P3NK-2192-01Z0

GeoStream Si-R シリーズ

コマンドリファレンス

V32

FUJITSU

はじめに

このたびは、本装置をお買い上げいただき、まことにありがとうございます。
インターネットやLANをさらに活用するために、本装置をご利用ください。

2006年 9月初版

本ドキュメントには「外国為替及び外国貿易管理法」に基づく特定技術が含まれています。
従って本ドキュメントを輸出または非居住者に提供するとき、同法に基づく許可が必要となります。
Microsoft Corporationのガイドラインに従って画面写真を使用しています。

All rights reserved, Copyright© 富士通株式会社 2006

本書の構成と使いかた

本書は、本装置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。
また、CD-ROMの中のREADMEファイルには大切な情報が記載されていますので、併せてお読みください。

本書の読者と前提知識

本書は、ネットワーク管理を行っている方を対象に記述しています。
本書を利用するにあたって、ネットワークおよびインターネットに関する基本的な知識が必要です。

本書の構成

本書の第1～19章では構成定義コマンドを、第20～61章では運用管理コマンドを、第62章ではその他のコマンド、63章以降は付録情報を説明しています。

マークについて

[機能]	コマンドの機能概要を記載しています。
[適用機種]	対象となる装置種別を記載しています。
[入力形式]	入力形式を記載しています。以下の規約に従って記載しています。 < > ：パラメタ名称を示しています。 [ ] ：括弧内のオプションやパラメタを省略できることを示しています。 { } ：括弧内のオプションやパラメタのうち、どれかを選択することを示しています。
[オプション]	各オプションの意味を記載しています。
[パラメタ]	各パラメタの意味を記載しています。
[動作モード]	コマンドを実行可能な動作モードを記載しています。
[説明]	コマンドの解説を記載しています。
[注意]	コマンドの注意事項を記載しています。
[メッセージ]	コマンドの応答またはエラーメッセージを記載しています。
[実行例]	コマンドの実行例を記載しています。
[未設定時]	コマンドの未設定時について説明し、設定したとみなされるコマンドを記載しています。

使用上の注意事項

構成定義コマンドを使用する場合は、以下の点にご注意ください。

- コマンドの設定および変更が終了したら、saveコマンドを実行してからcommitコマンドまたはresetコマンドを実行し、設定を有効にしてください。saveコマンドを実行せずresetコマンドまたは電源再投入を行った場合は、コマンドの設定が元の状態にもどります。また、saveコマンドを実行しないでcommitコマンドを実行した場合、一時的に設定は有効になりますが、resetコマンドまたは電源再投入を行った場合にコマンドの設定が元の状態に戻ります。ただし、password、terminalコマンドについては設定直後から有効となります。
- 構成定義コマンドを削除する場合は、deleteコマンドを使用します。削除した構成定義コマンドは、showコマンド（コマンド名未指定）を実行しても、構成定義コマンド文字列として表示されません。
  例. ログオンパスワードの削除

```
# delete password set
```

- show コマンドにより構成定義を表示する場合、コマンド未設定時の値と同じ物は表示されません。コマンド未設定時の値を表示したい場合は、show コマンドに続けて、表示したいパラメタの直前のコマンドまで入力します。
  例. LAN インタフェースの IP アドレスの表示

```
# show candidate-config lan 0 ip address
192.168.1.1/24 3
```

本文中で使用しているコマンドのパラメタに時間を指定する場合は、特別な指示がある場合を除き s（秒）、m（分）、h（時）、d（日）の単位をつけて設定します。
例：1m = 1 分
なお、60s、60m、24h を指定した場合は、それぞれ、1m、1h、1d を指定したものとみなされます。

本書における商標の表記について

Microsoft、Windows および Windows NT は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。

Hi/fn および LZS は、Hi/fn,inc. の登録商標です。

本書に記載されているその他の会社名および製品名は、各社の商標または登録商標です。

本装置のマニュアルの構成

本装置の取扱説明書は、以下のとおり構成されています。使用する目的に応じて、お使いください。

マニュアル名称	内容
Si-R 効率化運用ツール使用手引書	Si-R 効率化運用ツールを使用する方法を説明しています。
Si-R180　ご利用にあたって	Si-R180 の設置方法やソフトウェアのインストール方法を説明しています。
Si-R220B　ご利用にあたって	Si-R220B の設置方法やソフトウェアのインストール方法を説明しています。
Si-R240　ご利用にあたって	Si-R240 の設置方法やソフトウェアのインストール方法を説明しています。
Si-R260B　ご利用にあたって	Si-R260B の設置方法やソフトウェアのインストール方法を説明しています。
Si-R370　ご利用にあたって	Si-R370 の設置方法やソフトウェアのインストール方法を説明しています。
Si-R570　ご利用にあたって	Si-R570 の設置方法やソフトウェアのインストール方法を説明しています。
Si-R シリーズ　機能説明書	本装置の便利な機能について説明しています。
Si-R シリーズ　トラブルシューティング	トラブルが起きたときの原因と対処方法を説明しています。
Si-R シリーズ　メッセージ集	システムログ情報などのメッセージの詳細な情報を説明しています。
Si-R シリーズ　仕様一覧	本装置のハード／ソフトウェア仕様と MIB/Trap 一覧を説明しています。
Si-R シリーズ　コマンドユーザーズガイド	コマンドを使用して、時計などの基本的な設定またはメンテナンスについて説明しています。
Si-R シリーズ　コマンド設定事例集	コマンドを使用した、基本的な接続形態または機能の活用方法を説明しています。
Si-R シリーズ　コマンドリファレンス（本書）	コマンドの項目やパラメタの詳細な情報を説明しています。
Si-R シリーズ　Web ユーザーズガイド	Web 画面を使用して、時計などの基本的な設定またはメンテナンスについて説明しています。
Si-R シリーズ　Web 設定事例集	Web 画面を使用した、基本的な接続形態または機能の活用方法を説明しています。
Si-R シリーズ　Web リファレンス	Web 画面の項目の詳細な情報を説明しています。

目　次

第 1 章　パスワード 情報 30
1.1　パスワード 情報 31
1.1.1　password format 31
1.1.2　password set 33
1.1.3　password user set 34

第 2 章　WAN 情報の設定 35
2.1　回線共通情報 36
2.1.1　wan bind 36
2.1.2　wan line 38
2.2　ISDN 回線情報 40
2.2.1　wan isdn global 40
2.2.2　wan isdn number 41
2.2.3　wan isdn numbersend 43
2.2.4　wan isdn limit charge 45
2.2.5　wan isdn limit time 46
2.2.6　wan isdn accept 47
2.2.7　wan isdn autodial 48
2.2.8　wan isdn activation 49
2.3　専用線情報 51
2.3.1　wan hsd flagdetect 51
2.4　フレームリレー回線情報 52
2.4.1　wan fr lmi 52
2.4.2　wan fr fecn 53
2.4.3　wan fr becn 54
2.4.4　wan fr cllm 55
2.5　ATM 回線情報 56
2.5.1　wan atm vpi 56
2.5.2　wan atm rate 57
2.5.3　wan atm oam 59
2.6　データ通信カード 情報 60
2.6.1　wan cardmodem pin 60

第 3 章　ATM 情報の設定 61
3.1　ATM 情報 62
3.1.1　atm send clock 62

第 4 章　スイッチ情報の設定 64
4.1　スイッチ共通情報 65
4.1.1　switch use 65
4.1.2　switch tag transparent 66

4.1.3 switch age . . . 67
4.2 スイッチポート情報 . . . 68
4.2.1 switch port use . . . 68
4.2.2 switch port mode . . . 69
4.2.3 switch port duplex . . . 70
4.2.4 switch port mdi . . . 71
4.2.5 switch port flowctl . . . 72
4.2.6 switch port vlan tag . . . 73
4.2.7 switch port vlan untag . . . 74

第 5 章 LAN 情報の設定 . . . 75
5.1 lan 共通情報 . . . 76
5.1.1 lan bind . . . 76
5.1.2 lan mode . . . 78
5.1.3 lan mdi . . . 80
5.1.4 lan flowctl . . . 82
5.1.5 lan type . . . 83
5.1.6 lan mtu . . . 84
5.1.7 lan shaping . . . 85
5.2 LAN ポートバックアップ関連情報 . . . 87
5.2.1 lan backup bind . . . 87
5.2.2 lan backup mode . . . 89
5.3 LAN ポート閉塞関連情報 . . . 90
5.3.1 lan recovery . . . 90
5.4 IP 関連情報 . . . 92
5.4.1 lan ip address . . . 92
5.4.2 lan ip alias . . . 94
5.4.3 lan ip dhcp service . . . 96
5.4.4 lan ip dhcp info . . . 98
5.4.5 lan ip dhcp macauth use . . . 101
5.4.6 lan ip dhcp macauth db . . . 102
5.4.7 lan ip dhcp macauth aaa . . . 103
5.4.8 lan ip proxyarp . . . 104
5.4.9 lan ip localproxyarp . . . 105
5.4.10 lan ip route . . . 106
5.4.11 lan ip rip use . . . 109
5.4.12 lan ip rip filter act . . . 111
5.4.13 lan ip rip filter move . . . 113
5.4.14 lan ip rip filter route . . . 114
5.4.15 lan ip rip filter set metric . . . 116
5.4.16 lan ip ospf use . . . 117
5.4.17 lan ip ospf cost . . . 119
5.4.18 lan ip ospf hello . . . 120
5.4.19 lan ip ospf dead . . . 121
5.4.20 lan ip ospf retrans . . . 122
5.4.21 lan ip ospf delay . . . 123
5.4.22 lan ip ospf priority . . . 124
5.4.23 lan ip ospf auth type . . . 125
5.4.24 lan ip ospf auth textkey . . . 126
5.4.25 lan ip ospf auth md5key . . . 127

5.4.26 lan ip ospf passive . . . 128
5.4.27 lan ip vrf use . . . 129
5.4.28 lan ip vrf route . . . 130
5.4.29 lan ip nat mode . . . 132
5.4.30 lan ip nat static . . . 134
5.4.31 lan ip nat static default . . . 136
5.4.32 lan ip nat rule . . . 137
5.4.33 lan ip nat wellknown . . . 139
5.4.34 lan ip nat destination . . . 141
5.4.35 lan ip nat appli . . . 143
5.4.36 lan ip filter . . . 145
5.4.37 lan ip filter move . . . 151
5.4.38 lan ip filter default . . . 152
5.4.39 lan ip tos . . . 153
5.4.40 lan ip tos move . . . 157
5.4.41 lan ip priority . . . 158
5.4.42 lan ip in-policy . . . 163
5.4.43 lan ip in-policy move . . . 165
5.4.44 lan ip icmp redirect . . . 166
5.4.45 lan ip multicast mode . . . 167
5.4.46 lan ip multicast ttl threshold . . . 168
5.4.47 lan ip multicast pim preference . . . 169
5.4.48 lan ip multicast pim upstream type . . . 170
5.4.49 lan ip arp cycle . . . 171
5.4.50 lan ip arp static . . . 172
5.4.51 lan ip ids use . . . 174
5.5 IPv6 関連情報 . . . 175
5.5.1 lan ip6 use . . . 175
5.5.2 lan ip6 ifid . . . 176
5.5.3 lan ip6 address . . . 177
5.5.4 lan ip6 ra mode . . . 179
5.5.5 lan ip6 ra interval . . . 180
5.5.6 lan ip6 ra mtu . . . 181
5.5.7 lan ip6 ra reachabletime . . . 182
5.5.8 lan ip6 ra retranstimer . . . 183
5.5.9 lan ip6 ra curhoplimit . . . 184
5.5.10 lan ip6 ra flags . . . 185
5.5.11 lan ip6 route . . . 186
5.5.12 lan ip6 rip use . . . 189
5.5.13 lan ip6 rip site-local . . . 191
5.5.14 lan ip6 rip aggregate . . . 192
5.5.15 lan ip6 rip filter act . . . 193
5.5.16 lan ip6 rip filter move . . . 195
5.5.17 lan ip6 rip filter route . . . 196
5.5.18 lan ip6 rip filter set metric . . . 198
5.5.19 lan ip6 filter . . . 199
5.5.20 lan ip6 filter move . . . 205
5.5.21 lan ip6 filter default . . . 206
5.5.22 lan ip6 trafficclass . . . 207
5.5.23 lan ip6 trafficclass move . . . 211

5.5.24 lan ip6 priority . . . 212
5.5.25 lan ip6 in-policy . . . 216
5.5.26 lan ip6 in-policy move . . . 218
5.6 ブリッジ関連情報 . . . 219
5.6.1 lan bridge use . . . 219
5.6.2 lan bridge group . . . 220
5.6.3 lan bridge static . . . 221
5.6.4 lan bridge stp use . . . 222
5.6.5 lan bridge stp cost . . . 223
5.6.6 lan bridge stp priority . . . 225
5.6.7 lan bridge filter . . . 226
5.6.8 lan bridge filter move . . . 230
5.6.9 lan bridge priority . . . 231
5.7 VRRP 関連情報 . . . 233
5.7.1 lan vrrp use . . . 233
5.7.2 lan vrrp auth . . . 234
5.7.3 lan vrrp group id . . . 235
5.7.4 lan vrrp group ad . . . 237
5.7.5 lan vrrp group preempt . . . 238
5.7.6 lan vrrp group trigger ifdown . . . 240
5.7.7 lan vrrp group trigger route . . . 242
5.7.8 lan vrrp group trigger node . . . 244
5.7.9 lan vrrp group action . . . 247
5.7.10 lan vrrp group vaddr icmp . . . 252
5.8 MPLS 関連情報 . . . 254
5.8.1 lan mpls use . . . 254
5.8.2 lan mpls distribution . . . 255
5.8.3 lan mpls ldp hello-timers . . . 256
5.8.4 lan mpls ldp keepalive-timers . . . 257
5.8.5 lan mpls ldp advertisement . . . 258
5.8.6 lan mpls ldp retention . . . 259
5.8.7 lan mpls ldp interface-label . . . 260
5.8.8 lan mpls ldp ip transport . . . 261
5.8.9 lan mpls l2-circuit vc . . . 262
5.8.10 lan mpls l2-circuit exp . . . 265
5.9 VLAN 関連情報 . . . 266
5.9.1 lan vlan bind . . . 266
5.9.2 lan vlan tag vid . . . 268
5.9.3 lan vlan tag pri . . . 269
5.9.4 lan vlan tag primap . . . 270
5.10 MAC アドレス認証関連情報 . . . 272
5.10.1 lan macauth use . . . 272
5.10.2 lan macauth expire . . . 273
5.10.3 lan macauth aaa . . . 274
5.10.4 lan macauth security . . . 275

第 6 章　シリアル情報の設定 276
6.1　シリアル共通情報 277
6.1.1　serial use 277
6.1.2　serial speed 278
6.2　モデム関連情報 279
6.2.1　serial modem dial 279
6.2.2　serial modem tonedetect 280
6.2.3　serial modem speaker mode 281
6.2.4　serial modem speaker volume 282

第 7 章　相手情報の設定 283
7.1　相手共通情報 284
7.1.1　remote name 284
7.1.2　remote autodial 285
7.1.3　remote mtu 286
7.1.4　remote shaping 287
7.2　接続先情報 289
7.2.1　remote ap name 289
7.2.2　remote ap move 290
7.2.3　remote ap datalink type 291
7.2.4　remote ap datalink bind 293
7.2.5　remote ap recovery 295
7.2.6　remote ap ip dns 296
7.2.7　remote ap multiroute pattern 298
7.2.8　remote ap multiroute pattern move 301
7.2.9　remote ap limit charge 302
7.2.10　remote ap limit time 303
7.2.11　remote ap disconnect time 304
7.2.12　remote ap disconnect packet 305
7.2.13　remote ap ppp auth type 306
7.2.14　remote ap ppp auth send 307
7.2.15　remote ap ppp auth receive 309
7.2.16　remote ap ppp mp use 310
7.2.17　remote ap ppp mp bap use 311
7.2.18　remote ap pppoe acname 312
7.2.19　remote ap pppoe svname 313
7.2.20　remote ap dial number 314
7.2.21　remote ap dial speed 315
7.2.22　remote ap called accept 317
7.2.23　remote ap called clid 318
7.2.24　remote ap called number 319
7.2.25　remote ap connect priority 321
7.2.26　remote ap idle 322
7.2.27　remote ap step 323
7.2.28　remote ap step2 324
7.2.29　remote ap step3 325
7.2.30　remote ap keep 326
7.2.31　remote ap fr dlci 327
7.2.32　remote ap fr cir 328
7.2.33　remote ap atm vci 329

7.2.34 remote ap atm rate . . . 331
7.2.35 remote ap atm ast . . . 333
7.2.36 remote ap atm oam . . . 336
7.2.37 remote ap atm vcwatch . . . 337
7.2.38 remote ap ipsec type . . . 339
7.2.39 remote ap ipsec send spi . . . 341
7.2.40 remote ap ipsec send protocol . . . 342
7.2.41 remote ap ipsec send range . . . 344
7.2.42 remote ap ipsec send encrypt . . . 346
7.2.43 remote ap ipsec send auth . . . 348
7.2.44 remote ap ipsec receive spi . . . 350
7.2.45 remote ap ipsec receive protocol . . . 351
7.2.46 remote ap ipsec receive range . . . 352
7.2.47 remote ap ipsec receive encrypt . . . 354
7.2.48 remote ap ipsec receive auth . . . 356
7.2.49 remote ap ipsec ike protocol . . . 358
7.2.50 remote ap ipsec ike encrypt . . . 359
7.2.51 remote ap ipsec ike auth . . . 361
7.2.52 remote ap ipsec ike pfs . . . 362
7.2.53 remote ap ipsec ike lifetime . . . 363
7.2.54 remote ap ipsec ike lifebyte . . . 364
7.2.55 remote ap ipsec ike newsa initiator . . . 365
7.2.56 remote ap ipsec ike newsa responder . . . 366
7.2.57 remote ap ipsec ike range . . . 368
7.2.58 remote ap ipsec extension-range . . . 370
7.2.59 remote ap ike port . . . 372
7.2.60 remote ap ike shared key . . . 373
7.2.61 remote ap ike proposal move . . . 375
7.2.62 remote ap ike proposal encrypt . . . 377
7.2.63 remote ap ike proposal hash . . . 378
7.2.64 remote ap ike proposal pfs . . . 379
7.2.65 remote ap ike proposal lifetime . . . 380
7.2.66 remote ap ike retry . . . 381
7.2.67 remote ap ike idtype . . . 382
7.2.68 remote ap ike name local . . . 383
7.2.69 remote ap ike name remote . . . 384
7.2.70 remote ap ike release . . . 385
7.2.71 remote ap ike initial . . . 387
7.2.72 remote ap ike sessionwatch . . . 389
7.2.73 remote ap ike mode . . . 391
7.2.74 remote ap ike bind . . . 393
7.2.75 remote ap ike nat-traversal use . . . 395
7.2.76 remote ap dvpn client . . . 397
7.2.77 remote ap dvpn remotenet . . . 398
7.2.78 remote ap dvpn remoteid . . . 400
7.2.79 remote ap tunnel local . . . 401
7.2.80 remote ap tunnel remote . . . 403
7.2.81 remote ap overlap to . . . 404
7.2.82 remote ap overlap nexthop . . . 406
7.2.83 remote ap overlap nexthop6 . . . 407

7.2.84 remote ap sessionwatch address . . . 408
7.2.85 remote ap sessionwatch interval . . . 410
7.2.86 remote ap sessionwatch ttl . . . 412
7.2.87 remote ap sessionwatch mode . . . 413
7.2.88 remote ap sessionwatch recovery . . . 415
7.2.89 remote ap sessionwatch error-wait . . . 417
7.2.90 remote ap mpls to . . . 418
7.2.91 remote ap mpls nexthop . . . 420
7.3 PPP 関連情報 . . . 421
7.3.1 remote ppp compress . . . 421
7.3.2 remote ppp mp start . . . 422
7.3.3 remote ppp mp max . . . 423
7.3.4 remote ppp mp divide . . . 424
7.3.5 remote ppp mp traffic use . . . 425
7.3.6 remote ppp mp traffic increase . . . 426
7.3.7 remote ppp mp traffic decrease . . . 427
7.3.8 remote ppp mp order . . . 428
7.3.9 remote ppp ipcp vjcomp . . . 429
7.3.10 remote ppp ipcp iphc . . . 430
7.3.11 remote ppp ipv6cp iphc . . . 431
7.4 IP 関連情報 . . . 432
7.4.1 remote ip address local . . . 432
7.4.2 remote ip address remote . . . 433
7.4.3 remote ip route . . . 434
7.4.4 remote ip rip use . . . 437
7.4.5 remote ip rip filter act . . . 439
7.4.6 remote ip rip filter move . . . 441
7.4.7 remote ip rip filter route . . . 442
7.4.8 remote ip rip filter set metric . . . 444
7.4.9 remote ip ospf use . . . 445
7.4.10 remote ip ospf cost . . . 447
7.4.11 remote ip ospf hello . . . 448
7.4.12 remote ip ospf dead . . . 449
7.4.13 remote ip ospf retrans . . . 450
7.4.14 remote ip ospf delay . . . 451
7.4.15 remote ip ospf auth type . . . 452
7.4.16 remote ip ospf auth textkey . . . 453
7.4.17 remote ip ospf auth md5key . . . 454
7.4.18 remote ip ospf passive . . . 455
7.4.19 remote ip ospf multicast . . . 456
7.4.20 remote ip ospf checkmtu . . . 457
7.4.21 remote ip nat mode . . . 458
7.4.22 remote ip nat static . . . 460
7.4.23 remote ip nat static default . . . 462
7.4.24 remote ip nat rule . . . 463
7.4.25 remote ip nat wellknown . . . 465
7.4.26 remote ip nat destination . . . 467
7.4.27 remote ip nat appli . . . 469
7.4.28 remote ip filter . . . 471
7.4.29 remote ip filter move . . . 477

7.4.30 remote ip filter default . . . 478
7.4.31 remote ip tos . . . 479
7.4.32 remote ip tos move . . . 483
7.4.33 remote ip priority . . . 484
7.4.34 remote ip clp . . . 489
7.4.35 remote ip clp move . . . 493
7.4.36 remote ip in-policy . . . 494
7.4.37 remote ip in-policy move . . . 496
7.4.38 remote ip msschange . . . 497
7.4.39 remote ip multicast mode . . . 498
7.4.40 remote ip multicast ttl threshold . . . 499
7.4.41 remote ip multicast pim preference . . . 500
7.4.42 remote ip multicast pim upstream type . . . 501
7.4.43 remote ip dvpn . . . 502
7.4.44 remote ip dvpn move . . . 504
7.4.45 remote ip exp . . . 505
7.4.46 remote ip exp move . . . 509
7.4.47 remote ip ids use . . . 510
7.5 IPv6 関連情報 . . . 511
7.5.1 remote ip6 use . . . 511
7.5.2 remote ip6 ifid . . . 512
7.5.3 remote ip6 address . . . 513
7.5.4 remote ip6 ra mode . . . 515
7.5.5 remote ip6 ra interval . . . 516
7.5.6 remote ip6 ra mtu . . . 517
7.5.7 remote ip6 ra reachabletime . . . 518
7.5.8 remote ip6 ra retranstimer . . . 519
7.5.9 remote ip6 ra curhoplimit . . . 520
7.5.10 remote ip6 ra flags . . . 521
7.5.11 remote ip6 route . . . 522
7.5.12 remote ip6 rip use . . . 525
7.5.13 remote ip6 rip site-local . . . 527
7.5.14 remote ip6 rip aggregate . . . 528
7.5.15 remote ip6 rip filter act . . . 529
7.5.16 remote ip6 rip filter move . . . 531
7.5.17 remote ip6 rip filter route . . . 532
7.5.18 remote ip6 rip filter set metric . . . 534
7.5.19 remote ip6 filter . . . 535
7.5.20 remote ip6 filter move . . . 541
7.5.21 remote ip6 filter default . . . 542
7.5.22 remote ip6 trafficclass . . . 543
7.5.23 remote ip6 trafficclass move . . . 547
7.5.24 remote ip6 priority . . . 548
7.5.25 remote ip6 in-policy . . . 552
7.5.26 remote ip6 in-policy move . . . 554
7.5.27 remote ip6 dhcp service . . . 555
7.5.28 remote ip6 dhcp duid . . . 556
7.5.29 remote ip6 dhcp client option pd . . . 557
7.5.30 remote ip6 dhcp client option dns . . . 558
7.5.31 remote ip6 dhcp client iaid . . . 559

7.5.32 remote ip6 dhcp client route . . . 560
7.5.33 remote ip6 dhcp server preference . . . 561
7.5.34 remote ip6 dhcp server info dns . . . 562
7.5.35 remote ip6 dhcp server info prefix . . . 563
7.5.36 remote ip6 dvpn . . . 565
7.5.37 remote ip6 dvpn move . . . 567
7.5.38 remote ip6 exp . . . 568
7.5.39 remote ip6 exp move . . . 570
7.5.40 remote ip6 clp . . . 571
7.5.41 remote ip6 clp move . . . 573
7.6 ブリッジ関連情報 . . . 574
7.6.1 remote bridge use . . . 574
7.6.2 remote bridge group . . . 575
7.6.3 remote bridge static . . . 576
7.6.4 remote bridge stp use . . . 577
7.6.5 remote bridge stp cost . . . 578
7.6.6 remote bridge stp priority . . . 580
7.6.7 remote bridge filter . . . 581
7.6.8 remote bridge filter move . . . 585
7.6.9 remote bridge priority . . . 586
7.7 MPLS 関連情報 . . . 588
7.7.1 remote mpls use . . . 588
7.7.2 remote mpls distribution . . . 589
7.7.3 remote mpls ldp hello-timers . . . 590
7.7.4 remote mpls ldp keepalive-timers . . . 591
7.7.5 remote mpls ldp advertisement . . . 592
7.7.6 remote mpls ldp retention . . . 593
7.7.7 remote mpls ldp interface-label . . . 594
7.7.8 remote mpls ldp ip transport . . . 595
7.7.9 remote mpls ldp multicast-hello . . . 596

第 8 章　着信デフォルト情報の設定 . . . 597
8.1 発信者番号 (CLID) で相手が判別できないときの着信動作情報 . . . 598
8.1.1 answer accept . . . 598
8.1.2 answer ppp auth type . . . 599
8.1.3 answer ppp auth receive add . . . 600
8.1.4 answer ppp mp use . . . 601
8.1.5 answer ppp mp bap use . . . 602

第 9 章　テンプレート情報の設定 . . . 603
9.1 テンプレート共通情報 . . . 604
9.1.1 template name . . . 604
9.1.2 template mtu . . . 605
9.1.3 template idle . . . 606
9.1.4 template interface pool . . . 608
9.1.5 template aaa . . . 610
9.1.6 template datalink type . . . 611
9.1.7 template datalink bind . . . 612
9.1.8 template combine use . . . 613
9.1.9 template tunnel local . . . 614

9.1.10 template sessionwatch address . . . 616
9.1.11 template sessionwatch interval . . . 618
9.2 PPP 関連情報 . . . 620
9.2.1 template ppp auth type . . . 620
9.2.2 template ppp compress . . . 621
9.2.3 template ppp ipcp vjcomp . . . 622
9.2.4 template ppp ipcp iphc . . . 623
9.2.5 template ppp ipv6cp iphc . . . 624
9.3 IP 関連情報 . . . 625
9.3.1 template ip dns . . . 625
9.3.2 template ip address remote-pool . . . 626
9.3.3 template ip nat mode . . . 627
9.3.4 template ip nat static . . . 629
9.3.5 template ip nat static default . . . 631
9.3.6 template ip nat rule . . . 632
9.3.7 template ip nat wellknown . . . 634
9.3.8 template ip nat destination . . . 636
9.3.9 template ip nat appli . . . 638
9.3.10 template ip filter . . . 640
9.3.11 template ip filter move . . . 646
9.3.12 template ip filter default . . . 647
9.3.13 template ip tos . . . 648
9.3.14 template ip tos move . . . 652
9.3.15 template ip priority . . . 653
9.3.16 template ip msschange . . . 658
9.3.17 template ip ids use . . . 659
9.3.18 template ip in-policy . . . 660
9.3.19 template ip in-policy move . . . 662
9.4 IPv6 関連情報 . . . 663
9.4.1 template ip6 use . . . 663
9.4.2 template ip6 ifid . . . 664
9.4.3 template ip6 filter . . . 665
9.4.4 template ip6 filter move . . . 671
9.4.5 template ip6 filter default . . . 672
9.4.6 template ip6 trafficclass . . . 673
9.4.7 template ip6 trafficclass move . . . 677
9.4.8 template ip6 priority . . . 678
9.4.9 template ip6 in-policy . . . 682
9.4.10 template ip6 in-policy move . . . 684
9.5 動的 VPN 関連情報 . . . 685
9.5.1 template dvpn client . . . 685
9.5.2 template dvpn server address . . . 687
9.5.3 template dvpn server auth . . . 689
9.5.4 template dvpn expire register . . . 690
9.5.5 template dvpn expire session . . . 691
9.5.6 template dvpn ua . . . 692
9.5.7 template dvpn domain . . . 694
9.5.8 template dvpn localnet . . . 695
9.5.9 template dvpn localid . . . 697
9.5.10 template dvpn interface . . . 698

9.5.11 template dvpn global . . . 700
9.6 IPsec 関連情報 . . . 701
9.6.1 template ipsec ike protocol . . . 701
9.6.2 template ipsec ike encrypt . . . 702
9.6.3 template ipsec ike auth . . . 704
9.6.4 template ipsec ike pfs . . . 705
9.6.5 template ipsec ike lifetime . . . 706
9.6.6 template ipsec ike lifebyte . . . 707
9.6.7 template ipsec ike newsa initiator . . . 708
9.6.8 template ipsec ike newsa responder . . . 709
9.7 IKE 関連情報 . . . 710
9.7.1 template ike shared key . . . 710
9.7.2 template ike proposal move . . . 712
9.7.3 template ike proposal encrypt . . . 713
9.7.4 template ike proposal hash . . . 714
9.7.5 template ike proposal pfs . . . 715
9.7.6 template ike proposal lifetime . . . 716
9.7.7 template ike retry . . . 717
9.7.8 template ike idtype . . . 718
9.7.9 template ike release . . . 719
9.7.10 template ike mode . . . 721
9.7.11 template ike nat-traversal use . . . 722

