式] **traceroute6** *destination*

[設定値] ◦ *destination*送信する宛先の IPv6 アドレス

[説明] 指定した宛先までの経路を調べて表示する。

6. PPP の設定

6.1 相手の名前とパスワードの設定

[書式] **pp auth username** *username password*

- [設定値] ◦ *username*.....名前 (64 文字以内)
◦ *password*.....パスワード (64 文字以内)

[説明] 相手の名前とパスワードを設定する。複数設定可。

6.2 相手の名前の削除

[書式] **pp auth delete username** *username*

- [設定値] ◦ *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。

6.3 要求する認証タイプの設定

[書式] **pp auth request *auth*** [arrive-only]

[設定値] ◦ *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
- mschap.....CHAPによる認証 (MS 方式) を要求する
- mschap-v2.....CHAPによる認証 (MS 方式 Version2) 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 の選択が失敗した場合に適用される。**chap-pap** キーワードの場合には、最初 CHAP を要求し、それが相手から拒否された場合には改めて PAP を要求するよう動作する。これにより、相手が PAP または CHAP の片方しかサポートしていない場合でも容易に接続できるようになる。**arrive-only** キーワードが指定された場合には、着信時にのみ PPP による認証を要求するようになり、発信時には要求しない。PP 毎のコマンドである。

[初期値] none

6.4 受け入れる認証タイプの設定

[書式] **pp auth accept** *accept*

[設定値] ◦ *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
- **mschap** CHAP による認証 (MS 方式) を受け入れる
- **mschap-v2**..... CHAP による認証 (MS 方式 Version2) を受け入れる
- **pap chap** PAP と CHAP のいずれによる認証も受け入れる
- **chap pap** PAP と CHAP のいずれによる認証も受け入れる

[説明] 相手からの PPP 認証要求を受け入れるかどうかを設定する。発信時には常に適用される。
anonymous でない着信の場合には発番号により PP が選択されてから適用される。
anonymous での着信時には、発番号による PP の選択が失敗した場合に適用される。PP 毎のコマンドである。

[初期値] none

6.5 自分の名前とパスワードの設定

〔書式〕 **pp auth myname** *myname password*

- 〔設定値〕 ◦ *myname*.....名前 (64 文字以内)
◦ *password*.....パスワード (64 文字以内)

〔説明〕 PAP、CHAP、MSCHAP、MSCHAP-Version2 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。

6.6 自分の名前の消去

〔書式〕 **pp auth clear myname**

〔設定値〕 なし

〔説明〕 自分の名前とパスワードを消去する。

6.7 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

[書式] **pp auth multi connect prohibit** *prohibit*

[設定値] ◦*prohibit*

- on.....禁止する
- off禁止しない

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

[ノート] 定額制プロバイダを営む場合に便利。
anonymous が選択された場合のみ有効である。

[初期値] off

6.8 LCP 関連の設定

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

[書式] **ppp lcp acfc** *acfc*

[設定値] ◦ *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場合は用いない。また、このオプションを相手から要求された場合には、本コマンドの設定に関わらず常にアクセプトする。

[初期値] **off**

6.8.2 Magic Number オプション使用の設定

[書式] **ppp lcp magicnumber** *magic_num*

[設定値] ◦ *magic_num*

- **on**.....用いる
- **off**用いない

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

[ノート] **on** を設定していても相手に拒否された場合は用いない。

[初期値] **on**

6.8.3 Maximum Receive Unit オプション使用の設定

[書式] **ppp lcp mru mru** [*length*]

[設定値] ◦ *mru*

- **on**.....用いる
- **off**用いない

◦ *length*MRU の値 (1280..1792)

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

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

[初期値] *mru* = on
length = 1792

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

[書式] **ppp lcp pfc** *pfc*

[設定値] ◦*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** に設定していても相手に拒否された場合は用いない。また、このオプションを相手から要求された場合には、本コマンドの設定にかかわらず常に受け付ける。

[初期値] **off**

6.8.5 パラメータ lcp-restart の設定

[書式] **ppp lcp restart time**

[設定値] ◦ *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。

[初期値] 3000

6.8.6 パラメータ lcp-max-terminate の設定

[書式] **ppp lcp maxterminate count**

[設定値] ◦ *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。

[初期値] 2

6.8.7 パラメータ lcp-max-configure の設定

[書式] **ppp lcp maxconfigure** *count*

[設定値] ◦ *count*回数 (1..10)

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

[初期値] 10

6.8.8 パラメータ lcp-max-failure の設定

[書式] **ppp lcp maxfailure** *count*

[設定値] ◦ *count*回数 (1..10)

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

[初期値] 10

6.9 PAP 関連の設定

6.9.1 パラメータ pap-restart の設定

[書式] **ppp pap restart** *time*

[設定値] ◦ *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。

[初期値] 3000

6.9.2 パラメータ pap-max-authreq の設定

[書式] **ppp pap maxauthreq** *count*

[設定値] ◦ *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。

[初期値] 10

6.10 CHAP 関連の設定

6.10.1 パラメータ chap-restart の設定

[書式] **ppp chap restart** *time*

[設定値] ◦ *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。

[初期値] 3000

6.10.2 パラメータ chap-max-challenge の設定

[書式] **ppp chap maxchallenge** *count*

[設定値] ◦ *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。

[初期値] 10

6.11 IPCP 関連の設定

6.11.1 Van Jacobson Compressed TCP/IP 使用の設定

[書式] **ppp ipcp vjc comp**

[設定値] ◦ *comp*

- **on**.....使用する
- **off**使用しない

[説明] 選択されている相手について [PPP,IPCP] Van Jacobson Compressed TCP/IP を使用するか否かを設定する。

[ノート] **on** を設定していても相手に拒否された場合は用いない。

[初期値] **off**

6.11.2 PP 側 IP アドレスのネゴシエーションの設定

[書式] **ppp ipcp ipaddress negotiation**

[設定値] ◦ *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] 4.3.1 自分の PP 側 IP アドレスの設定、4.3.2 相手の PP 側 IP アドレスの設定を参照。

[初期値] off

6.11.3 パラメータ ipcp-restart の設定

[書式] **ppp ipcp restart time**

[設定値] ◦ *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。

[初期値] 3000

6.11.4 パラメータ ipcp-max-terminate の設定

[書式] **ppp ipcp maxterminate** *count*

[設定値] ◦ *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。

[初期値] 2

6.11.5 パラメータ ipcp-max-configure の設定

[書式] **ppp ipcp maxconfigure** *count*

[設定値] ◦ *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。

[初期値] 10

6.11.6 パラメータ ipcp-max-failure の設定

[書式] **ppp ipcp maxfailure count**

[設定値] ◦ *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。

[初期値] 10

6.11.7 IPCP の MS 拡張オプションを使うか否かの設定

[書式] **ppp ipcp msex** *msex*

[設定値] ◦ *msex*

- **on**.....使用する
- **off**使用しない

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

[初期値] off

6.11.8 PPP で IPv6 を流せるようにするか否かの設定

[書式] **ppp ipv6cp use use**

[設定値] ◦ *use*

- **on**.....IPV6CP を利用し PPP で IPv6 を流す
- **off**IPV6CP を利用せず、PPP で IPv6 を流さない

[説明] IPV6CP の利用の有無を設定する。

[初期値] on

6.11.9 WINS サーバの IP アドレスの設定

[書式] **wins server** *server* [*server*]
wins server clear

- [設定値] ◦ *server*.....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。

[初期値] clear

6.12 MSCBCP 関連の設定

6.12.1 パラメータ `mscbcpr-restart` の設定

[書式] **ppp mscbcpr restart** *time*

[設定値] ◦ *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。

[初期値] 1000

6.12.2 パラメータ `mscbcpr-maxretry` の設定

[書式] **ppp mscbcpr maxretry** *count*

[設定値] ◦ *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。

[初期値] 30

6.13 CCP 関連の設定

6.13.1 全パケットの圧縮・暗号化のタイプの設定

[書式] **ppp ccp type type**

[設定値] ◦ *type*

- **mppe-40** 40bit MPPE で暗号化する
- **mppe-128** 128bit MPPE で暗号化する
- **mppe-any** 40bit, 128bit MPPE いずれかの暗号化を行う
- **none** 圧縮・暗号化しない

[説明] 選択されている相手について [PPP,CCP] 圧縮方式または暗号方式を選択する。
Van Jacobson Compressed TCP/IP との併用も可能である。

[ノート] **mppe-40**, **mppe-128**, **mppe-any** の場合には 1 パケット毎に鍵交換される。
MPPE は Microsoft Point-To-Point Encryption (Protocol) の略。

[初期値] none

6.13.2 パラメータ ccp-restart の設定

[書式] **ppp ccp restart time**

[設定値] ◦ *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。

[初期値] 3000

6.13.3 パラメータ ccp-max-terminate の設定

[書式] **ppp ccp maxterminate count**

[設定値] ◦ *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。

[初期値] 2

6.13.4 パラメータ ccp-max-configure の設定

[書式] **ppp ccp maxconfigure** *count*

[設定値] ◦ *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。

[初期値] 10

6.13.5 パラメータ ccp-max-failure の設定

[書式] **ppp ccp maxfailure** *count*

[設定値] ◦ *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。

[初期値] 10

7. PPPoE の設定

7.1 PPPoE で使用する LAN インタフェースの設定

[書式] **pppoe use** *lan_if*
pppoe use off

[設定値] ◦ *lan_if*

- **lan1** LAN インタフェース
- **lan2** WAN インタフェース
- **off**..... 設定しない

[説明] 選択されている相手に対して、PPPoE で使用する LAN インタフェースを設定する。設定がない場合は、PPPoE は使われない。

[初期値] off

7.2 アクセスコンセントレータ名の設定

[書式] **pppoe access concentrator name**

[設定値] ◦ *name*アクセスコンセントレータの名前を表す文字列 (7bit US-ASCII、255 文字以内)

[説明] 選択されている相手について PPPoE で接続するアクセスコンセントレータの名前を設定する。接続できるアクセスコンセントレータが複数ある場合に、どのアクセスコンセントレータに接続するのかを設定するために使用する。

7.3 セッションの自動接続の設定

[書式] **pppoe auto connect switch**

[設定値] ◦ *switch*

- **on**.....自動接続する
- **off**自動接続しない

[説明] 選択されている相手に対して、PPPoE のセッションを自動で接続するか否かを設定する。

[初期値] on

7.4 セッションの自動切断の設定

〔書式〕 **pppoe auto disconnect** *switch*

〔設定値〕 ◦ *switch*

- on.....自動切断する
- off自動切断しない

〔説明〕 選択されている相手に対して、PPPoE のセッションを自動で切断するか否かを設定する。

〔初期値〕 on

7.5 PADI パケットの最大再送回数の設定

〔書式〕 **pppoe padi maxretry** *times*

〔設定値〕 ◦ *times*回数 (1..10)

〔説明〕 PPPoE プロトコルにおける PADI パケットの最大再送回数を設定する。

〔初期値〕 5

7.6 PADI パケットの再送時間の設定

[書式] **pppoe padi restart time**

[設定値] ◦ *time*ミリ秒 (20..10000)

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

[初期値] 3000

7.7 PADR パケットの最大再送回数の設定

[書式] **pppoe padr maxretry times**

[設定値] ◦ *times*回数 (1..10)

[説明] PPPoE プロトコルにおける PADR パケットの最大再送回数を設定する。

[初期値] 5

7.8 PADR パケットの再送時間の設定

[書式] **pppoe padr restart time**

[設定値] ◦ *time*ミリ秒 (20..10000)

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

[初期値] 3000

7.9 PPPoE セッションの切断タイマの設定

[書式] **pppoe disconnect time time**

[設定値] ◦ *time*

- 秒数 (1..21474836)
- offタイマを設定しない

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

[初期値] off

7.10 TCP パケットの MSS の制限の有無とサイズの設定

[書式] **pppoe tcp mss limit** *length*

[設定値] ◦ *length*

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

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

[初期値] auto

7.11 サービス名の指定

[書式] **pppoe service-name** *name*

[設定値] ◦ *name*サービス名を表す文字列 (7bit US-ASCII、255 文字以内)

[説明] 選択されている相手について PPPoE で要求するサービス名を設定する。
接続できるアクセスコンセントレータが複数ある場合に、要求するサービスを提供することが可能なアクセスコンセントレータを選択して接続するために使用する。

[初期値] 指定なし

8. DHCP の設定

本機は DHCP¹ 機能として、DHCP サーバ機能、DHCP リレーエージェント機能、および DHCP クライアント機能を実装しています。DHCP クライアント機能は Windows 95, 98 や Windows NT 等で実装されており、これらと本機の DHCP サーバ機能、DHCP リレーエージェント機能を組み合わせることにより DHCP クライアントの基本的なネットワーク環境の自動設定を実現します。

ルータが DHCP サーバとして機能するか DHCP リレーエージェントとして機能するか、どちらとしても機能させないかは **dhcp service** コマンドにより設定します。現在どのようになっているかは **show dhcp** コマンドにより知ることができます。

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

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

IP アドレスの範囲は複数の設定が可能であり、それぞれの範囲を DHCP スコープ番号で管理します。DHCP クライアントからの設定要求があると DHCP サーバは DHCP スコープの中で未割り当ての IP アドレスを自動的に通知します。なお、特定の DHCP クライアントに特定の IP アドレスを固定的にリースする場合には、**dhcp scope** コマンドで定義したスコープ番号を用いて **dhcp scope bind** コマンドで予約します。予約の解除は **dhcp scope unbind** コマンドで行います。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

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

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。

ルータを DHCP クライアントとして機能させるかどうかは、**ip lan_if address**、**ip lan_if secondary address**、**ip pp remote address**、**ip pp remote address pool** の各コマンドの設定値により決定されます。設定されている内容は、**show dhcpc status** コマンドにより知ることができます。

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。

DHCP クライアント機能は、DHCP サーバから配布される設定情報から適切にサーバを選択し、そのサーバが配布する設定情報を利用して自動設定する機能を持ちます。

8.1 DHCP の動作の設定

[書式] **dhcp service** *type*

[設定値] ◦ *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。

[初期値] **server**

8.2 RFC2131 対応動作設定

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

[設定値] ◦ *comp*

- **on**.....RFC2131 準拠
- **off**RFC1541 準拠

◦ **except**指定した機能以外が RFC2131 対応となるキーワード

◦ *function*

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

[説明] DHCP サーバの動作を指定する。on の場合には RFC2131 準拠となる。off の場合には、RFC1541 準拠の動作となる。
また RFC1541 をベースとして RFC2131 記述の個別機能のみを対応させる場合には以下のパラメータで指定する。これらのパラメータはスペースで区切り複数指定できる。except キーワードを指定すると、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 を受信した場合に、そのクライアントのリース情報を持っていない場合には DHCPNAK を送らないようにする。
- **reply-ack**.....クライアントから、リース期間などで許容できないオプション値（リクエスト IP アドレスは除く）を要求された場合でも、DHCPNAK を返さずに許容値を格納した DHCPACK を返す。
- **use-clientid**クライアントの識別に chaddr フィールドより Client-Identifier オプションを優先して使用する。

[初期値] except remain-silent

8.3 DHCP スコープの定義の設定

[書式] **dhcp scope** *scope_num ip_address-ip_address/netmask* [except *ex_ip* ...] [gateway *gw_ip*]
[expire *time*] [maxexpire *time*]

- [設定値]
- *scope_num*スコープ番号 (1..65535)
 - *ip_address-ip_address* 対象となるサブネットで割り当てる IP アドレスの範囲
 - *netmask* 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。

〔初期値〕 `expire time = 72:00`
`maxexpire time = 72:00`

8.4 DHCP スコープの削除

〔書式〕 **dhcp delete scope** *scope_num*

〔設定値〕 ◦ *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。

8.5 DHCP 予約アドレスの設定

[書式] **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*

- [設定値]
- *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* 省略時 2 桁 16 進数の列で先頭は **type** フィールド
 - *mac_address*..... xx:xx:xx:xx:xx:xx (xxは 16 進数) 予約 DHCP クライアントの MAC アドレス
 - *ipcp*..... IPCP でリモート側に与えることを示す

[説明] IP アドレスをリースする DHCP クライアントを固定的に設定する。

[ノート] IP アドレスは、*scope_num* パラメータで指定された DHCP スコープ範囲内でなければならない。1 つの DHCP スコープ内では、1 つの MAC アドレスに複数の IP アドレスを設定することはできない。他の DHCP クライアントにリース中の IP アドレスを予約設定した場

合、リース終了後にその IP アドレスの割り当てが行われる。

dhcp scope コマンド、あるいは **dhcp delete scope** コマンドを実行した場合、関連する予約はすべて消去される。

ipcp の指定は、同時に接続できる B チャネルの数に限られる。また、ipcp で与えるアドレスや擬似 LAN に与えるアドレスは、LAN 側のスコープから選択される。

コマンドの第 1 の書式を使う場合は、あらかじめ **dhcp server rfc2131 compliant on** あるいは **use-clientid** 機能を使用するよう設定されていなければならない。また **dhcp server rfc2131 compliant off** あるいは **use-clientid** 機能が使用されないよう設定された時点で、コマンドの第 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、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-Identifer オプションで送られる値で予約し直す必要がある。

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

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

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

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

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

すなわち、リースしているクライアントとして MAC アドレスが表示されていれば Client-Identifier オプションは使用されておらず、16 進文字列あるいは文字列でクライアントが表

示されていれば、Client-Identifier オプションが使われている。この場合、Client-Identifier オプションを使うクライアントへの予約は、ここで表示される 16 進文字列あるいは文字列を使用する。

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

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

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

なお、クライアントとの相互動作に関して下記の留意点がある。

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

8.6 DHCP 予約アドレスの解除

[書式] **dhcp scope unbind** *scope_num ip_address*

- [設定値]
- *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。

8.7 重複チェック動作の設定

[書式] **dhcp server duplicate check** *chk1 chk2*

[設定値] ◦ *chk1*

- 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

◦ *chk2*

- 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。

[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。

[初期値] *chk1* = on
chk2 = on

8.8 DHCP サーバの指定の設定

[書式] **dhcp relay server** *host* [*host...*]

[設定値] ◦ *host*.....DHCP サーバの IP アドレス

[説明] DHCP BOOTREQUEST パケットを中継するサーバを最大 4 つまで設定する。
サーバが複数指定された場合は、BOOTREQUEST パケットを複製してすべてのサーバに中継するか、あるいは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。

8.9 DHCP サーバの選択方法の設定

[書式] **dhcp relay select** *type*

[設定値] ◦ *type*

- **hash**..... Hash 関数を利用して一つだけサーバを選択する
- **all** すべてのサーバを選択する

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

[初期値] **hash**

8.10 DHCP BOOTREQUEST パケットの中継基準の設定

[書式] **dhcp relay threshold** *time*

[設定値] ◦ *time*.....秒数 (0..65535)

[説明] DHCP BOOTREQUEST パケットの secs フィールドと本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。

[初期値] 0

8.11 DHCP クライアントの設定

8.11.1 Client-identifier Option の設定

[書式] **dhcp client client-identifier lan_if primary** [type type] id
dhcp client client-identifier lan_if secondary [type type] id
dhcp client client-identifier pp peer_num [type type] id
dhcp client client-identifier pool pool_num [type type] id

dhcp client client-identifier lan_if primary clear
dhcp client client-identifier lan_if secondary clear
dhcp client client-identifier pp peer_num clear
dhcp client client-identifier pool pool_num clear

- [設定値]
- *lan_if*
 - lan1 LAN インタフェース
 - lan2 WAN インタフェース
 - *type* Client-identifier Option の type フィールドの値を入力することを示すキーワード
 - *type* Client-identifier Option の type フィールドの値 (0..255)
 - *id*
 - 'text' ASCII 文字列で表した ID
 - 2 桁の 16 進数列で表した ID

- *peer_num*
 - 相手先情報番号 (1..30)
 - *anonymous*
- *pool_num* **ip pp remote address pool dhcpc** コマンドで取得するアドレスの番号 (1..2)
1 または 2 を指定することで、それぞれの Client-identifier Option に任意の ID を付けることが可能
- **clear**..... 設定した ID のクリア

[説明] Client-identifier Option の type フィールドの値と ID を設定する。

[初期値] *type* = 1

[設定例] # dhcp client client-identifier lan1 primary 00 a0 de 11 22 33 44 55
dhcp client client-identifier lan1 primary text yamaha
dhcp client client-identifier lan1 primary type 0 00 a0 de 11 22 33
dhcp client client-identifier lan1 primary type 0 text hamamatsu

8.11.2 Client-identifier Option の type フィールドの値の設定

[書式] **dhcp client client-identifier type** *type*

[設定値] ◦ *type*.....Client-identifier Option の type フィールドの値 (0..255)

[説明] Client-identifier Option の type フィールドの値を設定する。

[ノート] Client-identifier Option の ID はルータによって自動的に設定される。

[初期値] 1

8.11.3 DHCP クライアントのホスト名の設定

[書式] **dhcp client hostname *lan_if* primary *hostname***
dhcp client hostname *lan_if* secondary *hostname*
dhcp client hostname *pp* *peer_num* *hostname*
dhcp client hostname *pool* *pool_num* *hostname*

- [設定値]
- *lan_if*
 - *lan1* LAN インタフェース
 - *lan2* WAN インタフェース
 - *peer_num*
 - 相手先情報番号 (1..30)
 - *anonymous*
 - *pool_num* **ip pp remote address pool dhcpc** コマンドで取得するアドレスの番号 (1..2)1 または 2 を指定することで、それぞれ *hostname* に異なる名前を付けることが可能
 - *hostname* DHCP クライアントのホスト名

[説明] DHCP クライアントのホスト名を設定する。
空文字列を設定する場合には、**dhcp client hostname lan primary** のように *hostname* の手前まで入力する。

[初期値] 空文字列

9. ICMP の設定

9.1 IPv4 の設定

9.1.1 ICMP Echo Reply を送信するか否かの設定

[書式] **ip icmp echo-reply send** *send*

[設定値] ◦ *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。

[初期値] on

9.1.2 ICMP Mask Reply を送信するか否かの設定

[書式] **ip icmp mask-reply send** *send*

[設定値] ◦ *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。

[初期値] on

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

[書式] **ip icmp parameter-problem send** *send*

[設定値] ◦ *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。

[初期値] on

9.1.4 ICMP Redirect を送信するか否かの設定

[書式] **ip icmp redirect send** *send*

[設定値] ◦ *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。

[初期値] on

9.1.5 ICMP Redirect 受信時の処理の設定

[書式] **ip icmp redirect receive** *action*

[設定値] ◦ *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。

[初期値] off

9.1.6 ICMP Time Exceeded を送信するか否かの設定

[書式] **ip icmp time-exceeded send** *send*

[設定値] ◦ *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。

[初期値] on

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

[書式] **ip icmp timestamp-reply send** *send*

[設定値] ◦ *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。

[初期値] on

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

[書式] **ip icmp unreachable send** *send*

[設定値] ◦ *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。

[初期値] on

9.1.9 受信した ICMP のログを記録するか否かの設定

[書式] **ip icmp log** *log*

[設定値] ◦ *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。

[初期値] off

9.1.10 ステルス機能の設定

[書式] **ip stealth all**
ip stealth clear
ip stealth interface [*interface...*]

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

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

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

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

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

[初期値] clear

9.2 IPv6 の設定

9.2.1 ICMP Echo Reply を送信するか否かの設定

[書式] **ipv6 icmp echo-reply send** *send*

[設定値] ◦ *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。

[初期値] on

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

[書式] **ipv6 icmp parameter-problem send** *send*

[設定値] ◦ *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。

[初期値] off

9.2.3 ICMP Redirect を送信するか否かの設定

[書式] **ipv6 icmp redirect send** *send*

[設定値] ◦ *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。

[初期値] on

9.2.4 ICMP Redirect 受信時の処理の設定

[書式] **ipv6 icmp redirect receive** *action*

[設定値] ◦ *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。

[初期値] off

9.2.5 ICMP Time Exceeded を送信するか否かの設定

[書式] **ipv6 icmp time-exceeded send** *send*

[設定値] ◦ *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。

[初期値] on

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

[書式] **ipv6 icmp unreachable send** *send*

[設定値] ◦ *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。

[初期値] on

9.2.7 受信した ICMP のログを記録するか否かの設定

[書式] **ipv6 icmp log** *log*

[設定値] ◦ *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。

[初期値] off

9.2.8 ICMP Packet-Too-Big を送信するか否かの設定

[書式] **ipv6 icmp packet-too-big send** *send*

[設定値] ◦ *send*

- **on**.....送信する
- **off**送信しない

[説明] ICMP Packet-Too-Big を出すか否かを設定する。

[初期値] on

9.2.9 ステルス機能の設定

[書式] **ipv6 stealth** all
ipv6 stealth clear
ipv6 stealth *interface* [*interface...*]

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

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

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

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

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

[初期値] clear

10. NAT の設定

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

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

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

アドレス変換規則を表す記述を NAT ディスクリプタと呼び、それぞれの NAT ディスクリプタには、アドレス変換の対象とすべきアドレス空間が定義される。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。

10.1 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

[書式] **ip lan_if nat descriptor nat_descriptor_list**
ip lan_if nat descriptor clear

- [設定値]
- *lan_if*
 - *lan1* LAN インタフェース
 - *lan2* WAN インタフェース
 - *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。

[初期値] **clear**

10.2 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

[書式] **ip pp nat descriptor** *nat_descriptor_list*
ip pp nat descriptor clear

- [設定値] ◦ *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。

[初期値] clear

10.3 トンネルインタフェースに NAT ディスクリプタを適用する設定

[書式] **ip tunnel nat descriptor** *nat_descriptor_list*
ip tunnel nat descriptor clear

- [設定値] ◦ *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。

[初期値] clear

10.4 NAT ディスクリプタの動作タイプの設定

[書式] **nat descriptor type** *nat_descriptor type*

- [設定値]
- *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設定する。

[初期値] *type* = none

10.5 NAT 処理の外側 IP アドレスの設定

[書式] **nat descriptor address outer** *nat_descriptor outer_ipaddress_list*

- [設定値]
- *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 if address** コマンドで設定されている IP アドレス
 - *secondary*..... **ip lan if 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	
	有線 LAN	PP
<i>ipcp</i>	×	○

	適用インタフェース	
	有線LAN	PP
primary	○	×
secondary	○	×
IP アドレス	○	○

[初期値] ipcp

10.6 NAT 処理の内側 IP アドレスの設定

[書式] **nat descriptor address inner** *nat_descriptor inner_ipaddress_list*

- [設定値]
- *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**..... すべて

[説明] NAT/IP マスカレード処理の対象である内側の IP アドレスの範囲を設定する。
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。

[初期値] auto

10.7 静的 NAT エントリの設定

[書式] **nat descriptor static** *nat_descriptor id outer_ip=inner_ip* [*count*]

- [設定値]
- *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。初期値がそれぞれ **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。

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

[書式] **nat descriptor masquerade rlogin nat_descriptor use**

[設定値] ◦ *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。

[初期値] **off**

10.9 静的 IP マスカレードエントリの設定

[書式] **nat descriptor masquerade static** *nat_descriptor id inner_ip protocol port*

- [設定値]
- *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
 - *icmp* icmp プロトコル
 - プロトコル番号I ANA 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。

10.10 NAT ディスクリプタテーブルの TTL の制御方式の設定

[書式] **nat descriptor masquerade ttl hold *type***

[設定値] ◦ *type*..... TTL を同期させる方法

- **all**すべてのコネクションを対象とする
- **ftp**FTP の制御チャンネルのみを対象とする

[説明] 本コマンドによって IP マスカレードテーブルの TTL の扱いを制御することができる。通常、テーブルの TTL は単調に減少するが、FTP のように制御チャンネルとデータチャンネルからなるアプリケーションでは、制御チャンネルに対応するテーブルをデータ転送中に削除するべきではないため、制御チャンネルとデータチャンネルの両テーブルの TTL を同期させている。ただし、現有の機能では、制御チャンネルとデータチャンネルの対応を把握することが難しいため、同じホスト間の通信については、すべてのコネクションを関係づけ、TTL を同期させている。しかし、このような動作では、多くのテーブルの TTL が同期し、多くのテーブルが長く残留するという現象が起きる。

状況によっては、ルータのメモリが枯渇する可能性があるため、この処理を FTP の制御チャンネルに限定し、枯渇を予防する選択肢を提供する。TTL の同期を FTP の制御チャンネルに限定するときには、パラメータに **ftp** を設定する。FTP に限定せず、従来と同じように動作させるためには、パラメータに **all** を設定する。

[初期値] **all**

10.11 NATのIPアドレスマップの消去タイマの設定

[書式] **nat descriptor timer** *nat_descriptor time*

- [設定値] ◦ *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。

[初期値] 900

10.12 NAT ディスクリプタの削除

[書式] **nat descriptor delete** *nat_descriptor*

- [設定値] ◦ *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。

10.13 静的 NAT エントリの削除

[書式] **nat descriptor static delete** *nat_descriptor id*

- [設定値] ◦ *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。

10.14 静的 IP マスカレードエントリの削除

[書式] **nat descriptor masquerade static delete** *nat_descriptor id*

- [設定値] ◦ *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。

10.15 IP マスカレードで利用するポートの範囲の設定

[書式] **nat descriptor masquerade port range** *nat_descriptor start [port_num]*

[設定値] ◦ *nat_descriptor*.NAT ディスクリプタの識別番号 (1..21474836)

◦ *start*.....開始ポート番号 (1024..65534)