第 10 章　動的 VPN 情報の設定 . . . 724
10.1 動的 VPN サーバ情報 . . . 725
10.1.1 dvpn server use . . . 725
10.1.2 dvpn server domain . . . 726
10.1.3 dvpn server auth use . . . 727
10.1.4 dvpn server auth aaa . . . 728
10.2 動的 VPN クライアント情報 . . . 729
10.2.1 dvpn client encode . . . 729
10.2.2 dvpn client server address . . . 730
10.2.3 dvpn client server auth . . . 732
10.2.4 dvpn client expire register . . . 733
10.2.5 dvpn client expire session . . . 734
10.2.6 dvpn client ua . . . 735
10.2.7 dvpn client domain . . . 737
10.2.8 dvpn client localnet . . . 738
10.2.9 dvpn client localid . . . 740
10.2.10 dvpn client interface . . . 741
10.2.11 dvpn client global . . . 743
10.2.12 dvpn client priority . . . 744
10.2.13 dvpn client ip route distance . . . 745
10.2.14 dvpn client ip6 route distance . . . 746

第 11 章　ルーティングプロトコル情報の設定 . . . 747
11.1 ルーティングマネージャ情報 . . . 748
11.1.1 routemanage ip distance . . . 748
11.1.2 routemanage ip redist rip . . . 750
11.1.3 routemanage ip redist bgp . . . 752

11.1.4 routemanage ip redist ospf . . . 754
11.1.5 routemanage ip ecmp mode . . . 756
11.1.6 routemanage ip ecmp ospf . . . 757
11.1.7 routemanage ip redist ldp . . . 758
11.1.8 routemanage interface floating . . . 760
11.1.9 routemanage ip6 distance . . . 762
11.1.10 routemanage ip6 redist rip . . . 764
11.2 RIP 情報 . . . 766
11.2.1 rip ip timers basic . . . 766
11.2.2 rip ip timers jitter . . . 768
11.2.3 rip ip multipath . . . 769
11.2.4 rip ip redist . . . 770
11.2.5 rip ip redist move . . . 772
11.2.6 rip ip neighbor . . . 773
11.2.7 rip ip gwfilter . . . 774
11.2.8 rip ip gwfilter move . . . 776
11.2.9 rip ip6 timers basic . . . 777
11.2.10 rip ip6 multipath . . . 778
11.2.11 rip ip6 redist . . . 779
11.2.12 rip ip6 redist move . . . 781
11.3 BGP 情報 . . . 782
11.3.1 bgp as . . . 782
11.3.2 bgp id . . . 783
11.3.3 bgp vrf rd . . . 784
11.3.4 bgp mpls-resolution . . . 785
11.3.5 bgp network route . . . 786
11.3.6 bgp network igp . . . 787
11.3.7 bgp aggregate . . . 788
11.3.8 bgp full-route . . . 790
11.3.9 bgp redist . . . 792
11.3.10 bgp redist move . . . 794
11.4 BGP 相手側情報 . . . 795
11.4.1 bgp neighbor address . . . 795
11.4.2 bgp neighbor as . . . 796
11.4.3 bgp neighbor timers . . . 797
11.4.4 bgp neighbor medmetric . . . 799
11.4.5 bgp neighbor asprepend . . . 800
11.4.6 bgp neighbor localpref . . . 801
11.4.7 bgp neighbor nexthopself . . . 802
11.4.8 bgp neighbor ebgp-multihop . . . 803
11.4.9 bgp neighbor enforce-multihop . . . 804
11.4.10 bgp neighbor default-originate . . . 806
11.4.11 bgp neighbor family . . . 807
11.4.12 bgp neighbor source . . . 808
11.4.13 bgp neighbor authentication . . . 809
11.4.14 bgp neighbor filter act . . . 810
11.4.15 bgp neighbor filter move . . . 812
11.4.16 bgp neighbor filter as . . . 813
11.4.17 bgp neighbor filter route . . . 814
11.4.18 bgp neighbor filter set medmetric . . . 816

11.4.19 bgp neighbor filter set asprepend . . . 818
11.4.20 bgp neighbor filter set localpref . . . 820
11.5 OSPF 情報 . . . 822
11.5.1 ospf ip id . . . 822
11.6 OSPF エリア情報 . . . 823
11.6.1 ospf ip area id . . . 823
11.6.2 ospf ip area type . . . 824
11.6.3 ospf ip area defcost . . . 826
11.6.4 ospf ip area range . . . 827
11.6.5 ospf ip area type3-lsa . . . 829
11.6.6 ospf ip area type3-lsa move . . . 832
11.7 OSPF バーチャルリンク情報 . . . 833
11.7.1 ospf ip area vlink id . . . 833
11.7.2 ospf ip area vlink hello . . . 834
11.7.3 ospf ip area vlink dead . . . 836
11.7.4 ospf ip area vlink retrans . . . 838
11.7.5 ospf ip area vlink delay . . . 839
11.7.6 ospf ip area vlink auth type . . . 841
11.7.7 ospf ip area vlink auth textkey . . . 843
11.7.8 ospf ip area vlink auth md5key . . . 845
11.8 ASBR 情報 . . . 847
11.8.1 ospf ip definfo . . . 847
11.8.2 ospf ip summary . . . 849
11.8.3 ospf ip redist . . . 850
11.8.4 ospf ip redist move . . . 853

第 12 章　ブリッジ情報の設定 . . . 854
12.1 ブリッジ情報 . . . 855
12.1.1 bridge age . . . 855
12.1.2 bridge stp priority . . . 857
12.1.3 bridge stp age . . . 858
12.1.4 bridge stp hello . . . 859
12.1.5 bridge stp delay . . . 860
12.1.6 bridge ip routing . . . 861
12.1.7 bridge ip policy . . . 862
12.1.8 bridge ip6 routing . . . 864
12.1.9 bridge ip6 policy . . . 865
12.1.10 bridge vlan tag transmit . . . 867
12.1.11 bridge inter-remote . . . 868
12.1.12 bridge control . . . 869

第 13 章　MPLS 情報の設定 . . . 870
13.1 LDP 情報 . . . 871
13.1.1 mpls ldp router-id . . . 871
13.1.2 mpls ldp control . . . 872
13.1.3 mpls ldp ip transport . . . 873
13.1.4 mpls ip propagate-ttl . . . 874

第 14 章　マルチキャスト情報の設定 875
14.1　マルチキャスト情報 876
14.1.1　multicast ip pimsm candrp mode 876
14.1.2　multicast ip pimsm candrp address 877
14.1.3　multicast ip pimsm candrp priority 878
14.1.4　multicast ip pimsm candbsr mode 879
14.1.5　multicast ip pimsm candbsr address 880
14.1.6　multicast ip pimsm candbsr priority 881
14.1.7　multicast ip pimsm spt mode 882
14.1.8　multicast ip pimsm spt rate 883
14.1.9　multicast ip pimsm register checksum 884
14.1.10　multicast ip route 885

第 15 章　UPnP 情報の設定 887
15.1　UPnP 情報 888
15.1.1　upnp use 888
15.1.2　upnp portmapping lease 890

第 16 章　ACL 情報の設定 891
16.1　ACL 情報 892
16.1.1　acl mac 892
16.1.2　acl ip 894
16.1.3　acl ip6 897
16.1.4　acl tcp 900
16.1.5　acl udp 902
16.1.6　acl icmp 904
16.1.7　acl description 906

第 17 章　ポリシーグループ定義情報の設定 907
17.1　ポリシーグループ定義情報 908
17.1.1　policy-group pattern 908
17.1.2　policy-group pattern move 910
17.1.3　policy-group interface 911
17.1.4　policy-group nexthop 912
17.1.5　policy-group nexthop6 913
17.1.6　policy-group sessionwatch address 914
17.1.7　policy-group sessionwatch interval 916
17.1.8　policy-group sessionwatch ttl 918
17.1.9　policy-group sessionwatch recovery 919
17.1.10　policy-group sessionwatch error-wait 921

第 18 章　AAA 情報の設定 922
18.1　グループ ID 情報 923
18.1.1　aaa name 923
18.2　AAA ユーザ情報 924
18.2.1　aaa user id 924
18.2.2　aaa user password 925
18.2.3　aaa user called number 927
18.2.4　aaa user ip address local 928
18.2.5　aaa user ip address remote 929
18.2.6　aaa user ip route 930

18.2.7 aaa user ip6 ifid . . . 932
18.2.8 aaa user ip6 route . . . 933
18.2.9 aaa user sessionwatch . . . 935
18.2.10 aaa user ipsec ike range . . . 936
18.2.11 aaa user ipsec extension-range . . . 938
18.2.12 aaa user ike shared key . . . 940
18.2.13 aaa user supplicant vid . . . 942
18.2.14 aaa user supplicant mac . . . 943
18.3 RADIUS 情報 . . . 944
18.3.1 aaa radius service . . . 945
18.3.2 aaa radius auth source . . . 947
18.3.3 aaa radius auth message-authenticator . . . 948
18.3.4 aaa radius accounting source . . . 949
18.3.5 aaa radius server client-info secret . . . 950
18.3.6 aaa radius server client-info address . . . 951
18.3.7 aaa radius client server-info auth secret . . . 952
18.3.8 aaa radius client server-info auth address . . . 953
18.3.9 aaa radius client server-info auth port . . . 954
18.3.10 aaa radius client server-info auth deadtime . . . 955
18.3.11 aaa radius client server-info auth priority . . . 957
18.3.12 aaa radius client server-info auth source . . . 958
18.3.13 aaa radius client server-info accounting secret . . . 959
18.3.14 aaa radius client server-info accounting address . . . 960
18.3.15 aaa radius client server-info accounting port . . . 961
18.3.16 aaa radius client server-info accounting deadtime . . . 962
18.3.17 aaa radius client server-info accounting priority . . . 964
18.3.18 aaa radius client server-info accounting source . . . 965
18.3.19 aaa radius client retry . . . 966
18.3.20 aaa radius client nas-identifier . . . 967

第 19 章　装置情報の設定 . . . 968
19.1 SNMP 情報 . . . 969
19.1.1 snmp service . . . 969
19.1.2 snmp agent contact . . . 970
19.1.3 snmp agent sysname . . . 971
19.1.4 snmp agent location . . . 972
19.1.5 snmp agent address . . . 973
19.1.6 snmp manager . . . 974
19.1.7 snmp trap coldstart . . . 976
19.1.8 snmp trap linkdown . . . 977
19.1.9 snmp trap linkup . . . 978
19.1.10 snmp trap authfail . . . 979
19.1.11 snmp trap newroot . . . 980
19.1.12 snmp trap topologychange . . . 981
19.1.13 snmp trap vrrpnewmaster . . . 982
19.1.14 snmp trap vrrpauthfail . . . 983
19.1.15 snmp trap noserror . . . 984
19.2 システムログ情報 . . . 985
19.2.1 syslog server . . . 985
19.2.2 syslog pri . . . 986

19.2.3 syslog facility . . . 987
19.2.4 syslog security . . . 988
19.2.5 syslog dupcut . . . 989
19.3 自動時刻設定情報 . . . 990
19.3.1 time auto server . . . 990
19.3.2 time auto interval . . . 992
19.3.3 time zone . . . 993
19.4 ProxyDNS 情報 . . . 994
19.4.1 proxydns domain . . . 994
19.4.2 proxydns domain move . . . 998
19.4.3 proxydns address . . . 999
19.4.4 proxydns address move . . . 1002
19.4.5 proxydns unicode . . . 1003
19.5 ホストデータベース情報 . . . 1004
19.5.1 host name . . . 1004
19.5.2 host ip address . . . 1005
19.5.3 host ip6 address . . . 1006
19.5.4 host mac . . . 1007
19.5.5 host rpon . . . 1008
19.6 スケジュール情報 . . . 1009
19.6.1 schedule at . . . 1009
19.6.2 schedule in . . . 1011
19.6.3 schedule syslog . . . 1013
19.7 電話番号変更予約情報 . . . 1014
19.7.1 dnconvinfo date . . . 1014
19.7.2 dnconvinfo dial . . . 1016
19.8 ファームウェア更新情報 . . . 1018
19.8.1 updateinfo . . . 1018
19.9 MAC アドレス認証情報 . . . 1020
19.9.1 macauth password . . . 1020
19.10 その他 . . . 1021
19.10.1 addact . . . 1021
19.10.2 watchdog service . . . 1023
19.10.3 consoleinfo . . . 1024
19.10.4 telnetinfo . . . 1025
19.10.5 sysdown harderr fan . . . 1026
19.10.6 sysdown harderr thermal . . . 1027
19.10.7 sysdown power . . . 1028
19.10.8 mflag . . . 1029
19.10.9 sysname . . . 1030
19.10.10 loopback ip address . . . 1031
19.10.11 loopback ip ospf use . . . 1032
19.10.12 loopback mpls ldp interface-label . . . 1034
19.10.13 serverinfo ftp . . . 1035
19.10.14 serverinfo ftp ip6 . . . 1036
19.10.15 serverinfo ftp filter . . . 1037
19.10.16 serverinfo ftp filter move . . . 1039
19.10.17 serverinfo ftp filter default . . . 1040
19.10.18 serverinfo sftp . . . 1041
19.10.19 serverinfo sftp ip6 . . . 1042

19.10.20 serverinfo telnet 1043
19.10.21 serverinfo telnet ip6 1044
19.10.22 serverinfo telnet filter 1045
19.10.23 serverinfo telnet filter move 1047
19.10.24 serverinfo telnet filter default 1048
19.10.25 serverinfo ssh 1049
19.10.26 serverinfo ssh ip6 1050
19.10.27 serverinfo ssh filter 1051
19.10.28 serverinfo ssh filter move 1053
19.10.29 serverinfo ssh filter default 1054
19.10.30 serverinfo http 1055
19.10.31 serverinfo http ip6 1056
19.10.32 serverinfo http filter 1057
19.10.33 serverinfo http filter move 1059
19.10.34 serverinfo http filter default 1060
19.10.35 serverinfo dns 1061
19.10.36 serverinfo dns ip6 1062
19.10.37 serverinfo dns filter 1063
19.10.38 serverinfo dns filter move 1065
19.10.39 serverinfo dns filter default 1066
19.10.40 serverinfo sntp 1067
19.10.41 serverinfo sntp ip6 1068
19.10.42 serverinfo sntp filter 1069
19.10.43 serverinfo sntp filter move 1071
19.10.44 serverinfo sntp filter default 1072
19.10.45 serverinfo time ip tcp 1073
19.10.46 serverinfo time ip6 tcp 1074
19.10.47 serverinfo time ip udp 1075
19.10.48 serverinfo time ip6 udp 1076
19.10.49 serverinfo time filter 1077
19.10.50 serverinfo time filter move 1079
19.10.51 serverinfo time filter default 1080

第 20 章　構成定義情報表示、削除、および操作コマンド 1081
20.1 構成定義情報表示 1082
20.1.1 show candidate-config 1082
20.1.2 show running-config 1083
20.1.3 show startup-config 1084
20.1.4 diff 1085
20.2 構成定義情報削除 1086
20.2.1 delete 1086
20.3 構成定義情報操作 1087
20.3.1 load 1087
20.3.2 save 1088
20.3.3 commit 1089
20.3.4 discard 1090

第 21 章　モード 操作コマンド /ターミナル操作コマンド 1091
21.1　モード 操作 1092
21.1.1　admin 1092
21.1.2　su 1093
21.1.3　exit 1094
21.1.4　configure 1095
21.1.5　end 1096
21.1.6　quit 1097
21.1.7　top 1098
21.1.8　up 1099
21.1.9　！ 1100
21.2　ターミナル操作 1101
21.2.1　terminal pager 1101
21.2.2　terminal window 1104
21.2.3　terminal charset 1105
21.2.4　terminal prompt 1106
21.2.5　terminal timestamp 1108
21.2.6　terminal bell 1109
21.2.7　terminal logging 1110
21.2.8　show terminal 1111
21.3　コマンド 実行履歴 1112
21.3.1　show logging command 1112
21.3.2　clear logging command 1114
21.4　コマンド エイリアス 1115
21.4.1　alias 1115
21.4.2　show alias 1117
21.4.3　clear alias 1118
21.5　コマンド 出力操作 1119
21.5.1　more 1119
21.5.2　tail 1120

第 22 章　システム操作および表示コマンド 1121
22.1　システム操作および表示 1122
22.1.1　show system information 1122
22.1.2　show system status 1125
22.1.3　show tech-support 1134
22.1.4　show logging error 1135
22.1.5　clear logging error 1139
22.1.6　show logging syslog 1140
22.1.7　clear logging syslog 1141
22.1.8　clear statistics 1142
22.1.9　show date 1143
22.1.10　date 1144
22.1.11　rdate 1145
22.1.12　reset 1146
22.1.13　update 1147

第 23 章　Ethernet のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド 1149
23.1 Ethernet のカウンタ・ログ・統計・状態などの表示 1150
23.1.1 show ether 1150
23.1.2 show ether statistics 1153
23.2 Ethernet のカウンタ・ログ・統計などのクリア 1159
23.2.1 clear ether statistics 1159

第 24 章　ISDN のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド 1161
24.1 ISDN のカウンタ・ログ・統計・状態などの表示 1162
24.1.1 show isdn 1162
24.1.2 show isdn account 1165
24.1.3 show isdn statistics circuit 1167
24.1.4 show isdn statistics piafs 1173
24.2 ISDN のカウンタ・ログ・統計などのクリア 1177
24.2.1 clear isdn statistics circuit 1177
24.2.2 clear isdn account 1178
24.2.3 clear isdn statistics piafs 1179

第 25 章　フレームリレーのカウンタ・ログ・統計・状態などの表示、クリア操作コマンド 1180
25.1 フレームリレーのカウンタ・ログ・統計・状態などの表示 1181
25.1.1 show fr 1181
25.1.2 show fr statistics circuit 1183
25.1.3 show fr statistics vc 1189
25.2 フレームリレーのカウンタ・ログ・統計などのクリア 1192
25.2.1 clear fr statistics circuit 1192
25.2.2 clear fr statistics vc 1193

第 26 章　専用線のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド 1194
26.1 専用線のカウンタ・ログ・統計・状態などの表示 1195
26.1.1 show hsd 1195
26.1.2 show hsd statistics circuit 1197
26.1.3 clear hsd statistics circuit 1203

第 27 章　ATM 回線のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド 1204
27.1 ATM 回線のカウンタ・ログ・統計・状態などの表示 1205
27.1.1 show atm 1205
27.1.2 show atm statistics circuit 1212
27.1.3 show atm statistics vc 1215
27.1.4 show atm statistics llc-snap 1219
27.2 ATM 回線のカウンタ・ログ・統計などのクリア 1221
27.2.1 clear atm statistics 1221

第 28 章　モデム／データ通信カード 接続のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド 1222
28.1 モデム／データ通信カード 接続のカウンタ・ログ・統計・状態などの表示 1223
28.1.1 show modem 1223
28.1.2 show modem account 1226
28.1.3 show modem statistics 1228
28.2 モデム／データ通信カード 接続のカウンタ・ログ・統計などのクリア 1230
28.2.1 clear modem account 1230
28.2.2 clear modem statistics 1231

第 29 章　インタフェースのカウンタ・ログ・統計・状態などの表示、クリア操作コマンド 1232
29.1　インタフェースのカウンタ・ログ・統計・状態などの表示 1233
29.1.1　show interface 1233
29.1.2　show interface brief 1236
29.1.3　show interface summary 1238
29.1.4　show interface detail 1239
29.1.5　show interface statistics 1243
29.1.6　show access-point 1245
29.1.7　show template 1251
29.1.8　show template statistics 1255
29.2　インタフェースのカウンタ・ログ・統計などのクリア 1256
29.2.1　clear interface statistics 1256
29.2.2　clear template statistics 1257

第 30 章　ARP エントリの表示、削除コマンド 1258
30.1　ARP エントリの表示、削除 1259
30.1.1　show arp 1259
30.1.2　clear arp 1261

第 31 章　Neighbor Cache テーブルエントリの表示、削除コマンド 1262
31.1　Neighbor Cache テーブルエントリの表示、削除 1263
31.1.1　show ndp 1263
31.1.2　clear ndp 1265

第 32 章　ルーティングテーブル情報・統計などの表示、クリア操作コマンド 1266
32.1　IPv4 ルーティングテーブル情報・統計などの表示、クリア操作 1267
32.1.1　show ip route 1267
32.1.2　show ip route summary 1270
32.1.3　clear ip route 1272
32.1.4　show ip route kernel 1273
32.1.5　show ip route kernel ecmp statistics 1275
32.1.6　clear ip route kernel ecmp statistics 1276
32.2　IPv6 ルーティングテーブル情報・統計などの表示 1277
32.2.1　show ipv6 route 1277
32.2.2　show ipv6 route summary 1280
32.2.3　clear ipv6 route 1282
32.2.4　show ipv6 route kernel 1283

第 33 章　RIP 情報の表示、クリア操作コマンド 1286
33.1　RIP 情報の表示、クリア操作 1287
33.1.1　show ip rip route 1287
33.1.2　show ip rip protocol 1289
33.1.3　clear ip rip statistics 1292
33.2　IPv6 RIP 情報の表示 1293
33.2.1　show ipv6 rip route 1293
33.2.2　show ipv6 rip protocol 1295

第 34 章　BGP 情報の表示、クリア操作コマンド 1297
34.1 BGP 情報の表示、クリア操作 1298
34.1.1 show ip bgp route 1298
34.1.2 show ip bgp route summary 1303
34.1.3 show ip bgp status 1305
34.1.4 show ip bgp neighbors 1307
34.1.5 show ip bgp vpnv4 route 1310
34.1.6 clear ip bgp statistics 1312

第 35 章　OSPF 情報の表示、クリア操作コマンド 1313
35.1 OSPF 情報の表示、クリア操作 1314
35.1.1 show ip ospf route 1314
35.1.2 show ip ospf protocol 1316
35.1.3 show ip ospf database 1319
35.1.4 show ip ospf interface 1328
35.1.5 show ip ospf neighbor 1331
35.1.6 clear ip ospf statistics 1334

第 36 章　VPNv4 ルーティングテーブル情報の表示コマンド 1335
36.1 VPNv4 ルーティングテーブル情報の表示 1336
36.1.1 show ip vpnv4 route 1336
36.1.2 show ip vpnv4 route summary 1338

第 37 章　パケットの統計情報の表示、クリア操作コマンド 1340
37.1 IPv4 パケットの統計情報の表示、クリア操作 1341
37.1.1 show ip traffic 1341
37.1.2 clear ip traffic 1345
37.2 IPv6 パケットの統計情報の表示、クリア操作 1346
37.2.1 show ipv6 traffic 1346
37.2.2 clear ipv6 traffic 1350

第 38 章　IP フィルタのカウンタ・ログ・統計・状態などの表示、クリア操作コマンド 1351
38.1 IPv4 フィルタのカウンタ・ログ・統計・状態などの表示、クリア操作 1352
38.1.1 show ip filter 1352
38.1.2 show ip filter statistics 1355
38.1.3 show ip filter summary 1357
38.1.4 clear ip filter statistics 1359
38.2 IPv6 フィルタのカウンタ・ログ・統計・状態などの表示、クリア操作 1360
38.2.1 show ipv6 filter 1360
38.2.2 show ipv6 filter statistics 1363
38.2.3 show ipv6 filter summary 1365
38.2.4 clear ipv6 filter statistics 1367

第 39 章　IDS のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド 1368
39.1 IPv4 IDS のカウンタ・ログ・統計・状態などの表示、クリア操作 1369
39.1.1 show ip ids statistics 1369
39.1.2 clear ip ids statistics 1372

第 40 章　NAT のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド 1373
40.1 NAT のカウンタ・ログ・統計・状態などの表示 1374
40.1.1 show ip nat interface 1374
40.1.2 show ip nat statistics 1376
40.1.3 show ip nat summary 1378
40.2 NAT のカウンタ・ログ・統計などのクリア 1379
40.2.1 clear ip nat statistics 1379

第 41 章　マルチキャスト のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド 1380
41.1 マルチキャストのカウンタ・ログ・統計・状態などの表示 1381
41.1.1 show ip multicast group 1381
41.1.2 show ip multicast interface 1383
41.1.3 show ip multicast interface statistics 1385
41.1.4 show ip multicast pimsm rp 1386
41.1.5 show ip multicast protocol 1387
41.1.6 show ip multicast route 1388
41.1.7 show ip multicast route kernel 1391
41.1.8 show ip multicast route kernel statistics 1393
41.1.9 show ip multicast statistics 1394
41.2 マルチキャストのカウンタ・ログ・統計などのクリア 1395
41.2.1 clear ip multicast interface statistics 1395
41.2.2 clear ip multicast route kernel statistics 1396
41.2.3 clear ip multicast statistics 1397

第 42 章　DHCP のカウンタ・ログ・統計・状態などの表示コマンド 1398
42.1 IPv4 DHCP のカウンタ・ログ・統計・状態などの表示 1399
42.1.1 show ip dhcp 1399
42.2 IPv6 DHCP のカウンタ・ログ・統計・状態などの表示 1402
42.2.1 show ipv6 dhcp 1402

第 43 章　動的 VPN の状態などの表示、情報の削除コマンド 1405
43.1 動的 VPN の情報交換クライアントの状態などの表示 1406
43.1.1 show dvpn client user 1406
43.1.2 show dvpn client session 1408
43.2 動的 VPN サーバの状態などの表示 1410
43.2.1 show dvpn server 1410
43.2.2 show dvpn server user 1412
43.2.3 show dvpn server session 1414
43.3 動的 VPN サーバの情報の削除 1416
43.3.1 clear dvpn server user 1416
43.3.2 clear dvpn server session 1417

第 44 章　IPsec/IKE のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド 1418
44.1 IPsec/IKE のカウンタ・ログ・統計・状態などの表示、クリア操作 1419
44.1.1 show ipsec sa 1419
44.1.2 show ike statistics 1427
44.1.3 clear ike statistics 1433

第 45 章　VRRP のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド 1434
45.1 VRRP のカウンタ・ログ・統計・状態などの表示 1435
45.1.1 show vrrp 1435
45.2 VRRP のカウンタ・ログ・統計などのクリア 1439
45.2.1 clear vrrp statistics 1439

第 46 章　ブリッジのカウンタ・ログ・統計・状態などの表示、クリア操作コマンド 1440
46.1 ブリッジのカウンタ・ログ・統計・状態などの表示 1441
46.1.1 show bridge 1441
46.1.2 show bridge status 1443
46.2 ブリッジのカウンタ・ログ・統計などのクリア 1445
46.2.1 clear bridge statistics 1445
46.3 スパニングツリーのカウンタ・ログ・統計・状態などの表示 1446
46.3.1 show spanning-tree 1446
46.4 スパニングツリーのカウンタ・ログ・統計のクリア 1456
46.4.1 clear spanning-tree statistics 1456

第 47 章　MPLS のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド 1457
47.1 MPLS のカウンタ・ログ・統計・状態などの表示 1458
47.1.1 show mpls 1458
47.1.2 show mpls ftn 1459
47.1.3 show mpls ilm 1461
47.1.4 show mpls ldp 1463
47.1.5 show mpls ldp adjacency 1466
47.1.6 show mpls ldp fec 1467
47.1.7 show mpls ldp session 1468
47.1.8 show mpls ldp summary 1472
47.1.9 show mpls ldp vc 1474
47.1.10 show mpls statistics 1475
47.1.11 show mpls summary 1477
47.1.12 show mpls vc 1478
47.1.13 show mpls vrf 1480
47.2 MPLS のカウンタ・ログ・統計などのクリア 1482
47.2.1 clear mpls statistics 1482
47.2.2 clear mpls statistics ftn 1483
47.2.3 clear mpls statistics ilm 1484
47.2.4 clear mpls statistics vc 1485
47.2.5 clear mpls statistics vrf 1486

第 48 章　MAC アドレス認証のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド 1487
48.1 MAC アドレス認証のカウンタ・ログ・統計・状態などの表示 1488
48.1.1 show macauth 1488
48.2 MAC アドレス認証のカウンタ・ログ・統計などのクリア 1490
48.2.1 clear macauth statistics 1490

第 49 章　SNMP 統計情報の表示、クリア操作コマンド 1491
49.1 SNMP 統計情報の表示 1492
49.1.1 show snmp statistics 1492
49.2 SNMP 統計などのクリア 1494
49.2.1 clear snmp statistics 1494

第 50 章　NETTIME(time/sntp) サーバ、クライアント の統計情報表示、クリア操作コマンド . . 1495
50.1 NETTIME(time/sntp) 統計情報の表示 1496
50.1.1 show nettime statistics 1496
50.2 NETTIME(time/sntp) 統計などのクリア 1500
50.2.1 clear nettime statistics 1500

第 51 章　UPnP のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド 1501
51.1 UPnP のカウンタ・ログ・統計・状態などの表示、クリア 1502
51.1.1 show upnp 1502
51.1.2 show upnp statistics 1504
51.1.3 show upnp portmapping 1506
51.1.4 clear upnp statistics 1507
51.1.5 clear upnp portmapping 1508

第 52 章　ポリシーグループの状態の表示コマンド 1509
52.1 ポリシーグループの状態の表示 1510
52.1.1 show policy-group 1510

第 53 章　SSH ホスト 認証用公開鍵の表示コマンド 1512
53.1 SSH ホスト認証用公開鍵の表示 1513
53.1.1 show ssh server key 1513

第 54 章　AAA の状態の表示コマンド 1515
54.1 AAA の状態の表示 1516
54.1.1 show aaa radius client server-info 1516

第 55 章　ソケット 状態の表示コマンド 1518
55.1 ソケット状態の表示 1519
55.1.1 show socket 1519

第 56 章　トレースの表示、クリア操作コマンド 1523
56.1 トレースの表示 1524
56.1.1 show trace ppp 1524
56.1.2 show trace pppoe 1528
56.1.3 show trace ike 1531
56.1.4 show trace modem 1535
56.1.5 show trace ssh 1538
56.2 トレースのクリア 1540
56.2.1 clear trace ssh 1540