◦ *port_num*

- ポート数 (1..4096)
- 省略時は 4096

[説明] IP マスカレードで利用するポート番号の範囲を設定する。
start+port_num <= 65535 でなくてはならない。

[初期値] 60000 4096

10.16 IP マスカレードで外側から受信したパケットに該当する変換テーブルが存在しないときの動作の設定

[書式] **nat descriptor masquerade incoming** *nat_descriptor* *action* [*ip_address*]

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

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

[初期値] **reject**

10.17 NATでのアドレス割当の記録

[書式] **nat descriptor log** *switch*

[設定値] ◦ *switch*

- 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。

[初期値] off

10.18 FTPとして認識するポート番号の設定

[書式] **nat descriptor ftp port** *nat_descriptor port* [*port...*]

[設定値] ◦ *nat_descriptor.*NAT ディスクリプタの識別番号 (1..21474836)

◦ *port*.....ポート番号 (1..65535)

[説明] TCPで、このコマンドにより設定されたポート番号をFTPの制御チャンネルの通信だとみなして処理をする。

[初期値] 21

10.19 IP マスカレードで変換しないポート番号の範囲の設定

[書式] **nat descriptor masquerade unconvertible port** *nat_descriptor* if-possible
[clear]
nat descriptor masquerade unconvertible port *nat_descriptor protocol*
clear
nat descriptor masquerade unconvertible port *nat_descriptor protocol*
port

- [設定値] ◦ *nat_descriptor*.NAT ディスクリプタの識別番号 (1..21474836)
◦ *protocol* プロトコル
- tcp..... TCP
 - udp..... UDP
- *port*.....ポート番号の範囲

[説明] IP マスカレードで変換しないポート番号の範囲を設定する。
if-possible が指定されている時には、処理しようとするポート番号が他の通信で使われていない場合には値を変換せずそのまま利用する。

[初期値] clear

11. DNS の設定

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

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

リカーシブサーバ機能は、本機宛に届いた 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。

11.1 DNS サーバの IP アドレスの設定

[書式] **dns server** *ip_address* [*ip_address* ...]
dns server clear

[設定値] ◦ *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**.....設定のクリア

[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。

[初期値] clear

11.2 DNS サーバを通知してもらう相手先情報番号の設定

[書式] **dns server pp** *peer_num*

[設定値] ◦ *peer_num*

- DNS サーバを通知してもらう相手先情報番号
- none.....設定しない

[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。本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つたり、接続できても DNS サーバの通知がなかった場合には名前解決は行われない。

dns server コマンドで DNS サーバが明示的に指定されている場合には、そちらの設定が優先される。**dns server** コマンドに指定したサーバから返事がない場合には、相手先への接続と DNS サーバの通知取得が行われる。

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

[初期値] none

11.3 DNS サーバを取得する LAN インタフェースの設定

[書式] **dns server dhcp** *lan_if*
dns server dhcp none

[設定値] ◦ *lan_if*

- **lan1** LAN インタフェース
- **lan2** WAN インタフェース
- **none** 設定しない

[説明] DNS サーバを取得する LAN インタフェースを設定する。本コマンドで LAN インタフェースが設定されていると、DNS での名前解決を行う場合にこの LAN インタフェースで DHCP サーバから取得した DNS サーバに対して問合せを行う。DHCP サーバから DNS サーバを取得できなかった場合には名前解決は行われず、**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、および **dns server select**、あるいは、**dns server pp** コマンドの設定により問い合わせをすべき DNS サーバが決定された場合には、そちらの設定が優先される。

[ノート] 本コマンドを使用するには、指定された LAN インタフェースが DHCP クライアントとして動作していなければならない。

[初期値] none

11.4 DNS 問い合わせの内容に応じた DNS サーバの選択

[書式] **dns server select** *id server* [*type*] *query* [*original-sender*][*restrict pp connection-pp*]

dns server select *id pp peer_num* [*default-server*] [*type*] *query* [*original-sender*] [*restrict pp connection-pp*]

dns server select *id dhcp lan_if* [*default-server*] [*type*] *query* [*original-sender*] [*restrict pp connection-pp*]

dns server select *id reject* [*type*] *query* [*original-sender*]

dns server select delete *id*

- [設定値]
- *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
 - *reject* QUERY がマッチした場合、その DNS 問い合わせパケットを破棄し、DNS 問い合わせを解決しない
 - *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、xyz.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
- *peer_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*... *peer_num* パラメータで指定した接続相手から DNS サーバを獲得できなかったときに使う DNS サーバの IP アドレス
- *lan_if* DHCP サーバより取得する DNS サーバを使う場合の LAN インタフェース
 - *lan1* LAN インタフェース
 - *lan2* WAN インタフェース

[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。

11.5 DNS リカーシブサーバとして動作させるか否かの設定

[書式] **dns service** *service*

[設定値] ◦ *service*

- **recursive**DNS リカーシブサーバとして動作する
- **off**サービスを停止させる

[説明] DNS リカーシブサーバとして動作するかどうかを設定する。

[初期値] **recursive**

[ノート] DNS リカーシブサーバとして動作する場合には 53/udp(domain) ポートを開け、DNS リカーシブサーバとして動作していない場合には該当ポートを閉じる。

11.6 DNS ドメイン名の設定

[書式] **dns domain** *domain_name*

[設定値] ◦ *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。

11.7 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

[書式] **dns private address spoof** *spoof*

[設定値] ◦ *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。

[初期値] off

11.8 ルータの FQDN の設定

[書式] **dns private name** *name*

[設定値] ◦ *name*ルータの FQDN

[説明] ルータの FQDN を設定する。

[ノート] 本コマンドで設定された FQDN は、**show ip host**、**show dns static** コマンドで静的 DNS レコードとして表示される。

[初期値] `setup.netvolante.jp`

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

[書式] **dns notice order protocol server** [*server*]

[設定値] ◦*protocol*

- **dhcp**.....DHCP による通知
- **msex**t.....IPCP MS 拡張による通知

◦*server*

- **none**.....一切通知しない
- **me**.....本機自身
- **server**..... **dns server** コマンドに設定したサーバ群

[説明] DHCP や IPCP MS 拡張では DNS サーバを複数通知できるが、それをどのような順序で通知するかを設定する。

none を設定すれば、他の設定に関わらず DNS サーバの通知を行わなくなる。**me** は、本機自身の DNS リカーシブサーバ機能を使うことを通知する。**server** では、**dns server** コマンドに設定したサーバ群を通知することになる。IPCP MS 拡張では通知できるサーバの数が最大 2 に限定されているので、後ろに **me** が続く場合は先頭の 1 つだけと本機自身を、**server** 単独で設定されている場合には先頭の 2 つだけを通知する。

[初期値] **dhcp me server**
mnext me server

11.10 SYSLOG 表示で DNS により名前解決するか否かの設定

[書式] **dns syslog resolv** *resolv*

[設定値] ◦ *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。

[初期値] off

11.11 静的 DNS レコードの登録

[書式] **ip host** *fqdn value*
dns static *type name value*

- [設定値] ◦ *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>
a	FQDN	IP アドレス
ptr	IP アドレス	FQDN
mx	FQDN	FQDN
ns	FQDN	FQDN
cname	FQDN	FQDN

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

[説明] 静的な DNS レコードを定義する。

ip host コマンドは、**dns static** コマンドで **a** と **ptr** を両方設定することを簡略化したものである。

[ノート] 問い合わせに対して返される DNS レコードは以下のような特徴を持つ。

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

[設定例] # ip host pc1.rupro.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

11.12 静的 DNS レコードの削除

[書式] **ip host delete** *fqdn*
dns static delete *type name*

- [設定値]
- *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>
a	FQDN
ptr	IP アドレス
mx	FQDN
ns	FQDN
cname	FQDN

[説明] 静的な DNS レコードを削除定義する。

12. アナログ通信機能の設定

RT56v 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活用マニュアル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。

RT56v 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。

RT56v 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、アナログ通信機器の発着信回数は **show analog account** コマンドで知ることができます。

12.1 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
アナログポート使用制限の設定	14	analog use
インターネット電話着信制限の設定	15	analog sip use arrive
インターネット電話発信制限の設定	16	analog sip use call
即時発信	22	analog rapid call
ポーズを判定する時間	23	analog pause timer
識別着信	32	analog arrive restrict
識別着信の番号登録	33	analog arrive restrict list add
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
送話PADの音量設定	61	analog pad send
受話PADの音量設定	62	analog pad receive

機能	機能番号	対応するコンソールコマンド
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_if address
LAN 側のネットマスク設定	72	ip lan_if netmask
着信時サービス設定	82	analog arrive incoming-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
L メール利用の設定	86	analog l-mail-service
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 analog arrive ringer-type list
着信ベルの番号削除	93	delete
発着信回数の消去	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
ダイヤルの種別選択	201	pstn dial type
ナンバー・ディスプレイ着信識別	203	pstn number display
付加サービス機能設定	204	pstn supplementary-service

機能	機能番号	対応するコンソールコマンド
回線側のポーズ時間設定	205	pstn pause timer
フッキング時間設定	206	pstn hooking timer
受話PADの音量設定	207	pstn pad receive
送話PADの音量設定	208	pstn pad send
LINEポート使用制限の設定	209	pstn disable, pstn enable

12.2 電話回線側の設定

12.2.1 ダイヤル種別の選択

[書式] **pstn dial type** *type*

[設定値] ◦ *type*

- 10pps.....パルス (10pps)
- 20pps.....パルス (20pps)
- pbPB

[説明] 電話回線に対するダイヤルの種別を選択する。

[ノート] 10ppsの回線については、このコマンドで "10pps" に明示的に指定する必要がある。

[初期値] 20pps

12.2.2 ナンバーディスプレイ (ダイヤルイン/L モード) の着信識別設定

[書式] **pstn number display switch**

[設定値] ◦ *switch*

- **off**ナンバーディスプレイ (ダイヤルイン/L モード) の着信を判別しない
- **auto**ナンバーディスプレイ (ダイヤルイン/L モード) の着信を自動判別

[説明] 電話回線に対するナンバーディスプレイ (ダイヤルイン/L モードメッセージ到着お知らせ機能) の着信に対する動作を設定する。

[ノート] **auto** に設定すると、ナンバーディスプレイの他、ダイヤルイン・L モードメッセージ到着お知らせ機能に対する着信を自動的に判別する。**off** に設定すると、上記の着信においても、通常の着信と同様な動作を行う。

[初期値] **auto**

12.2.3 付加サービス機能の設定

〔書式〕 **pstn supplementary-service service**

〔設定値〕 ◦ *service*

- **off**付加サービスを契約していない回線
- **on**.....付加サービスを契約している回線

〔説明〕 電話回線に対して付加サービス（キャッチホン／ボイスワープ／トリオホン）を契約しているかどうかを設定する。

〔初期値〕 off

12.2.4 電話回線に対するポーズ時間の設定

〔書式〕 **pstn pause timer time**

〔設定値〕 ◦ *time*秒数 (1..10)

〔説明〕 電話回線に対してポーズ操作を行う場合のポーズ時間を設定する。

〔初期値〕 2

12.2.5 電話回線に対するフッキング時間の設定

[書式] **pstn hooking timer** *time*

[設定値] ◦ *time*秒数 (0.3..1)

[説明] 電話回線に対してフッキング操作を行う場合のフッキング時間を設定する。秒数は0.1 秒単位で設定できる。

[初期値] 0.5

12.2.6 電話回線に対する受話 PAD の設定

[書式] **pstn pad receive** *pad*

[設定値] ◦*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] 電話回線に対する受話 PAD を設定する。

[初期値] off

12.2.7 電話回線に対する送話 PAD の設定

[書式] **pstn pad send pad**

[設定値] ◦*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] 電話回線に対する送話 PAD を設定する。

[初期値] off

12.2.8 電話回線の使用不許可の設定

[書式] **pstn disable**

[設定値] なし

[説明] 電話回線を使用できない状態にする。ルータが電話回線に接続していない場合は、この設定を行う必要がある。

12.2.9 電話回線の使用許可の設定

〔書式〕 **pstn enable**

〔設定値〕 なし

〔説明〕 電話回線を使用できる状態にする。

12.3 TEL ポートごとの設定

12.3.1 アナログポートを使うか否かの設定

[書式] **analog use port use**

[設定値] ◦ *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。

[初期値] on

12.3.2 アナログポートのダイヤルイン番号の設定

[書式] **analog local address** *port dialin_num* [*dialin_num_list*]
analog local address *port* clear

- [設定値]
- *port*.....アナログポート
 - 1 TEL1 ポート
 - 2 TEL2 ポート
 - 3 TEL3 ポート
 - *dialin_num*.....ダイヤルイン番号
 - *dialin_num_list*ダイヤルイン番号を空白で区切った並び (最大 4 つ)
 - **clear**.....すべてのダイヤルイン番号をクリア

[説明] アナログポートのダイヤルイン番号を設定する。最大 5 つまで設定できる。

12.3.3 相手先番号による即時発信を許可するか否かの設定

[書式] **analog rapid call port rapid**

[設定値] ◦ *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、'#' ボタンを押さなくても、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。
過去に、発信により通話状態となった相手先が即時発信の対象となる。

[ノート] 電話回線に対する発信に対しては、この設定に関係なく、すぐに電話回線に対するダイヤル動作を行う。

[初期値] on

12.3.4 アナログポートでの識別着信をするか否かの設定

[書式] **analog arrive restrict** *port restrict*

- [設定値]
- *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、すべての発番号に対して着信許可となる。

[初期値] **reject**

12.3.5 識別着信リストの登録

〔書式〕 **analog arrive restrict list add** *port number dial_num*

- 〔設定値〕
- *port*.....アナログポート
 - 1 TEL1 ポート
 - 2 TEL2 ポート
 - 3 TEL3 ポート
 - *number*.....リスト番号
 - *dial_num*.....電話番号

〔説明〕 識別着信用の電話番号を識別着信リストへ登録する。
リスト番号とは、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。

12.3.6 識別着信リストの削除

[書式] **analog arrive restrict list delete** *port number*

- [設定値]
- *port*.....アナログポート
 - 1 TEL1 ポート
 - 2 TEL2 ポート
 - 3 TEL3 ポート
 - *number*.....リスト番号

[説明] パラメータで指定されたリスト番号を識別着信リストから削除する。

12.3.7 優先着信機能の設定

[書式] **analog arrive prior-port** *port prior*

[設定値] ◦ *port*.....アナログポート

- 1 TEL1 ポート
- 2 TEL2 ポート
- 3 TEL3 ポート

◦ *prior*

- 1 優先順位高い
- 2 優先順位普通
- 3 優先順位低い

[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。

[初期値] 2

12.3.8 着信ベルリストの登録

〔書式〕 **analog arrive ringer-type list add** *port type number calling_num*

- 〔設定値〕
- *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
 - *calling_num*相手発信者の電話番号