第 57 章　回線制御コマンド 1541
57.1 回線制御 1542
57.1.1 addlink 1542
57.1.2 dellink 1544
57.1.3 offline 1546
57.1.4 online 1549

第 58 章　VRRP 制御コマンド 1552
58.1 VRRP 制御 1553
58.1.1 vrrp action 1553
58.1.2 vrrp preempt-permit 1555

第 59 章　動的 VPN サーバ制御コマンド 1557
59.1　動的 VPN サーバ制御 1558
59.1.1　dvpnserver disable 1558
59.1.2　dvpnserver enable 1559

第 60 章　RADIUS 制御コマンド 1560
60.1　RADIUS 制御 1561
60.1.1　radius recovery 1561

第 61 章　データ通信カード の PIN 制御コマンド 1562
61.1　データ通信カード の PIN 制御 1563
61.1.1　pinctl change 1563
61.1.2　pinctl unlock 1565
61.1.3　pinctl use 1567
61.1.4　pinctl nouse 1569

第 62 章　その他のコマンド 1571
62.1　その他 1572
62.1.1　ping 1572
62.1.2　traceroute 1575
62.1.3　telnet 1578
62.1.4　pwconv 1580
62.1.5　dnconv 1582
62.1.6　rpon 1583
62.1.7　diag 1584

第 63 章　commit コマンド 実行時の影響について 1585

第 64 章　運用管理コマンド の仕様変更について (V30) 1591

第 65 章　V30 との非互換について 1608
65.1　remote ap/template ipsec ike encrypt/ike proposal encrypt コマンド について 1609
65.2　template sessionwatch コマンド について 1610
65.3　RADIUS クライアント 機能のサーバ定義について 1611

第 1 章　パスワード 情報

1.1　パスワード 情報

1.1.1　password format

[機能]

暗号化パスワード 文字列形式の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

password format <format>

[オプション]

<format>

暗号化パスワード 形式

- common
  共通パスワード 形式
  他装置でも使用可能な暗号化パスワード 文字列。
- unique
  装置固有パスワード 形式
  本装置でのみ使用可能な暗号化パスワード 文字列。

[動作モード]

構成定義モード (管理者クラス)

[説明]

構成定義の各種パスワード 項目に平文でパスワード 文字列を設定すると、暗号化パスワード 文字列に変換されます。show コマンド および save コマンド を実行したとき、暗号化パスワード 文字列に"encrypted"の文字列を付加した形式で表示および保存されます。
本コマンド では、表示および保存するときの暗号化パスワード 文字列形式を設定します。本設定は、構成定義のすべてのパスワード 項目に対して有効です。
本コマンド は、設定した直後に有効となります。
common に設定した場合、暗号化パスワード 文字列は各装置で同じ共通パスワード 形式になります。故障などにより装置交換した場合は、共通パスワード 形式で保存してある構成定義を交換後の装置に復元することができます。common に設定した状態では、平文または共通パスワード 形式のパスワード 文字列を設定できます。装置固有パスワード 形式のパスワード 文字列は設定できません。
unique に設定した場合、暗号化パスワード 文字列は装置ごとに異なる装置固有パスワード 形式になります。装置固有パスワード 形式で表示および保存した構成定義は、その装置にしか設定および復元することができません。故障などにより装置交換した場合は、装置固有パスワード 形式で保存してある構成定義を復元できませんので、交換後の装置には平文パスワード で再設定してください。unique に設定した状態では、平分、共通パスワード 形式およびその装置で表示した装置固有パスワード 形式のパスワード 文字列を設定できます。
TPM(Trusted Platform Module) が実装されている装置で unique に設定した場合、TPM を利用した装置固有パスワード 形式になります。なお、unique に設定する際に TPM が正常か検査され、ハード エラーを検出した場合は以下のメッセージが出力されて設定は common になります。

```
<ERROR> detected HARD ERROR, cannot execute
```

[注意]

unique に設定すると、common に再設定したり本設定を削除することはできません。common に再設定したい場合は、reset clear コマンドを実行して工場出荷時設定に戻してから、構成定義を設定し直してください。unique に設定したとき、設定済みのパスワード項目はすべて装置固有パスワード形式に変換されて表示および保存されます。

[未設定時]

common を設定したものとみなされます。

```
password format common
```

1.1.2　password set

[機能]

管理者パスワード の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

password set <password> [encrypted]

[オプション]

<password>

- パスワード

  パスワード の文字列を、0x21,0x23〜0x7e の 16 文字以内の ASCII 文字で指定します。

- 暗号化されたパスワード

  show candidate-config、show running-config または show startup-config コマンド で表示される暗号化されたパスワード を encrypted と共に指定します。

  show candidate-config、show running-config または show startup-config コマンド で表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化パスワード 指定

  <password>に暗号化されたパスワード を指定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本装置に管理者がログインするためのパスワード を設定します。また、admin コマンド を実行して管理者になる場合にも本コマンド で設定した管理者パスワード の入力が必要になります。
本コマンド は設定した直後に有効となります。
ユーザ名に admin、パスワード に本パスワード を入力すると、管理者クラスでログインでき、管理者クラス用コマンド および Web メニューを使用できます。

[注意]

show candidate-config、show running-config および show startup-config コマンド では、暗号化されたパスワード が encrypted と共に表示されます。

[未設定時]

管理者パスワード は設定されていません。

1.1.3 password user set

[機能]

一般ユーザパスワードの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

password user set <password> [encrypted]

[オプション]

<password>

- パスワード

  パスワードの文字列を、0x21,0x23～0x7e の 16 文字以内の ASCII 文字で指定します。

- 暗号化されたパスワード

  show candidate-config、show running-config または show startup-config コマンドで表示される暗号化されたパスワードを encrypted と共に指定します。

  show candidate-config、show running-config または show startup-config コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化パスワード指定

  <password>に暗号化されたパスワードを指定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本装置に一般ユーザがログインするためのパスワードを設定します。
本コマンドは設定した直後に有効となります。
ユーザ名に user、パスワードに本パスワードを入力すると、一般ユーザクラスでログインでき、一般ユーザクラス用コマンドおよび Web メニューを使用できます。

[注意]

ftp 接続時には、一般ユーザパスワードではログインできません。
一般ユーザパスワードを設定する場合、管理者パスワードも設定してください。
管理者パスワードを設定しない場合、パスワードなしでログインできます。
一般ユーザパスワードでログインした場合、terminal コマンドと alias コマンドで設定した内容は保存されず、admin コマンド実行時やログアウト時に設定した内容が破棄されます。
また、show logging command コマンドでは管理者が実行したコマンドは表示されず、履歴番号は不連続になります。
show candidate-config、show running-config および show startup-config コマンドでは、暗号化されたパスワードが encrypted と共に表示されます。

[未設定時]

一般ユーザパスワードは設定されていません。

第 2 章　WAN 情報の設定

- wan 定義番号の指定範囲

  本章のコマンド の [オプション] に記載されている<number>(wan 定義番号) に指定する wan 定義の通し番号 (10 進数値) は、機種ごとに以下に示す範囲で指定してください。

範囲	機種
0〜131	Si-R570
0〜15	Si-R370　Si-R260B
0	Si-R240　Si-R220B

2.1 回線共通情報

2.1.1 wan bind

[機能]

利用する物理回線の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B

[入力形式]

wan [<number>] bind <slot> [<line>]

[オプション]

<number>

- wan 定義番号
  wan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<slot>

利用する回線のボードが、どのスロットに挿入されているかを指定します。
Si-R260B Si-R220B では、必ず"mb"(基本ボード) を指定してください。
Si-R240 では、必ず"0"(SLOT0) を指定してください。

- mb
  利用する回線が、基本ボード上にある場合に指定します。
- スロット番号
  ボードが挿入されているスロットの番号を、10 進数値で指定します。

範囲	機種
0〜3	Si-R570
0〜1	Si-R370
0	Si-R240

<line>

- 回線番号
  同一のボードに複数の回線がある場合に、どの回線を利用するか指定します。
  省略時は、0 を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

wan 定義で利用する回線を設定します。
複数の wan 定義で同一の回線を指定すると、回線種別により有効になる定義が異なります。

- ATM 以外
  一番小さい番号の wan 定義のみ有効
- ATM
  定義可能 VPC 数まで有効

なお、本コマンドで指定した回線が Ethernet の場合、この wan 定義は無効となります。

[未設定時]

基本ボード上の回線番号が定義番号<number>となる回線を設定するものとみなされます。

```
wan <number> bind mb <number>
```

扱いは装置により以下のようになります。

- Si-R220B Si-R260B 以外
  WAN 定義は無効とみなされます。
- Si-R260B
  wan 定義番号 0 の WAN 定義は
  wan 0 bind mb 0
  と同じ扱いになり、有効になります。それ以外の WAN 定義は無効になります。
- Si-R220B
  WAN 定義は有効とみなされます。

2.1.2 wan line

[機能]

回線インタフェースおよび通信速度の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B

[入力形式]

wan [<number>] line unuse (未使用)
wan [<number>] line isdn (ISDN)
wan [<number>] line hsd <speed> (専用線)
wan [<number>] line fr <speed> (フレームリレー)
wan [<number>] line atm (ATM)
wan [<number>] line cardmodem (データ通信カード)

[オプション]

<number>

- wan 定義番号
  wan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<speed>

- 回線速度
  専用線またはフレームリレー利用時の回線速度を以下の範囲で指定します。

インタフェース	回線速度(指定範囲)	Si-R570 Si-R370	Si-R220B
BRI	64k, 128k	○	○
PRI	192k, 256k, 384k, 512k, 768k, 1m, 1.5m	○	―

[動作モード]

構成定義モード (管理者クラス)

[説明]

wan 定義で利用する回線の、回線種別を設定します。

回線種別	Si-R570 Si-R370	Si-R260B	Si-R220B	Si-R240
ISDN	○	―	○	―
専用線(64Kbps～128Kbps) (192Kbps～1.5Mbps)	○ ○	― ―	○ ―	― ―
フレームリレー(64Kbps～128Kbps) (192Kbps～1.5Mbps)	○ ○	― ―	○ ―	― ―
ATM	○	○	―	―
データ通信カード	―	―	―	○

以下を指定した場合、wan 定義は無効となります。

- unuse(未使用) を指定した場合
- wan bind で設定した回線では使用できない回線種別を指定した場合
- 専用線またはフレームリレーのときに、wan bind で設定した回線では使用できない回線速度を指定した場合
- BRI4 ポート拡張モジュールで、フレームリレーを指定した場合

[未設定時]

wan 定義を使用しないものとみなされます。

```
wan <number> line unuse
```

2.2 ISDN 回線情報

2.2.1 wan isdn global

[機能]

グローバル着信の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

wan [<number>] isdn global <mode>

[オプション]

<number>

- wan 定義番号
  wan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

グローバル着信を受け付けるかどうかを指定します。

- accept
  グローバル着信を受け付けます。
- reject
  グローバル着信を受け付けません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

グローバル着信を受け付けるかどうかを設定します。
通常は<mode>に accept を指定してください。ただし、ダイヤルイン番号または i・ナンバーあての着信だけを受け付ける場合は reject を指定し、wan isdn number で着信を受け付ける着信番号を指定してください。

[未設定時]

グローバル着信を受け付けるものとみなされます。

```
wan <number> isdn global accept
```

2.2.2　wan isdn number

[機能]

自局電話番号の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

wan [<number>] isdn number <count> <tel_number> [<subaddress>]

[オプション]

<number>

- wan 定義番号
  wan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

着信番号チェックを行う電話番号は、2 組まで設定できます。2 組のうちのどちらを設定するか、番号を指定します。

- 0
  着信番号チェックの電話番号 1 を設定します。
- 1
  着信番号チェックの電話番号 2 を設定します。

<tel_number>

着信番号チェックを行う電話番号を指定します。

- 電話番号
  着信時にチェックする電話番号を、0〜9 の数字と、*、#、-、(、)、\ の文字で構成される 32 桁以内の ASCII 文字列で指定します。
- any
  着信時に電話番号のチェックを行わない場合に指定します。
- in1
  i・ナンバーサービス契約時に、i・ナンバー情報 1(契約者回線番号) の着信を受け付ける場合に指定します。
- in2
  i・ナンバーサービス契約時に、i・ナンバー情報 2(追加の番号) の着信を受け付ける場合に指定します。
- in3
  i・ナンバーサービス契約時に、i・ナンバー情報 3(追加の番号) の着信を受け付ける場合に指定します。

<subaddress>

- サブアドレス
  着信時にチェックするサブアドレスを、0x22(ダブルクォーテーション) を除くコードで構成される 19 桁以内の ASCII 文字列で指定します。
  省略時は、サブアドレス通知がない着信のみを指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

着信番号チェックについて設定します。
ダイヤルイン番号、i・ナンバー、サブアドレスを利用して着信機器を識別するかどうかを、<tel_number>と<subaddress>の組み合わせで指定します。着信番号チェックの電話番号は、2 組まで設定できます。
着信時に網から通知される電話番号とサブアドレスが着信番号チェックの電話番号と一致しない場合は、着信を受け付けません。
<tel_number>に any を指定し、かつ<subaddress>を指定した場合は、<subaddress>だけが着信番号チェックの対象となります。また、<tel_number>に any を指定し、<subaddress>が未指定の場合は、サブアドレス通知がないすべての着信を指定したものとみなされます。
i・ナンバーサービス契約時は、<tel_number>に in1、in2、または in3 のどれかを指定してください。

[注意]

任意のサブアドレス通知を着信するように指定することはできません。

[未設定時]

サブアドレス通知のないすべての着信を指定したものとみなされます。

```
wan <number> isdn number 0 any
```

2.2.3　wan isdn numbersend

[機能]

発信者番号通知の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

wan [<number>] isdn numbersend <mode> [<tel_number> [<subaddress>]]

[オプション]

<number>

- wan 定義番号
  wan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

発信者番号の通知形態を指定します。

- specified
  <tel_number>および<subaddress>で指定する電話番号を、発信者番号として通知します。
- default
  網契約に従います。回線の加入契約で選択した内容の設定になります。
- off
  接続先に発信者の電話番号を通知しません。

以下のパラメタは、<mode>に specified を設定した場合にだけ有効です。

<tel_number>

<mode>に specified を設定した場合、必ず以下のどれかを指定してください。

- 通知電話番号
  発信者番号として通知する電話番号を、0〜9 の数字と、*、#、-、(、)、\ の文字で構成される 32 桁以内の ASCII 文字列で指定します。
- in1
  発信者番号として、i・ナンバー情報 1 を通知します。
- in2
  発信者番号として、i・ナンバー情報 2 を通知します。
- in3
  発信者番号として、i・ナンバー情報 3 を通知します。

<subaddress>

- サブアドレス
  発信者番号の一部として通知するサブアドレスを、0x22(ダブルクォーテーション) を除くコードで構成される 19 桁以内の ASCII 文字列で指定します。
  省略時は、サブアドレスを通知しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

発信者番号を通知するかどうかを設定します。また、通知する場合の、通知番号を設定します。

[注意]

Si-R370 Si-R220B は PIAFS 接続に対応しています。PIAFS(64Kbps) 発信時には、<subaddress> で設定したサブアド レスは無視され、相手に通知されません。

[未設定時]

網契約に従うとみなされます。

```
wan <number> isdn numbersend default
```

2.2.4　wan isdn limit charge

[機能]

上限課金額による (発呼抑止) 条件の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

wan [<number>] isdn limit charge <charge> [<diallock>]

[オプション]

<number>

- wan 定義番号
  wan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<charge>

- 上限課金額
  自動発信を制限する上限課金額を、0～999999 の 10 進数値 (単位:円) で指定します。
  0 を指定した場合は、課金額による自動発信制限を行いません。

<diallock>

自動発信を制限するかどうかを指定します。

- yes
  上限課金額に達した場合に、以降の自動発信を制限します。
  ただし、回線の手動接続は、制限の対象外となります。
- no
  上限課金額に達した場合に、以降の自動発信を制限しません。

省略時は、yes を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

データ通信で、通信課金の累計が上限課金額に達した場合に、自動発信を制限するかどうかを設定します。<diallock>の指定内容にかかわらず、<charge>で指定した上限課金額を超えて自動発信しようとした場合は、syslog が採取されます。

[未設定時]

課金額による自動発信制限を行わないとみなされます。

```
wan <number> isdn limit charge 0 yes
```

2.2.5 wan isdn limit time

[機能]

上限通信時間による (発呼抑止) 条件の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

wan [<number>] isdn limit time <time> [<diallock>]

[オプション]

<number>

- wan 定義番号
  wan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<time>

- 上限接続時間
  自動発信を制限する接続時間の上限時間を、0 秒〜999 時間の 10 進数値で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。
  0 を指定した場合は、接続時間による自動発信制限を行いません。

<diallock>

自動発信を制限するかどうかを指定します。

- yes
  接続時間の上限に達した場合に、以降の自動発信を制限します。
  ただし、回線の手動接続は、制限の対象外となります。
- no
  接続時間の上限に達した場合に、自動発信を制限しません。

省略時は、yes を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

データ通信で、通信時間の累計が接続時間の上限に達した場合に、自動発信を制限するかどうかを設定します。
<diallock>の指定内容にかかわらず、<time>で指定した上限接続時間を超えて自動発信しようとした場合は、syslog が採取されます。

[未設定時]

接続時間による自動発信制限を行わないとみなされます。

```
wan <number> isdn limit time 0d yes
```

2.2.6　wan isdn accept

[機能]

装置単位の着信可否の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

wan [<number>] isdn accept <mode>

[オプション]

<number>

- wan 定義番号
  wan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

データ着信時の動作について指定します。

- enable
  remote ap called accept の設定に従います。
- disable
  着信を禁止します。着信をすべて拒否し、発信専用の装置となります。

[動作モード]

構成定義モード (管理者クラス)

[説明]

外部から本装置に着信したときの動作について設定します。

[未設定時]

remote ap called accept の設定に従うものとみなされます。

```
wan <number> isdn accept enable
```

2.2.7 wan isdn autodial

[機能]

装置単位の自動発信可否の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

wan [<number>] isdn autodial <mode>

[オプション]

<number>

- wan 定義番号
  wan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

自動的にダイヤルするかどうかについて指定します。

- enable
  remote autodial の設定に従います。
- disable
  本装置からの自動ダイヤルを禁止します。どのような通信データが発生した場合も、自動的にはダイヤルしません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

通信データが発生したときに、自動的にダイヤルするかどうかを設定します。

[未設定時]

remote autodial の設定に従います。

```
wan <number> isdn autodial enable
```

2.2.8　wan isdn activation

[機能]

レイヤ 1 起動種別の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

wan [<number>] isdn activation <type> [<time>]

[オプション]

<number>

- wan 定義番号
  wan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<type>

レイヤ 1 起動種別を指定します。

- always
  常時起動動作を指定します。
- per-call
  呼毎起動動作を指定します。

<time>

- 回線停止猶予時間
  <type>に per-call を指定した場合に通信終了後の回線同期停止猶予時間を、1 秒～300 秒の範囲で指定します。単位は、m(分)、s(秒) のどちらかを指定します。
  省略時は、60 秒を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

レイヤ 1 起動種別 (回線同期確立手順の方式) を設定します。
また、レイヤ 1 起動種別に呼毎起動動作を指定した場合は、回線停止猶予時間を設定します。

[注意]

呼毎起動動作を指定した場合は、回線同期外れ (線抜けなど) を検出することはできません。
また、回線の発着信が常時起動動作と比べて遅くなる場合があります。
通信終了後、指定した回線停止猶予時間後に D チャネルのデータリンク層 (レイヤ 2) を停止します。
その後、ISDN 網の仕様により、一定時間後に物理層 (レイヤ 1) が停止します。
呼毎起動動作を指定し、常時起動回線に接続した場合は、データリンク層 (レイヤ 2) は停止しますが、物理層 (レイヤ 1) は停止しません。
常時起動動作を指定し、呼毎起動回線に接続した場合は、データリンク層、物理層とも停止しません。
PRI インタフェースに対して呼毎起動動作を指定しても、常時起動動作となります。

[未設定時]

常時起動動作を指定したものとみなされます。

```
wan <number> isdn activation always
```

2.3　専用線情報

2.3.1　wan hsd flagdetect

[機能]

専用線のフラグ監視の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

wan [<number>] hsd flagdetect <mode>

[オプション]

<number>

- wan 定義番号
  wan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

フラグ監視機能の有無を指定します。

- disable
  フラグ監視機能を利用しません。
- enable
  フラグ監視機能を利用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

専用線接続で、フラグ監視機能を利用するかどうかを指定します。

[注意]

この機能を使用する場合は、相手装置がフラグ送出を実施していなければなりません。

[未設定時]

フラグ監視機能を利用しません。

```
wan <number> hsd flagdetect disable
```

2.4 フレームリレー回線情報

2.4.1 wan fr lmi

[機能]

フレームリレーの PVC 状態確認手順の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

wan [<number>] fr lmi <type>

[オプション]

<number>

- wan 定義番号
  wan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<type>

PVC 状態確認の手順を指定します。

- q933a
  ITU-T Q.933 Annex A に準拠します。
- off
  PVC 状態確認を行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

フレームリレーでの PVC 状態確認手順を、網契約に合わせて設定します。

[注意]

- この機能を使用する場合は、通信事業者との契約が必要です。
- PVC 状態確認の双方向手順はサポートしていません。

[未設定時]

ITU-T Q.933 Annex A に準拠するとみなされます。

```
wan <number> fr lmi q933a
```

2.4.2　wan fr fecn

[機能]

FECN による輻輳制御の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

wan [<number>] fr fecn <mode>

[オプション]

<number>

- wan 定義番号
  wan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

FECN によって輻輳制御を行うかどうかを指定します。

- on
  輻輳制御を行います。
- off
  輻輳制御を行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

FECN による輻輳制御について設定します。

[未設定時]

FECN によって輻輳制御を行うとみなされます。

```
wan <number> fr fecn on
```

2.4.3 wan fr becn

[機能]

BECN による輻輳制御の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

wan [<number>] fr becn <mode>

[オプション]

<number>

- wan 定義番号
  wan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

BECN によって輻輳制御を行うかどうかを指定します。

- on
  輻輳制御を行います。
- off
  輻輳制御を行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

BECN による輻輳制御について設定します。

[未設定時]

BECN によって輻輳制御を行うとみなされます。

```
wan <number> fr becn on
```

2.4.4　wan fr cllm

[機能]

CLLM による輻輳制御の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

wan [<number>] fr cllm <mode>

[オプション]

<number>

- wan 定義番号
  wan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

CLLM によって輻輳制御を行うかどうかを指定します。

- on
  輻輳制御を行います。
- off
  輻輳制御を行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

CLLM による輻輳制御について設定します。

[未設定時]

CLLM によって輻輳制御を行うとみなされます。

```
wan <number> fr cllm on
```

2.5 ATM 回線情報

2.5.1 wan atm vpi

[機能]

VPC の VPI 値の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B

[入力形式]

wan [<number>] atm vpi <vpi_value>

[オプション]

<number>

- wan 定義番号

  wan 定義の通し番号を、10 進数値で指定します。

  省略時は、0 を指定したものとみなされます。

<vpi_value>

- VPI 値

  使用する VPC の VPI 値を以下の範囲で指定します。

機種	拡張モジュール	範囲
Si-R570	ATM25M拡張モジュールL2 ATM155M拡張モジュールL2	0〜127
	ATM25M拡張モジュールH1 ATM155M拡張モジュールH1	0〜255
Si-R370	ATM25M拡張モジュールL2 ATM155M拡張モジュールL2	0〜127
Si-R260B		0〜127

[動作モード]

構成定義モード (管理者クラス)

[説明]

VPC(Virtual Path Connection) の VPI(Virtual Path Identifier) 値を設定します。

[未設定時]

0 が設定されたとみなされます。

```
wan <number> atm vpi 0
```

2.5.2　wan atm rate

[機能]

VPC の VP 速度の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B

[入力形式]

wan [<number>] atm rate <rate>

[オプション]

<number>

- wan 定義番号
  wan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<rate>

- VP 速度
  VP 速度を以下の範囲で指定します。

機種	拡張モジュール	範囲
Si-R570	ATM25M拡張モジュールL2 ATM155M拡張モジュールL2	64k～ 25m:8k刻み、または50k刻み
	ATM25M拡張モジュールH1	64k～ 25m:8k刻み、または50k刻み
	ATM155M拡張モジュールH1	200k～50m:8k刻み、または50k刻み
Si-R370	ATM25M拡張モジュールL2 ATM155M拡張モジュールL2	64k～ 25m:8k刻み、または50k刻み
Si-R260B		64k～ 25m:8k刻み、または50k刻み

kとmは単位を表し、kはKbpsをmはMbpsを示します。
0を指定した場合は、VP速度を設定しないものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

使用する VPC(Virtual Path Connection) の速度にあわせて VP 速度を設定します。

[注意]

ATM 拡張モジュール使用時には以下のことに注意してください。

- VP 速度設定なしの VPC と VP 速度設定ありの VPC は併用することができません。

Si-R260B 、ATM25M 拡張モジュール L2 および ATM155M 拡張モジュール L2 を使用する場合は、以下のことに注意してください。

- 複数 VPC 契約の場合は、同一 VPC 内は 1-VCC としてください。
  また、VP 契約速度は VP 速度として設定しないで、VC 速度として設定してください。

[未設定時]

VP 速度を設定しないものとみなされます。

```
wan <number> atm rate 0
```

2.5.3　wan atm oam

[機能]

VPC の OAM(F4) による制御の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B

[入力形式]

wan [<number>] atm oam <mode>

[オプション]

<number>

- wan 定義番号
  wan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- on
  以下 OAM(F4) の受信を受け付けます。
  - OAM(F4)-AIS
  - OAM(F4)-RDI
  - OAM(F4)-LPB
- off
  OAM(F4) の受信を受け付けません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

VPC(Virtual Path Connection) で OAM(F4) の受信を受け付けるかどうかを設定します。
OAM(F4) の受信を受け付ける場合、OAM(F4) の故障通知による VPC の故障検出が可能です。

[未設定時]

OAM(F4) の受信を受け付けないとみなされます。

```
wan <number> atm oam off
```

2.6　データ通信カード 情報

2.6.1　wan cardmodem pin

[機能]

PIN コード の設定

[適用機種]

			Si-R 240		

[入力形式]

wan [<number>] cardmodem pin <pin> [encrypted]

[オプション]

<number>

- wan 定義番号

  wan 定義の通し番号を、10 進数値で指定します。

  省略時は、0 を指定したものとみなされます。

<pin>

- PIN コード

  PIN コード を、4〜8 文字以内の数字で指定します。

  show コマンド で表示される暗号化された PIN コード を encrypted とともに指定することもできます。その場合、表示された文字列をそのまま正確に入力してください。文字列は 8 文字を超えていてもかまいません。

encrypted

- 暗号化認証パスワード 指定

  <password>に暗号化された PIN コード を設定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

PIN コード を設定します。

[注意]

PIN コード に対応しているデータ通信カード (Vodafone VC701SI) のみ有効です。

[未設定時]

PIN コード を照合しないものとみなされます。
もし、データ通信カード が PIN コード 照合する設定になっていた場合は、カード の初期化は失敗します。

第 3 章　ATM 情報の設定

3.1 ATM 情報

3.1.1 atm send clock

[機能]

送信クロックの設定

[適用機種]

Si-R 570	Si-R 370	Si-R 260B			

[入力形式]

atm [<slot>] send clock <source>

[オプション]

<slot>

- スロット番号
  ATM 拡張モジュールを挿入したスロット番号を、10 進数値で指定します。
  ただし、Si-R260B では、必ず"mb"(基本ボード) を指定してください。
  省略時は、
  Si-R260B 以外
  0 を指定したものとみなされます。
  Si-R260B
  mb を指定したものとみなされます。

範囲	機種
0〜3	Si-R570
0〜1	Si-R370

<source>

データ送信時に使用するクロックの参照元を指定します。

- self
  本装置で生成したクロックを送信クロックとして使用します。
- recovery
  受信データから再生したクロックを送信クロックとして使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

データ送信時に使用するクロックの参照元を設定します。

[注意]

ATM155M 拡張モジュール H1 で DSU 接続する場合は、送信クロックの設定を recovery にする必要があります。

[未設定時]

本装置で生成したクロックを送信クロックとして使用するものとみなされます。

```
atm <slot> send clock self
```

第 4 章　スイッチ情報の設定

- スイッチ定義番号の指定範囲

  本章のコマンドの [オプション] に記載されている<number>(スイッチ定義番号) に指定するスイッチ定義の通し番号 (10 進数値) は、機種ごとに以下に示す範囲で指定してください。

範囲	機種
0	Si-R180

- ポート番号の指定範囲

  本章のコマンドの [オプション] に記載されている<port_no>に指定するポートの番号 (10 進数値) は、機種ごとに以下に示す範囲で指定してください。

範囲	機種
1〜4	Si-R180

4.1　スイッチ共通情報

4.1.1　switch use

[機能]

スイッチポート (SW1〜SW4) 切り替えの設定

[適用機種]

Si-R 180

[入力形式]

switch [<number>] use <mode>

[パラメタ]

<number>

- スイッチ定義番号
  スイッチ定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

LAN1 ポートをスイッチポートとして利用するかを指定します。

- on
  スイッチポートを使用
- off
  スイッチポートを使用しない

[動作モード]

構成定義モード (管理者クラス)

[説明]

LAN1 ポートのモードを設定します。
モードとして on を指定した場合、LAN1 はスイッチポートとして利用できます。

[注意]

LAN1 ポートをスイッチポートとして利用するとした場合、スイッチポートでは STP を利用することはできません。
スイッチポートを利用し、複数のネットワークまたは Tagged VLAN を利用する場合は、必ずスイッチ定義の VLAN ID と同じ VLAN ID を lan 定義で設定してください。一致する ID が定義されていない場合は通信ができなくなります。

[未設定時]

LAN1 ポートでスイッチポートは利用しないものとみなされます。

```
switch <number> mode off
```

4.1.2 switch tag transparent

[機能]

スイッチポート (SW1～SW4) の VLAN tag 透過転送の設定

[適用機種]