〔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。
ナンバー・ディスプレイサービスの契約が必要。

12.3.9 着信ベルリストの削除

[書式] **analog arrive ringer-type list delete** *port type number*

- [設定値]
- *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。

12.3.10 ナンバー・ディスプレイ設定

[書式] **analog arrive number display port mode**

[設定値] ◦ *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・ディスプレイを使用しない
- **on**..... ナンバー・ディスプレイを使用する

[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。

[ノート] キャッチホン・ディスプレイ契約されている電話回線を使用して通話中は、設定に関係なく通話中の電話機でキャッチホン・ディスプレイが機能する。

[初期値] off

12.3.11 ナンバー・ディスプレイ信号の設定

[書式] **analog arrive modem signal type** *port type*

- [設定値]
- *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)
 - 3 ストップビット信号長が 1 ビット

[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。

[初期値] 3

12.3.12 ダイヤル桁間タイマの設定

[書式] **analog wait dial timer** *port time*

- [設定値]
- *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..20)

[説明] ダイヤル桁間タイマ値を設定する。
ダイヤル中に本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。

[初期値] 6

12.3.13 フッキングを判定する時間の設定

[書式] **analog hooking timer port time**

- [設定値] ◦ *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。

[初期値] 1

12.3.14 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

[書式] **analog hooking inhibit timer** *port time*

[設定値] ◦ *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。

[初期値] **off**

12.3.15 送話 PAD の設定

[書式] **analog pad send** *port pad*

- [設定値]
- *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。

[初期値] off

12.3.16 受話 PAD の設定

[書式] **analog pad receive port pad**

- [設定値] ◦ *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] 受話 PAD を設定する。

[初期値] off

12.3.17 TEL ポートへの切断信号の送出手設定

[書式] **analog disc-signal** *port use*

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

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

[ノート] 電話回線を使用した通話時はこのコマンドは無効である。

[初期値] on

12.3.18 DTMF 検出レベルの設定

[書式] **analog dtmf level** *port level*

- [設定値]
- *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)
 - off off
 - -3dB -3dB
 - -6dB -6dB
 - -9dB -9dB
 - -12dB -12dB
 - -15dB -15dB
 - -18dB -18dB
 - -21dB -21dB
 - -24dB -24dB
 - -27dB -27dB
 - -30dB -30dB

[説明] アナログポートのDTMF 信号検出レベルを設定する。

[初期値] off

12.3.19 アナログダイヤルインと無鳴動着信機能の設定

[書式] **analog arrive incoming-signal** *port number address type signal dial_in-num*
analog arrive incoming-signal delete *port number*

- [設定値]
- *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
 - *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
 - *type* 機器の種別
 - *all* すべて
 - *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-num* ... 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* 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-num* で設定されたダイヤルイン信号を出す。
- 【ノート】 モデム信号方式のダイヤルインサービスの契約が必要。PB 信号方式のダイヤルインサービスを契約しても利用できない。
電話回線側に対して F ネットの 1,300Hz の呼出信号には対応していない。

12.3.20 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

[書式] **analog arrive without-calling-number** port type [option]

[設定値] ◦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.... 本設定を公衆電話からの着信に限定する
- rejected-by-user..... 本設定をユーザによる通知拒否の着信に限定する
- service-unavailable 本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。

[ノート] ナンバー・ディスプレイサービスの契約が必要。

[初期値] type = permit

option = all

12.3.21 Lモードのメッセージ到着お知らせ機能 (Lメール) の設定

[書式] **analog l-mail-service** *port service*

[設定値] ◦ *port*.....アナログポート

- 1 TEL1 ポート
- 2 TEL2 ポート
- 3 TEL3 ポート

◦ *service*

- **on**.....使用する
- **off**使用しない

[説明] アナログポートにLモード対応のアナログ機器を接続時、Lモードのメッセージ到着お知らせ機能 (Lメール) を利用するか否かを設定する。

[ノート] NTT (NTT 東日本、NTT 西日本) とLモード契約する必要がある。

[初期値] off

12.3.22 ポーズを判定する時間の設定

[書式] **analog pause timer** *port time*

- [設定値]
- *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..10)

[説明] ポーズとして判断する最小の時間を設定する。

[初期値] 2

13. 機器間アナログ通話機能の設定

RT56v では、「機器間アナログ通話機能」により複数の RT56v のうちの 1 台が他の RT56v のアナログポート及び電話回線のアナログ通話を一括管理することが可能です。これにより、異なる RT56v に接続されているアナログ機器同士で内線通話が可能で、加えて電話回線に接続されていない RT56v から、他の RT56v に接続された電話回線を使用して外線通話をすることも可能です。

複数の RT56v のうち、アナログポート及び電話回線のアナログ通話を管理する RT56v を「アナログ親機」と呼び、その他の RT56v を「アナログ子機」と呼びます。ひとつのアナログ親機が管理できる RT56v は、アナログ親機も含めて最大 9 台です。アナログ親機または子機に設定するには、**analog extension mode** コマンドを使います。

アナログ子機は、同一ネットワーク内にアナログ親機があるかどうか自動で検索することが可能です。これは **analog extension master** コマンドにより設定します。

アナログ親機と子機には、機器番号を設定してください。機器番号を設定していない場合には、機器を指定した内線呼び出しができません (" * * " による一斉内線呼び出しは可能です)。機器番号は **analog extension machine-id** コマンドで設定します。

13.1 機器間アナログ通話モードの設定

[書式] **analog extension mode** *mode*

[設定値] ◦ *mode*

- **standalone** 単独動作モード
- **master** アナログ親機モード
- **slave** アナログ子機モード

[説明] 機器間アナログ通話モードを設定する。

[ノート] 複数機器で協調してアナログ通話を行う場合、同一ネットワーク上で必ず一つをアナログ親機モードとし、残りはアナログ子機モードとすること。

[初期値] standalone

13.2 機器間アナログ通話に使用する IP アドレス取得インターフェースの設定

[書式] **analog extension address refer interface**
analog extension address refer pp peer_num

- [設定値] ◦ *interface*
- lan1 LAN インターフェース
 - lan2 WAN インターフェース
- *peer_num* PP インターフェース
- 相手先情報番号 (1..30)
 - anonymous

[説明] 機器間アナログ通話に使用する IP アドレスを取得するインターフェースを設定する。

[ノート] PP インターフェースで NAT を使用する場合、静的 NAT を UDP ポートの 2427-2429 および 5004-(5004+(アナログポート数 + 電話回線数 × 2) × 2) に設定する必要がある。またフィルタ設定も、上記ポートを通す設定が必要である。

[初期値] lan1

13.3 アナログ親機となる機器の設定

[書式] **analog extension master** *master*

[設定値] ◦ *master*

- IP アドレス
- **auto**.....自動検索

[説明] アナログ子機モードにおいて、アナログ親機となる機器の IP アドレスを設定する。
auto の場合、同一ネットワーク内のアナログ親機を自動検索する。

[ノート] 自動検索失敗時は、10 秒毎に再検索を行う。

[初期値] **auto**

13.4 アナログ子機受け入れモードの設定

[書式] **analog extension slave permit mode**

[設定値] ◦ *mode*

- **all**すべて受け入れる
- **registered-only**機器番号を設定している機器のみを受け入れる

[説明] アナログ親機モードにおいて、アナログ子機の受け入れモードを設定する。

[ノート] 受け入れ拒否された子機では、電話回線のアナログ発着信としての使用およびアナログポートの使用 ([* #] をダイヤルすることによるアナログポートからの設定を除く) が不可能となる。

本コマンドの設定が **show analog extension** コマンドで表示される「接続拒否中子機一覧」に反映されるまでに、数十秒程度時間を要する。

[初期値] **all**

13.5 アナログ親機 / 子機の機器番号の設定

[書式] **analog extension machine-id** *id mac_address*

[設定値] ◦ *id*.....機器番号 (1..9)

◦ *mac_address*....MAC アドレス **xx:xx:xx:xx:xx:xx** (x は 16 進数)

[説明] アナログ親機モードにおいて、アナログ親機 / 子機の機器番号を設定する。

[ノート] 機器番号を設定することにより、そのアナログ子機を着呼側とする機器間内線通話が可能になる。ただし、機器番号を設定していなくても外線及び一斉内線 (" ** ") による呼び出しは可能。

既に同じ *id* のアナログ子機が設定されている場合は、現在の設定が消されて新しい設定が上書きされる。同じ *mac_address* の機器が既に設定されている場合は、エラーとなる。

[初期値] なし

13.6 アナログ親機 / 子機の機器番号の削除

[書式] **analog extension machine-id delete** *id*

[設定値] ◦ *id*.....機器番号 (1..9)

[説明] アナログ親機モードにおいて、アナログ親機 / 子機の機器番号を削除する。

[ノート] 機器番号を削除することにより、その後、そのアナログ機器を着呼側とする機器間内線通話が不可能になる。ただし、機器番号を設定していなくても外線及び一斉内線 (" ** ") による呼び出しは可能。

[初期値] なし

13.7 機器間アナログ通話のログを記録するか否かの設定

[書式] **analog extension log** *switch*

[設定値] ◦ *switch*

- on.....ログを出力する
- offログを出力しない

[説明] 機器間アナログ通話のログを出力するか否かを設定する。

[初期値] off

14. インターネット電話機能の設定

14.1 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
インターネット電話着信制限の設定	15	analog sip use arrive
インターネット電話発信制限の設定	16	analog sip use call

14.2 SIP プロトコルによるインターネット電話機能を使用するか否かの設定

[書式] **sip use use**

[設定値] ◦use

- off使用しない
- on.....使用する

[説明] SIP プロトコルによるインターネット電話機能を使用するか否かを設定する。

[ノート] offの場合、設定した機器及び設定した機器をアナログ親機とするアナログ子機において SIP プロトコルによるインターネット電話機能の発着信ができない。

[初期値] off

14.3 SIP プロトコルによる発信時の呼制御に使用する IP プロトコルの選択

〔書式〕 **sip ip protocol** *protocol*

〔設定値〕 ◦*protocol*

- udpUDP を使用
- tcpTCP を使用

〔説明〕 SIP プロトコルによるインターネット電話の発信時、呼制御に使用する IP プロトコルを選択する。

〔ノート〕 SIP メソッドを受信した場合は、この設定に関わらず、受信したプロトコルで送信を行う。

〔初期値〕 udp

14.4 アナログポートからの特定のダイヤルに対応する SIP 発信の設定

[書式] **analog extension sip address** *number dial_number sip_address*

- [設定値] ◦ *number*.....登録番号 (1-65535)
◦ *dial_number* ...アナログポートからのダイヤル番号
◦ *sip_address*.....SIP で発呼する先の SIP URI

[説明] アナログポートからの特定のダイヤルに対応するインターネット電話 (SIP) 発信の設定を行う。

- [ノート] ダイヤル番号に合致する設定を登録番号順に検索し、はじめに合致した設定が適用される。
sip_address は、"sip:user_name@domain_name" という形式。

[初期値] なし

14.5 アナログポートからの特定のダイヤルに対応する SIP 発信の設定削除

[書式] **analog extension sip address delete** *number*

- [設定値] ◦ *number*.....登録番号 (1-65535)

[説明] アナログポートからの特定のダイヤルに対応するインターネット電話 (SIP) 発信の設定削除を行う。

14.6 アナログポートからの特定のプレフィックスによる発呼経路の設定

[書式] **analog extension dial prefix route** [*dial*]

[設定値] ◦ *route*

- **line** 公衆回線 (PSTN) でかけるためのプレフィックス設定
- **sip** インターネット電話 (SIP) でかけるためのプレフィックス設定

◦ *dial*

- 入力なし プレフィックスなし
- 2#..9# 2#, 3#, ..., 9# のプレフィックスに対する設定

[説明] アナログポートからのダイヤル時に、特定のプレフィックスによる発呼経路を設定する。プレフィックスの設定が重複した場合、line -> sip の順番で設定が優先される。

[初期値] **line**

sip 9#

14.7 SIP プロトコルによる宛先アドレスに対する着信制限の設定

[書式] **analog sip use arrive port mode**

[設定値] ◦ *port*.....アナログポート

- 1TEL1 ポート
- 2TEL2 ポート
- 3TEL3 ポート

◦ *mode*

- *off*アナログポートへの着信を全て拒否
- *myname* **analog sip call myname** 及び **analog sip arrive myaddress** で登録されているユーザ名 / アドレスに対する着信のみ許可
- *on*.....アナログポートへの着信を全て許可

[説明] SIP プロトコルによるインターネット電話の宛先アドレスに対する着信制限を設定する。

[ノート] *myname* に設定されている場合の動作は以下の通りになる。

- ・ SIP の To: フィールドのドメインが RT 自身の場合、**analog sip call myname** の設定及び **analog sip arrive myaddress** の設定でドメイン指定のないものを検索し、To: フィールドのユーザ名と一致する設定があれば着信する。
- ・ SIP の To: フィールドのドメインが RT 自身でない場合 (サーバを経由した着信など)、**analog sip arrive myaddress** の設定でドメイン指定があるものを検索し、To: フィールドと一致する設定があれば着信する。

[初期値] on

14.8 SIP プロトコルによる着信識別で使用する自己 SIP アドレスの設定

[書式] **analog sip arrive myaddress** *port number sip_address*

[設定値] ◦ *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..65535)

◦ *sip_address*..... SIPアドレス (sip: で始まり @ を含んだ SIP URI または sip: で始まる @ を含まない SIP ユーザ名)

[説明] SIP プロトコルによるインターネット電話の着信識別に使用する自己 SIP アドレスを設定する。

[初期値] なし

14.9 SIP プロトコルによる着信識別で使用する自己 SIP アドレス設定の削除

[書式] **analog sip arrive myaddress delete** *port number*

- [設定値]
- *port*.....アナログポート
 - 1TEL1 ポート
 - 2TEL2 ポート
 - 3TEL3 ポート
 - *number*.....登録番号 (1..65535)

[説明] SIP プロトコルによるインターネット電話の着信識別で使用する自己 SIP アドレス設定を削除する。

14.10 SIP プロトコルによる発信で使用する自己 SIP ユーザ名の設定

[書式] **analog sip call myname port username**

[設定値] ◦ *port*.....アナログポート

- 1TEL1 ポート
- 2TEL2 ポート
- 3TEL3 ポート

◦ *username*.....ユーザ名 (sip: で始まり、@ を含まない SIP ユーザ名)

[説明] SIP プロトコルによるインターネット電話発信で使用する自己 SIP ユーザ名を設定する。

[ノート] SIP 着信時の宛先による着信制限では、このコマンドと **analog sip arrive myaddress** で設定されたアドレスに対する着信を **analog sip use arrive myname** によって許可することができる。

[初期値] sip:rt56v

14.11 SIP プロトコルによるインターネット電話の発信制限の設定

[書式] **analog sip use call** *port mode*

- [設定値] ◦ *port*.....アナログポート
- 1TEL1 ポート
 - 2TEL2 ポート
 - 3TEL3 ポート
- *mode*
- **off**SIP への発信を拒否
 - **on**.....SIP への発信を許可

[説明] SIP プロトコルによるインターネット電話の発信制限を設定する。

[初期値] on

14.12 ネットボランチ電話番号への宛先アドレスに使用するドメイン名の設定

[書式] **sip netvolante dial domain** *name*

[設定値] ◦ *name* ネットボランチ電話番号への宛先アドレスに使用するドメイン名

[説明] [#][#] のプレフィックスを使用するネットボランチ電話番号への発呼での宛先アドレスに使用するドメイン名を設定する。rtpro.yamaha.co.jp に設定し、##87654321 をダイヤルした場合、sip:NetVolatantePhone@87654321.rtpro.yamaha.co.jp に対して SIP の発呼を行う。

[ノート] ネットボランチ DNS サービス以外の DDNS による電話番号割り当てサービスを利用する場合に設定する。

[初期値] tel.netvolante.jp

15. メール着信確認、メール転送、メール通知機能の設定

メール着信確認機能は、プロバイダに新しいメールがあるかどうかを本機が確認して、その結果を MSG LED を点滅させたり、ブラウザで確かめたりする機能です。

メール転送機能は、指定したメールサーバのメールを別のメールサーバに転送する機能です。

メール通知機能は、不正アクセス検知情報を指定した宛先にメールで通知する機能です。

15.1 メール着信確認機能

15.1.1 メールサーバの設定

[書式] **mail-check server** *server_num destination protocol userid password [name]*
mail-check server *server_num clear*

- [設定値]
- *server_num*.....サーバ番号 (1..5)
 - *destination*
 - メールサーバの IP アドレス
 - ホスト名
 - *protocol*
 - **pop3**メール通信プロトコルとして POP3 を使用
 - **apop**メール通信プロトコルとして APOP を使用
 - *userid* ユーザ ID (64 文字以内)
 - *password* パスワード (64 文字以内)
 - *name* 識別名 (64 文字以内)
 - **clear** メールサーバの宛先なし

[説明] メールサーバの IP アドレス等の情報を設定する。

15.1.2 メールチェックの実行

[書式] **mail-check go** *server_num*

[設定値] ◦ *server_num*サーバ番号 (1..5)

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

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

15.1.3 メールチェックの実行を許可するか否かの設定

[書式] **mail-check prohibit** *server_num prohibit*

[設定値] ◦ *server_num*サーバ番号 (1..5)

◦ *prohibit*

- **on** 実行禁止
- **off** 実行許可

[説明] メール着信確認の実行を許可するか否かを設定する。

[初期値] off

15.1.4 メールチェックによる LED の消灯

[書式] **mail-check led off** [*server_num*]

- [設定値] ◦ off.....LED の消灯を表すキーワード
◦ *server_num*.....サーバ番号 (1..5、省略時はすべてのサーバ番号)

[説明] メール着信を通知する MSG LED の点滅を止める。

15.1.5 メールチェックの状態表示

[書式] **show mail-check status** [*server_num*]

- [設定値] ◦ *server_num*.....サーバ番号 (1..5、省略時はすべてのサーバ番号)

[説明] 先のメールチェックの実行結果を表示する。

15.1.6 メールチェックタイムアウトの設定

[書式] **mail-check timeout** *server_num time*

- [設定値]
- *server_num* サーバ番号 (1..5)
 - *time* メール到着チェック時にタイムアウトするまでの秒数 (1..180)

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

15.2 メール転送機能

15.2.1 送信メールサーバの設定

[書式] **mail-transfer server** *server_num destination protocol from to [name]*
mail-transfer server *server_num clear*

- [設定値]
- *server_num*.....サーバ番号 (1..5)
 - *destination*.....送信メールサーバの IP アドレス or ホスト名
 - *protocol*
 - *smtp*.....SMTP
 - *from*転送元ユーザのメールアドレス (255 文字以内)
 - *to*転送先ユーザのメールアドレス (255 文字以内)
 - *name*識別名 (64 文字以内)
 - *clear*.....送信メールサーバの宛先なし

[説明] 送信メールサーバの IP アドレス等の情報を設定する。

[初期値] clear

15.2.2 送信先サーバの設定

[書式] **mail-transfer send to** *server_num*
mail-transfer send to clear

[設定値] ◦ *server_num*.....メッセージを転送するサーバ番号 (1..5、複数設定可)
◦ clear.....メールサーバなし

[説明] **mail-transfer server** コマンドで設定された送信用メールサーバをメール転送用に設定する。

[初期値] clear

15.2.3 受信メッセージサーバの設定

[書式] **mail-transfer receive from** *server_num*
mail-transfer receive from clear

- [設定値] ◦ *server_num*.....メッセージを受信するサーバ番号 (1..5、複数設定可)
◦ clear.....メールサーバなし

[説明] **mail-check server** コマンドで設定された受信用メールサーバをメール転送用に設定する。

[初期値] clear

15.2.4 受信メッセージの最大長の設定

[書式] **mail-transfer receive maxlength** *max_length*

- [設定値] ◦ *max_length*.....取り込み可能なメッセージ長 (1..100 : 1024bytes 単位)

[説明] 受信するメッセージの最大長を設定します。
かんたん設定ページからの設定では 10240byte に制限される。設定した最大長を超えるメールは受信しない。

[初期値] 10

15.2.5 メール転送の実行

[書式] **mail-transfer go** [from *pop_servers*] [to *smtp_servers*]

- [設定値] ◦ *pop_servers*メッセージを受信するサーバ番号 (1..5、スペースで区切り複数設定可)
◦ *smtp_servers*メッセージを転送するサーバ番号 (1..5、スペースで区切り複数設定可)

[説明] メール転送を実行する。

- [ノート] *pop_servers* には、**mail-check server** コマンドで設定された受信用メールサーバをメール転送用に指定する。
smtp_servers のサーバ番号指定には、**mail-transfer server** コマンドで設定された送信用メールサーバをメール転送用に指定する。
pop_servers を省略した場合、**mail-transfer receive from** コマンドで登録された番号の受信サーバから受信する。
smtp_servers を省略した場合、**mail-transfer send to** コマンドで登録された番号の送信サーバへ送信する。
本コマンドで *pop_servers* や *smtp_servers* を指定して実行した場合、**mail-transfer receive from** コマンドや **mail-transfer send to** コマンドの設定に関係なく、メール転送が実行可能になる。
メッセージの取り込みは、指定されたサーバに対して未読分のみ行う。取り込んだメッセージは、設定された転送先に応じて設定されたフィルタに従って転送の拒否が決定され、必要なメッセージのみが転送される。

15.2.6 メール転送タイムアウトの設定

[書式] **mail-transfer timeout** *server_num time*

- [設定値] ◦ *server_num* サーバ番号 (1..5)
◦ *time* メール転送時にタイムアウトするまでの秒数 (1..180)

[説明] メール転送でのタイムアウトするまでの時間を設定します。

- [ノート] ここで指定するタイムアウトの時間はメール転送機能全体に要する時間ではなく、あるサーバへの転送時の SMTP コネクションの時間。

[初期値] 120

15.2.7 転送メッセージの最大長の設定

[書式] **mail-transfer send maxlength** *server_num len*

[設定値] ◦ *server_num*サーバ番号 (1..5)

◦ *len*

- メッセージが *len* の長さを超えたら超過部分を削除する (0..4096)
- *infinity*..... **mail-transfer receive maxlength** コマンドで設定された長さまでを転送する

[説明] 転送するメッセージの最大長を設定する。

[初期値] *infinity*

15.2.8 受信メッセージサーバ制限の設定

[書式] **mail-transfer receive restrict** *server_num* from *smtp_server* [*smtp_server...*]

- [設定値] ◦ *server_num*.....サーバ番号 (1..5)
◦ *smtp_server*.....メッセージを受信するサーバ (複数設定可)

[説明] 指定したサーバに転送するメッセージを受信するサーバを制限する。

- [初期値] mail-transfer receive restrict 1 from 1 2 3 4
mail-transfer receive restrict 2 from 1 2 3 4
mail-transfer receive restrict 3 from 1 2 3 4
mail-transfer receive restrict 4 from 1 2 3 4

15.2.9 転送メッセージのフィルタ設定

[書式] **mail-transfer filter** *server_num condition*

- [設定値]
- *server_num* サーバ番号 (1..5)
 - *condition* フィルタ条件
 - **from** *string* From フィールドに *string* が含まれるメッセージ
 - **to** *string* To フィールドに *string* が含まれるメッセージ
 - **subject** *string* Subject フィールドに *string* が含まれるメッセージ
 - **length** <= *N* 長さが *N* オクテット以下のメッセージ
 - **and** 上記 2 つの条件の AND
 - **or** 上記 2 つの条件の OR
 - **not** 上記 1 つの条件の NOT
 - **clear** フィルタを削除する

[説明] メール転送フィルタを定義する。
フィルタを指定する文字列全体の大きさに制限はない。

[初期値] clear

15.2.10 メッセージ転送を禁止するか否かの設定

[書式] **mail-transfer prohibit** *server_num prohibit*

[設定値] ◦ *server_num*サーバ番号 (1..5)

◦ *prohibit*

- **on**.....禁止する
- **off**禁止しない

[説明] メール着信確認の実行を許可するか否かを設定する。
メッセージの取り込みが行われた後に転送が行われない動作となる。

[初期値] off

15.3 メール通知機能

15.3.1 送信情報の文字コードの設定

[書式] **mail-notify charset** *server_num charset*

[設定値] ◦ *server_num*サーバ番号 (1..5)

◦ *charset*文字コード

- us-ascii
- iso-2022-jp

[説明] メール通知機能で使用する文字コードを指定する。

[初期値] iso-2022-jp

15.3.2 不正アクセス検知時のメール通知設定

[書式] **mail-notify intrusion server_num notify [count]**

- [設定値]
- *server_num*サーバ番号 (1..5)
 - *notify*
 - **auto**自動通知する
 - **manual**手動通知する
 - **off**通知しない
 - *count*不正アクセス検知回数 (1..50)

[説明] 不正アクセスを検知した場合にメールで通知するか否かを設定する。
count パラメータで設定した回数の不正アクセスを検知した場合にメール通知をする。
notify パラメータを **on** に設定している場合には、*count* パラメータの設定が有効となる。
count パラメータが設定されていない場合には、**1** に設定される。

[初期値] *notify* = off
count = 1

15.3.3 不正アクセス検知時に通知されるメールのサブジェクト設定

[書式] **mail-notify intrusion subject** *server_num subject*

- [設定値] ◦ *server_num* サーバ番号 (1..5)
◦ *subject* サブジェクト

[説明] 不正アクセスを検知した場合に通知するメールのサブジェクトを設定する。

[初期値] 空文字

15.3.4 不正アクセス検知情報をメールで通知する

[書式] **mail-notify intrusion go** *server_num*

- [設定値] ◦ *server_num* サーバ番号 (1..5)

[説明] 不正アクセス検知情報をメールで送信する。

[ノート] サーバ番号には、**mail-transfer server** コマンドで設定された送信用メールサーバをメール通知先として指定して実行する。

16. HTTP サーバ機能 (かんたん設定 / プロバイダ設定) の設定

HTTP サーバ機能は、かんたん設定ページのプロバイダの設定に利用され、設定ページの「登録」ボタンをクリックすることで自動設定されます。本章のコマンドを使用した場合には、登録されている設定の内容が変わるため、手動による変更を行う場合は十分に機能や動作を理解した上で行ってください。

プロバイダの情報は最大 10 個まで登録でき、既に設定されている相手先情報番号のいずれかに **provider set on** コマンドを使用して対応させます。解除する場合には **provider set off** コマンドを使用します。

設定されたプロバイダを選択するには、**provider select** コマンドを使用します。本コマンドによりプロバイダを変更すると、プロバイダごとに異なる DNS やデフォルトルートの設定など、そのプロバイダに接続するために必要な事項を自動的に設定変更します。プロバイダ設定の状況はかんたん設定ページで調べるか、**show config** コマンドで調べます。

16.1 プロバイダ接続タイプの設定

[書式] **provider type** *provider_type*

[設定値] ◦ *provider_type*

- **pppoe-terminal**PPPOE 型の端末接続
- **pppoe-network**.....PPPOE 型のネットワーク接続
- **none**.....設定なし

[説明] プロバイダの接続タイプを設定する。

[初期値] none

16.2 プロバイダ名称の設定

[書式] **pp name** *type:name*

[設定値] ◦ *type*

- PRV/1..10 プロバイダ型の識別 (1..10)
- RAS リモートアクセスサーバ型の識別
- WAN LAN 間接続の識別

◦ *name* ユーザが設定したプロバイダの名称

[説明] *かんたん*設定用の識別コマンド。*かんたん*設定で、プロバイダ名称等を入力した名称がここに設定される。

[設定例] **pp name PRV/1:Provider1**

16.3 プロバイダ情報の PP との関連付けと名前の設定

[書式] **provider set on** *peer_num* [*name*]

- [設定値] ◦ *peer_num*相手先情報番号 (1..30)
◦ *name*32 文字以内の名前

[説明] プロバイダ切り替えを利用するために設定する。
結び付けられた相手先情報番号はプロバイダとして扱われる。何も設定されていない相手先情報番号に対しては無効である。

16.4 プロバイダ情報の PP との関連付けの解除

[書式] **provider set off** *peer_num*

- [設定値] ◦ *peer_num*相手先情報番号 (1..30)

[説明] プロバイダとして相手先情報番号の情報を扱うことを解除する。

- [ノート] 本コマンドを実行すると、**provider** で始まるコマンドで設定されたプロバイダ情報も同時にクリアされる。
プロバイダ設定以外で相手先情報番号に対して設定された内容はクリアされない。

16.5 プロバイダの接続設定

[書式] **provider select** *peer_num*

[設定値] ◦ *peer_num*相手先情報番号 (1..30)

[説明] 接続するプロバイダ情報を選択し、利用可能にセットアップする。
本コマンドが実行されると、各種プロバイダ設定コマンドに記録された情報に基づき、デフォルトルート、DNS サーバ、スケジュール等の変更が行われる。
また、かんたん設定のプロバイダ接続設定において、接続先の変更や手動接続を行った場合にも、本コマンドが実行され接続先が切り換えられる。

本コマンドの上書き対象コマンドは以下のとおり。

すべてのプロバイダ情報:**pp disable**

選択されたプロバイダ情報:**pp enable**、**ip route**、**dns server**、及び **ntupdate** の **schedule at**。

[ノート] **provider set on** コマンドに設定されていない相手先情報番号に対しては無効。
かんたん設定のプロバイダに接続設定において、「複数のプロバイダに同時接続する」を選択している場合は、本コマンドを実行していけない。

16.6 プロバイダの DNS サーバのアドレス設定

[書式] **provider dns server** *peer_num ip_address [ip_address]*

[設定値] ◦ *peer_num*相手先情報番号 (1..30)

◦ *ip_address*

- DNS サーバの IP アドレス
- **clear**IP アドレスをクリア

[説明] プロバイダ毎の情報として DNS サーバのアドレスを設定する。DNS サーバは 2 つまで設定できる。
プロバイダが選択された場合にこのアドレスが **dns server** コマンドに上書きされる。