Si-R 180

[入力形式]

switch [<number>] tag transparent <mode>

[パラメタ]

<number>

- スイッチ定義番号
  スイッチ定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

スイッチポート上で tag 付 VLAN フレームの透過モードを指定します。

- disable
  VLAN tag を透過的に転送しません。
- enable
  VLAN tag をすべて透過します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

スイッチポートの VLAN フレームの tag の扱いについて設定します。
モードとして enable を指定した場合、すべての VLAN tag は透過的に転送されます。

[注意]

- <mode>に enable を設定した場合、スイッチ定義で定義された VLAN 定義はすべて無視されます。

[未設定時]

スイッチポート上で VLAN tag は透過的に転送しないものとみなされます。

```
switch <number> tag transparent disable
```

4.1.3　switch age

[機能]

スイッチポート (SW1～SW4) の学習テーブル生存時間の設定

[適用機種]

Si-R 180

[入力形式]

switch [<number>] age <timer>

[パラメタ]

<number>

- スイッチ定義番号
  スイッチ定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<timer>

スイッチのブリッジ学習テーブルの生存時間を 0～4080 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒) のどれかを指定します。
ただし、設定された値は設定値を超えない最大の 16 の倍数に丸められます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

スイッチのブリッジ学習テーブルの生存時間を設定します。

[未設定時]

スイッチの学習テーブル生存時間として 288 秒が指定されたものとみなされます。

```
switch <number> age 288s
```

4.2 スイッチポート情報

4.2.1 switch port use

[機能]

スイッチポート (SW1〜SW4) 利用可否の設定

[適用機種]

Si-R 180

[入力形式]

switch [<number>] port <port_no> use <mode> [<tag_mode>]

[パラメタ]

<number>

- スイッチ定義番号
  スイッチ定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<port_no>

- スイッチポート番号
  スイッチポートの番号を、10 進数値で指定します。

<mode>

スイッチポートの利用有無を指定します。

- on
  スイッチポートを利用します。
- off
  スイッチポートを利用しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

スイッチポート利用可否を設定します。
スイッチポートを利用しない場合は、そのポートのリンクは UP しません。

[未設定時]

スイッチポートを利用するものとみなされます。

```
switch <number> port <port_no> use on
```

4.2.2　switch port mode

[機能]

通信速度の設定

[適用機種]

Si-R 180

[入力形式]

switch [<number>] port <port_no> mode <speed>

[パラメタ]

<number>

- スイッチ定義番号
  スイッチ定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<port_no>

- スイッチポート番号
  スイッチポートの番号を、10 進数値で指定します。

<speed>

スイッチポートの通信速度を指定します。

- auto
  通信速度を接続先とのネゴシエーションによって自動的に設定されます。
- 通信速度
  速度固定で動作させる場合に、以下の値のどちらかを設定します。

10	10Mbps 固定で動作します。
100	100Mbps 固定で動作します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

スイッチポート (SW1～SW4) の通信速度の設定を行います。

[未設定時]

スイッチポートを通信速度として自動決定するものとみなされます。

```
switch <number> port <port_no> mode auto
```

4.2.3 switch port duplex

[機能]

全二重/半二重の設定

[適用機種]

Si-R 180

[入力形式]

switch [<number>] port <port_no> duplex <duplex>

[パラメタ]

<number>

- スイッチ定義番号
  スイッチ定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<port_no>

- スイッチポート番号
  スイッチポートの番号を、10 進数値で指定します。

<duplex>

- 全二重/半二重モード
  - **full** 全二重 (Full duplex) 固定で動作します。
  - **half** 半二重 (Half duplex) 固定で動作します。

本コマンドは,switch port mode コマンドで通信速度の固定値を指定した場合にだけ指定できます。
(通信速度を auto に設定すると、このコマンドの設定は無効になります。)

[動作モード]

構成定義モード (管理者クラス)

[説明]

スイッチポート (SW1～SW4) の全二重／半二重を設定します。

[注意]

- switch <number> mode コマンドで auto を指定した場合は、本コマンドの設定内容は無効となり、接続装置とのオートネゴシエーションの結果により動作します。

[未設定時]

スイッチポートが全二重モードに設定されたものとみなします。

```
switch <number> port <port_no> duplex full
```

4.2.4　switch port mdi

[機能]

MDI 機能の設定

[適用機種]

Si-R 180

[入力形式]

switch [<number>] port <port_no> mdi <mode>

[パラメタ]

<number>

- スイッチ定義番号
  スイッチ定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<port_no>

- スイッチポート番号
  スイッチポートの番号を、10 進数値で指定します。

<mode>

MDI のモードを指定します。

- auto
  オートネゴシエーションにより MDI/MDI-X を決定します。
- mdi
  MDI モード固定に設定します。
- mdix
  MDI-X モード固定に設定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

スイッチポート (SW1～SW4) の MDI 機能の設定を行います。

[注意]

- MDI の自動検出は、switch port mode の設定が auto である場合にのみ有効となります。
  switch port mode の設定が auto でない場合は、MDI の自動検出を指定しても、MDI-X として動作します。また、switch port mode が auto と設定されいる場合は本設定にかかわらず常に auto が指定されたものとみなされます。

[未設定時]

スイッチポートの MDI 機能として auto が設定されたものとみなします。

```
switch <number> port <port_no> mdi auto
```

4.2.5 switch port flowctl

[機能]

フロー制御機能の設定

[適用機種]

Si-R 180

[入力形式]

switch [<number>] port <port_no> flowctl <mode>

[パラメタ]

<number>

- スイッチ定義番号
  スイッチ定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<port_no>

- スイッチポート番号
  スイッチポートの番号を、10 進数値で指定します。

<mode>

- on
  フロー制御を有効にします。
- off
  フロー制御を無効にします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

スイッチポート (SW1～SW4) でフロー制御機能を使用するかどうかを設定します。

[未設定時]

スイッチポートのフロー制御機能を送受信ともに使用するものとみなされます。

```
switch <number> port <port_no> flowctl on
```

4.2.6　switch port vlan tag

[機能]

Tag あり VLAN 登録

[適用機種]

Si-R 180

[入力形式]

switch [<number>] port <port_no> vlan tag <vidlist>

[オプション]

<number>

- スイッチ定義番号
  スイッチ定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<port_no>

- スイッチポート番号
  スイッチポートの番号を、10 進数値で指定します。

<vidlist>

- tag 付き VLAN-ID リスト
  tag 付き vlan の ID を設定します。
  複数の ID を指定する場合は、","(コンマ) で区切ります。(例:"10,20,30")
  複数の番号が続く場合、"-"(ハイフン) で区切ります (例:"1-4")

[動作モード]

構成定義モード (管理者クラス)

[説明]

Tagged VLAN ID の設定を行います。

[注意]

- スイッチポート (SW1～SW4) をスイッチング HUB として利用する場合、設定は不要です。また、スイッチポートを利用する lan 定義では lan [<number>] vlan bind 定義で<bind_type>に"switch"を選択し、lan [<number>] vlan tag vid は設定不要です。
- スイッチポートを利用する lan vlan tag vid で指定された VLAN-ID と同じ ID が switch port vlan tag または switch port vlan untag のどちらかで設定されている必要があります。同一 ID が設定されていない場合は通信ができません。

[未設定時]

Tagged VLAN ID は存在しないものとみなされます。

4.2.7 switch port vlan untag

[機能]

Tag なし VLAN 登録

[適用機種]

Si-R 180

[入力形式]

switch [<number>] port <port_no> vlan untag <vidlist>

[オプション]

<number>

- スイッチ定義番号
  スイッチ定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<port_no>

- スイッチポート番号
  スイッチポートの番号を、10 進数値で指定します。

<vidlist>

- tag なし VLAN-ID リスト
  tag なし vlan の ID を設定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

Untagged VLAN ID の設定を行います。

[注意]

- tag なし VLAN-ID は複数設定することはできません。
- スイッチポート (SW1～SW4) をスイッチング HUB として利用する場合、設定は不要です。また、スイッチポートを利用する lan 定義では lan [<number>] vlan bind 定義で<bind_type>に"switch"を選択し、lan [<number>] vlan tag vid は設定不要です。
- スイッチポートを利用する lan vlan tag vid で指定された VLAN-ID と同じ ID が switch port vlan tag または switch port vlan untag のどちらかで設定されている必要があります。同一 ID が設定されていない場合は通信ができません。

[未設定時]

tag なし VLAN-ID として 1 が指定されたものとみなされます。

```
switch <number> port <port_no> vlan untag 1
```

第 5 章　LAN 情報の設定

- lan 定義番号の指定範囲

  本章のコマンド の [オプション] に記載されている<number>(lan 定義番号) に指定する lan 定義の通し番号 (10 進数値) は、機種ごとに以下に示す範囲で指定してください。

範囲	機種
0〜19	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
0〜9	Si-R180

5.1 lan 共通情報

5.1.1 lan bind

[機能]

利用する物理回線の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] bind <slot> [<line>]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<slot>

利用する回線のボードが、どのスロットに挿入されているかを指定します。
Si-R260B Si-R240 Si-R220B Si-R180 では、必ず"mb"(基本ボード) を指定してください。
Si-R180 では TAG 透過モードで使用する場合は"switch"(スイッチポート (SW1〜SW4)) を指定し、[<line>] には使用するスイッチ情報設定の<number>を指定してください。

- mb
  利用する回線が、基本ボード上にある場合に指定します。
- switch
  TAG 透過モードを利用しかつスイッチポートを利用する場合に指定します。
- スロット番号
  ボードが挿入されているスロットの番号を、10 進数値で指定します。

範囲	機種
0〜3	Si-R570
0〜1	Si-R370

<line>

- 回線番号
  同一のボードに複数の回線がある場合に、どの回線を利用するか指定します。
  Si-R180 では LAN0 ポートを利用する場合は 0、LAN1 ポートを利用する場合は 1 を指定します。
  Si-R180 でスイッチポートを利用する場合 (<slot>に"switch"を指定した場合) はスイッチ情報定義の<number>を指定します。
  省略時は、0 を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

lan 定義で利用する物理回線を設定します。
複数の lan 定義で同一の回線を指定すると、もっとも小さい定義番号を持つ lan 定義だけが有効となり、ほかの lan 定義は無効となります。

[注意]

Si-R570 Si-R370 の場合は以下に注意してください。

- 本コマンドで指定した回線が Ethernet ではない場合、この lan 定義は無効となります。

Si-R180 の場合は以下に注意してください。

- 本コマンドで指定したスイッチ情報定義が TAG 透過モードでない場合、通信ができません。

[未設定時]

基本ボード上の、回線番号が定義番号<number>となる回線を設定したものとみなされます。

```
lan <number> bind mb <number>
```

5.1.2 lan mode

[機能]

通信速度および通信モードの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] mode <speed> [<duplex>]

[オプション]

<number>

- lan 定義番号

  lan 定義の通し番号を、10 進数値で指定します。

  省略時は、0 を指定したものとみなされます。

<speed>

通信速度を指定します。

- auto

  通信速度を自動的に設定する場合に指定します。通信速度と共に、全二重/半二重モードが HUB とのネゴシエーションによって自動的に設定されます。

- 通信速度

  通信速度を固定して動作させる場合に、以下のどれかを指定します。

  1000(1Gbps 固定で動作する) の指定は、Si-R570 の基本ボード上の LAN ポートに対してだけ有効です。Si-R570 以外では指定できません。

  10 10Mbps 固定で動作します。

  100 100Mbps 固定で動作します。

  1000 1Gbps 固定で動作します。

<duplex>

- 全二重/半二重モード

  <speed>で通信速度の固定値を指定した場合にだけ指定できます。以下のどちらかを指定します。

  <speed>に 1000 を指定した場合は、<duplex>の指定は無効となり、全二重 (Full duplex) 固定で動作します。

  full 全二重 (Full duplex) 固定で動作します。

  half 半二重 (Half duplex) 固定で動作します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

Ethernet インタフェースの動作モードを設定します。

[未設定時]

通信速度および全二重/半二重モードを自動設定するものとみなされます。

```
lan <number> mode auto
```

5.1.3 lan mdi

[機能]

MDI の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] mdi <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

MDI のモードを指定します。

- auto
  MDI を自動検出します。
  Si-R260B Si-R240 Si-R220B Si-R180 では指定できません。
- mdi
  MDI として動作します。
- mdix
  MDI-X として動作します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

MDI のモードを設定します。

[注意]

MDI の自動検出は、lan mode の設定が auto である場合にのみ有効です。
lan mode の設定が auto でない場合は、MDI の自動検出を指定しても、MDI として動作します。
MDI の設定は、基本ボード上の LAN ポートでのみ有効です。
スロットに挿入してあるボード上では動作しません。
Si-R260B Si-R240 Si-R220B の LAN0 ポートに対する本コマンドの設定は無効です。LAN0 ポートは、装置前面の to HUB to PC スイッチでだけ設定を変更することができます。
Si-R180 の LAN1 ポート (スイッチ機能未使用時) に対する本コマンドの設定は無効です。MDI として動作します。

[未設定時]

(Si-R570 Si-R370 の場合)MDI を自動検出するものとみなされます。

```
lan <number> mdi auto
```

(Si-R260B Si-R240 Si-R220B Si-R180 の場合)MDI として動作します。

```
lan <number> mdi mdi
```

5.1.4 lan flowctl

[機能]

フロー制御機能の設定

[適用機種]

Si-R 570 | Si-R 370

[入力形式]

lan [<number>] flowctl <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- on
  フロー制御機能を使用します。
- off
  フロー制御機能を使用しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

フロー制御機能を使用するかどうかを設定します。
フロー制御機能は、基本ボード上の LAN ポートでのみ有効です。
スロットに挿入してあるボード上では動作しません。

[未設定時]

フロー制御機能を使用するものとみなされます。

```
lan <number> flowctl on
```

5.1.5　lan type

[機能]

使用ポートの設定

[適用機種]

Si-R 570					

[入力形式]

lan [<number>] type <type>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<type>

- auto
  ポートを自動選択します。
- metal
  通常ポート (RJ45) を使用します。
- fiber
  ファイバポートを使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

Si-R570 では、基本ボード上の LAN0/1 ポートと LAN0/1 ファイバポートを排他利用することができます。
本コマンドでは、どちらのポートを利用するかの設定をします。

[未設定時]

ポートを自動選択するものとみなされます。

```
lan <number> type auto
```

5.1.6 lan mtu

[機能]

送信パケット最大長 (MTU 値) の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] mtu <mtu>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mtu>

- MTU 値
  MTU 値を、200〜1500 の 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

LAN に対して送信するパケットの MTU 値を設定します。
MTU 値を変更すると、この LAN に対して送信するパケットの最大長が変更されます。

[未設定時]

MTU 値に 1500 を指定したものとみなされます。

```
lan <number> mtu 1500
```

5.1.7　lan shaping

[機能]

シェーピング機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] shaping <mode> [<rate>]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- on
  シェーピングを使用します。
- off
  シェーピングを使用しません。

<rate>

- 最大送出レート
  最大送出レートを、10 進数値と単位文字で指定します。
  10 進数値の末尾に k または m の単位文字を付与することで単位を指定できます。
  単位文字を付与しない場合、単位は Kbps となります。
  単位文字 k を付与した場合、単位は Kbps となります。
  単位文字 m を付与した場合、単位は Mbps となります。
  1Kbps は 1000bps、1Mbps は 1000Kbps です。

範囲	機種
1～1000000 1k～1000000k 1m～1000m	Si-R570
1～100000 1k～100000k 1m～100m	上記以外

[動作モード]

構成定義モード (管理者クラス)

[説明]

シェーピング機能について設定します。
<mode>が on の場合、<rate>で設定したレートに送信を抑制します。回線速度を上回る値を設定した場合は、実質的にシェーピングは機能しません。
<mode>が off の場合、<rate>は設定できません。

[注意]

シェーピングを使用しない場合、帯域制御は有効に動作しません。

[未設定時]

シェーピングを使用しないものとみなされます。

```
lan <number> shaping off
```

5.2　LAN ポート バックアップ関連情報

5.2.1　lan backup bind

[機能]

バックアップとして利用する物理回線の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B

[入力形式]

lan [<number>] backup bind <slot> [<line>]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<slot>

利用する回線のボードが、どのスロットに挿入されているかを指定します。
Si-R260B Si-R240 Si-R220B では、必ず"mb"(基本ボード) を指定してください。

- mb
  利用する回線が、基本ボード上にある場合に指定します。
- スロット番号
  ボードが挿入されているスロットの番号を、10 進数値で指定します。

範囲	機種
0〜3	Si-R570
0〜1	Si-R370

<line>

- 回線番号
  同一のボードに複数の回線がある場合に、どの回線を利用するか指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

LAN ポートバックアップ機能を利用する場合に、lan 定義でバックアップとして利用する物理回線を設定します。ここで、バックアップ用として設定された物理回線は、別の lan 定義で利用することはできません。
また、すでに別の lan 定義で利用されている物理回線は、バックアップ用として利用できません。

[注意]

Si-R570 Si-R370 の場合は以下に注意してください。

- 本コマンドで指定した回線が Ethernet ではない場合、この backup 定義は無効となります。

[未設定時]

LAN ポートバックアップ機能を利用しないものとみなされます。

5.2.2　lan backup mode

[機能]

使用するポートの選択方法の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B

[入力形式]

lan [<number>] backup mode <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

master ポートと backup ポートの両方が使用可能のときに使用するポートの選択方法を指定します。

- master
  master ポートを優先的に使用します。
- earlier
  先にリンクアップして使用可能になったほうのポートを使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

master ポートと backup ポートの両方が使用可能のときに使用するポートの選択方法を指定します。

[未設定時]

master ポートを優先的に使用します。

```
lan <number> backup mode master
```

5.3 LAN ポート 閉塞関連情報

5.3.1 lan recovery

[機能]

自動復旧モード の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] recovery <mode> <startup>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- auto
  LAN 障害復旧時に自動復旧します。
- manual
  LAN 障害発生時に自動的に閉塞状態となり、LAN 障害が復旧した場合でもオペレータ指示があるまで復旧させません。

<startup>

- up
  装置起動時、および動的定義反映時は閉塞していない状態で動作を開始します。
- down
  装置起動時、および動的定義反映時は閉塞状態で動作を開始し、オペレータからの閉塞状態解除指示を待ちます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

LAN 障害の復旧時の動作モード を設定します。
起動時の動作は以下のようになります。

<mode>/<startup>	起動時のLANポートの状態	
	リンクアップ可能	リンクアップ不可能
auto / up	リンクアップ／通信可能	リンクダウン／通信不可
auto /down	閉塞状態に入り通信不可	閉塞状態に入り通信不可
manual/ up	リンクアップ／通信可能	リンクダウン／通信不可(※)
manual/down	閉塞状態に入り通信不可	閉塞状態に入り通信不可

※ リンクアップ不可であっても、起動時に最初から
閉塞状態に入るわけではないので注意してください

[注意]

VLAN インタフェースに対して本コマンドを設定しても、無効となります。閉塞状態に入ると、リンクランプは消灯します。
閉塞状態では、LAN 定義がない場合と同じ状態になります。ランプ表示もそれに準じたものになります。

[未設定時]

装置起動時、および動的定義反映時に閉塞していない状態で動作を開始し、LAN 障害発生時には障害復旧後に自動復旧します。

```
lan <number> recovery auto up
```

5.4 IP 関連情報

5.4.1 lan ip address

[機能]

IP アドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip address <address>/<mask> <broadcast>

[オプション]

<number>

- lan 定義番号

  lan 定義の通し番号を、10 進数値で指定します。

  省略時は、0 を指定したものとみなされます。

<address>/<mask>

- IP アドレス/マスクビット数 (またはマスク値)

  LAN インタフェースに割り当てる IP アドレスとマスクビット数の組み合わせを指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。

  IP アドレスの指定可能な範囲は以下のとおりです。

  0.0.0.0

  1.0.0.1 ～ 126.255.255.254

  128.0.0.1 ～ 191.255.255.254

  192.0.0.1 ～ 223.255.255.254

マスクビット数の場合は、2～30 の 10 進数値で指定します。
マスク値の場合は、192.0.0.0～255.255.255.252 の範囲で指定します。
以下に、有効な記述形式を示します。

- IP アドレス/マスクビット数 (例: 192.168.1.1/24)
- IP アドレス/マスク値 (例: 192.168.1.1/255.255.255.0)

<broadcast>

ブロードキャストアドレスを指定します。

- 0

  0.0.0.0 の場合に指定します。

- 1

  255.255.255.255 の場合に指定します。

- 2

  <address>/<mask>から求められる、ネットワークアドレス + オール 0 の場合に指定します。

- 3

  <address>/<mask>から求められる、ネットワークアドレス + オール 1 の場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本装置上の LAN インタフェースに、IP アドレス、マスクビット数 (またはマスク値)、およびブロードキャストアドレスを設定します。
LAN インタフェースに割り当てる IP アドレス、ネットマスクを設定します。IP アドレスを設定していないと通信できません。
DHCP クライアントで運用しない LAN インタフェースの場合は、<address>/<mask>に 0.0.0.0/0 を設定すると通信できなくなります。
DHCP クライアントで運用する LAN インタフェースの場合は、DHCP サーバから IP アドレスなどを割り当てられるので、<address>/<mask>に 0.0.0.0/0 を設定しなければなりません。

[未設定時]

IP アドレスがないものとみなされます。

```
lan <number> ip address 0.0.0.0/0 0
```

5.4.2 lan ip alias

[機能]

セカンダリ IP アドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip alias <address>/<mask> <broadcast>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<address>/<mask>

- セカンダリ IP アドレス/マスクビット数 (またはマスク値) LAN インタフェースに割り当てるセカンダリ IP アドレスとマスクビット数の組み合わせを指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。
  セカンダリ IP アドレスの指定可能な範囲は以下のとおりです。

  0.0.0.0
  1.0.0.1 〜 126.255.255.254
  128.0.0.1 〜 191.255.255.254
  192.0.0.1 〜 223.255.255.254

マスクビット数の場合は、2〜30 の 10 進数値で指定します。
マスク値の場合は、192.0.0.0〜255.255.255.252 の範囲で指定します。
以下に、有効な記述形式を示します。

- セカンダリ IP アドレス/マスクビット数 (例: 192.168.1.1/24)
- セカンダリ IP アドレス/マスク値 (例: 192.168.1.1/255.255.255.0)

<broadcast>

ブロードキャストアドレスを指定します。

- 0
  0.0.0.0 の場合に指定します。
- 1
  255.255.255.255 の場合に指定します。
- 2
  <address>/<mask>から求められる、ネットワークアドレス + オール 0 の場合に指定します。
- 3
  <address>/<mask>から求められる、ネットワークアドレス + オール 1 の場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本装置上の LAN インタフェースに、セカンダリ IP アドレス、マスクビット数 (またはマスク値)、およびブロードキャストアドレスを設定します。

[注意]

セカンダリ IP アドレスが属するネットワークには、以下の機能を適用できません。

- RIP の送受信機能
- OSPF の送受信機能
- DHCP 機能

[未設定時]

セカンダリ IP アドレスがないものとみなされます。

```
lan <number> ip alias 0.0.0.0 0
```

5.4.3 lan ip dhcp service

[機能]

DHCP 機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip dhcp service <mode> [<address1> [<address2>]]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

DHCP 機能のモード を指定します。

- server
  LAN インタフェースに対して DHCP サーバサービスを行います。
- relay
  LAN インタフェースに対して DHCP リレーエージェントサービスを行います。
- client
  LAN インタフェースに対して DHCP サービスを要求します。
- off
  LAN インタフェースに対して DHCP 機能を提供しません。

<address1>,<address2>

- DHCP サーバアドレス
  <mode>に relay を指定した場合に有効なパラメタです。DHCP サービス要求を転送する、中継先 DHCP サーバの IP アドレスを 2 つまで指定することができます。
  指定可能な範囲は以下のとおりです。

  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[動作モード]

構成定義モード (管理者クラス)

[説明]

LAN インタフェースに対して、DHCP 機能情報を設定します。

[未設定時]

DHCP サーバ機能を使用しないものとみなされます。

```
lan <number> ip dhcp service off
```

5.4.4 lan ip dhcp info

[機能]

DHCP 配布情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip dhcp info dns <dns1> [<dns2>]
lan [<number>] ip dhcp info address <address>/<mask> [<num>]
lan [<number>] ip dhcp info time <time>
lan [<number>] ip dhcp info gateway <gateway>
lan [<number>] ip dhcp info domain <domain>
lan [<number>] ip dhcp info timeserver <timeserver>
lan [<number>] ip dhcp info ntpserver <ntpserver>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<dns1>

- DNS サーバ IP アドレス
  DHCP クライアントに配布する、DNS サーバの IP アドレスを指定します。
  0.0.0.0 を指定した場合は、設定が削除されます。
  指定可能な範囲は以下のとおりです。

  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

<dns2>

- セカンダリ DNS サーバ IP アドレス
  DHCP クライアントに配布する、セカンダリ DNS サーバの IP アドレスを指定します。
  0.0.0.0 を指定した場合は、設定が削除されます。
  指定可能な範囲は以下のとおりです。

  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

<address>/<mask>

- 割り当て開始 IP アドレス/マスクビット数 (またはマスク値)
  DHCP クライアントにリースする先頭アドレス (IP アドレスとマスクビット数の組み合わせ) を指定します。
  マスク値は、最上位ビットから 1 で連続した値にしてください。
  以下に、有効な記述形式を示します。

- IP アドレス/マスクビット数 (例: 192.168.1.2/24 注)
- IP アドレス/マスク値 (例: 192.168.1.2/255.255.255.0 注)

<num>が 16、<address>が 192.168.1.2 の場合に、192.168.1.2〜192.168.1.17 のアドレスがリースされます。

0.0.0.0/0(0.0.0.0/0.0.0.0) を指定した場合は、設定が削除されます。

指定可能な範囲は以下のとおりです。

1.0.0.1 〜 126.255.255.254
128.0.0.1 〜 191.255.255.254
192.0.0.1 〜 223.255.255.254

<num>

- 割り当てアドレス数

lan ip dhcp service の<mode>に server を指定した場合にだけ有効です。DHCP サーバサービスの場合に、割り当て可能な IP アドレスの総数を 1〜253 の 10 進数値で指定します。

省略時は、32 を指定したものとみなされます。

ホストデータベース機能を使用すると、特定の DHCP クライアントに対して固有の IP アドレスを割り当てることができます。この場合の IP アドレスは、割当て先頭 IP アドレスと割当てアドレス数によって規定される動的割当て範囲である必要はありません。

<time>

- 割り当て時間

DHCP クライアントに配布する情報の有効時間を、0 秒〜365 日の範囲で指定します。

単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。

0 秒を指定した場合は、設定が削除され、有効時間監視なし (無限) とみなされます。

<gateway>

- デフォルトルータ IP アドレス

DHCP クライアントに配布する、デフォルトルータの IP アドレスを設定します。

0.0.0.0 を指定した場合は、設定が削除されます。

指定可能な範囲は以下のとおりです。

1.0.0.1 〜 126.255.255.254
128.0.0.1 〜 191.255.255.254
192.0.0.1 〜 223.255.255.254

<domain>

- ドメイン名

DHCP クライアントに配布するドメイン名を、0x21,0x23〜0x7e の 80 文字以内の ASCII 文字列で指定します。なお、RFC1034 では英数字、"-"(ハイフン)、"."(ピリオド) でドメイン名をつけることを推奨しています。

<timeserver>

- TIME サーバ IP アドレス

DHCP クライアントに配布する、TIME サーバの IP アドレスを設定します。

0.0.0.0 を指定した場合は、設定が削除されます。

指定可能な範囲は以下のとおりです。

1.0.0.1 〜 126.255.255.254
128.0.0.1 〜 191.255.255.254
192.0.0.1 〜 223.255.255.254

<ntpserver>

- NTP サーバ IP アドレス
  DHCP クライアントに配布する、NTP サーバの IP アドレスを設定します。
  0.0.0.0 を指定した場合は、設定が削除されます。
  指定可能な範囲は以下のとおりです。

  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[動作モード]

構成定義モード (管理者クラス)

[説明]

DHCP サーバ機能を使用する場合に、クライアントに配布する情報を設定します。

[未設定時]

DHCP で配布される情報は設定されないものとみなされます。

5.4.5　lan ip dhcp macauth use

[機能]

DHCP MAC アドレスチェック機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip dhcp macauth use <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- on
  DHCP MAC アドレスチェック機能を使用します。
- off
  DHCP MAC アドレスチェック機能を使用しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

DHCP クライアントからの要求に対して、MAC アドレスのチェックを行うかどうかを設定します。

[未設定時]

MAC アドレスチェックを行わないものとみなされます。

```
lan <number> ip dhcp macauth use off
```

5.4.6 lan ip dhcp macauth db

[機能]

DHCP MAC アドレスチェック機能の使用するデータベースの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip dhcp macauth db <db>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<db>

- host
  ホストデータベース情報を使用します。
- aaa
  AAA 情報を使用します。
- both
  ホストデータベース情報と AAA 情報の両方を使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

DHCP MAC アドレスチェック機能で使用するデータベースを設定します。
"both"を設定した場合、ホストデータベース情報が優先され、ホストデータベース情報に該当する MAC アドレスがない場合に AAA 情報を使用します。

[未設定時]

ホストデータベース情報を使用するものとみなされます。

```
lan <number> ip dhcp macauth db host
```

5.4.7　lan ip dhcp macauth aaa

[機能]

DHCP MAC アドレスチェック機能で使用する AAA グループの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip dhcp macauth aaa <group_id>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

DHCP MAC アドレスチェック機能で使用する AAA 情報のグループ ID を設定します。

[未設定時]

AAA 情報のグループを指定していないものとみなされます。

5.4.8 lan ip proxyarp

[機能]

ProxyARP 機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip proxyarp <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- on
  ProxyARP 機能を使用します。
- off
  ProxyARP 機能を使用しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ProxyARP 機能を使用するかどうかを設定します。

[未設定時]

ProxyARP 機能を使用するものとみなされます。

```
lan <number> ip proxyarp on
```

5.4.9　lan ip localproxyarp

[機能]

ローカル ProxyARP 機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip localproxyarp <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- on
  ローカル ProxyARP 機能を使用します。
- off
  ローカル ProxyARP 機能を使用しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ローカル ProxyARP 機能を使用するかどうかを設定します。
on を設定した場合は、ローカル ProxyARP が動作すると共に ICMP redirect パケットの送出が抑止されます。

[注意]

ローカル ProxyARP 機能は、端末間の直接通信が意図的に禁止されているネットワークでのみ使用してください。

[未設定時]

ローカル ProxyARP 機能を使用しないものとみなされます。

```
lan <number> ip localproxyarp off
```

5.4.10 lan ip route

[機能]

IPv4 スタティック経路情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip route <count> <address>/<mask> <next_hop> [<metric> [<distance>]]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- スタティック経路情報定義番号
  スタティック経路情報の定義番号を、10 進数値で指定します。

範囲	機種
0〜1999	Si-R570
0〜1249	Si-R370
0〜255	Si-R260B Si-R240 Si-R220B
0〜127	Si-R180

<address>/<mask>

- IPv4 アドレス/マスクビット数 (またはマスク値)
  あて先ネットワークを IPv4 アドレスとマスクビット数の組み合わせで指定します。
  マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
  - IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
  - IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)
- default
  あて先ネットワークとしてデフォルトルートを設定する場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<next_hop>

- 中継ルータ IPv4 アドレス
  あて先ネットワークへパケットを送信するときの中継ルータの IPv4 アドレスを指定します。
- dhcp
  DHCP サーバから受け取った router オプションのゲートウェイアドレスを中継ルータとして使用する場合に指定します。
  <number>で指定した lan の定義上に、DHCP クライアントの設定がある場合のみ有効となります。

<metric>

- RIP メトリック値
  このスタティック経路情報を RIP に再配布するときのメトリック値を、1〜15 の 10 進数値で指定します。
  省略時は、1 を指定したものとみなされます。

<distance>

- 優先度
  このスタティック経路情報の優先度を 10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。
  <next_hop>に中継ルータ IPv4 アドレスを指定した場合は、0〜254 の範囲となり、省略時は、0 を指定したものとみなされます。
  <next_hop>に dhcp を指定した場合は、1〜254 の範囲となり、省略時は、1 を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv4 スタティック経路 (静的経路) 情報を設定します。
RIP メトリック値は、スタティック経路情報を RIP に再配布するときのメトリック値を設定します。
RIP に再配布したときは、設定した RIP メトリック値+1 のメトリック値で RIP テーブルに登録されます。
優先度は、同じあて先への経路情報が複数ある場合、優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。各ダイナミックルーティングプロトコルの優先度については、routemanage ip distance コマンドを参照してください。
優先度に 0 が設定されているときは、routemanage interface floating コマンドでのフローティング設定に応じてフローティング動作が切り替わります。優先度に 1 以上が設定されているときは、常にフローティング動作します。
フローティング動作する場合、<next_hop>で指定した中継ルータと隣接しているインタフェースが通信可能な状態 (リンクアップなど) であれば、スタティック経路情報をルーティングテーブルに追加します。通信不可能な状態 (リンクダウンなど) であれば、ルーティングテーブルから削除します。
フローティング動作しない場合は、インタフェースの状態にかかわらず常にスタティック経路情報をルーティングテーブルに追加します。
以下に、各設定値とフローティング動作の関係を示します。

<distance> 設定値	インタフェース経路の フローティング設定	スタティック経路の フローティング動作
0(省略値)	使用しない	しない
0(省略値)	使用する	する
1以上	使用しない	する
1以上	使用する	する

以下のような用途でスタティック経路情報を使用する場合、フローティング動作するとなるように設定してください。

- IP ルーティングおよびダイナミックルーティングでの広報で、スタティック経路の出口
  インタフェースで異常が発生した場合、ルーティングテーブルよりスタティック経路を削除します。
- あて先が同じ経路をダイナミックルーティングで受信した場合、優先度関係により経路を決定します。

複数のスタティック経路情報でECMP機能を使用するときは、あて先、RIPメトリック値、優先度がそれぞれ同じとなるようにスタティック経路情報を設定します。また、ECMP機能を使用する場合は、routemanage ip ecmp modeコマンドでECMPを使用するように設定します。
ECMPとなるスタティック経路情報は、同じあて先への経路情報ごとに装置全体で4個まで定義できます。
DHCPクライアント運用を行う場合で、Routerオプションでゲートウェイアドレスが通知された場合、通常はこのゲートウェイアドレス向け優先度0のデフォルトルートが自動生成されます。ここで、優先度0のデフォルトルートではなく、任意のあて先で任意の優先度のスタティック経路として生成したい場合は、<next_hop>にdhcpと指定するIPv4スタティック経路を設定することで実現できます。この場合、優先度0のデフォルトルートは自動生成されません。
このIPv4スタティック経路は、DHCPクライアントがDHCPサーバからRouterオプションを受け取った時点で有効となります。
ゲートウェイアドレスを受け取れるのは、IPv4スタティック経路と同じlan定義番号で動作するDHCPクライアントからのみです。
IPv4スタティック経路情報は、本装置全体で以下の数まで定義できます。

最大定義数	機種
2000	Si-R570
1250	Si-R370
256	Si-R260B Si-R240 Si-R220B
128	Si-R180

[注意]

同じあて先へのスタティック経路情報を複数設定する場合、以下の点に注意してください。

- 優先度が0のスタティック経路情報と、優先度が0または1以上のスタティック経路情報は同時に設定できません。
- 優先度が同じで、RIPメトリック値が違うスタティック経路情報は同時に設定できません。

[未設定時]

IPv4スタティック経路情報を使用しないものとみなされます。
ただし、DHCPクライアントを有効としたインタフェース上の場合、優先度が0で<next_hop>にdhcpが指定されたdefaultルートが設定されたものとみなします。

5.4.11　lan ip rip use

[機能]

RIP 基本情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip rip use <send> <receive> <metric> [<ignore> [<password>]]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<send>

RIP の送信について指定します。

- v1
  RIPv1(Broadcast) を送信します。
- v2
  RIPv2(Broadcast) を送信します。
- v2m
  RIPv2(Multicast) を送信します。
- off
  RIP を送信しません。

<receive>

RIP の受信について指定します。

- v1
  RIPv1 を受信します。
- v2
  RIPv1, RIPv2 を受信します。
- off
  RIP を受信しません。

<metric>

- 加算メトリック値
  RIP パケット送信時の加算メトリック値を、0～16 の 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ignore>

自装置に<password>を設定していないときに、パスワード付きの RIPv2 パケットを受信したときの破棄の動作を指定します。
省略時は、off を指定したものとみなされます。

- on
  受信した RIPv2 パケットを破棄します。
- off
  受信した RIPv2 パケットを破棄しません。

<password>

- RIPv2 パスワード
  <send>または<receive>に v2 を指定した場合のパスワードを、0x21,0x23〜0x7e のコードで構成される 16 文字以内の ASCII 文字列で指定します。
  省略時は、パスワードなしとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP の基本的な動作を設定します。
<metric>は、RIP パケットを送信する際に加算するメトリック値を設定します。
RIP(IPv4) を使用するインタフェースは、本装置全体で以下の数まで定義できます。

最大定義数	機種
220	Si-R570
120	Si-R370 Si-R260B Si-R240 Si-R220B
50	Si-R180

[注意]

lan mtu コマンドを使用し、MTU 値を 576 よりも小さい値を設定すると、RIPv1(Broadcast), RIPv2(Broadcast) パケットを送信しない場合があります。MTU 値は 576 以上を設定してください。
NAT との併用はできません。

[未設定時]

RIP 機能を使用しないものとみなされます。

```
lan <number> ip rip use off off 0 off
```

5.4.12　lan ip rip filter act

[機能]

RIP フィルタ動作の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip rip filter <count> act <action> <direction>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜799	Si-R570
0〜399	Si-R370　Si-R260B　Si-R240　Si-R220B
0〜199	Si-R180

<action>

フィルタリング条件に一致した場合の動作を指定します。

- pass
  該当する経路情報を透過します。
- reject
  該当する経路情報を遮断します。

<direction>

フィルタリングを行う方向を指定します。

- in
  受信時にフィルタリングを行います。
- out
  送信時にフィルタリングを行います。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP での経路情報送受信時に、フィルタリング条件に一致した経路情報を通過 (pass) させるか遮断 (reject) させるかを設定します。フィルタリング条件は優先度順に検索し、条件に一致した経路情報があった時点でフィルタリングが行われ、それ以降の条件は参照されません。全条件に不一致の経路情報は遮断されます。
フィルタリング条件は、lan ip rip filter route コマンドを使用し経路情報を設定します。
<count>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。
RIP フィルタは、本装置全体で以下の数まで定義できます。

最大定義数	機種
800	Si-R570
400	Si-R370 Si-R260B Si-R240 Si-R220B
200	Si-R180

[注意]

フィルタリング条件が設定されていない場合、本コマンドの設定は無効となります。

[未設定時]

RIP フィルタを使用しないものとみなされ、すべての RIP の経路情報が透過します。

5.4.13　lan ip rip filter move

[機能]

RIP フィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip rip filter move <count> <new_count>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0〜799	Si-R570
0〜399	Si-R370　Si-R260B　Si-R240　Si-R220B
0〜199	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP フィルタの優先順序を変更します。
<new_count>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、<new_count>は順番にソートされてリナンバリングされます。

5.4.14 lan ip rip filter route

[機能]

RIP フィルタの経路情報設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip rip filter <count> route <address>/<mask> [<prefix_match>]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜799	Si-R570
0〜399	Si-R370 Si-R260B Si-R240 Si-R220B
0〜199	Si-R180

<address>/<mask>

- IPv4 アドレス/マスクビット数 (またはマスク値)
  フィルタリング対象とする経路情報を、IPv4 アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
  - IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
  - IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)
- any
  すべての経路情報をフィルタリング対象とする場合に指定します。
- default
  デフォルトルートをフィルタリング対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<prefix_match>

経路情報 (IPv4 アドレス/マスク) の検索条件を指定します。
省略時は、exact を指定したものとみなされます。
<address>/<mask>に"any"または"default"を指定した場合は、<prefix_match>は指定できません。

- exact
  指定した<address>/<mask>と経路情報の IPv4 アドレス/マスクを比較し、一致した場合に、フィルタリング対象とします。

- inexact

  指定した<address>と経路情報の IPv4 アドレスを比較し、<mask>まで一致した場合、フィルタリング対象とします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

フィルタリング条件として経路情報を設定します。

[未設定時]

フィルタリング条件が設定されていないものとみなされます。

5.4.15 lan ip rip filter set metric

[機能]

RIP フィルタのメトリック設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip rip filter <count> set metric <metric>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜799	Si-R570
0〜399	Si-R370 Si-R260B Si-R240 Si-R220B
0〜199	Si-R180

<metric>

- メトリック値
  メトリック値を、0〜16 の 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

フィルタリング条件に一致した経路情報のメトリック値を変更します。
<metric>に 1〜16 を設定した場合、メトリック値は設定した値に変更されます。また、この場合、lan ip rip use コマンドで設定した加算メトリック値は加算されません。0 を指定した場合、メトリック値の変更は行われません。

[注意]

フィルタリング条件が設定されていない場合、本コマンドの設定は無効となります。
フィルタリング条件の"any"と一致した場合、本コマンドの設定は無効となります。

[未設定時]

フィルタリング条件に一致した経路情報のメトリック値を変更しないものとみなされます。

5.4.16　lan ip ospf use

[機能]

OSPF 利用可否の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip ospf use <mode> [<area_number>]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- off
  OSPF を利用しません。
- on
  OSPF を利用します。

<area_number>

- エリア定義番号
  OSPF を利用する場合は、エリアの定義番号を指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜9	Si-R570
0〜3	Si-R370
0〜2	Si-R260B　Si-R240　Si-R220B
0〜1	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

OSPF を利用するかどうかと、インタフェースが属するエリアの定義番号を設定します。
OSPF を使用するインタフェースは、本装置全体で以下の数まで定義できます。

最大定義数	機種
100	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
50	Si-R180

[注意]

OSPF の利用は、"ospf ip area id"を設定した場合にだけ有効です。

[未設定時]

OSPF を使用しないものとみなされます。

```
lan <number> ip ospf use off
```

5.4.17　lan ip ospf cost

[機能]

OSPF 出力コストの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip ospf cost <cost>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<cost>

- 出力コスト
  出力コストを、1～65535 で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

OSPF 出力コストを設定します。

[未設定時]

OSPF 出力コストに 10 が設定されているものとみなされます。

```
lan <number> ip ospf cost 10
```

5.4.18 lan ip ospf hello

[機能]

OSPF Hello パケット送信間隔の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip ospf hello <hello_interval>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<hello_interval>

- Hello パケット送信間隔
  Hello パケットの送信間隔時間を、1 秒〜65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、1s〜65535s、1m〜1092m、1h〜18h です。

[動作モード]

構成定義モード (管理者クラス)

[説明]

OSPF 隣接関係の維持に用いられる Hello パケットの送信間隔を設定します。
hello_interval の値は OSPF 隣接ルータ間で同じ値を設定します。

[注意]

OSPF 隣接ルータ間で異なる Hello パケットの送信間隔を設定した場合、ルーティングが行えません。

[未設定時]

Hello パケット送信間隔に 10 秒が設定されているものとみなされます。

```
lan <number> ip ospf hello 10s
```

5.4.19　lan ip ospf dead

[機能]

OSPF 隣接ルータ停止確認間隔の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip ospf dead <dead_interval>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<dead_interval>

- 隣接ルータ停止確認間隔
  隣接ルータ停止確認の間隔時間を、1 秒～65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、1s～65535s、1m～1092m、1h～18h です。

[動作モード]

構成定義モード (管理者クラス)

[説明]

OSPF 隣接関係の維持に用いられる隣接ルータ停止確認間隔を設定します。
隣接ルータ停止確認間隔の間に Hello パケットを受信しなかった場合は、そのルータとの隣接関係は解除されます。
dead_interval の値は OSPF 隣接ルータ間で同じ値を設定します。
dead_interval の値は Hello パケット送信間隔よりも大きな値を設定する必要があります。
Hello パケット送信間隔の 4 倍を設定することを推奨します。

[注意]

OSPF 隣接ルータ間で異なる隣接ルータ停止確認間隔を設定した場合、ルーティングが行えません。
隣接ルータ停止確認間隔の設定値は、装置起動時で指定ルータ/副指定ルータの選出を開始するまでの待機時間にも使用されます。大きな値を設定した場合は、経路交換の開始が遅れます。

[未設定時]

隣接ルータ停止確認間隔に 40 秒が設定されているものとみなされます。

```
lan <number> ip ospf dead 40s
```

5.4.20 lan ip ospf retrans

[機能]

OSPF パケット再送間隔の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip ospf retrans <retransmit_interval>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<retransmit_interval>

- パケット再送間隔
  パケットの再送間隔を、3 秒〜65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、3s〜65535s、1m〜1092m、1h〜18h です。

[動作モード]

構成定義モード (管理者クラス)

[説明]

OSPF パケットを再送する間隔を設定します。

[未設定時]

OSPF パケットの再送間隔に 5 秒が設定されているものとみなされます。

```
lan <number> ip ospf retrans 5s
```

5.4.21　lan ip ospf delay

[機能]

OSPF LSU パケット送信遅延時間の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip ospf delay <transmit_delay>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<transmit_delay>

- LSU パケット送信遅延時間
  LSU パケットを送信する場合の遅延時間を、1 秒～65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、1s～65535s、1m～1092m、1h～18h です。

[動作モード]

構成定義モード (管理者クラス)

[説明]

LSU(Link State Update) パケットの送信遅延時間を設定します。
LSU パケットでは、LSA(Link State Advertisement) を作成してからの経過時間に<transmit_delay>の値を加算して広報します。

[注意]

一般的な装置では、作成してからの経過時間が 1 時間となった LSA を破棄します。このため、LSU 送信遅延時間に 1 時間以上を設定した場合は、正しくルーティングできない場合があります。

[未設定時]

LSU パケット送信遅延時間に 1 秒が設定されているものとみなされます。

```
lan <number> ip ospf delay 1s
```

5.4.22 lan ip ospf priority

[機能]

OSPF 指定ルータ優先度の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip ospf priority <priority>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<priority>

- 指定ルータ優先度
  指定ルータ優先度を、0〜255 で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

指定ルータ、副指定ルータを決定するための優先度を設定します。
priority の値は、大きいほど優先度が高くなります。値が 0 の場合は、指定ルータ、副指定ルータにはなりません。

[未設定時]

指定ルータ優先度に 1 を指定したものとみなされます。

```
lan <number> ip ospf priority 1
```

5.4.23　lan ip ospf auth type

[機能]

OSPF パケット認証方式の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip ospf auth type <authtype>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<authtype>

パケット認証方式を指定します。

- off
  認証を行いません。
- text
  テキスト認証を使用します。
- md5
  MD5 認証を使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

OSPF パケットに対する認証方式を設定します。

[注意]

テキスト認証の使用は、"lan ip ospf auth textkey"を設定した場合にだけ有効です。
MD5 認証の使用は、"lan ip ospf auth md5key"を設定した場合にだけ有効です。

[未設定時]

OSPF パケット認証を使用しないものとみなされます。

```
lan <number> ip ospf auth type off
```

5.4.24 lan ip ospf auth textkey

[機能]

OSPF テキスト認証鍵の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip ospf auth textkey <kind> <key> [encrypted]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<kind>

鍵種別を指定します。

- text
  文字列鍵を使用します。
- hex
  16 進数鍵を使用します。

<key>

- テキスト認証鍵
  文字列鍵の場合は、0x21,0x23～0x7e のコードで構成される 8 文字以内の ASCII 文字列で指定します。
  16 進数鍵の場合は、16 桁以内の 16 進数値で指定します。16 桁未満の値を指定したときは左詰めで設定され、残りは 16 桁になるまで 0x0 でパディングされます。
- 暗号化されたテキスト認証鍵
  show コマンドで表示される暗号化されたテキスト認証鍵を encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化テキスト認証鍵指定
  <key>に暗号化されたテキスト認証鍵を指定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

テキスト認証で使用する鍵を設定します。
show コマンドでは、暗号化されたテキスト認証鍵が encrypted と共に表示されます。

[未設定時]

テキスト認証鍵が設定されていないものとみなされます。

5.4.25　lan ip ospf auth md5key

[機能]

OSPF MD5 認証鍵情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip ospf auth md5key <key_id> <key> [encrypted]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<key_id>

- MD5 認証鍵 ID
  MD5 認証鍵 ID を、1～255 で指定します。
- 暗号化された MD5 認証鍵 ID
  show コマンドで表示される暗号化された MD5 認証鍵 ID を encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

<key>

- MD5 認証鍵
  MD5 認証鍵を、0x21,0x23～0x7e のコードで構成される 16 文字以内の ASCII 文字列で指定します。
- 暗号化された MD5 認証鍵
  show コマンドで表示される暗号化された MD5 認証鍵を encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化 MD5 認証鍵情報指定
  <key_id>と<key>に暗号化された MD5 認証鍵 ID と MD5 認証鍵を指定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

MD5 認証で使用する鍵情報 (MD5 認証鍵 ID、MD5 認証鍵) を設定します。
show コマンドでは、暗号化された MD5 認証鍵 ID と MD5 認証鍵が encrypted と共に表示されます。

[未設定時]

MD5 認証で使用する鍵情報が設定されていないものとみなされます。

5.4.26 lan ip ospf passive

[機能]

OSPF パケット送信抑止の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip ospf passive <interface_type>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<interface_type>

- on
  パケットの送信を抑止します。
- off
  パケットの送信を抑止しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

OSPF パケット送信の抑止を設定します。

[未設定時]

OSPF パケットの送信は抑止しないものとみなされます。

```
lan <number> ip ospf passive off
```

5.4.27　lan ip vrf use

[機能]

BGP/MPLS VPN 利用可否の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip vrf use <mode> [<vrf_number>]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- off
  VRF を利用しません。
- on
  VRF を利用します。

<vrf_number>

- VRF 定義番号
  VRF を利用する場合は、VRF の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜3	Si-R570　Si-R370
0〜1	Si-R260B　Si-R240　Si-R220B　Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

BGP/MPLS VPN を利用するかどうかを設定します。
利用する場合は、VRF の定義番号を設定します。

[未設定時]

BGP/MPLS VPN を使用しないものとみなされます。

```
lan <number> ip vrf use off
```

5.4.28 lan ip vrf route

[機能]

BGP/MPLS VPN 用 IPv4 スタティック経路情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip vrf route <count> <address>/<mask> <next_hop>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- スタティック経路情報定義番号
  スタティック経路情報の定義番号を、10 進数値で指定します。

範囲	機種
0〜255	Si-R570 Si-R370
0〜63	Si-R260B Si-R240 Si-R220B
0〜31	Si-R180

<address>/<mask>

- IPv4 アドレス/マスクビット数 (またはマスク値)
  あて先ネットワークを IPv4 アドレスとマスクビット数の組み合わせで指定します。
  マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
  - IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
  - IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)
- default
  あて先ネットワークとしてデフォルトルートを設定する場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<next_hop>

- 中継ルータ IPv4 アドレス
  あて先ネットワークへパケットを送信するときの中継ルータの IPv4 アドレスを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

BGP/MPLS VPN で使用する IPv4 スタティック経路情報を設定します。
本装置全体で以下の数まで定義できます。

最大定義数	機種
256	Si-R570　Si-R370
64	Si-R260B　Si-R240　Si-R220B
32	Si-R180

[注意]

メトリック、優先度は設定できません。

[未設定時]

BGP/MPLS VPN 用 IPv4 スタティック経路を使用しないものとみなされます。

5.4.29 lan ip nat mode

[機能]

アドレス変換の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip nat mode <mode> [<address> <addr_number> [<time>]]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

アドレス変換 (NAT) を使用するかどうかを設定します。

- off
  NAT を使用しません。
- nat
  NAT を使用します。
- multi
  マルチ NAT を使用します。
- static
  静的 NAT だけを使用します。

以下のパラメタは、<mode>に nat または multi または static を設定した場合に有効です。

<address>

- 先頭グローバル IP アドレス
  動的変換に使用するグローバル IP アドレスの先頭アドレスを指定します。
- any
  グローバル IP アドレスの先頭アドレスとしてインタフェースの IP アドレスを使用します。

<addr_number>

- グローバル IP アドレスの個数
  動的アドレス変換に使用するグローバル IP アドレスの個数を、1〜16 の 10 進数値で指定します。
  <address>に any を指定した場合は、1 を指定してください。

<time>

- 割当時間
  割り当てられた変換テーブルを解放するための無通信監視時間を、0 秒〜86400 秒 (1 日) の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。
  0 秒を指定した場合は、変換テーブル解放のための監視を行いません。
  省略時は、5 分を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

LAN インタフェースに対するアドレス変換 (NAT) の動作を設定します。

[未設定時]

アドレス変換は使用しないものとみなされます。

```
lan <number> ip nat mode off
```

5.4.30 lan ip nat static

[機能]

静的アドレス変換の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip nat static <count> <private_addr> <private_port> <global_addr> <global_port> [<protocol>]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 静的アドレス変換定義番号
  静的アドレス変換定義番号を、10 進数値で指定します。

範囲	機種
0〜499	Si-R570
0〜299	Si-R370
0〜199	Si-R260B Si-R240 Si-R220B
0〜63	Si-R180

<private_addr>

- プライベート IP アドレス
  静的アドレス変換の対象となるプライベート側の IP アドレスを指定します。

<private_port>

- プライベートポート番号
  静的アドレス変換の対象となるプライベート側のポート番号を、1〜65535 の 10 進数値で指定します。
  グローバルポート番号に複数ポート番号を指定した場合は、変換後の複数ポートの先頭ポート番号を指定します。
- any
  すべてのプライベートポート番号に対して有効な設定となります。

<global_addr>

- グローバル IP アドレス
  静的アドレス変換の対象となるグローバル側の IP アドレスを指定します。
  範囲指定する場合は、「172.16.0.2-172.16.0.254」のように"-"(ハイフン) を使用して指定します。なお、アドレスの範囲指定は一組だけ指定可能です。

- any

  lan ip nat mode コマンドで<address>に any を指定した場合はインタフェースの IP アドレスをグローバル側の IP アドレスとして用います。

  lan ip nat mode コマンドで<address>に any 以外を指定した場合は指定したアドレスをグローバル側の IP アドレスとして用います。

<global_port>

- グローバルポート番号

  静的アドレス変換の対象となるグローバル側のポート番号を、1〜65535 の 10 進数値で指定します。

  範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。

  なお、ポート番号の範囲指定は一組だけ指定可能です。

- any

  すべてのグローバルポート番号に対して有効な設定となります。

<protocol>

- プロトコル番号

  静的アドレス変換の対象となるプロトコル番号を指定します。

  省略時は、any を指定したものとみなされます。

- any

  すべてのプロトコル番号に対して有効な設定となります。

[動作モード]

構成定義モード (管理者クラス)

[説明]

LAN インタフェースに対する静的アドレス変換を設定します。
静的アドレス変換の対象となるパケットは、プロトコル番号<protocol>のプライベート側の IP アドレス <private_addr> とポート番号 <private_port>、グローバル側の IP アドレス<global_addr>とポート番号 <global_port>の指定内容により交換されます。静的アドレス変換は、本装置全体で以下の数まで定義できます。

最大定義数	機種
500	Si-R570
300	Si-R370
200	Si-R260B　Si-R240　Si-R220B
64	Si-R180

[未設定時]

静的アドレス変換は設定されません。

5.4.31 lan ip nat static default

[機能]

テーブルに一致しないパケットの扱いの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip nat static default <action>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<action>

すべての NAT テーブルにも一致しなかったパケットをどう扱うかを指定します。

- pass
  該当するパケットの IP アドレスやポート番号を変換しないで透過させます。
- reject
  該当するパケットを破棄します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

すべての NAT テーブルに一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

すべての NAT テーブルにも一致しないパケットは破棄します。

```
lan <number> ip nat static default reject
```

5.4.32　lan ip nat rule

[機能]

アドレス変換ルールの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip nat rule <count> ftp <server_addr> <server_port> [<check>]
lan [<number>] ip nat rule <count> dns <server_addr> <server_port> [<check>]
lan [<number>] ip nat rule <count> irc <server_addr> <server_port>
lan [<number>] ip nat rule <count> sip <server_addr> <server_port>
lan [<number>] ip nat rule <count> mldt <server_addr> <server_port>
lan [<number>] ip nat rule <count> ipbs <server_addr> <server_port>
lan [<number>] ip nat rule <count> dch <server_addr> <server_port>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 変換ルール番号
  変換ルール番号を、0～31 の 10 進数値で指定します。

ftp, irc, dns, sip, mldt, ipbs, dch

変換ルールの対象となるアプリケーションを指定します。

<server_addr>

- IP アドレス
  NAT に割り当てたグローバルアドレス以外のアドレスを指定します。ここで指定したアドレスを変換ルールの対象とします。
- any
  すべての IP アドレスを変換ルールの対象とします。
  any を指定した場合は、グローバル側とプライベート側の両方のアプリケーションサーバに対応します。
- global
  NAT に割り当てたグローバルアドレス以外のすべてのアドレスを変換ルールの対象とします。
  global を指定した場合は、グローバル側のアプリケーションサーバに対応します。
- local
  NAT に割り当てたグローバルアドレスを変換ルールの対象とします。
  local を指定した場合は、プライベート側のアプリケーションサーバに対応します。
- off
  指定したアプリケーションに対する変換ルールを無効にします。

<server_port>

アプリケーションサーバで待ち受けるポート番号を指定します。

- ポート番号

  アプリケーションサーバで待ち受けるポート番号を、1〜65535 の 10 進数値で指定します。

  範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。

  なお、ポート番号の範囲指定は一組だけ指定可能です。

<check>

- on

  アプリケーションに ftp を指定した場合、ftp サーバのデータ転送用 IP アドレスおよびポート番号のチェックを行います。

  アプリケーションに dns を指定した場合、グローバル側にサーバが存在するときだけ有効となります。DNS の応答の UDP パケットのソース IP アドレスおよびソースポート番号が問い合わせの UDP パケットのディスティネーション IP アドレスおよびディスティネーションポート番号と同一かどうかチェックします。

  省略時は、on を指定したものとみなされます。

- off

  アプリケーションに ftp を指定した場合、ftp サーバのデータ転送用 IP アドレスおよびポート番号のチェックを行いません。

  アプリケーションに dns を指定した場合、IP アドレスおよびポート番号のチェックを行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

LAN インタフェースに対するアドレス変換ルールを設定します。
指定 IP アドレス、指定ポート番号で動作する指定アプリケーションに対応するサーバに対する
アドレス変換の特殊対応の設定を行います。
アドレス変換ルールは、本装置全体で 32 個まで定義できます。

[未設定時]

アドレス変換ルールは設定されません。

5.4.33　lan ip nat wellknown

[機能]

ポート番号変換の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip nat wellknown <count> <port> <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

ポート番号変換定義番号を、0〜99 の 10 進数値で指定します。

<port>

- プライベートポート番号
  プライベートポート番号を、1〜65535 の 10 進数値で指定します。
  範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。
  以下に、有効な記述形式を示します。
  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
- any
  すべてのプライベートポート番号を対象とする場合に指定します。

<mode>

- on
  well-known ポート番号とみなし、変換を行いません。
- off
  well-known ポート番号とみなさず、変換を行います。

[動作モード]

構成定義モード (管理者クラス)

[説明]

プライベートポート番号の変換を行うかどうかの設定をします。プライベートポート番号がどの設定にもあてはまらない場合は、未設定時と同様にプライベートポート番号の変換を行います。
ポート番号変換の設定は本装置全体で 100 個まで定義できます。

[未設定時]

以下のポート番号についてはポート番号の変換を行いません。
1～1024(本来の well-known ポート番号)
28800～28830(Microsoft Internet Gaming Zone)

```
 1558(StreamWorks)
 8000(StreamWorks)
  118(Diablo)
  116(Diablo)
 6112(Battle.net)
 6799(NETSTORM)
 6800(NETSTORM)
 9000(HEAVY GEAR)
 7070(Real Player)
 7000(VDO Live Video)
 6667(IRC)
 7648(CU-SeeMe)
 7649(CU-SeeMe)
40027(SurfV)
40026(SurfV)
 1638(DARK REIGN)
```