[ノート] **provider set on** コマンドが実行されていない相手先情報番号に対しては無効。
削除時、**dns server** コマンドの内容はクリアされない。クリアされるのは **provider dns server** コマンドで設定された内容だけである。

16.7 DNS サーバを通知してくれる相手の相手先情報番号 の設定

[書式] **provider dns server pp** *peer_num*

[設定値] ◦ *peer_num*

- 相手先情報番号 (1..30)
- DNS 通知相手先情報番号 (1..30)

◦ none

[説明] プロバイダ情報として DNS サーバを通知してくれる相手先情報番号 を設定する。

16.8 フィルタ型ルーティングの形式の設定

[書式] **provider filter routing type**

[設定値] ◦ *type*..... フィルタ型ルーティングの形式

- **off** かんたん設定で手動接続をした場合に、自動接続先が自動的に切り変わる
- **connection** ... かんたん設定で手動接続をした場合に、手動接続している間だけ有効な default 経路が選択される。
手動接続先が切断されると自動接続先に接続される
- **mail** メールとそれ以外のプロトコルの種類を区別し、プロバイダを切り換える
- **host** ホスト (IP アドレス) を区別してプロバイダを切り換える。
最大同時に 2 つのホストに接続。

[説明] かんたん設定専用の識別コマンド。かんたん設定ページで選択中のフィルタ型ルーティングの形式を設定する。

[ノート] コンソールなどから設定した場合の動作は保証されない。

[初期値] off

16.9 LAN 側のプロバイダ名称の設定

〔書式〕 **provider lan_if name type:name**
provider lan_if name clear

- 〔設定値〕
- *lan_if*
 - *lan1* LAN インタフェース
 - *lan2* WAN インタフェース
 - *type*..... プロバイダ情報の識別情報 ("PRV" など)
 - *name* ユーザが設定したプロバイダの名称など
 - *clear*..... 設定のクリア

〔説明〕 *かんたん*設定専用の識別コマンド。*かんたん*設定ページでプロバイダ名称等を入力した名称が設定される。

〔ノート〕 コンソールなどから手動設定した場合の動作は保証されない。

〔初期値〕 *clear*

16.10 プロバイダの NTP サーバのアドレス設定

〔書式〕 **provider ntp server** *peer_num ip_address*

〔設定値〕 ◦ *peer_num*相手先情報番号 (1..30)

◦ *ip_address*

- NTP サーバの IP アドレス
- **clear**設定のクリア

〔説明〕 プロバイダ毎の情報として NTP サーバのアドレスを設定する。

本コマンドで IP アドレスが設定されていると、プロバイダが選択されている場合に、定期的に時刻を問い合わせる。プロバイダが選択された場合にスケジュールに組み込まれる。

〔ノート〕 **provider set on** コマンドが実行されていない相手先情報番号に対しては無効。
dns server コマンドの内容はクリアされない。クリアされるのは **provider dns server** コマンドで設定された内容だけである。
現在のかんたん設定では、本コマンドは使用されていない。

16.11 NTP サーバの設定

【書式】 **provider ntpdate** *server_name*

【設定値】 ◦ *server_name*....NTP サーバ名 (IP アドレスまたは FQDN)

【説明】 かんたん設定専用のコマンド。
NTP サーバを 1 箇所設定する。**provider ntp server** コマンドでは接続先毎の IP アドレス情報を設定し、本コマンドでは 1 箇所の IP アドレスまたは FQDN を設定する。

【ノート】 コンソールなどから手動設定した場合の動作は保証されない。

16.12 http サーバ機能の有無の設定

[書式] **httpd service switch**

[設定値] ◦ *switch* スイッチ

- **on** http サーバ機能を有効にする
- **off** http サーバ機能を無効にする

[説明] http サーバを有効にするか否かを選択する。

[ノート] 変更した設定値は再起動しなければ動作に反映されない。

[初期値] **on**

16.13 http サーバ機能の listen ポートの設定

[書式] **httpd listen** *port*

[設定値] ◦*port*ポート番号 (1..65535)

[説明] http サーバの待ち受けるポートを設定する。

[ノート] 変更した設定値は再起動しなければ動作に反映されない。

[初期値] 80

16.14 http サーバへアクセスできるホストの IP アドレス設定

[書式] **httpd host host**

[設定値] ◦ *host*

- **any** すべてのホストからのアクセスを許可する
- **lan** LAN インタフェースと WAN インタフェースに属するネットワーク内ならば許可する
- **lan1** LAN インタフェースに属するネットワーク内ならば許可する
- **lan2** WAN インタフェースに属するネットワーク内ならば許可する
- **none** すべてのホストからのアクセスを禁止する
- **http** サーバへアクセスを許可するホストの IP アドレス
- **http** サーバへアクセスを許可するホストの IP アドレス範囲 (*ip_address-ip_address*)

[説明] http サーバへのアクセスを許可するホストを設定します。

[ノート] **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 **limited 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。

[初期値] **lan**

16.15 HTML フレームの使用許可の設定

[書式] **httpd frame use** *use* [*type*]

[設定値] ◦ *use* フレームの使用可否

- *on* 使用する
- *off* 使用しない

◦ *type* フレームを使用した表示形式を選択 (1..21474836)

[説明] *かんたん*設定専用の識別コマンド。

*かんたん*設定で、HTML の表示方法としてフレームを使用するか設定する。

[初期値] *off*

16.16 かんたん設定ページで IPv6 接続を行うか否かの設定

[書式] **provider ipv6 connect pp connect**

[設定値] ◦ *connect*

- off接続する
- on.....接続しない

[説明] プロバイダ情報として IPv6 接続を有効にする場合は on にする。

[ノート] かんたん設定ページで IPv6 接続設定をした時に自動的に on になる。

[初期値] off

16.17 電話アドレスの設定

[書式] **provider netvolante-dns hostname sip name**

[設定値] ◦ *name*電話アドレス

[説明] 電話アドレスを設定する。

[ノート] かんたん設定専用の識別コマンドである。

[初期値] なし

16.18 LAN 側 DNS サーバアドレスの設定コマンド

[書式] **provider *lan_if* dns server *ip_address* [*ip_address*]**

[設定値] ◦ *lan_if*

- *lan1* LAN インタフェース
- *lan2* WAN インタフェース

◦ *ip_address*

- IP アドレス DNS サーバの IP アドレス
- *clear* 設定しない

[説明] プロバイダ情報として LAN 側の DNS サーバアドレスを設定する。

DNS サーバは 2 つまで設定できる。

イーサネット接続を含んだ複数プロバイダの設定をするときに、かんたん設定でのみ使用するコマンド。

[初期値] *clear*

17. PPTP 機能の設定

本機能を使用するためには、Microsoft 社の Windows95 や Windows98 などの「Microsoft(R) VPN Adaptor/ マイクロソフト (R) 仮想プライベートネットワーク」が必要となります。

17.1 共通の設定

17.1.1 トンネルインタフェースの種別の選択

[書式] **tunnel encapsulation type**

[設定値] ◦ *type*

- **ipip**.....IP over IP トンネル
- **pptp**PPTP トンネル

[説明] トンネルインタフェースの種別を選択する。

[初期値] **ipip**

17.1.2 相手先情報番号にバインドされるトンネルインタフェースの設定

[書式] **pp bind tunnel** *tunnel_num* [*tunnel_num* ...]

[設定値] ◦ *tunnel_num*

- トンネルインタフェース番号 (1..4)
- none.....選択しない

[説明] 選択されている相手先情報番号にバインドされるトンネルインタフェースを指定する。

[初期値] none

17.1.3 PPTP の動作タイプの設定

[書式] **pptp service type** *type*

[設定値] ◦ *type*

- server.....サーバとして動作
- client.....クライアントとして動作

[説明] PPTP サーバとして動作するか、PPTP クライアントとして動作するかを設定する。

[初期値] server

17.1.4 PPTP ホスト名の設定

[書式] **pptp hostname** *name*

[設定値] ◦ *name*ホスト名

[説明] PPTP ホスト名を設定する。

17.1.5 PPTP ホスト名の削除

[書式] **pptp clear hostname**

[設定値] なし

[説明] PPTP ホスト名を削除する。

17.1.6 PPTP パケットのウィンドウサイズの設定

[書式] **pptp window size** *size*

[設定値] ◦ *size*.....パケットサイズ (1..128)

[説明] 受信済みで無応答の PPTP パケットをバッファに入れることができるパケットの最大数を設定する。

[初期値] 32

17.1.7 PPTP の動作モードの設定

[書式] **pptp call-id mode** *mode*

[設定値] ◦ *mode*

- **normal**..... 通常モード
- **backward-compatibility**.Rev.4.06.16 互換モード

[説明] PPTP の動作モードを設定する。
接続相手が Rev.4.06.16 の場合にのみ、動作モードを **backward-compatibility**にする。

[初期値] normal

17.2 リモートアクセス VPN 機能

17.2.1 PPTP トンネルの切断タイマの設定

[書式] **pptp tunnel disconnect time** *time*

[設定値] ◦ *time*切断タイマの秒数 (1..21474836)

[説明] 選択されている PPTP トンネルに対して、データパケット無入力・無送信時に、タイムアウトにより PPTP トンネルを切断する時間を設定する。

[初期値] 60

17.2.2 PPTP トンネルの端点の名前の設定

[書式] **tunnel endpoint name** [*local_name*] *remote_name*

[設定値] ◦ *local_name*自分側端点

◦ *remote_name*相手側端点

[説明] トンネル端点の名前を指定する。

17.2.3 PPTP トンネルの端点の名前の削除

〔書式〕 **tunnel endpoint clear name**

〔設定値〕 なし

〔説明〕 トンネル端点の名前を削除する。

17.2.4 PPTP キープアライブの設定

〔書式〕 **pptp keepalive use use**

〔設定値〕 ◦ *use*

- **on**.....使用する
- **off**使用しない

〔説明〕 トンネルキープアライブを使用するか否かを選択する。

〔初期値〕 off

17.2.5 PPTP キープアライブのログ設定

[書式] **pptp keepalive log** *log*

[設定値] ◦ *log*

- on.....ログにとる
- offログにとらない

[説明] トンネルキープアライブをログに取るかどうか選択する。

[初期値] off

17.2.6 PPTP キープアライブを出すインターバルとカウントの設定

[書式] **pptp keepalive interval** *interval* [*count*]

[設定値] ◦ *interval*.....インターバル (1..65535)

◦ *count*カウント (3..100)

[説明] トンネルキープアライブを出すインターバルとダウン検出用のカウントを設定する。

[初期値] 30 6

17.2.7 PPTP 接続において暗号化の有無により接続を許可するか否かの設定

[書式] **ppp ccp no-encryption mode**

[設定値] ◦ *mode*

- **reject** 暗号化なしでは接続拒否
- **accept**..... 暗号化なしでも接続許可

[説明] MPPE の暗号化がネゴシエーションされないときの動作を設定する。

[初期値] **accept**

18. ネットボランチ DNS サービスの設定

18.1 ネットボランチ DNS サービスの使用の可否

[書式] **netvolante-dns use** *lan_if* *switch*
netvolante-dns use pp *peer_num* *switch*

[設定値] ◦ *lan_if*

- *lan1* LAN インタフェース
- *lan2* WAN インタフェース

◦ *peer_num* PP インタフェース番号 (1..30)

◦ *switch*

- *auto* 自動更新する
- *off* 自動更新しない

[説明] ネットボランチ DNS サービスを使用するか否かを設定する。
IP アドレスが更新された時にネットボランチ DNS サーバに自動で IP アドレスを更新する。

[初期値] off

18.2 ネットボランチ DNS サーバに手動で更新する

[書式] **netvolante-dns go** *lan_if*
netvolante-dns go pp *peer_num*

[設定値] ◦ *lan_if*

- **lan1** LAN インタフェース
- **lan2** WAN インタフェース

◦ *peer_num* PP インタフェース番号 (1..30)

[説明] ネットボランチ DNS サーバに手動で IP アドレスを更新する。

18.3 ネットボランチ DNS サーバから削除する

[書式] **netvolante-dns delete go** *lan_if* [*host*]
netvolante-dns delete go pp *peer_num* [*host*]

- [設定値] ◦ *lan_if*
- **lan1** LAN インタフェース
 - **lan2** WAN インタフェース
 - **peer_num** PP インタフェース番号 (1..30)
 - **host**..... ホスト名

[説明] ネットボランチ DNS サーバから削除する。
インタフェースの後にホスト名を指定することで、指定したホスト名のみを削除可能。

18.4 ネットボランチ DNS サーバに登録済みのホスト名一覧を取得

[書式] **netvolante-dns get hostname list** *lan_if*
netvolante-dns get hostname list pp *peer_num*

- [設定値] ◦ *lan_if*
- **lan1** LAN インタフェース
 - **lan2** WAN インタフェース
 - **all** すべてのインタフェース
- *peer_num* PP インタフェース番号 (1..30)

[説明] ネットボランチ DNS サーバに登録済みのホスト名一覧を取得し、表示する。

18.5 ホスト名の登録

[書式] **netvolante-dns hostname host** *lan_if host* [duplicate]
netvolante-dns hostname host pp *peer_num host* [duplicate]

- [設定値]
- *lan_if*
 - *lan1* LAN インタフェース
 - *lan2* WAN インタフェース
 - *peer_num* PP インタフェース番号 (1..30)
 - *host*..... ホスト名
 - **duplicate**

[説明] ネットボランチ DNS サービス (ホストアドレスサービス) で使用するホスト名を登録する。**duplicate** を付加すると、異なるインタフェースで登録済みのホストアドレスと同じアドレスを登録できるようになる。

[初期値] なし

18.6 インターネット電話用ホスト名の使用の可否

[書式] **netvolante-dns sip use** *lan_if switch* [duplicate]
netvolante-dns sip use pp *peer_num switch* [duplicate]

- [設定値]
- *lan_if*
 - **lan1** LAN インタフェース
 - **lan2** WAN インタフェース
 - *peer_num* PP インタフェース番号 (1..30)
 - *switch*
 - **on** 使用する
 - **off** 使用しない
 - **duplicate**

[説明] ネットボランチ DNS サービス（電話アドレスサービス）で使用する電話アドレスを使用するか否かを設定する。
duplicate を付加すると、異なるインタフェースで登録済みの電話アドレスと同じアドレスを登録できるようになる。

[初期値] off

18.7 通信タイムアウトの設定

[書式] **netvolante-dns timeout** *lan_if time*
netvolante-dns timeout pp *peer_num*

[設定値] ◦ *lan_if*

- *lan1* LAN インタフェース
- *lan2* WAN インタフェース

◦ *peer_num* PP インタフェース番号 (1..30)

◦ *time* タイムアウト秒数 (1..180)