5.4.34　lan ip nat destination

[機能]

あて先変換の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip nat destination <count> <private_addr> <global_addr>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- あて先変換定義番号
  あて先変換の優先度を表す番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜499	Si-R570
0〜299	Si-R370
0〜199	Si-R260B　Si-R240　Si-R220B
0〜63	Si-R180

<private_addr>

- プライベート IP アドレス
  あて先変換の対象となるプライベート側の IP アドレスを指定します。

<global_addr>

- グローバル IP アドレス
  あて先変換の対象となるグローバル側の IP アドレスを指定します。
  範囲指定する場合は、「172.16.0.2-172.16.0.254」のように"-"(ハイフン) を使用して指定します。なお、アドレスの範囲指定は一組だけ指定可能です。

[動作モード]

構成定義モード (管理者クラス)

[説明]

LAN インタフェースに対するあて先変換を設定します。
あて先変換の対象となるパケットは、プライベート側の IP アドレス<private_addr> とグローバル側の IP アドレス<global_addr>の指定内容により交換されます。
あて先変換は、本装置全体で以下の数まで定義できます。

最大定義数	機種
500	Si-R570
300	Si-R370
200	Si-R260B　Si-R240　Si-R220B
64	Si-R180

[未設定時]

あて先変換は設定されません。

5.4.35　lan ip nat appli

[機能]

アプリ対応の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip nat appli <function> <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<function>

設定する機能を指定します。

- ftp
  FTP に対する設定を行います。
- sip
  SIP に対する設定を行います。
- h323
  H.323 に対する設定を行います。
- dns
  DNS に対する設定を行います。
- snmp
  SNMP Trap に対する設定を行います。
- irc
  IRC に対する設定を行います。
- ntdomain
  NT ドメインログオンに対する設定を行います。
- stream
  各種ストリーミングに対する設定を行います。
  CU-SeeMe、RealPlayer、VDO Live、Stream Works、SurfV が含まれます。
- game
  各種オンラインゲームに対する設定を行います。
  DIABLO(Battle.net)、NETSTORM、信長の野望 (KOEI)、AGE of EMPIRES が含まれます。

<mode>

- on
  アプリ対応を有効にします。
- off
  アプリ対応を無効にします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

各アプリケーションに対する特殊対応を有効にするかどうかを設定します。

[注意]

このコマンドは、アプリケーションに対するデフォルトの特殊対応動作を設定するものです。
ここで機能を無効に設定した場合でも、rule コマンドで指定されたものは有効になります。

[未設定時]

すべてのアプリ対応を有効にするとみなされます。

```
lan [<number>] ip nat appli ftp on
lan [<number>] ip nat appli sip on
lan [<number>] ip nat appli h323 on
lan [<number>] ip nat appli dns on
lan [<number>] ip nat appli snmp on
lan [<number>] ip nat appli irc on
lan [<number>] ip nat appli ntdomain on
lan [<number>] ip nat appli stream on
lan [<number>] ip nat appli game on
```

5.4.36　lan ip filter

[機能]

IP フィルタの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip filter <count> <action> acl <acl_count> [<direction>]
lan [<number>] ip filter <count> <action> <src_addr>/<mask> <src_port> <dst_addr>/<mask> <dst_port> <protocol> <tcpconnect> [<tos> [<direction> [<icmptype> [<icmpcode>]]]]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す番号を、10 進数値で指定します。
  指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つフィルタリング定義がすでに存在する場合は、既存の定義を変更します。

範囲	機種
0〜999	Si-R570　Si-R370
0〜199	Si-R260B　Si-R240　Si-R220B
0〜63	Si-R180

<action>

フィルタリング対象に該当するパケットを透過するかどうかを設定します。

- pass
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、そのフィルタ定義は無効となり、無視されます。
  IP フィルタでは、ACL の以下の定義を使用します。
  - ip
    ip 値が設定されていない場合、そのフィルタ定義は無効となり、無視されます。

- tcp

  ip の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。

- udp

  ip の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp

  ip の<protocol>値が 1 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip の<protocol>値が 1 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B Si-R240 Si-R220B
0〜149	Si-R180

<src_addr>/<mask>

フィルタリング対象とする送信元 IP アドレスとマスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)

  フィルタリング対象とする送信元 IP アドレスとマスクビット数の組み合わせを指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。

  以下に、有効な記述形式を示します。

  - IP アドレス/マスクビット数 (例: 192.168.1.1/24)
  - IP アドレス/マスク値 (例: 192.168.1.1/255.255.255.0)

- any

  すべての送信元 IP アドレスをフィルタリング対象とする場合に指定します。

  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<src_port>

フィルタリング対象とする送信元ポート番号を指定します。

- ポート番号

  フィルタリング対象とする送信元ポート番号を、1〜65535 の 10 進数値で指定します。

  複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。

  ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。

  以下に、有効な記述形式を示します。

  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)

- ポート番号- (例: 1- = 1 から 65535 までのポート)
- -ポート番号 (例: -1000 = 1 から 1000 までのポート)
- ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)

- any
  すべての送信元ポート番号をフィルタリング対象とする場合に指定します。

<dst_addr>/<mask>

フィルタリング対象とするあて先 IP アドレスとマスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  フィルタリング対象とするあて先 IP アドレスとマスクビット数の組み合わせを指定します。
  記述形式は、<src_addr>/<mask>と同様です。
- any
  すべてのあて先 IP アドレスをフィルタリング対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<dst_port>

フィルタリング対象とするあて先ポート番号を指定します。

- ポート番号
  フィルタリング対象とするあて先ポート番号を、1～65535 の 10 進数値で指定します。
  記述形式は、<src_port>と同様です。
- any
  すべてのあて先ポート番号をフィルタリング対象とする場合に指定します。

<protocol>

フィルタリング対象とするプロトコル番号を指定します。

- プロトコル番号
  フィルタリング対象とするプロトコル番号を、1～255 の 10 進数値で指定します
  (例: ICMP:1、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号をフィルタリング対象とする場合に指定します。

<tcpconnect>

- yes
  TCP プロトコルでコネクション接続要求をフィルタリング対象に含めます。
- no
  TCP プロトコルでコネクション接続要求をフィルタリング対象に含めません。

<tos>

フィルタリング対象とする TOS 値を指定します。
省略時は、any を指定したものとみなされます。

- TOS 値
  フィルタリング対象とする TOS 値を、0～ff の 16 進数値で指定します。
  複数の TOS 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。TOS 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。

- 00～ff の 16 進数値 (例: ff = ff の TOS 値)
- TOS 値-TOS 値 (例: 32-64 = 32 から 64 までの TOS 値)
- TOS 値- (例: 80- = 80 から ff までの TOS 値)
- -TOS 値 (例: -7f = 0 から 7f までの TOS 値)
- TOS 値,TOS 値,… (例: 10,20,30- = 10 と 20 と 30 以降の TOS 値)

- any
  すべての TOS 値をフィルタリング対象とする場合に指定します。

<direction>

フィルタリングする方向を指定します。
省略時は、any を指定したものとみなされます。

- any
  入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。
- in
  入力パケットだけをフィルタリング対象とする場合に指定します。
- out
  出力パケットだけをフィルタリング対象とする場合に指定します。
- reverse
  入力パケットと出力パケットの両方をフィルタリング対象とします。
  ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。
  - 送信元 IP アドレス/マスクとあて先 IP アドレス/マスク
  - 送信元ポート番号とあて先ポート番号

<icmptype>

フィルタリング対象とする ICMP TYPE を指定します。

- ICMP TYPE
  フィルタリング対象とする送信元 ICMP TYPE を、0～255 の 10 進数値で指定します。
  複数の ICMP TYPE を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「8-30」のように"-"(ハイフン) を使用して指定します。
  ICMP TYPE は、","(カンマ) および"-"(ハイフン) を使用して、10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 0～255 の 10 進数値 (例: 8 = ICMP TYPE 8)
  - ICMP TYPE-ICMP TYPE (例: 2-8 = 2 から 8 までの ICMP TYPE)
  - ICMP TYPE- (例: 8- = 8 から 255 までの ICMP TYPE)
  - -ICMP TYPE (例: -200 = 0 から 200 までの ICMP TYPE)
  - ICMP TYPE,ICMP TYPE,… (例: 0,8,30- = 0 と 8 と 30 以降の ICMP TYPE)
- any
  すべての ICMP TYPE をフィルタリング対象とする場合に指定します。

<icmpcode>

フィルタリング対象とする ICMP CODE を指定します。

- ICMP CODE

  フィルタリング対象とする送信元 ICMP CODE を、0〜255 の 10 進数値で指定します。

  複数の ICMP CODE を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「8-30」のように"-"(ハイフン) を使用して指定します。

  ICMP CODE は、","(カンマ) および"-"(ハイフン) を使用して、10 個まで指定できます。

  以下に、有効な記述形式を示します。

  - 0〜255 の 10 進数値 (例: 8 = ICMP CODE 8)
  - ICMP CODE-ICMP CODE (例: 2-8 = 2 から 8 までの ICMP CODE)
  - ICMP CODE- (例: 8- = 8 から 255 までの ICMP CODE)
  - -ICMP CODE (例: -200 = 0 から 200 までの ICMP CODE)
  - ICMP CODE,ICMP CODE,… (例: 0,8,30- = 0 と 8 と 30 以降の ICMP CODE)

- any

  すべての ICMP CODE をフィルタリング対象とする場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

LAN インタフェースに対する IP フィルタを設定します。
IP フィルタは、指定したアドレス、ポート番号、プロトコル、TOS 値と ICMP TYPE, ICMP CODE と一致するパケットを透過または遮断します。設定した優先度順に一致するか調べ、一致した時点でフィルタリングされ、それ以降の設定は参照されません。
IP フィルタリングの旧定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
1000	Si-R570　Si-R370
200	Si-R260B　Si-R240　Si-R220B
64	Si-R180

また、ACL 参照定義は、ほかの ACL 参照定義 (IP フィルタ、帯域制御 (WFQ) など) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B　Si-R240　Si-R220B
450	Si-R180

旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

[注意]

<direction>に reverse を指定した場合は、入力パケットは IP アドレス/マスクとポート番号だけを逆転した条件でフィルタリングされます。このため、<tcpconnect>を有効にしている場合は、入力パケットに対しても、TCP プロトコルのコネクション接続要求がフィルタリング対象に含まれます。

[未設定時]

IP フィルタを設定しないものとみなされ、すべてのパケットが透過します。

5.4.37　lan ip filter move

[機能]

IP フィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip filter move <count> <new_count>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0〜999	Si-R570　Si-R370
0〜199	Si-R260B　Si-R240　Si-R220B
0〜63	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

IP フィルタの優先順序を変更します。
旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

5.4.38 lan ip filter default

[機能]

どの IP フィルタテーブルにも不一致時の動作の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip filter default <action> [<time>]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<action>

どの IP フィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- pass
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。
- spi
  該当するパケットに対して SPI を動作させます。

<time>

- 割当時間
  action に spi を指定したときに、接続に割り当てられたテーブルを解放するための無通信監視時間を、0 秒〜86400 秒 (1 日) の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。
  0 秒を指定した場合は、変換テーブル解放のための監視を行いません。
  省略時は、5 分を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

どの IP フィルタテーブルにも一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

どの IP フィルタテーブルにも一致しないパケットは透過します。

```
lan <number> ip filter default pass
```

5.4.39　lan ip tos

[機能]

TOS 値書き換え条件の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip tos <count> acl <acl_count> <new_tos>
lan [<number>] ip tos <count> <src_addr>/<mask> <src_port> <dst_addr>/<mask> <dst_port> <protocol> <tos> <new_tos>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- TOS 値書き換え定義番号
  TOS 値書き換え条件の優先度を表す定義番号を、10 進数値で指定します。
  指定した値は、設定完了時に順方向にソートされてリナンバリングされます。
  また、指定した定義番号と同じ値を持つ TOS 値書き換え定義がすでに存在する場合は、既存定義の値を変更します。

範囲	機種
0〜499	Si-R570　Si-R370
0〜99	Si-R260B　Si-R240　Si-R220B
0〜31	Si-R180

<acl_count>

- ACL 定義番号使用する ACL 定義の番号を、10 進数値で指定します。指定した<acl_count>の ACL が定義されていない場合、その TOS 値書き換え定義は無効となり、無視されます。TOS 値書き換えでは、ACL の以下の定義を使用します。
  - ip
    ip 値が設定されていない場合、その TOS 値書き換え定義は無効となり、無視されます。
  - tcp
    ip の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。
  - udp
    ip の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp

  ip の<protocol>値が 1 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip の<protocol>値が 1 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B Si-R240 Si-R220B
0〜149	Si-R180

<src_addr>/<mask>

- IP アドレス/マスクビット数 (またはマスク値)

  TOS 値書き換え対象となる送信元 IP アドレスとマスクビット数の組み合わせを指定します。マスク値は最上位ビットから 1 で連続した値にしてください。

  以下に、有効な記述形式を示します。

  - IP アドレス/マスクビット数 (例: 192.168.1.1/24)
  - IP アドレス/マスク値 (例: 192.168.1.1/255.255.255.0)

- any

  すべての送信元 IP アドレスを TOS 値書き換えの対象とする場合に指定します。

  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<src_port>

TOS 値書き換え対象となる送信元ポート番号を指定します。

- ポート番号

  TOS 値書き換え対象となる送信元ポート番号を、1〜65535 の 10 進数値で指定します。

  複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。

  ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。

  以下に、有効な記述形式を示します。

  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)

- any

  すべてのポート番号を対象とする場合に指定します。

<dst_addr>/<mask>

TOS 値書き換え対象となるあて先 IP アドレス、マスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  TOS 値書き換え対象となるあて先 IP アドレスとマスクビット数の組み合わせを指定します。
  記述形式は、<src_addr>/<mask>と同様です。
- any
  すべてのあて先 IP アドレスを TOS 値書き換えの対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<dst_port>

TOS 値書き換え対象となるあて先ポート番号を指定します。

- ポート番号
  TOS 値書き換え対象となるあて先ポート番号を、1〜65535 の 10 進数値で指定します。
  記述形式は、<src_port>と同様です。
- any
  すべてのポート番号を対象とする場合に指定します。

<protocol>

TOS 値書き換え対象となるプロトコル番号を指定します。

- プロトコル番号
  TOS 値書き換え対象となるプロトコル番号を、1〜255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号を TOS 値書き換え対象とする場合に指定します。

<tos>

- TOS 値
  書き換え対象となる TOS 値を、0〜ff の 16 進数値で指定します。
  複数の TOS 値を指定する場合は、","(カンマ) で区切って指定します。また、
  範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。
  TOS 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 00〜ff の 16 進数値 (例: ff = ff の TOS 値)
  - TOS 値-TOS 値 (例: 32-64 = 32 から 64 までの TOS 値)
  - TOS 値- (例: 80- = 80 から ff までの TOS 値)
  - -TOS 値 (例: -7f = 0 から 7f までの TOS 値)
  - TOS 値,TOS 値,… (例: 10,20,30- = 10 と 20 と 30 以降の TOS 値)
- any
  すべての TOS 値を、TOS 値書き換えの対象とする場合に指定します。

<new_tos>

- TOS 値
  書き換える TOS 値を、0〜ff の 16 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

TOS 値書き換え条件を設定します。
条件に一致したパケットの TOS 値を、指定した TOS 値に書き換えます。
TOS 値書き換えの旧定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
500	Si-R570 Si-R370
100	Si-R260B Si-R240 Si-R220B
32	Si-R180

また、ACL 参照定義は、ほかの ACL 参照定義 (IP フィルタ、帯域制御 (WFQ) など) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B Si-R240 Si-R220B
450	Si-R180

旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

[未設定時]

TOS 値書き換えを行わないものとみなされます。

5.4.40　lan ip tos move

[機能]

TOS 値書き換え条件の優先度の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip tos move <count> <new_count>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象 TOS 値書き換え定義番号
  優先順序を変更する前の TOS 値書き換え定義番号を指定します。

<new_count>

- 移動先 TOS 値書き換え定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0～499	Si-R570　Si-R370
0～99	Si-R260B　Si-R240　Si-R220B
0～31	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

TOS 値書き換え条件の優先度を変更します。
旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

5.4.41 lan ip priority

[機能]

帯域制御の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip priority <count> acl <acl_count> <width>
lan [<number>] ip priority <count> <src_addr>/<mask> <src_port> <dst_addr>/<mask> <dst_port> <protocol> <tos> <width>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 帯域制御定義番号
  帯域制御定義番号を、10 進数値で指定します。

範囲	機種
0～999	Si-R570
0～499	Si-R370
0～99	Si-R260B Si-R240 Si-R220B
0～63	Si-R180

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、その定義は無効となり、無視されます。
  帯域制御では、ACL の以下の定義を使用します。

  - ip
    ip 値が設定されていない場合、その定義は無効となり、無視されます。
  - tcp
    ip の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。
  - udp
    ip の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp
  ip の<protocol>値が 1 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip の<protocol>値が 1 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0～2999	Si-R570
0～1499	Si-R370
0～299	Si-R260B　Si-R240　Si-R220B
0～149	Si-R180

<src_addr>/<mask>

帯域制御の対象となる送信元 IP アドレス、マスクビット数を指定します。

- 送信元 IP アドレス/マスクビット数 (またはマスク値)
  帯域制御の対象となる送信元 IP アドレスとマスクビット数の組み合わせを指定します。
  マスク値は、最上位ビットから 1 で連続した値にしてください。
  以下に、有効な記述形式を示します。
  - IP アドレス/マスクビット数 (例: 192.168.1.1/24)
  - IP アドレス/マスク値 (例: 192.168.1.1/255.255.255.0)
- any
  すべての IP アドレスを帯域制御の対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<src_port>

帯域制御の対象となる送信元ポート番号を指定します。

- ポート番号
  帯域制御の対象となる送信元ポート番号を、1～65535 の 10 進数値で指定します。
  複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。
  ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 1～65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)
- any
  すべてのポート番号を対象とする場合に指定します。

<dst_addr>/<mask>

帯域制御の対象となるあて先 IP アドレス、マスクビット数を指定します。

- あて先 IP アドレス/マスクビット数 (またはマスク値)
  帯域制御の対象となるあて先 IP アドレスとマスクビット数の組み合わせを指定します。
  記述形式は<src_addr>/<mask>と同様です。
- any
  すべての IP アドレスを帯域制御の対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<dst_port>

帯域制御の対象となるあて先ポート番号を指定します。

- ポート番号
  帯域制御の対象となるあて先ポート番号を、1～65535 の 10 進数値で指定します。
  記述形式は<src_port>と同様です。
- any
  すべてのポート番号を対象とする場合に指定します。

<protocol>

帯域制御の対象となるプロトコル番号を指定します。

- プロトコル番号
  帯域制御の対象となるプロトコル番号を、1～255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号を帯域制御の対象とする場合に指定します。

<tos>

- TOS 値
  帯域制御の対象となる TOS 値を、0～ff の 16 進数値で指定します。
  複数の TOS 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。
  TOS 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 00～ff の 16 進数値 (例: ff = ff の TOS 値)
  - TOS 値-TOS 値 (例: 32-64 = 32 から 64 までの TOS 値)
  - TOS 値- (例: 80- = 80 から ff までの TOS 値)
  - -TOS 値 (例: -7f = 0 から 7f までの TOS 値)
  - TOS 値,TOS 値,… (例: 10,20,30- = 10 と 20 と 30 以降の TOS 値)
- any
  すべての TOS 値を、帯域制御の対象とする場合に指定します。

<width>

- express
  最優先データとして扱います。
- besteffort
  非優先 (ベストエフォート) として扱います。
- 帯域
  1〜99 の 10 進数値で指定した場合、それぞれ指定した値の比で帯域を割り当てます。たとえば、同じ相手ネットワーク中の定義が 3 つあり、それぞれ<width>の値が 30、30、60 であった場合、帯域として 25%、25%、50%が割り当てられます。なお、1〜99 を指定した定義のそれぞれの合計値が 100 未満の場合、残った帯域は定義に一致しないデータ用の帯域となります。
  「数字 + "kbps"(,"mbps")」で指定した場合、指定した帯域をそのまま割り当てます。
  1kbps〜100000kbps または、1mbps〜100mbps の範囲で指定します。全定義の帯域の合計が回線速度を超えた場合は、それぞれ指定した値の比で帯域を割り当てます。
  指定した値の合計値が回線速度に達しない場合、残った帯域は定義に一致しないデータ用の帯域となります。
  「"share" + 数字」で指定した場合、数字で指定した帯域制御定義番号で定義された帯域を共有します。この場合、指定する数字は自分自身の帯域制御定義番号より小さい、すでに定義されているものを指定しなければなりません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

帯域制御を設定します。任意のプロトコル、アドレス、ポート、TOS 値を指定して、割り当てる帯域を指定します。
帯域制御の旧定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
1000	Si-R570
500	Si-R370
100	Si-R260B　Si-R240　Si-R220B
64	Si-R180

また、ACL 参照定義は、ほかの ACL 参照定義 (IP フィルタ、帯域制御 (WFQ) など) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B　Si-R240　Si-R220B
450	Si-R180

旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

[注意]

シェーピングを使用しない場合、帯域制御は有効に動作しません。

[未設定時]

帯域制御を行わないものとみなされます。

5.4.42　lan ip in-policy

[機能]

Ingress ポリシールーティングの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip in-policy <in-policy_number> policy-group <policy-group_number>

[オプション]

<number>

- lan 定義番号

  lan 定義の通し番号を、10 進数値で指定します。

  省略時は、0 を指定したものとみなされます。

<in-policy_number>

- Ingress ポリシールーティング定義番号

  この I/F での Ingress ポリシールーティング定義の通し番号を、10 進数値で指定します。

  本定義は、ほかのポリシーグループ参照定義を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
2000	Si-R570
1000	Si-R370
200	Si-R260B　Si-R240　Si-R220B
100	Si-R180

<policy-group_number>

- ポリシーグループ番号

  参照するポリシーグループ番号を、10 進数値で指定します。

  IPv4 Ingress ポリシールーティングでは、ポリシーグループで指定された ACL の以下の定義を使用します。

  - ip

    ip 値が設定されていない場合、その定義は無効となり、無視されます。

  - tcp

    ip の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。

    また、ip の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。

  - udp

    ip の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。

    また、ip の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp

  ip の<protocol>値が 1 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip の<protocol>値が 1 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B　Si-R220B
0〜49	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

Ingress ポリシールーティングに使用するポリシーグループを指定します。

[注意]

Ingress ポリシールーティングを行う場合は、必ずポリシーグループ指定を行う必要があります。
また、定義されている全ポリシーグループと不一致の場合は、アドレスによる経路探索が行われます。

[未設定時]

Ingress ポリシールーティングを設定しないとみなされます。

5.4.43　lan ip in-policy move

[機能]

Ingress ポリシールーティングの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip in-policy move <count> <new_count>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象 Ingress ポリシールーティング定義番号
  優先順序を変更するフィルタリング定義の番号を指定します。

<new_count>

- 移動先 Ingress ポリシールーティング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

Ingress ポリシールーティングの優先順序を変更します。

5.4.44 lan ip icmp redirect

[機能]

ICMP リダイレクトパケットの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip icmp redirect <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

ICMP リダイレクトパケットを送信するかどうかを指定します。

- on
  ICMP リダイレクトパケットを送信します。
- off
  ICMP リダイレクトパケットを送信しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ICMP リダイレクトパケットを送信するかどうかを指定します。
<mode>に on が指定されている場合、ICMP リダイレクトパケットを送信します。
<mode>に off が指定されている場合、ICMP リダイレクトパケットを送信しません。

[未設定時]

ICMP リダイレクトパケットを送信するものとみなされます。

```
lan <number> ip icmp redirect on
```

5.4.45　lan ip multicast mode

[機能]

マルチキャストインタフェースの定義

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip multicast mode <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

マルチキャスト定義の動作を指定します。

- off
  マルチキャストパケットを中継しません。
- static
  スタティックルーティングのみで動作します。
- pimdm
  PIM-DM として動作します。
- pimsm
  PIM-SM として動作します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

<number>で指定したインタフェースのマルチキャスト・ルーティングプロトコルを有効化し、マルチキャストパケットを中継します。

[注意]

複数インタフェースで異なるプロトコルが選択された場合は、最初に見つかったインタフェースのプロトコルが有効になります。

[未設定時]

マルチキャストパケットを中継しません。

```
lan [<number>] ip multicast mode off
```

5.4.46 lan ip multicast ttl threshold

[機能]

マルチキャストインタフェースの TTL しきい値の定義

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip multicast ttl threshold <threshold>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<threshold>

- TTL しきい値
  マルチキャストパケットを中継するインタフェースの TTL の
  しきい値を 1〜255 の 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

TTL が<threshold>で指定したしきい値以上のマルチキャストパケットだけ中継します。

[注意]

PIM-SM の PIM Register パケットによりカプセル化されるマルチキャスト・パケットは、出力先インタフェースの TTL しきい値の設定によらずに出力されます。

[未設定時]

1 になります。

```
lan [<number>] ip multicast ttl threshold 1
```

5.4.47　lan ip multicast pim preference

[機能]

マルチキャストインタフェースの PIM プリファレンス値の定義

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip multicast pim preference <preference>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<preference>

- プリファレンス値
  マルチキャストパケットを中継するインタフェースの PIM プリファレンス値を
  1〜65535 の 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

マルチキャスト・パケットの配送経路が重複した場合は、プリファレンス値の小さい経路で配送されます。

[注意]

PIM Assert 発行時には Assert 対象となるパケットの発信元へのユニキャスト経路を参照し、発信元へ向かうインタフェースのプリファレンス値を Assert メッセージに格納します。Assert メッセージが出力されるインタフェースのプリファレンス値が格納されるわけではありません。

[未設定時]

1024 になります。

```
lan [<number>] ip multicast pim preference 1024
```

5.4.48 lan ip multicast pim upstream type

[機能]

上流ルータの種類によるマルチキャストパケット転送許可設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip multicast pim upstream type <type>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<type>

- pim
  上流ルータが PIM ルータのときだけ、マルチキャストパケットを転送します。
- any
  上流ルータが PIM ルータでない場合でも、マルチキャストパケットを転送します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本装置より上流にルータが存在し、そのルータを経由してマルチキャストパケットが転送されてくる場合、どの種類のルータからのマルチキャストパケットを転送するかを指定します。上流ルータが PIM ルータでない場合 (マルチキャストパケットをスタティック経路によって転送するルータであった場合) に転送を許可したい場合は <type> に any を指定することで転送を可能にします。

[注意]

受信インタフェースと同一の IP セグメントから送信された (直接接続されたホストからの) マルチキャストパケットについては、本コマンドの指定にかかわらず転送が行われます。

[未設定時]

上流ルータが PIM ルータのときだけ、マルチキャストパケットを転送します。

```
lan [<number>] ip multicast pim upstream type pim
```

5.4.49　lan ip arp cycle

[機能]

ARP 定期送信機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip arp cycle <interval>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<interval>

- ARP 定期送信のインターバル
  ARP Request の送信間隔を、10 秒～20 分の範囲で指定します。
  単位は、m(分)、s(秒) のどれかを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ARP 定期送信を利用する場合に、送信間隔を設定します。

[注意]

IP アドレスが設定されていないインタフェースでは、ARP 定期送信は動作しません。
定期送信のタイマは 5 秒刻みで動作するため、実際の送信間隔は 5 秒単位で繰り上げられます。たとえばインターバルを 21 秒に設定したときには、実際の送信間隔は 25 秒になります。

[未設定時]

ARP Request の定期送信を行いません。

5.4.50 lan ip arp static

[機能]

スタティック ARP の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip arp static <count> <dst> <mac>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- スタティック ARP テーブル定義番号
  指定した定義番号と同じ値を持つ定義がすでに存在する場合は、既存の設定に対する修正とみなされます。

範囲	機種
0〜199	Si-R570 Si-R370
0〜 99	Si-R260B Si-R240 Si-R220B
0〜 49	Si-R180

<dst>

- あて先 IP アドレス
  スタティック ARP テーブルに登録するあて先 IP アドレスを指定します。
  IP アドレスの指定可能な範囲は以下のとおりです。
  1.0.0.1 〜 126.255.255.254
  128.0.0.1 〜 191.255.255.254
  192.0.0.1 〜 223.255.255.254

<mac>

- MAC アドレス
  あて先 IP アドレスへパケットを送信する場合に使用する MAC アドレスを指定します。
  xx:xx:xx:xx:xx:xx(xx は 2 桁の 16 進数値) の形式で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ARP テーブルに静的な ARP エントリを設定する場合に、IP アドレスと MAC アドレスの対応を設定します。

[注意]

同じあて先 IP アドレスを持つスタティック ARP 定義を複数設定することはできません。
IP アドレスが設定されていないインタフェースでは、スタティック ARP 機能は動作しません。

[未設定時]

スタティック ARP 機能を使用しないものとみなされます。

5.4.51 lan ip ids use

[機能]

IDS の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip ids use <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- off
  IDS を利用しません。
- on
  IDS を利用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

このインタフェースで、IPv4 パケットに対して IDS を利用するかどうかを設定します。

[未設定時]

IPv4 パケットに対して IDS を利用しないものとみなされます。

```
lan <number> ip ids use off
```

5.5　IPv6 関連情報

5.5.1　lan ip6 use

[機能]

IPv6 機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 use <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

IPv6 パケットの送受信を行うかどうか指定します。

- on
  このインタフェースで、IPv6 パケットの送受信を行います。
- off
  このインタフェースで、IPv6 パケットの送受信を行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

このインタフェースで、IPv6 機能を利用するかどうかを設定します。

[未設定時]

IPv6 機能を利用しないものとみなされます。

```
lan <number> ip6 use off
```

5.5.2 lan ip6 ifid

[機能]

IPv6 インタフェース ID の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 ifid <interfaceID>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<interfaceID>