[説明] 通信タイムアウトを設定する。

[初期値] 30

18.8 ネットボランチ DNS サービスで使用するポート番号の設定

[書式] **netvolante-dns port** *port*

[設定値] ◦ *port* ポート番号

[説明] ネットボランチ DNS サービスで使用するポート番号を設定する。

[初期値] 2002

18.9 ネットボランチ DNS サーバの設定

[書式] **netvolante-dns server** *ip_address*
netvolante-dns server *name*

[設定値] ◦ *ip_address*IP アドレス
◦ *name*ドメイン名

[説明] ネットボランチ DNS サーバの IP アドレスまたはホスト名を設定する。

[初期値] netvolante-dns.netvolante.jp

19. UPnP の設定

19.1 UPnP を使用するか否かの設定

[書式] **upnp use** *use*

[設定値] ◦ *use*

- **on**.....使用する
- **off**使用しない

[説明] UPnP 機能を使用するか否かを設定する。

[初期値] on

19.2 UPnP に使用する IP アドレスを取得するインタフェースの設定

[書式] **upnp external address refer** *lan_if*
upnp external address refer pp *peer_num*

[設定値] *lan_if*

- **lan1** LAN インタフェース
- **lan2** WAN インタフェース
- **default** デフォルトルートのインタフェース

◦ *peer_num*

- 相手先情報番号 (1..30)
- **anonymous** ...PP インタフェース (anonymous)

[説明] UPnP に使用する IP アドレスを取得するインタフェースを設定する。

[初期値] default

19.3 UPnP のポートマッピングの消去タイマの設定

[書式] **upnp port mapping timer** *time*

[設定値] *time*

- 秒数 (600..21474836)
- off消去しない

[説明] UPnP によって生成されたポートマッピングを消去するまでの時間を設定する。

[初期値] 172800

20. 操作

20.1 相手先情報番号の選択

[書式] **pp select** *peer_num*

[設定値] ◦ *peer_num*

- 相手先情報番号 (1..30)
- **none**.....相手を選択しない
- **anonymous**...番号が不明である相手の設定

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

[ノート] 本操作コマンドは一般ユーザでも実行できる。

20.2 トンネルインタフェース番号の選択

〔書式〕 **tunnel select** *tunnel_num*

〔設定値〕 ◦ *tunnel_num*

- トンネルインタフェース番号 (1..4)
- none.....選択しない

〔説明〕 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、トンネルインタフェース番号が表示される。
none を設定すると、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〕 本操作コマンドは一般ユーザでも実行できる。

20.3 設定に関する操作

20.3.1 管理ユーザへの移行

〔書式〕 **administrator**

〔設定値〕 なし

〔説明〕 本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。

20.3.2 設定内容の保存

[書式] **save**

[設定値] なし

[説明] 現在の設定内容を不揮発性メモリに保存する。

20.3.3 終了

[書式] **quit** [save]

exit [save]

[設定値] ◦ **save**..... 管理ユーザから抜ける場合に **save** を設定すると、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。

20.3.4 相手先の初期化

[書式] **pp default** *peer_num*

[設定値] ◦ *peer_num*

- 相手先情報番号 (1..30)
- **anonymous**

[説明] 指定した相手先の設定を初期値に戻す。

20.3.5 トンネルインタフェースの初期化

[書式] **tunnel default** *tunnel_num*

[設定値] ◦ *tunnel_num*

- トンネルインタフェース番号 (1..4)
- **all** すべてのトンネルインタフェース

[説明] 指定したトンネルインタフェースの設定を初期値に戻す。

20.3.6 相手先毎の設定の複写

〔書式〕 **pp copy** *peer_num1* *peer_num2*

〔設定値〕 ◦*peer_num1*, *peer_num2*

- 相手先情報番号 (1..30)
- **anonymous**

〔説明〕 *peer_num1* の設定内容を *peer_num2* 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。

20.3.7 設定の初期化

〔書式〕 **cold start**

〔設定値〕 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。

20.4 動的情報のクリア操作

20.4.1 ARP テーブルのクリア

[書式] **clear arp**

[設定値] なし

[説明] ARP テーブルをクリアする。

20.4.2 IP の動的経路情報のクリア

[書式] **clear ip dynamic routing**

[設定値] なし

[説明] 動的に設定された IP の経路情報をクリアする。

20.4.3 IPv6 の動的経路情報のクリア

[書式] **clear ipv6 dynamic routing**

[設定値] なし

[説明] 経路制御プロトコルが得た IPv6 の経路情報をクリアする。

20.4.4 近隣キャッシュのクリア

[書式] **clear ipv6 neighbor cache**

[設定値] なし

[説明] 近隣キャッシュをクリアする。

20.4.5 NAT アドレステーブルのクリア

[書式] **clear nat descriptor dynamic *nat_descriptor***

[設定値] ◦ *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。

[初期値] **all**

20.4.6 各インタフェースの NAT アドレステーブルのクリア

[書式] **clear nat descriptor interface dynamic** *lan_if*
clear nat descriptor interface dynamic *pp peer_num*
clear nat descriptor interface dynamic *tunnel*

- [設定値]
- *lan_if*
 - *lan1* LAN インタフェース
 - *lan2* WAN インタフェース
 - *peer_num*
 - 相手先情報番号 (1..30)
 - *anonymous* ... 電話番号が不明である相手の設定
 - *tunnel*..... トンネルインタフェース番号 (1..4)

[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。

20.4.7 ログのクリア

[書式] **clear log**

[設定値] なし

[説明] ログをクリアする。

20.4.8 アナログポートに関するアカウントのクリア

[書式] **clear analog account** [*port*]

[設定値] ◦ *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、すべてのアナログポートのアカウントがクリアされる。

20.4.9 DNS キャッシュのクリア

[書式] **clear dns cache**

[設定値] 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。

20.5 スケジュール

20.5.1 スケジュールの設定

[書式] **schedule at** *[date] time peer_num command*

[設定値] ◦ *date*日付省略可

- 月 / 日
- 省略時は */* 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

◦ *time*時刻

- 時 (0..23 または *) : 分 (0..59 または *)
- *startup*起動時

◦ *peer_num*

- 相手先情報番号
- *anonymous*
- *peer_num* 省略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_num* を指定する必要が無い場合)

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

◦ *command*実行するコマンド制限あり

[説明] *time* パラメータで指定した時刻に *peer_num* パラメータで指定した相手先に *command* パラメータを実行する。

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**、**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場合には、何を実行しようとしたかを INFO タイプの SYSLOG に出力する。*date* に数字と曜日を混在させて指定はできない。**startup** を指定したスケジュールはルータ起動時に実行される。電源を入れたらすぐ発信したい場合などに便利。