このインタフェースで利用する ID を指定します。

- auto
  本装置が持つ MAC アドレスから、EUI-64 形式の ID を自動生成する場合に指定します。
- インタフェース ID
  このインタフェースで利用する ID を、16 進数値で指定します。4 桁ずつ":"(コロン) で区切ってください。なお、各フィールドの先頭の 0 は省略できます (例: 2a0:c9ff:fe84:759)。

通常は auto を指定してください。特定のインタフェース ID を指定する場合は、同一の link 上でホストと衝突しない値を指定してください。

[動作モード]

構成定義モード (管理者クラス)

[説明]

このインタフェースで利用する、インタフェース ID を設定します。

[未設定時]

インタフェース ID を自動生成するものとみなされます。

```
lan <number> ip6 ifid auto
```

5.5.3　lan ip6 address

[機能]

IPv6 アドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 address [<count>] <address>/<prefixlen> <valid> <preferred> [<flags>]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- IPv6 アドレス定義番号
  IPv6 アドレスの定義番号を、0〜3 の 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<address>/<prefixlen>

- IPv6 アドレス/プレフィックス長
  IPv6 アドレスとプレフィックス長を指定します。リンクローカルアドレスは指定できません。
  IPv6 DHCP クライアントが取得したプレフィックスを使用する場合は上位を"dhcp@インタフェース名"の形式で指定し、下位 80bit 分を IPv6 アドレス形式で指定します。インタフェース名には、rmt インタフェースを以下の範囲で指定します。

範囲	機種
rmt0〜rmt999	Si-R570
rmt0〜rmt499	Si-R370
rmt0〜rmt99	Si-R260B　Si-R240　Si-R220B
rmt0〜rmt49	Si-R180

例)　rmt0 で動作する IPv6 DHCP クライアントが取得した IPv6 プレフィックスを使用する場合の設定例

```
dhcp@rmt0::/64
dhcp@rmt0::1:2:3:4/64
```

プレフィックス長には 64 を指定してください。

<valid>

- valid lifetime の時間
  このインタフェースから RA(Router Advertisement メッセージ) を送信するときに、このプレフィックスに対する valid lifetime を、0 秒〜365 日の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。
  <address>/<prefixlen>に IPv6 DHCP クライアントが取得したプレフィックスを使用する指定をした場合は、IPv6 DHCP クライアントが取得した valid lifetime と比較して短い方が有効になります。

- infinity

  このインタフェースから RA を送信するときに、このプレフィックスに対する valid lifetime を無限とする場合に指定します。

<preferred>

- preferred lifetime の時間

  このインタフェースから RA を送信する場合に、このプレフィックスに対する preferred lifetime を、0 秒〜365 日の範囲で指定します。

  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。

  <preferred>は、<valid>よりも短い時間となるように設定してください。<preferred>が<valid>よりも大きい場合、<valid>と同じ時間として扱われます。

  <address>/<prefixlen>に IPv6 DHCP クライアントが取得したプレフィックスを使用する指定をした場合は、IPv6 DHCP クライアントが取得した preferred lifetime と比較して短い方が有効になります。

- infinity

  このインタフェースから RA を送信する場合に、このプレフィックスに対する preferred lifetime を無限とします。

<flags>

- RA Prefix Information に付与されるフラグ

  このインタフェースから RA を送出する場合に、この prefix に対する flags フィールドの値を 0〜ff の 16 進数値で設定します。

  省略時は、c0 を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

このインタフェースの IPv6 アドレスを設定します。
<address>の指定で、<prefixlen>以降がすべて 0 の場合は、指定した値は IPv6 プレフィックスであると判断されます。この IPv6 プレフィックスとインタフェース ID によって、IPv6 アドレスが生成されます。

[注意]

IPv6 DHCP クライアントが取得したプレフィックスと設定値の重なる部分で、0 以外の値がある場合は、IPv6 アドレスは割り当てられません。

```
<-IPv6 DHCPクライアントが取得したプレフィックス->
                                <---------------ユーザ設定値(80bit)---------------------->
| ////////////                                                                          |
                                <------------>
                                設定値が重なる部分
```

例) IPv6 DHCP クライアントが 2001:db8:1000:5555::/64 を取得した場合

設定内容	利用されるアドレス
dhcp@rmt0:0:100::1/64	2001:db8:1000:5555:100::1/64
dhcp@rmt0:100:200::1/64	無効

[未設定時]

Link local アドレス以外の IPv6 アドレスを設定しないものとみなされます。

5.5.4　lan ip6 ra mode

[機能]

Router Advertisement の動作の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 ra mode <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- off
  RA の送信を行いません。
  定期送信、および host からの RS に対する RA の送信を行いません。
- send
  RA の送信を行います。
  定期送信、および host からの RS に対する RA の送信を行います。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RA(Router Advertisement メッセージ) を送信するかどうかを設定します。

[未設定時]

RA の送信を行わないものとみなされます。

```
lan <number> ip6 ra mode off
```

5.5.5 lan ip6 ra interval

[機能]

Router Advertisement メッセージ送信間隔の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 ra interval <max> <min> <lifetime>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<max>

- 最大送信間隔
  RA を定期送信する場合の最大送信間隔 (秒) を、4〜1800 の 10 進数値で設定します。

<min>

- 最小送信間隔
  RA を定期送信する場合の最小送信間隔 (秒) を、3〜<max>× 3/4 の 10 進数値で設定します。

<lifetime>

- Router Lifetime の値
  送信する RA の Router Lifetime の値を、0 または<max>〜9000 の 10 進数値で設定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RA の送信間隔、および RA の Router Lifetime の値の設定を行います。RA は<min>〜<max>でランダムに決定された間隔で定期送信されます。

[未設定時]

最大送信間隔に 600 秒、最小送信間隔に 200 秒、Router Lifetime の値に 1800 が設定されたものとみなされます。

```
lan <number> ip6 ra interval 600 200 1800
```

5.5.6　lan ip6 ra mtu

[機能]

Router Advertisement メッセージに含める MTU option の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 ra mtu <mtu>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mtu>

- MTU option の内容
  RA に含める MTU option の値を、0 または 1280～1500 の 10 進数値で設定します。
  0 を指定した場合は、RA に MTU option を含めません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RA に含める MTU option の値を設定します。

[未設定時]

送信する RA に MTU option を含めないものとみなされます。

```
lan <number> ip6 ra mtu 0
```

5.5.7 lan ip6 ra reachabletime

[機能]

Router Advertisement メッセージに含める Reachable Time の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 ra reachabletime <reachabletime>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<reachabletime>

- Reachable Time の値
  RA に含める Reachable Time の値を、0〜3600000 の 10 進数値で設定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RA に含める Reachable Time の値を設定します。

[未設定時]

Reachable Time の値として 0 が設定されたものとみなされます。

```
lan <number> ip6 ra reachabletime 0
```

5.5.8　lan ip6 ra retranstimer

[機能]

Router Advertisement メッセージに含める Retrans Timer の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 ra retranstimer <retranstimer>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<retranstimer>

- Retrans Timer の値
  RA に含める Retrans Timer の値を、0〜4294967295 の 10 進数値で設定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RA に含める Retrans Timer の値を設定します。

[未設定時]

Retrans Timer の値として 0 が設定されたものとみなされます。

```
lan <number> ip6 ra retranstimer 0
```

5.5.9 lan ip6 ra curhoplimit

[機能]

Router Advertisement メッセージに含める Cur Hop Limit の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 ra curhoplimit <curhoplimit>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<curhoplimit>

- Cur Hop Limit の値
  RA に含める Cur Hop Limit の値を、0〜255 の 10 進数値で設定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RA に含める Cur Hop Limit の値を設定します。

[未設定時]

Cur Hop Limit の値として 64 が設定されたものとみなされます。

```
lan <number> ip6 ra curhoplimit 64
```

5.5.10　lan ip6 ra flags

[機能]

Router Advertisement メッセージに含める flags field の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 ra flags <flags>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<flags>

- flags field の値
  RA に含める flags field の値を、00〜ff の 16 進数値で設定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RA に含める flags field の値を設定します。

[未設定時]

flags field の値として 00 が設定されたものとみなされます。

```
lan <number> ip6 ra flags 00
```

5.5.11 lan ip6 route

[機能]

IPv6 スタティック経路情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 route <count> <address>/<prefixlen> <next_hop> [<metric> [<distance>]]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- スタティック経路情報定義番号
  スタティック経路情報の定義番号を、10 進数値で指定します。

範囲	機種
0〜1999	Si-R570
0〜1249	Si-R370
0〜255	Si-R260B Si-R240 Si-R220B
0〜127	Si-R180

<address>/<prefixlen>

- IPv6 アドレス/プレフィックス
  あて先ネットワークを IPv6 アドレスとプレフィックスの組み合わせで指定します。
  リンクローカルアドレスは指定できません。
- default
  あて先ネットワークとしてデフォルトルートを設定する場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<next_hop>

- 中継ルータ IPv6 アドレス
  あて先ネットワークへパケットを送信するときの中継ルータの IPv6 アドレスを指定します。
  ICMPv6redirect を正常に動作させるため、link-local address を指定してください。また、中継ルータが存在するネットワーク設定側に対して、適切にスタティック経路情報を設定してください。

<metric>

- RIP メトリック値
  このスタティック経路情報を RIP に再配布するときのメトリック値を、1〜15 の 10 進数値で指定します。
  省略時は、1 を指定したものとみなされます。

<distance>

- 優先度
  このスタティック経路情報の優先度を、0〜254 の 10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。
  省略時は、0 を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv6 スタティック経路 (静的経路) 情報を設定します。
RIP メトリック値は、スタティック経路情報を RIP に再配布するときのメトリック値を設定します。
RIP に再配布したときは、設定した RIP メトリック値+1 のメトリック値で RIP テーブルに登録されます。
優先度は、同じあて先への経路情報が複数ある場合、優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。各ダイナミックルーティングプロトコルの優先度については、routemanage ip6 distance コマンドを参照してください。
優先度に 0 が設定されているときは、routemanage interface floating コマンドでのフローティング設定に応じてフローティング動作が切り替わります。優先度に 1 以上が設定されているときは、常にフローティング動作します。
フローティング動作する場合、<next_hop>で指定した中継ルータと隣接しているインタフェースが通信可能な状態 (リンクアップなど) であれば、スタティック経路情報をルーティングテーブルに追加します。通信不可能な状態 (リンクダウンなど) であれば、ルーティングテーブルから削除します。
フローティング動作しない場合は、インタフェースの状態にかかわらず常にスタティック経路情報をルーティングテーブルに追加します。
以下に、各設定値とフローティング動作の関係を示します。

<distance> 設定値	インタフェース経路の フローティング設定	スタティック経路の フローティング動作
0(省略値)	使用しない	しない
0(省略値)	使用する	する
1以上	使用しない	する
1以上	使用する	する

以下のような用途でスタティック経路情報を使用する場合、フローティング動作するとなるように設定してください。

- IP ルーティングおよびダイナミックルーティングでの広報で、スタティック経路の出口
  インタフェースで異常が発生した場合、ルーティングテーブルよりスタティック経路を削除します。
- あて先が同じ経路をダイナミックルーティングで受信した場合、優先度関係により経路を決定します。

IPv6 スタティック経路情報は、本装置全体で以下の数まで定義できます。

最大定義数	機種
2000	Si-R570
1250	Si-R370
256	Si-R260B　Si-R240　Si-R220B
128	Si-R180

[注意]

同じあて先へのスタティック経路情報を複数設定する場合、以下の点に注意してください。

- 優先度が 0 のスタティック経路情報と、優先度が 0 または 1 以上のスタティック経路情報は同時に設定できません。
- 優先度が同じスタティック経路情報は同時に設定できません。

[未設定時]

IPv6 スタティック経路情報を使用しないものとみなされます。

5.5.12　lan ip6 rip use

[機能]

IPv6 RIP 基本情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 rip use <send> <receive> [<metric>]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<send>

RIP(IPv6) パケットを送信するかどうか指定します。

- on
  RIP(IPv6) パケットを送信します。
- off
  RIP(IPv6) パケットを送信しません。

<receive>

RIP(IPv6) パケットを受信するかどうか指定します。

- on
  RIP(IPv6) パケットを受信します。
- off
  RIP(IPv6) パケットを受信しません。

<metric>

- 加算メトリック値
  RIP(IPv6) パケット送信時の加算メトリック値を、0～16 の 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP(IPv6) の基本的な動作を設定します。
<metric>は、RIP(IPv6) パケットを送信する際に加算するメトリック値を設定します。
RIP(IPv6) を使用するインタフェースは、本装置全体で以下の数まで定義できます。

最大定義数	機種
220	Si-R570　Si-R370
120	Si-R260B　Si-R240　Si-R220B
58	Si-R180

[未設定時]

RIP(IPv6) 機能を使用しないものとみなされます。

```
lan <number> ip6 rip use off off 0
```

5.5.13　lan ip6 rip site-local

[機能]

IPv6 RIP site-local プレフィックス送受信の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 rip site-local <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

site-local プレフィックスを送受信するかどうかを指定します。

- on
  site-local プレフィックスを送受信します。
- off
  site-local プレフィックスを送受信しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP(IPv6) で site-local プレフィックスを送受信するかどうかを設定します。

[未設定時]

site-local プレフィックスを送受信するものとみなされます。

```
lan <number> ip6 rip site-local on
```

5.5.14 lan ip6 rip aggregate

[機能]

IPv6 RIP の集約経路の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 rip aggregate <count> <address>/<prefixlen> <rejectroute>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 集約経路定義番号
  集約経路の定義番号を、0〜3 の 10 進数値で指定します。

<address>/<prefixlen>

- IPv6 アドレス/プレフィックス長
  集約経路のあて先ネットワークを IPv6 アドレスとプレフィックス長の組み合わせで指定します。
- default
  集約経路としてデフォルトルートを設定する場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<rejectroute>

- on
  集約経路に対する reject 経路を設定します。
- off
  集約経路に対する reject 経路を設定しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP の集約経路の設定を行います。
集約経路が設定された場合は、設定された集約経路に含まれる個々の経路は広報されず、集約経路だけを広報します。また、集約経路と等しいネットワークに対する経路情報を持たない場合は、実際に持たないあて先に対するパケットを破棄するために、設定された集約経路に対する reject 経路を設定することもできます。
集約経路情報のメトリック値は、集約された経路のメトリック値に関係なく 1 として広報され lan ip6 rip use および、lan ip6 rip filter set metric で広報するメトリック値を変更することができます。
同一 lan 定義内に同一の集約経路は設定できません。

[未設定時]

RIP(IPv6) で経路集約しないものとみなされます。

5.5.15　lan ip6 rip filter act

[機能]

IPv6 RIP フィルタ動作の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 rip filter <count> act <action> <direction>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜399	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
0〜199	Si-R180

<action>

フィルタリング条件に一致した場合の動作を指定します。

- pass
  該当する経路情報を透過します。
- reject
  該当する経路情報を遮断します。

<direction>

フィルタリングを行う方向を指定します。

- in
  受信時にフィルタリングを行います。
- out
  送信時にフィルタリングを行います。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP(IPv6) での経路情報送受信時に、フィルタリング条件に一致した経路情報を通過 (pass) させるか遮断 (reject) させるかを設定します。フィルタリング条件は優先度順に検索し、条件に一致した経路情報があった時点でフィルタリングが行われ、それ以降の条件は参照されません。全条件に不一致の経路情報は遮断されます。
フィルタリング条件は、lan ip6 rip filter route コマンドを使用し経路情報を設定します。
<count>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。
RIP フィルタ (IPv6) は、本装置全体で以下の数まで定義できます。

最大定義数	機種
400	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B
200	Si-R180

[注意]

フィルタリング条件が設定されていない場合、本コマンドの設定は無効となります。

[未設定時]

RIP(IPv6) フィルタを使用しないものとみなされ、すべての RIP(IPv6) の経路情報が透過します。

5.5.16　lan ip6 rip filter move

[機能]

IPv6 RIP フィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 rip filter move <count> <new_count>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0〜399	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
0〜199	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP(IPv6) フィルタの優先順序を変更します。
<new_count>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、<new_count>は順番にソートされてリナンバリングされます。

5.5.17 lan ip6 rip filter route

[機能]

IPv6 RIP フィルタの経路情報設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 rip filter <count> route <address>/<prefixlen> [<prefix_match>]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜399	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B
0〜199	Si-R180

<address>/<prefixlen>

- IPv6 アドレス/プレフィックス長
  フィルタリング対象とする経路情報を、IPv6 アドレスとプレフィックス長の組み合わせで指定します。
- any
  すべての経路情報をフィルタリング対象とする場合に指定します。
- default
  デフォルトルートをフィルタリング対象とする場合に指定します。

<prefix_match>

経路情報の検索条件を指定します。
省略時は、exact を指定したものとみなされます。
<address>/<prefixlen>に"any"または"default"を指定した場合は、<prefix_match>は指定できません。

- exact
  指定した<address>/<prefixlen>と経路情報の IPv6 アドレス/プレフィックス長を比較し、一致した場合に、フィルタリング対象とします。
- inexact
  指定した<address>と経路情報の IPv6 アドレスを比較し、<prefixlen>まで一致した場合、フィルタリング対象とします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

フィルタリング条件として経路情報を設定します。

[未設定時]

フィルタリング条件が設定されていないものとみなされます。

5.5.18 lan ip6 rip filter set metric

[機能]

IPv6 RIP フィルタのメトリック設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 rip filter <count> set metric <metric>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜399	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B
0〜199	Si-R180

<metric>

- メトリック値
  メトリック値を、0〜16 の 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

フィルタリング条件に一致した経路情報のメトリック値を変更します。
<metric>に 1〜16 を設定した場合、メトリック値は設定した値に変更されます。この場合、lan ip6 rip use コマンドで設定した加算メトリック値は加算されません。0 を指定した場合、メトリック値の変更は行われません。

[注意]

フィルタリング条件が設定されていない場合、本コマンドの設定は無効となります。
フィルタリング条件の"any"と一致した場合、本コマンドの設定は無効となります。

[未設定時]

フィルタリング条件に一致した経路情報のメトリック値を変更しないものとみなされます。

5.5.19　lan ip6 filter

[機能]

IPv6 フィルタの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 filter <count> <action> acl <acl_count> [<direction>]
lan [<number>] ip6 filter <count> <action> <src_addr>/<prefixlen> <src_port> <dst_addr>/<prefixlen> <dst_port> <protocol> <tcpconnect> [<trafficclass> [<direction> [<icmptype> [<icmpcode>]]]]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す番号を、10 進数値で指定します。
  指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つフィルタリング定義がすでに存在する場合は、既存の定義を変更します。

範囲	機種
0〜999	Si-R570　Si-R370
0〜199	Si-R260B　Si-R240　Si-R220B
0〜63	Si-R180

<action>

フィルタリング対象に該当するパケットを透過するかどうかを設定します。

- pass
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、そのフィルタ定義は無効となり、無視されます。IPv6 フィルタでは、ACL の以下の定義を使用します。
  - ip6
    ip6 値が設定されていない場合、そのフィルタ定義は無効となり、無視されます。

- tcp
  ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。
- udp
  ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。
- icmp
  ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B Si-R240 Si-R220B
0〜149	Si-R180

<src_addr>/<prefixlen>

フィルタリング対象とする送信元 IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長
  フィルタリング対象とする送信元 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- any
  すべての送信元 IPv6 アドレスをフィルタリング対象とする場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<src_port>

フィルタリング対象とする送信元ポート番号を指定します。

- ポート番号
  フィルタリング対象とする送信元ポート番号を、1〜65535 の 10 進数値で指定します。
  複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。
  ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)
- any
  すべての送信元ポート番号をフィルタリング対象とする場合に指定します。

<dst_addr>/<prefixlen>

フィルタリング対象とするあて先 IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長
  フィルタリング対象とするあて先 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- any
  すべてのあて先 IPv6 アドレスをフィルタリング対象とする場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<dst_port>

フィルタリング対象とするあて先ポート番号を指定します。

- ポート番号
  フィルタリング対象とするあて先ポート番号を、1〜65535 の 10 進数値で指定します。
  記述形式は、<src_port>と同様です。
- any
  すべてのあて先ポート番号をフィルタリング対象とする場合に指定します。

<protocol>

フィルタリング対象とするプロトコル番号を指定します。

- プロトコル番号
  フィルタリング対象とするプロトコル番号を、0〜254 の 10 進数値で指定します。
- any
  すべてのプロトコルをフィルタリング対象とします。

<tcpconnect>

- yes
  TCP プロトコルでコネクション接続要求をフィルタリング対象に含めます。
- no
  TCP プロトコルでコネクション接続要求をフィルタリング対象に含めません。

<trafficclass>

- フィルタリング対象 Traffic Class 値
  フィルタリング対象となる Traffic Class フィールドの値を 0-ff までの 16 進数値、または、"-"を使用して表現される 16 進数値の範囲を指定します。
  Traffic Class 値の指定は、"," を区切として 10 個まで設定可能です。
  複数の Traffic Class 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。
  Traffic Class 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 00〜ff の 16 進数値 (例: ff = ff の Traffic Class 値)
  - Traffic Class 値-Traffic Class 値 (例: 32-64 = 32 から 64 までの Traffic Class 値)
  - Traffic Class 値- (例: 80- = 80 から ff までの Traffic Class 値)
  - -Traffic Class 値 (例: -7f = 0 から 7f までの Traffic Class 値)
  - Traffic Class 値,Traffic Class 値,… (例: 10,20,30- = 10 と 20 と 30 以降の Traffic Class 値)
- any
  すべての Traffic Class 値をフィルタリング対象とします。省略時は any として扱われます。

<direction>

フィルタリングする方向を指定します。
省略時は、any を指定したものとみなされます。

- any
  入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。
- in
  入力パケットのみをフィルタリング対象とする場合に指定します。
- out
  出力パケットのみをフィルタリング対象とする場合に指定します。
- reverse
  入力パケットと出力パケットの両方をフィルタリング対象とします。
  ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。
  - 送信元 IP アドレス/プレフィックス長とあて先 IP アドレス/プレフィックス長
  - 送信元ポート番号とあて先ポート番号

<icmptype>

フィルタリングする ICMPv6 メッセージタイプ番号を指定します。

- フィルタリング対象 icmptype 値
  フィルタリング対象となる icmptype フィールドの値を 0-255 までの 10 進数値、または、"-"を使用して表現される 10 進数値の範囲を指定します。
  icmptype 値の指定は、"," を区切として 10 個まで設定可能です。
  記述形式は、<src_port>と同様です。
- any
  すべての icmptype 値をフィルタリング対象とします。省略時は any として扱われます。

<icmpcode>

フィルタリングする ICMPv6 メッセージコード番号を指定します。
icmpcode 指定時は、icmptype も指定する必要があります。

- フィルタリング対象 icmpcode 値
  フィルタリング対象となる icmpcode フィールドの値を 0-255 までの 10 進数値、または、"-"を使用して表現される 10 進数値の範囲を指定します。
  icmptype 値の指定は、"," を区切として 10 個まで設定可能です。
  記述形式は、<src_port>と同様です。
- any
  すべての icmpcode 値をフィルタリング対象とします。省略時は any として扱われます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

このインタフェースに対する IPv6 フィルタを設定します。
各パラメタに設定された値によって、動作が変化する場合があります。以下に説明します。

- <protocol>に指定した値によって、IPv6 拡張ヘッダの扱いが以下のように変化します。

- any を指定した場合は、0 個以上の IPv6 拡張ヘッダを含む、あらゆる upper-layer protocol(upper-layer protocol なしを含む) に一致します。
- 以下の IPv6 拡張ヘッダの値を指定した場合は、その拡張ヘッダが付与されている、あらゆる upper-layer protocol(upper-layerprotocol なしを含む) のパケットが一致します。

0　Hop-by-Hop Options Header

43　Routing Header

44　Fragment Header

60　Destination Options Header

- 以下の値を指定した場合は、0 個以上の IPv6 拡張ヘッダ (AH、ESP、IPComp を除く) を含む、upper-layer protocol ヘッダが付与されていないパケットが一致します。

59　no next header

- その他の値が設定されている場合は、upper-layer protocol ヘッダの protocol 番号に等しい値であるパケットが一致します。この場合、AH、ESP、IPComp を除くすべての IPv6 拡張ヘッダは無視されます。パケット中に AH、ESP が設定されている場合は、それ以降の拡張ヘッダおよび upper-layer protocol ヘッダの解釈は行いません。

● <src_port>、<dst_port>に指定した値によって、<protocol>の扱いが以下のように変化します。

- <protocol>に any を指定し、かつ<src_port>、<dst_port>のどちらか、または両方を指定している場合、TCP および UDP パケットの該当ポート番号を持つパケットのみが一致します。
- <protocol>に TCP(6) または UDP(17) を指定し、かつ<src_port>、<dst_port>のどちらか、または両方を指定している場合、指定プロトコルの該当ポート番号を持つパケットのみが一致します。
- <protocol>に TCP(6) または UDP(17) 以外を指定し、かつ<src_port>、<dst_port>のどちらか、または両方を指定している場合、あらゆるパケットが一致しません。

● <icmptype>、<icmpcode>に指定した値によって、<protocol>の扱いが以下のように変化します。

- <protocol>に any を指定し、かつ<icmptype>、<icmpcode>を指定している場合、ICMPv6 パケットの該当 type/code 番号を持つパケットのみが一致します。
- <protocol>に ICMPv6(58) を指定し、かつ<icmptype>、<icmpcode>を指定している場合、指定プロトコルの該当 type/code 番号を持つパケットのみが一致します。
- <protocol>に ICMPv6(58) 以外を指定し、かつ<icmptype>、<icmpcode>を指定している場合、あらゆるパケットが一致しません。

● <tcpconnect>の扱いを以下に示します。

- <protocol>に any を指定した場合、TCP パケットのときにこの設定値が適用されます。
- <protocol>に TCP(6) を指定した場合、常にこの設定値が適用されます。
- <protocol>に any または TCP(6) 以外を指定した場合、この設定値は適用されません。

IPv6 フィルタリングの旧定義は、本装置全体で次の数まで定義できます。

最大定義数	機種
1000	Si-R570　Si-R370
200	Si-R260B　Si-R240　Si-R220B
64	Si-R180

また、ACL 参照定義は、ほかの ACL 参照定義 (IP フィルタ、帯域制御 (WFQ) など) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B Si-R240 Si-R220B
450	Si-R180

旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

[未設定時]

IPv6 フィルタを設定しないものとみなされ、すべてのパケットが透過します。

5.5.20　lan ip6 filter move

[機能]

IPv6 フィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 filter move <count> <new_count>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義の番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0～999	Si-R570　Si-R370
0～199	Si-R260B　Si-R240　Si-R220B
0～63	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv6 フィルタの優先順序を変更します。
旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

5.5.21 lan ip6 filter default

[機能]

どの IP フィルタテーブルにも不一致時の動作の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 filter default <action> [<time>]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<action>

どの IPv6 フィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- pass
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。
- spi
  該当するパケットに対して SPI を動作させます。

<time>

- 割当時間
  action に spi を指定したときに接続に割り当てられたテーブルを解放するための無通信監視時間を、0 秒〜86400 秒 (1 日) の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。
  0 秒を指定した場合は、変換テーブル解放のための監視を行いません。
  省略時は、5 分を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

どの IPv6 フィルタテーブルにも一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

どの IPv6 フィルタテーブルにも一致しないパケットは透過します。

```
lan <number> ip6 filter default pass
```

5.5.22　lan ip6 trafficclass

[機能]

Traffic Class 値書き換え条件の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 trafficclass <count> acl <acl_count> <new_trafficclass>
lan [<number>] ip6 trafficclass <count> <src_addr>/<prefixlen> <src_port> <dst_addr>/<prefixlen> <dst_port> <protocol> <trafficclass> <new_trafficclass>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- Traffic Class 値書き換え定義番号
  Traffic Class 値書き換え条件の優先度を表す定義番号を、10 進数値で指定します。
  指定した値は、設定完了時に順方向にソートされてリナンバリングされます。
  また、指定した定義番号と同じ値を持つ Traffic Class 値書き換え定義がすでに存在する場合は、既存定義の値を変更します。

範囲	機種
0〜499	Si-R570　Si-R370
0〜99	Si-R260B　Si-R240　Si-R220B
0〜31	Si-R180

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、その定義は無効となり、無視されます。
  Traffic Class 書き換えでは、ACL の以下の定義を使用します。
  - ip6
    ip6 値が設定されていない場合、その定義は無効となり、無視されます。
  - tcp
    ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip6 の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。
  - udp
    ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip6 の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp
  ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B Si-R240 Si-R220B
0〜149	Si-R180

<src_addr>/<prefixlen>

書き換え対象とする送信元 IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長
  書き換え対象とする送信元 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- any
  すべての送信元 IPv6 アドレスを書き換え対象とする場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<src_port>

書き換え対象とする送信元ポート番号を指定します。

- ポート番号
  書き換え対象とする送信元ポート番号を、1〜65535 の 10 進数値で指定します。
  複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)
- any
  すべての送信元ポート番号を書き換え対象とする場合に指定します。

<dst_addr>/<prefixlen>

書き換え対象とするあて先 IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長
  書き換え対象とするあて先 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- any
  すべてのあて先 IPv6 アドレスを書き換え対象とする場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<dst_port>

書き換え対象とするあて先ポート番号を指定します。

- ポート番号

  書き換え対象とするあて先ポート番号を、1〜65535 の 10 進数値で指定します。

  記述形式は、<src_port>と同様です。

- any

  すべてのあて先ポート番号を書き換え対象とする場合に指定します。

<protocol>

書き換え対象とするプロトコル番号を指定します。

- プロトコル番号

  書き換え対象とするプロトコル番号を、0〜254 の 10 進数値で指定します。

- any

  すべてのプロトコルを書き換え対象とします。

<trafficclass>

- Traffic Class 値

  書き換え対象となる Traffic Class フィールドの値を 0-ff までの 16 進数値、または、"-"を使用して表現される 16 進数値の範囲を指定します。

  Traffic Class 値の指定は、"," を区切として 10 個まで設定可能です。

  複数の Traffic Class 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。Traffic Class 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。