[設定例] 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
```


20.5.2 スケジュールの削除

〔書式〕 **schedule delete** *schedule_num*

〔設定値〕 ◦ *schedule_num*.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。

20.5.3 スケジュールの確認

〔書式〕 **show schedule**

〔設定値〕 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。

20.6 本体に関する設定

20.6.1 アナログポート通信の接続・切断時のアラーム音の設定

[書式] **alarm connection analog switch**

[設定値] ◦ *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。

[初期値] off

20.6.2 データ通信の接続・切断・異常切断時のアラーム音の設定

[書式] **alarm connection data switch**

[設定値] ◦ *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。

[初期値] on

20.6.3 侵入検知に関するブザーの設定

[書式] **alarm intrusion switch**

[設定値] ◦ *switch*

- on.....鳴らす
- off鳴らさない

[説明] 侵入を検知したときにブザーを鳴らすかどうかを設定する。

[初期値] on

20.6.4 アラーム音の制御

[書式] **alarm entire switch**

[設定値] ◦ *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 intrusion** 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。

[初期値] on

20.7 その他の操作

20.7.1 常時接続の設定

[書式] **pp always-on switch** [*time*]

[設定値] ◦ *switch*

- **on**.....常時接続する
- **off**常時接続しない

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

[説明] 選択されている相手について常時接続するか否かを設定する。

また、常時接続での通信終了時に再接続を要求するまでの時間間隔を指定する。

常時接続に設定されている場合には、起動時に接続を起動し、通信終了時には再接続を起動し、キープアライブ機能により接続相手のダウン検出を行う。

接続失敗時あるいは通信の異常終了時には、*time* パラメータで設定した時間間隔を待った後に再接続の要求を行い、正常な通信終了時には直ちに再接続の要求を行う。

switch パラメータを **on** に設定している場合には、*time* パラメータの設定が有効となる。

time パラメータが設定されていない場合には、**60** に設定される。

[ノート] 相手先として **anonymous** が選択された場合には無効である。

[初期値] **off**

20.7.2 キープアライブの時間間隔の設定

[書式] **pp keepalive interval interval [count]**

- [設定値] ◦ *interval* [PPP,LCP] の echo-request を送出する時間間隔 (1..65535)
◦ *count* 応答が設定した回数連続してない場合、相手側のルータをダウンしたと判定 (3..100)

[説明] 選択されている相手について [PPP,LCP] の echo-request の送出間隔とダウン検出を判定する回数を設定する。

- [ノート] 一度 [PPP,LCP] の echo-request に対する応答が返ってこない事を検出した場合、その後の監視タイマは 1 秒に短縮される。
相手先としてとして anonymous が選択された場合には無効である。

[初期値] *interval* = 30
count = 6

20.7.3 相手先の使用許可の設定

〔書式〕 **pp enable** *peer_num*

〔設定値〕 ◦*peer_num*

- 相手先情報番号 (1..30)
- **anonymous**
- **all**

〔説明〕 相手先を使用できる状態にする。

工場出荷時、すべての相手先は **disable** 状態なので、使用する場合は必ず本コマンドで **enable** 状態にしなければならない。

20.7.4 相手先の使用不許可の設定

〔書式〕 **pp disable** *peer_num*

〔設定値〕 ◦*peer_num*

- 相手先情報番号 (1..30)
- **anonymous**
- **all**

〔説明〕 相手先を使用できない状態にする。

相手先の設定を行う場合は **disable** 状態であることが望ましい。

20.7.5 再起動

〔書式〕 **restart**

〔設定値〕 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。

20.7.6 発信

〔書式〕 **connect** *peer_num*

〔設定値〕 ◦*peer_num*発信相手の相手先情報番号 (1..30)

〔説明〕 手動で発信する。

20.7.7 切断

[書式] **disconnect** *peer_num*

[設定値] ◦ *peer_num*

- 切断する相手先情報番号 (1..30)
- **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。

20.7.8 ping

[書式] **ping** *host* [*count*]

[設定値] ◦ *host*

- ping をかけるホストの IP アドレス (*xxx.xxx.xxx.xxx* (*xxx* は 10 進数))
- ping をかけるホストの名称

◦ *count*

- 実行回数 (1..21474836)
- **infinity**..... Ctrl+C を入力するまで繰り返す

[説明] ICMP ECHO 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。

20.7.9 traceroute

【書式】 **traceroute** *host* [noresolv]

【設定値】 ◦ *host*

- traceroute をかけるホストの IP アドレス (xxx.xxx.xxx.xxx (xxx は 10 進数))
- traceroute をかけるホストの名称

【説明】 指定したホストまでの経路を調べて表示する。noresolv キーワードを指定した場合には、DNS による解決を行わない。

20.7.10 telnet

[書式] **telnet** *host* [*port* [*mode* [*negotiation* [*abort*]]]]

- [設定値]
- *host*..... TELNET をかける相手のホスト名、もしくは IP アドレス
 - *port*..... 使用するポート番号
 - 10 進数
 - ポート番号の二ーモニック
 - 省略時は 23(TELNET)
 - *mode*..... telnet 通信 (送信) の動作モード (省略時は **auto**)
 - **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
 - *negotiation*..... telnet オプションのネゴシエーションの選択 (省略時は **auto**)
 - **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
 - *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 (省略時は 29(^))
 - 10 進数の ASCII コード

[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。

[初期値] *port* = 23

mode = auto

negotiation = auto

abort = 29 (^)

20.7.11 telnet サーバ機能の ON/OFF の設定

[書式] **telnetd service service**

[設定値] ◦ *service*

- **on**.....telnet サーバ機能を有効にする
- **off**telnet サーバ機能を停止する

[説明] telnet サーバ機能の利用を選択する。

[ノート] 変更した設定値は再起動しなければ動作に反映されない。
telnet サーバが停止している場合、telnet サーバはアクセス要求に一切応答しない。

[初期値] on

20.7.12 telnet サーバ機能の listen ポートの設定

[書式] **telnetd listen** *port*

[設定値] ◦*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] 変更した設定値は再起動しなければ動作に反映されない。
telnetd は、TCP の 23 番ポートで待ち受けしているが、本コマンドにより待ち受けポートを変更することができる。
ただし、待ち受けポートを変更した場合には、ポート番号が変更されても、telnet オプションのネゴシエーションが行える telnet クライアントを用いる必要がある。

[初期値] 23

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

[書式] **telnetd host ip_range [ip_range...]**

[設定値] ◦ *ip_range*

- telnet サーバへアクセスを許可するホストの IP アドレス範囲のリストまたはニーモニック
- 1 個の IP アドレスまたは間にマイナス (-) をはさんだ IP アドレス (範囲指定)、及びこれらを任意に並べたもの
- **any** すべてのホストからのアクセスを許可する
- **lan** LAN インタフェースと WAN インタフェースに属するネットワーク内ならば許可する
- **lan1** LAN インタフェースに属するネットワーク内ならば許可する
- **lan2** WAN インタフェースに属するネットワーク内ならば許可する
- **none** すべてのホストからのアクセスを禁止する

[説明] telnet サーバへアクセスできるホストの IP アドレスを設定する。

[ノート] ニーモニックをリストにすることはできない。

lan の場合、**primary** および **secondary** が **clear** では無く、ネットワークアドレスと directed broadcast address を除くホストアドレスからのリクエストを許可する。
設定後の新しい telnet 接続から適用される。

[初期値] **any**

21. 設定の表示

21.1 機器設定の表示

21.1.1 機器設定の表示

[書式] **show environment**

[設定値] なし

[説明] 以下の項目内容が表示される。

- 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**
- **login timer**
- **console character**
- **console columns**
- **console lines**
- **console info**
- **account threshold**

21.1.2 SYSLOG 関連の表示

[書式] **show syslog**

[設定値] なし

[説明] 以下の項目内容が表示される。

- **syslog host**
- **syslog facility**
- 出力する SYSLOG のタイプ

21.1.3 TFTP 関連の表示

[書式] **show tftp**

[設定値] なし

[説明] 以下の項目内容が表示される。

- **tftp host**

21.1.4 すべての設定内容の表示

[書式] **show config**
less config

[設定値] 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、初期値以外に設定されたすべての設定内容を表示する。

21.1.5 指定した PP の設定内容の表示

[書式] **show config pp** [*peer_num*]
less config pp [*peer_num*]

[設定値] ◦ *peer_num* (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 (1..30)
• anonymous

[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。

21.1.6 PP 毎の設定内容の表示

[書式] **show pp config** [*peer_num*]

[設定値] ◦*peer_num* (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 (1..30)
- **anonymous**

[説明] 以下の項目内容が表示される。

- **pp account threshold**
- **pp encapsulation**

21.1.7 PP 毎のキューの表示

[書式] **show pp queue** [*peer_num*]

[設定値] ◦*peer_num* (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 (1..30)
- **anonymous**

[説明] 選択した相手に対して、キューの設定および状態を表示する。

21.2 IP 関連の表示

21.2.1 IP パケットの静的フィルタの一覧表示

[書式] **show ip filter list**

[設定値] なし

[説明] IP パケットの静的フィルタの一覧を表示する。

21.2.2 IP パケットの静的フィルタの表示

[書式] **show ip filter *filter_num***

[設定値] ◦*filter_num*.....静的フィルタ番号 (1..2147483647)

[説明] パラメータで指定した番号の IP パケットの静的フィルタの内容を表示する。

21.2.3 動的フィルタによって管理されているコネクションの表示

[書式] **show ip connection** *lan_if* [*direction*]
show ip connection pp *peer_num* [*direction*]

- [設定値] ◦ *lan_if*
- *lan1* LAN インタフェース
 - *lan2* WAN インタフェース
- *peer_num* 相手先情報番号 (1..30)
- *direction*..... 方向
- *in*..... インタフェース側から内側へ
 - *out*..... インタフェース側から外側へ

[説明] 指定したインタフェースについて、動的なフィルタによって管理されているコネクションを表示する。インタフェース名以降省略した場合には、すべてのインタフェースの情報について表示する。

21.2.4 侵入情報の履歴の表示

[書式] **show ip intrusion detection** *lan_if* [*direction*]
show ip intrusion detection *pp peer_num* [*direction*]

- [設定値]
- *lan_if*
 - *lan1* LAN インタフェース
 - *lan2* WAN インタフェース
 - *peer_num* 相手先情報番号 (1..30)
 - *direction* 方向
 - *in* インタフェース側から内側へ
 - *out* インタフェース側から外側へ

[説明] 最近の侵入情報を表示する。各インタフェースの各方向ごとに最大 50 件まで表示できる。インタフェース名以降省略した場合には、すべてのインタフェースの情報について表示する。

21.2.5 LAN 側 IP 設定の表示

[書式] **show ip lan_if**

[設定値] ◦lan_if

- lan1LAN インタフェース
- lan2WAN インタフェース

[説明] 以下の項目内容が表示される。

- ip routing**
- ip lan_if address**
- ip lan_if netmask**
- ip lan_if broadcast**
- ip lan_if proxyarp**
- ip lan_if secure filter**
- ip filter source-route**
- ip lan_if routing protocol**

ip lan_if routing protocol コマンドで **rip** が設定されている場合には、さらに以下の項目内容が表示される。

- ip lan_if rip filter**
- ip lan_if rip listen**

21.2.6 PP 側 IP 設定の表示

[書式] **show ip pp** [*peer_num*]

[設定値] ◦*peer_num*(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 (1..30)
- anonymous

[説明] 以下の項目内容が表示される。

- **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 コマンドで **rip** が設定されている場合には、さらに以下の項目内容が表示される。

- **ip pp rip connect send**
- **ip pp rip disconnect send**
- **ip pp rip disconnect interval...ip pp rip disconnect send** コマンドで **interval** が設定されている場合のみ表示される。
- **ip pp rip filter**
- **ip pp rip listen**

- **ip pp rip hop**
- **ip pp hold routing**

[ノート] IP アドレスは、ネゴシエーションで決定されたアドレスと、**ip pp local address**、**ip pp remote address** コマンドで設定したアドレスの両方を表示する。後者は小括弧で示される。

21.3 静的 DNS レコードの表示

[書式] **show ip host**
show dns static

[設定値] なし

[説明] 静的な DNS レコードを表示する。

21.4 PPP の設定の表示

21.4.1 認証関連の設定の表示

[書式] **show auth** [*peer_num*]

[設定値] ◦ *peer_num* (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 (1..30)
- **anonymous**

[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。

21.4.2 LCP 関連の設定の表示

[書式] **show ppp lcp** [*peer_num*]

[設定値] ◦*peer_num* (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 (1..30)
- anonymous

[説明] 以下の項目内容が表示される。

- **ppp lcp magicnumber**
- **ppp lcp mru**
- **ppp lcp authreq**
- **ppp lcp pap accept**
- **ppp lcp chap accept**

以下は共通に表示される。

- **ppp lcp restart**
- **ppp lcp maxconfigure**
- **ppp lcp maxterminate**
- **ppp lcp maxfailure**

21.4.3 PAP 関連の設定の表示

[書式] **show ppp pap** [*peer_num*]

[設定値] ◦*peer_num* (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 (1..30)
- **anonymous**

[説明] 以下の項目内容が表示される。

- **ppp pap restart**
- **ppp pap maxauthreq**

[ノート] **ppp pap arrive only** コマンドで **on** に設定されている場合のみ、"PAPの要求" の後ろに "(着信のみ)" または "(arrive only)" と表示する。

21.4.4 CHAP 関連の設定の表示

[書式] **show ppp chap** [*peer_num*]

[設定値] ◦*peer_num* (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 (1..30)
- **anonymous**

[説明] 以下の項目内容が表示される。

- **ppp chap restart**
- **ppp chap maxchallenge**

[ノート] **ppp chap arrive only** コマンドで **on** に設定されている場合のみ、"CHAPの要求"の後ろに "(着信のみ)" または "(arrive only)" と表示する。

21.4.5 IPCP 関連の設定の表示

[書式] **show ppp ipcp** [*peer_num*]

[設定値] ◦*peer_num* (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 (1..30)
- anonymous

[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**

以下の項目内容が表示される。

- **ppp ipcp restart**
- **ppp ipcp maxconfigure**
- **ppp ipcp maxterminate**
- **ppp ipcp maxfailure**

21.4.6 MSCBCP 関連の設定の表示

[書式] **show ppp mscbcp** [*peer_num*]

[設定値] ◦ *peer_num* (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 (1..30)
- **anonymous**

[説明] 以下の項目内容が表示される。

- **ppp mscbcp restart**
- **ppp mscbcp maxretry**

21.4.7 CCP 関連の設定の表示

[書式] **show ppp ccp** [*peer_num*]

[設定値] ◦*peer_num* (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 (1..30)
- anonymous

[説明] 以下の項目内容が表示される。

- **ppp ccp type**
- **ppp ccp restart**
- **ppp ccp maxconfigure**
- **ppp ccp maxterminate**
- **ppp ccp maxfailure**

21.5 DHCP 関連の表示

21.5.1 DHCP スコープの表示

[書式] **show dhcp** [scope [scope_num]]

[設定値] ◦ *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 と入力した場合にはすべてが表示される。**show dhcp scope** と入力した場合には全スコープの情報が表示される。**show dhcp scope scope_num** と入力した場合に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、以下の項目内容が表示される。

- 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、以下の項目内容が表示される。

- 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

21.5.2 DHCP サーバの状態の表示

[書式] **show dhcp status**

[設定値] なし

[説明] 各 DHCP スコープのリース状況を表示する。以下の項目内容が表示される。

- 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)

21.5.3 DHCP クライアントの状態の表示

[書式] **show dhcpc status**

[設定値] なし

[説明] 各 DHCP クライアントの状態を表示する。

ip lan_if address コマンド、**ip lan_if secondary address** コマンドで **dhcp** を指定して DNS サーバアドレスやゲートウェイアドレスを取得した場合は、それらも表示する。

◦各クライアントの状態

- インタフェース
- IP アドレス (取得できていない場合には、その状態)
- DHCP サーバ
- リース残時間
- クライアント ID
- ホスト名 (設定時)

◦共通情報

- DNS サーバ
- ゲートウェイ

21.6 NAT 関連の表示

21.6.1 設定した NAT ディスクリプタの設定の表示

[書式] **show nat descriptor config** *nat_descriptor*

[設定値] ◦ *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。

21.6.2 動作中の NAT ディスクリプタのアドレスマップの表示

[書式] **show nat descriptor address** [*nat_descriptor*]

[設定値] ◦ *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。

[初期値] all

21.6.3 動作中の NAT ディスクリプタの適用リストの表示

[書式] **show nat descriptor interface bind**

[設定値] 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。

21.6.4 各インタフェース毎に NAT のアドレスマップの表示

[書式] **show nat descriptor interface address *lan_if***
show nat descriptor interface address pp *peer_num*
show nat descriptor interface address tunnel *tunnel_num*

[設定値] ○ *lan_if*

- lan1 LAN インタフェース
- lan2 WAN インタフェース

○ *peer_num*

- 相手先情報番号 (1..30)
- anonymous

○ *tunnel_num*..... トンネルインタフェース番号 (1..4)

[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。

21.7 ICMP 関連の設定の表示

[書式] **show ip icmp**

[設定値] なし

[説明] 以下の項目内容が表示される。

- **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**

21.8 DNS 関連の設定の表示

[書式] **show dns**

[設定値] なし

[説明] DNS 関連の設定を表示する。

21.9 WINS 関連の設定の表示

[書式] **show wins**

[設定値] なし

[説明] WINS 関連の設定を表示する。

21.10 アナログ関連の設定の表示

21.10.1 アナログ関連の設定の表示

[書式] **show analog config** [*port*]

[設定値] ◦ *port*.....アナログポート (省略時はすべてのポートについて表示)

- 1TEL1 ポート
- 2TEL2 ポート
- 3TEL3 ポート

[説明] アナログ関連の設定を表示する。

21.10.2 機器間アナログ通話設定の表示

[書式] **show analog extension**

[設定値] なし

[説明] 機器間アナログ通話設定の内容を表示する。

- 機器間アナログ通話モード (単独動作 / アナログ親機 / アナログ子機)

アナログ親機モードにおいて以下の項目が表示される。

- analog extension machine-id によって設定されているアナログ親機 / 子機の一覧
- 現在アナログ親機に接続しているアナログ親機 / 子機の一覧

アナログ子機モードにおいて以下の項目が表示される。

- 現在設定されているアナログ親機の情報
- **analog extension master** コマンドの設定内容、親機との接続状態、親機の IP アドレス

21.10.3 アナログ親機に登録された各アナログポート設定内容の表示

[書式] **show analog extension config**

[設定値] なし

[説明] 機器間アナログ通話機能でアナログ親機に登録された、各アナログポートの設定内容を表示する。

[ノート] 各アナログポートの設定内容は、機器間通信によってアナログ親機に登録される。
本コマンドでは、機器間通信によってアナログ親機に登録された各アナログポート設定の内容を表示する。

22. 状態の表示

22.1 ARP テーブルの表示

[書式] **show arp**

[設定値] なし

[説明] ARP テーブルを表示する。

22.2 LAN 側の状態の表示

[書式] **show status lan_if**

[設定値] ◦ *lan_if*

- lan1 LAN インタフェース
- lan2 WAN インタフェース

[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

22.3 各相手先の状態の表示

[書式] **show status pp** [*peer_num*]

[設定値] ◦ *peer_num* (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 (1..30)
- **anonymous**

[説明] 各相手先の接続中または最後に接続された場合の状態を表示する。

- 現在接続されているか否か
- 直前の呼の状態
- 接続 (切断) した日時
- 回線の種類
- 通信時間
- 切断理由
- 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

22.4 IP の経路情報テーブルの表示

[書式] **show ip route** [*destination*]

[設定値] ◦ *destination* (省略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。

22.5 IPv6 の経路情報テーブルの表示

[書式] **show ipv6 route**

[設定値] なし

[説明] IPv6 の経路情報を表示する。

22.6 インタフェースに付与されている IPv6 アドレスの表示

[書式] **show ipv6 address**

[設定値] なし

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

22.7 近隣キャッシュの表示

[書式] **show ipv6 neighbor cache**

[設定値] なし

[説明] 近隣キャッシュの状態を表示する。

22.8 IPv6 の RIP テーブルの表示

[書式] **show ipv6 rip table**

[設定値] なし

[説明] IPv6 の RIP テーブルを表示する。

22.9 IPv6 の動的フィルタによって管理されている接続の表示

[書式] **show ipv6 connection** [*interface* [*interface_number*] [*direction*]]

- [設定値]
- *interface* インタフェース
 - lan/lan1/lan2
 - pp
 - tunnel
 - *interface_number*.....PP/TUNNEL インタフェースの番号
 - *direction*
 - in.....入力方向
 - out.....出力方向

[説明] 指定したインタフェースについて、動的なフィルタによって管理されている接続を表示する。インタフェースを指定しないときには、すべてのインタフェースの情報を表示する。

22.10 アナログ関係の状態の表示

[書式] **show status analog** [*port*]

[設定値] ◦*port*.....アナログポート (省略時はすべてのアナログポートを表示)

- 1TEL1 ポート
- 2TEL2 ポート
- 3TEL3 ポート

[説明] アナログ関係の状態を表示する。

22.11 ネットボランチ DNS の状態の表示

[書式] **show status netvolante-dns** *lan_if*
show status netvolante-dns pp *peer_num*

[設定値] ◦*lan_if*

- lan1LAN インタフェース
- lan2WAN インタフェース

◦*peer_num*PP インタフェース番号 (1..30)

[説明] ネットボランチ DNS の状態を表示する。

22.12 UPnP の状態の表示

[書式] **show status upnp**

[設定値] なし

[説明] UPnP に関する状態を表示する。

22.13 機器間アナログ通話機能の機器間の音声品質の表示

[書式] **show status rtp***[interface [port]]*

[設定値] ◦ *interface*

- pstn.....電話回線
- analog.....アナログポート
- *port*.....アナログポート (*interface* が analog の時のみ有効)
 - 1TEL1 ポート
 - 2TEL2 ポート
 - 3TEL3 ポート

[説明] 指定したインターフェースが機器間アナログ通話機能を使用していれば、そのインターフェースに関する音声品質の情報を表示する。パラメータを省略した場合は、すべてのインターフェースに関する情報を表示する。

22.14 SIP 端末のメンバ登録状況の表示

[書式] **show status sip presence**

[設定値] なし

[説明] Windows Messenger や、SIP プロトコルを使用する VoIP 端末のメンバ登録状況を表示する。

23. ログイン

23.1 ログの表示

〔書式〕 **show log**
less log

〔設定値〕 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

23.2 アナログ関係のアカウントの表示

[書式] **show analog account** [*port*]

[設定値] ◦*port*.....アナログポート（省略時はすべてのポートについて表示）

- 1TEL1 ポート
- 2TEL2 ポート
- 3TEL3 ポート

[説明] アナログポートの発着信回数を表示する。

23.3 相手先ごとの接続時間情報の表示

[書式] **show pp connect time** [*peer_num*]

[設定値] *peer_num*

- 相手先情報番号 (1..30)
- anonymous

[説明] 選択されている相手の接続時間情報を表示する。

23.4 通信履歴の表示

〔書式〕 **show history**

〔設定値〕 なし

〔説明〕 通信履歴を表示します。