  以下に、有効な記述形式を示します。

  - 00〜ff の 16 進数値 (例: ff = ff の Traffic Class 値)
  - Traffic Class 値-Traffic Class 値 (例: 32-64 = 32 から 64 までの Traffic Class 値)
  - Traffic Class 値- (例: 80- = 80 から ff までの Traffic Class 値)
  - -Traffic Class 値 (例: -7f = 0 から 7f までの Traffic Class 値)
  - Traffic Class 値,Traffic Class 値,… (例: 10,20,30- = 10 と 20 と 30 以降の Traffic Class 値)

- any

  すべての Traffic Class 値を書き換え対象とします。

<new_trafficclass>

- Traffic Class 値

  書き換える Traffic Class 値を、0〜ff の 16 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

Traffic Class 値書き換え条件を設定します。
条件に一致したパケットの Traffic Class 値を、指定した Traffic Class 値に書き換えます。
Traffic Class 値書き換えの旧定義は、本装置全体で次の数まで定義できます。

最大定義数	機種
500	Si-R570 Si-R370
100	Si-R260B Si-R240 Si-R220B
32	Si-R180

また、ACL 参照定義は、ほかの ACL 参照定義 (IP フィルタ、帯域制御 (WFQ) など) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B Si-R240 Si-R220B
450	Si-R180

旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

[未設定時]

Traffic Class 値書き換えを行わないものとみなされます。

5.5.23　lan ip6 trafficclass move

[機能]

Traffic Class 値書き換え条件の優先度の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 trafficclass move <count> <new_count>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象 Traffic Class 値書き換え定義番号
  優先順序を変更する前の Traffic Class 値書き換え定義番号を指定します。

<new_count>

- 移動先 Traffic Class 値書き換え定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0〜499	Si-R570　Si-R370
0〜99	Si-R260B　Si-R240　Si-R220B
0〜31	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

Traffic Class 値書き換え条件の優先度を変更します。
旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

5.5.24 lan ip6 priority

[機能]

IPv6 プロトコル帯域制御の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 priority <count> acl <acl_count> <width>
lan [<number>] ip6 priority <count> <src_addr>/<prefixlen> <src_port> <dst_addr>/<prefixlen> <dst_port> <protocol> <trafficclass> <width>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 帯域制御定義番号
  帯域制御定義番号を、10 進数値で指定します。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B Si-R240 Si-R220B
0〜63	Si-R180

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、その定義は無効となり、無視されます。
  IPv6 プロトコル帯域制御では、ACL の以下の定義を使用します。

  - ip6
    ip6 値が設定されていない場合、その定義は無効となり、無視されます。
  - tcp
    ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip6 の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。
  - udp
    ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip6 の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp
  ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B　Si-R240　Si-R220B
0〜149	Si-R180

<src_addr>/<prefixlen>

帯域制御の対象とする送信元 IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長
  帯域制御の対象とする送信元 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- any
  すべての送信元 IPv6 アドレスを帯域制御の対象とする場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<src_port>

帯域制御の対象となる送信元ポート番号を指定します。

- ポート番号
  帯域制御の対象となる送信元ポート番号を、1〜65535 の 10 進数値で指定します。
  複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)
- any
  すべてのポート番号を対象とする場合に指定します。

<dst_addr>/<prefixlen>

帯域制御の対象とするあて先 IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長
  帯域制御の対象とするあて先 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- any
  すべてのあて先 IPv6 アドレスを帯域制御の対象とする場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<dst_port>

帯域制御の対象となるあて先ポート番号を指定します。

- ポート番号

  帯域制御の対象となるあて先ポート番号を、1〜65535 の 10 進数値で指定します。

  記述形式は<src_port>と同様です。

- any

  すべてのポート番号を対象とする場合に指定します。

<protocol>

- プロトコル番号

  帯域制御の対象となるプロトコル番号を、0〜254 の 10 進数値で指定します (例: ICMPv6:58、TCP:6、UDP:17 など)。

- any

  すべてのプロトコル番号をフィルタリング対象とする場合に指定します。

<trafficclass>

- 帯域制御対象 Traffic Class 値

  帯域制御の対象となる Traffic Class フィールドの値を 0-ff までの 16 進数値、または、"-"を使用して表現される 16 進数値の範囲を指定します。

  Traffic Class 値の指定は、"," を区切として 10 個まで設定可能です。

  複数の Traffic Class 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。Traffic Class 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。

  以下に、有効な記述形式を示します。

  - 00〜ff の 16 進数値 (例: ff = ff の Traffic Class 値)
  - Traffic Class 値-Traffic Class 値 (例: 32-64 = 32 から 64 までの Traffic Class 値)
  - Traffic Class 値- (例: 80- = 80 から ff までの Traffic Class 値)
  - -Traffic Class 値 (例: -7f = 0 から 7f までの Traffic Class 値)
  - Traffic Class 値,Traffic Class 値,… (例: 10,20,30- = 10 と 20 と 30 以降の Traffic Class 値)

- any

  すべての Traffic Class 値を、帯域制御の対象とします。省略時は any として扱われます。

<width>

- express

  最優先データとして扱います。

- besteffort

  非優先 (ベストエフォート) として扱います。

- 帯域

  1〜99 の 10 進数値で指定した場合、それぞれ指定した値の比で帯域を割り当てます。たとえば、同じ相手ネットワーク中の定義が 3 つあり、それぞれ<width>の値が 30、30、60 であった場合、帯域として 25%、25%、50%が割り当てられます。なお、1〜99 を指定した定義のそれぞれの合計値が 100 未満の場合、残った帯域は定義に一致しないデータ用の帯域となります。

  「数字 + "kbps"(,"mbps")」で指定した場合、指定した帯域をそのまま割り当てます。1kbps〜100000kbps または、1mbps〜100mbps の範囲で指定します。全定義の帯域の合計が回線速度を超えた場合は、それぞれ指定した値の比で帯域を割り当てます。

指定した値の合計値が回線速度に達しない場合、残った帯域は定義に一致しないデータ用の帯域となります。

「"share" + 数字」で指定した場合、数字で指定した帯域制御定義番号で定義された帯域を共有します。この場合、指定する数字は自分自身の帯域制御定義番号より小さい、すでに定義されているものを指定しなければなりません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv6 プロトコル帯域制御を設定します。任意のプロトコル、アドレス、ポート、トラフィッククラスを指定して、割り当てる帯域を指定します。
IPv6 プロトコル帯域制御の旧定義は、本装置全体で次の数まで定義できます。

最大定義数	機種
1000	Si-R570
500	Si-R370
100	Si-R260B　Si-R240　Si-R220B
64	Si-R180

また、ACL 参照定義は、ほかの ACL 参照定義 (IP フィルタ、帯域制御 (WFQ) など) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B　Si-R240　Si-R220B
450	Si-R180

旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

[注意]

シェーピングを使用しない場合、帯域制御は有効に動作しません。

[未設定時]

IPv6 プロトコル帯域制御を行わないものとみなされます。

5.5.25 lan ip6 in-policy

[機能]

Ingress ポリシールーティングの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 in-policy <in-policy_number> policy-group <policy-group_number>

[オプション]

<number>

- lan 定義番号

  lan 定義の通し番号を、10 進数値で指定します。

  省略時は、0 を指定したものとみなされます。

<in-policy_number>

- Ingress ポリシールーティング定義番号

  この I/F での Ingress ポリシールーティング定義の通し番号を、10 進数値で指定します。

  本定義は、ほかのポリシーグループ参照定義を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
2000	Si-R570
1000	Si-R370
200	Si-R260B Si-R240 Si-R220B
100	Si-R180

<policy-group_number>

- ポリシーグループ番号

  参照するポリシーグループ番号を、10 進数値で指定します。

  IPv6 Ingress ポリシールーティングでは、ポリシーグループで指定された ACL の以下の定義を使用します。

  - ip6 ip6 値が設定されていない場合、その定義は無効となり、無視されます。
  - tcp ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。また、ip6 の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。
  - udp ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。また、ip6 の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。
  - icmp ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B　Si-R220B
0〜49	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

Ingress ポリシールーティングに使用するポリシーグループを指定します。

[注意]

Ingress ポリシールーティングを行う場合は、必ずポリシーグループ指定を行う必要があります。
また、定義されている全ポリシーグループと不一致の場合は、アドレスによる経路探索が行われます。

[未設定時]

Ingress ポリシールーティングを設定しないとみなされます。

5.5.26 lan ip6 in-policy move

[機能]

Ingress ポリシールーティングの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] ip6 in-policy move <count> <new_count>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象 Ingress ポリシールーティング定義番号
  優先順序を変更するフィルタリング定義の番号を指定します。

<new_count>

- 移動先 Ingress ポリシールーティング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

Ingress ポリシールーティングの優先順序を変更します。

5.6　ブリッジ関連情報

5.6.1　lan bridge use

[機能]

ブリッジ動作モードの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] bridge use <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

ブリッジを使用するかどうかを指定します。

- on
  ブリッジを使用する場合に指定します。
- off
  ブリッジを使用しない場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ブリッジを使用するかどうかを設定します。
ブリッジを使用する場合、IP および IPv6 のパケット以外をすべてブリッジします。

[注意]

IP および IPv6 以外のネットワークプロトコル (IPX など) をルーティングしているネットワークでブリッジを使用する場合は、ブリッジによって中継されることでネットワークがダウンすることがあります。ルーティングと併用する場合は、ルーティングによって転送するプロトコルをフィルタリングするように設定してください。

[未設定時]

ブリッジを使用しないものとみなされます。

```
lan <number> bridge use off
```

5.6.2 lan bridge group

[機能]

ブリッジグループ識別子の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] bridge group <group_id>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<group_id>

- グループ識別子
  グループ識別子を 10 進数値で指定します。

範囲	機種
0〜19	Si-R570 Si-R370 Si-R240 Si-R220B
0〜7	Si-R260B Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

ブリッジのグループ識別子を設定します。

[未設定時]

グループ識別子に 0 を指定したものとみなされます。

```
lan <number> bridge group 0
```

5.6.3　lan bridge static

[機能]

静的学習テーブル情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] bridge static <count> <mac>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 静的学習テーブル定義番号
  指定した定義番号と同じ値を持つ定義がすでに存在する場合は、既存の設定に対する修正とみなされます。

範囲	機種
0〜399	Si-R570　Si-R370
0〜199	Si-R260B　Si-R240　Si-R220B　Si-R180

<mac>

静的な定義として学習テーブルに追加する MAC アドレスを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

学習テーブルに指定された MAC アドレスを静的な学習テーブル情報として追加します。

5.6.4 lan bridge stp use

[機能]

STP 動作モード の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] bridge stp use <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- on
  STP を使用する場合に指定します。
- off
  STP を使用しない場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

スパニングツリーアルゴリズムで経路制御を行うかどうかを設定します。
本コマンド は、ブリッジを使用している場合にだけ有効です。

[注意]

ブリッジグループ 0 以外のブリッジグループでは STP は動作しません。

[未設定時]

STP を使用しないものとみなされます。

```
lan <number>  bridge stp use off
```

5.6.5　lan bridge stp cost

[機能]

パスコストの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] bridge stp cost <path_cost>

[オプション]

<number>

- lan 定義番号

  lan 定義の通し番号を、10 進数値で指定します。

  省略時は、0 を指定したものとみなされます。

<path_cost>

LAN を経由する通信のパスコストを指定します。
通常は auto を指定してください。ただし、ブリッジネットワークを構築するうえで、優先ブリッジ決定のために任意のパスコストを指定することができます。

- auto

  インタフェースの速度に応じて、パスコストが自動決定されます。

以下に、本パラメタ指定時のパスコストを示します。

回線種別	パスコスト	備考
Ethernet(1Gbps) Ethernet(100Mbps) Ethernet(10Mbps)	100 100 100	
HSD(64kbps) HSD(128kbps) HSD(192kbps) * HSD(256kbps) * HSD(384kbps) * HSD(512kbps) * HSD(768kbps) * HSD(1Mbps) * HSD(1.5Mbps) * FR(64kbps) FR(128kbps) FR(256kbps) * FR(384kbps) * FR(512kbps) * FR(768kbps) * FR(1Mbps) * FR(1.5Mbps) * ISDN MODEM	15620 7810 1000 1000 1000 1000 1000 667 667 16000 8500 1100 1100 1100 1100 680 680 16000 16000	*：192kbps～1.5Mbpsは PRIの場合
IPトンネル	16000	
その他 1Mbps>=速度 1.5Mbps>=速度>1Mbps 4Mbps>=速度>1.5Mbps 6Mbps>=速度>4Mbps 10Mbps>=速度>6Mbps 16Mbps>=速度>10Mbps 20Mbps>=速度>16Mbps 25Mbps>=速度>20Mbps 40Mbps>=速度>25Mbps 80Mbps>=速度>40Mbps 速度>80Mbps	 1000 667 250 167 100 62 50 40 25 12 10	

- パスコスト
  パスコストを、1～65535 の 10 進数値で指定します。
  値が小さいほど、優先度が高くなります。

[動作モード]

構成定義モード (管理者クラス)

[説明]

スパニングツリーアルゴリズムで使用するパスコストを設定します。
本コマンドは、STP を使用する場合にだけ有効です。

[未設定時]

パスコストを自動決定するとみなされます。

```
lan <number> bridge stp cost auto
```

5.6.6　lan bridge stp priority

[機能]

インタフェース優先度の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] bridge stp priority <port_priority>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<port_priority>

- インタフェース優先度
  インタフェースごとの優先度を、0～255 の 10 進数値で指定します。
  値が小さいほど、優先度が高くなります。

[動作モード]

構成定義モード (管理者クラス)

[説明]

スパニングツリーアルゴリズムで使用する、インタフェースごとの優先度を設定します。
本コマンドは、STP を使用する場合にだけ有効です。
本コマンドを設定しない場合は、<number>で指定したインタフェースが優先となり、remote 定義で定義されたインタフェースが非優先となります。lan 定義内で定義されたインタフェースでは、定義番号のもっとも小さいものが優先されます。

[未設定時]

インタフェース優先度に 128 が設定されたものとみなされます。

```
lan <number> bridge stp priority 128
```

5.6.7 lan bridge filter

[機能]

MAC フィルタの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] bridge filter <count> <action> acl <acl_count> [<direction>]
lan [<number>] bridge filter <count> <action> <src_mac> <dst_mac> <format> [<value> [<vlan_analyze>]]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す番号を、10 進数値で指定します。
  指定した値は、設定完了時に順方向にソートされリナンバリングされます。
  指定した定義番号と同じ値を持つ定義がすでに存在する場合は、既存の設定に対する修正とみなされます。指定した値を持つ定義が存在しない場合は、追加とみなされます。

範囲	機種
0〜255	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B
0〜127	Si-R180

<action>

フィルタリング対象に該当するフレームを透過するかどうかを指定します。

- pass
  該当するフレームを透過します。
- reject
  該当するフレームを遮断します。

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、そのフィルタ定義は無効となり、無視されます。
  MAC フィルタでは、ACL の以下の定義を使用します。
  - mac
    mac 値が設定されていない場合、そのフィルタ定義は無効となり、無視されます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B　Si-R240　Si-R220B
0〜143	Si-R180

<direction>

フィルタリングする方向を指定します。
ACL を利用した定義でのみ指定可能です。
省略時は、any を指定したものとみなされます。

- any
  入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。
- in
  入力パケットだけをフィルタリング対象とする場合に指定します。
- out
  出力パケットだけをフィルタリング対象とする場合に指定します。
- reverse
  入力パケットと出力パケットの両方をフィルタリング対象とします。
  ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。
  - 送信元 MAC アドレスとあて先 MAC アドレス

<src_mac>

フィルタリング対象とする送信元 MAC アドレスを指定します。

- any
  すべての MAC アドレスを対象とする場合に指定します。
- bcast
  ブロードキャスト MAC アドレスを対象とする場合に指定します。
- mcast
  マルチキャスト MAC アドレスを対象とする場合に指定します。
- 上記以外
  対象とする MAC アドレスを指定します。フィルタリング対象とする送信元 MAC アドレスを、xx:xx:xx:xx:xx:xx(xx は 2 桁の 16 進数値) の形式で指定します。

<dst_mac>

フィルタリング対象とするあて先 MAC アドレスを指定します。

- any
  すべての MAC アドレスを対象とする場合に指定します。
- bcast
  ブロードキャスト MAC アドレスを対象とする場合に指定します。
- mcast
  マルチキャスト MAC アドレスを対象とする場合に指定します。
- 上記以外
  対象とする MAC アドレスを指定します。フィルタリング対象とする送信元 MAC アドレスを、xx:xx:xx:xx:xx:xx(xx は 2 桁の 16 進数値) の形式で指定します。

<format> <value>

- llc

  <value>の値と LSAP が一致する LLC 形式フレームを対象とする場合に指定します。<value>には、0〜ffff の 16 進数値を指定します。

- ether

  <value>の値とタイプが一致する Ethernet 形式フレームを対象とする場合に指定します。<value>には、5dd〜ffff の 16 進数値を指定します。

- any

  すべてのフレームを対象とする場合に指定します。<value>は、指定不要です。

<vlan_analyze>

VLAN タグ付きフレームに対してタグの解析を行うかどうかを指定します。
<value>を指定したときだけ指定可能です。
省略時は、off を指定したものとみなされます。

- on

  VLAN タグ付きフレームの場合に VLAN タグを解析してフィルタリング処理を行います。VLAN タグ付きフレームの場合は、タグの長さ分ずれた位置にある LLC 形式フレームの LSAP や Ethernet 形式フレームのタイプに対してフィルタリング処理を行います。

- off

  VLAN タグ付きフレームの場合に VLAN タグを解析しないでフィルタリング処理を行います。VLAN タグ付きフレームの場合でもタグの長さ分ずらさずにそのままフィルタリング処理を行うため、VLAN タグの TPID が、<value>との比較対象になります。

[動作モード]

構成定義モード (管理者クラス)

[説明]

MAC フィルタを設定します。
本コマンドは、ブリッジ機能を使用する場合にだけ有効です。
指定した条件に一致するフレームを、指定した<action>に従って遮断または通過させます。
MAC フィルタの旧定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
256	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B
128	Si-R180

また、ACL 参照定義は、ほかの ACL 参照定義 (IP フィルタ、帯域制御 (WFQ) など) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B Si-R240 Si-R220B
432	Si-R180

旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

[注意]

IP および IPv6 以外のネットワークプロトコル (IPX など) をルーティングしているネットワークでブリッジを使用する場合は、ブリッジによって中継されることでネットワークがダウンすることがあります。ルーティングと併用する場合は、ルーティングによって転送するプロトコルをフィルタリングするように設定してください。

[未設定時]

MAC フィルタを設定しないものとみなされ、すべてのフレームが透過します。

5.6.8 lan bridge filter move

[機能]

MAC フィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] bridge filter move <count> <new_count>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象フィルタリング定義番号
  優先順序を変更する前のフィルタリング定義の番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0〜255	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B
0〜127	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

MAC フィルタの優先順序を変更します。
旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

5.6.9　lan bridge priority

[機能]

帯域制御の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] bridge priority <count> acl <acl_count> <width>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 帯域制御定義番号
  帯域制御定義番号を、10 進数値で指定します。

範囲	機種
0～999	Si-R570
0～499	Si-R370
0～99	Si-R260B　Si-R240　Si-R220B
0～63	Si-R180

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、その定義は無効となり、無視されます。
  帯域制御では、ACL の以下の定義を使用します。

  - mac
    mac 値が設定されていない場合、その定義は無効となり、無視されます。

範囲	機種
0～2999	Si-R570
0～1499	Si-R370
0～299	Si-R260B　Si-R240　Si-R220B
0～143	Si-R180

<width>

- express
  最優先データとして扱います。
- besteffort
  非優先 (ベストエフォート) として扱います。
- 帯域
  1〜99 の 10 進数値で指定した場合、それぞれ指定した値の比で帯域を割り当てます。たとえば、同じ相手ネットワーク中の定義が 3 つあり、それぞれ<width>の値が 30、30、60 であった場合、帯域として 25%、25%、50%が割り当てられます。なお、1〜99 を指定した定義のそれぞれの合計値が 100 未満の場合、残った帯域は定義に一致しないデータ用の帯域となります。
  「数字 + "kbps"(,"mbps")」で指定した場合、指定した帯域をそのまま割り当てます。1kbps〜100000kbps または、1mbps〜100mbps の範囲で指定します。全定義の帯域の合計が回線速度を超えた場合は、それぞれ指定した値の比で帯域を割り当てます。指定した値の合計値が回線速度に達しない場合、残った帯域は定義に一致しないデータ用の帯域となります。
  「"share" + 数字」で指定した場合、数字で指定した帯域制御定義番号で定義された帯域を共有します。この場合、指定する数字は自分自身の帯域制御定義番号より小さい、すでに定義されているものを指定しなければなりません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

帯域制御を設定します。任意の ACL 番号を指定して、割り当てる帯域を指定します。
ACL 参照定義は、ほかの ACL 参照定義 (IP フィルタ、TOS 書き換えなど) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B Si-R240 Si-R220B
432	Si-R180

[注意]

シェーピングを使用しない場合、帯域制御は有効に動作しません。

[未設定時]

帯域制御を行わないものとみなされます。

5.7　VRRP 関連情報

5.7.1　lan vrrp use

[機能]

VRRP 動作モード の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] vrrp use <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

VRRP 機能を使用するかどうかを指定します。

- on
  VRRP を使用する場合に指定します。
  <number>で指定した LAN インタフェースで VRRP が機能します。
- off
  VRRP を使用しない場合に指定します。
  <number>で指定した LAN インタフェースで VRRP は機能しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

この LAN インタフェースで、VRRP 機能を使用するかどうかを設定します。
VRRP 機能を使用しないと設定した場合、<number>で指定した LAN インタフェースでは VRRP 機能が動作しません。

[未設定時]

VRRP 機能を使用しないものとみなされます。

```
lan <number> vrrp use off
```

5.7.2 lan vrrp auth

[機能]

VRRP-AD の認証方法と認証パスワードの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] vrrp auth <method> [<password>]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<method>

認証方法について指定します。

- none
  <number>で指定した LAN インタフェースで VRRP-AD の認証を行いません。
- text
  <number>で指定した LAN インタフェースはテキストパスワードを用いて VRRP-AD の認証を行います。

<password>

- 認証パスワード
  <method>に text を指定した場合、<number>で指定した LAN インタフェースで使用する VRRP-AD の認証パスワードを、0x21,0x23 ～ 0x7e の 8 桁以内の ASCII 文字列で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

この LAN インタフェースで VRRP-AD の認証に使用する認証方法と認証パスワードを設定します。
設定はこの LAN インタフェースに関係する VRRP グループのすべてに適用されます。
<method>に text を指定した場合は、パスワードを設定する必要があります。<method>に none を指定した場合、パスワードは指定できません。

[未設定時]

VRRP-AD の認証を使用しないものとみなされます。

```
lan <number> vrrp auth none
```

5.7.3　lan vrrp group id

[機能]

VRRP グループの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] vrrp group <vrrp_number> id <vrid> <priority> [<virtual_ip#1> [<virtual_ip#2>]]

[オプション]

<number>

- lan 定義番号

  lan 定義の通し番号を、10 進数値で指定します。

  省略時は、0 を指定したものとみなされます。

<vrrp_number>

- VRRP グループ定義番号

  LAN インタフェースに対する VRRP グループ定義の通し番号を、

  0～1 の 10 進数値で指定します。

<vrid>

- VRID

  <vrrp_number>で定義した VRRP グループの保持する VRID を、1～255 の 10 進数値で指定します。

  VRID は装置内で一意でなければなりません。重複した VRID を指定した場合は<number>および<vrrp_number>の最小である設定だけが有効となり、ほかはすべて無効となります。

<priority>

- VRRP ルータの優先度

  VRRP ルータの優先度を、"master"、または 1～254 の 10 進数値で指定します。

  <priority>に"master"を指定した場合の VRRP グループは最優先度 255 の仮想ルータとして動作します。この場合、仮想ルータの IPv4 アドレスは<number>で指定した LAN インタフェースの実 IPv4 アドレスになります。

  lan <number> ip address <address>/<mask> <broadcast> で設定された<address>が実 IPv4 アドレスです。

  また、この場合は lan vrrp group preempt の指定は無効になり、プリエンプトモードは常に ON で動作します。

  それ以外の場合、VRRP グループは<priority>で指定した優先度の仮想ルータとして動作します。

  VRRP ルータの優先度は数値が大きいほど高くなります。

  トリガを使用する場合は優先度 1 の設定はさけてください。また、トリガを使用する場合は"master"を指定するとトリガが作動した場合に VRRP グループが設定された LAN が通信不能となります。トリガを使用する場合は"master"を指定しないでください。

<virtual_ip#X>

- 仮想ルータの IPv4 アドレス
  VRRP グループで使用する仮想ルータの IPv4 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  <priority>に"master"を指定した場合は、仮想ルータの IPv4 アドレスは<number>で指定した LAN インタフェースの実 IPv4 アドレスとなるため、指定する事はできません。このときセカンダリ IPv4 アドレスが設定されている場合はセカンダリ IPv4 アドレスも仮想ルータの IPv4 アドレスとなります。(lan <number> ip alias <address>/<mask> <broadcast> で設定された<address>がセカンダリ IPv4 アドレスです。)
  それ以外の場合は、1 つ以上の仮想ルータの IPv4 アドレスを指定しなければなりません。また、その場合は VRRP グループ内で重複した仮想ルータの IPv4 アドレスを設定することはできません。仮想ルータの IPv4 アドレスに装置内のインタフェース実 IPv4 アドレスまたは、セカンダリ IPv4 アドレスを指定した場合は、この VRRP グループは無効となります。

[動作モード]

構成定義モード (管理者クラス)

[説明]

VRRP グループの VRID、優先度、仮想ルータの IPv4 アドレスを設定します。
優先度が"master"である設定は VRRP グループにつき 1 台の VRRP ルータにだけ行ってください。複数の"master"を設定した場合、仮想ルータを正しくバックアップすることができません。(VRRP グループで同一の仮想ルータ IPv4 アドレスが設定できないため)
VRRP グループは VRID によって識別される同一 VRRP グループ内で優先度を競合し、マスタルータを決定します。
VRRP グループの仮想 MAC アドレスは VRID から自動的に生成されます。(00:00:5E:00:01:{VRID}) 優先度に"master"以外を設定した場合でも、指定した優先度が同一 VRRP グループ内でもっとも高い優先度であればマスタルータとして動作します。また、VRRP ルータの優先度は VRRP グループ内で、できるだけ大きな差がつくように設定してください。近い優先度であった場合、マスタルータの切り替わりがスムーズに行われない場合があります。
VRRP 機能を使用する場合、本定義は必須定義であり未設定の場合は VRRP 機能が動作しません。

[未設定時]

VRRP グループの情報は設定されないものとみなされます。

5.7.4　lan vrrp group ad

[機能]

VRRP-AD の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] vrrp group <vrrp_number> ad <interval>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<vrrp_number>

- VRRP グループ定義番号
  LAN インタフェースに対する VRRP グループ定義の通し番号を、0〜1 の 10 進数値で指定します。

<interval>

- VRRP-AD 送出間隔
  VRRP-AD の送出間隔を、1 秒〜255 秒の範囲で指定します。
  単位は、m(分)、s(秒) のどちらかを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

該当する自装置 VRRP グループが使用する VRRP-AD の送信間隔時間を設定します。
同一 VRRP グループ内では送出間隔時間を同じ値に設定してください。異なる値が設定された場合はスムーズにマスタルータの交代が行われなくなる可能性があります。

[未設定時]

VRRP-AD の送出間隔として 1 秒が設定されたものとみなされます。

```
lan <number> vrrp group <vrrp_number> ad 1s
```

5.7.5 lan vrrp group preempt

[機能]

プリエンプトモードの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] vrrp group <vrrp_number> preempt <mode> [<time>]

[オプション]

<number>

- lan 定義番号

  lan 定義の通し番号を、10 進数値で指定します。

  省略時は、0 を指定したものとみなされます。

<vrrp_number>

- VRRP グループ定義番号

  LAN インタフェースに対する VRRP グループ定義の通し番号を、0〜1 の 10 進数値で指定します。

<mode>

プリエンプトモードを指定します。

- on

  <vrrp_number>で指定した VRRP グループでプリエンプトモードを ON に設定します。

- off

  <vrrp_number>で指定した VRRP グループでプリエンプトモードを OFF に設定します。

<time>

- プリエンプトモード OFF への移行禁止時間

  VRRP が動作を開始してから、プリエンプトモード OFF へ移行するのを禁止する時間として 0 秒〜900 秒の範囲で指定します。

  単位は、m(分)、s(秒) のどれかを指定します。

  省略時は、0 秒を指定したものとみなされます。

  なお、<mode>が off に設定されている場合にだけ有効であり、<mode>が on に設定される場合は指定できません。

  禁止時間内ではプリエンプトモードが ON に設定されたのと同様に動作します。この設定はシステム起動時に優先度の低いルータが先に動作を開始して、優先度の高いルータにマスタルータが渡されないようなことが発生する場合に有効です。

[動作モード]

構成定義モード (管理者クラス)

[説明]

VRRP グループのプリエンプトモードを設定します。

[未設定時]

プリエンプトモードに ON が設定されたものとみなされます。

```
lan <number> vrrp group <vrrp_number> preempt on
```

5.7.6 lan vrrp group trigger ifdown

[機能]

インタフェースダウントリガの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] vrrp group <vrrp_number> trigger <trigger_no> ifdown <interface> [<priority>]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<vrrp_number>

- VRRP グループ定義番号
  LAN インタフェースに対する VRRP グループ定義の通し番号を、0〜1 の 10 進数値で指定します。

<trigger_no>

- トリガ定義番号
  VRRP グループに対するトリガ定義の通し番号を、10 進数値で指定します。

範囲	機種
0〜127	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B
0〜49	Si-R180

<interface>

トリガ対象インタフェースを指定します。

- インタフェース名
  lan または、rmt インタフェースを以下の範囲で指定します。

範囲	機種
lan0〜lan19 rmt0〜rmt999	Si-R570
lan0〜lan19 rmt0〜rmt499	Si-R370
lan0〜lan19 rmt0〜rmt99	Si-R260B Si-R240 Si-R220B
lan0〜lan9 rmt0〜rmt49	Si-R180

- any
  ループバックインタフェース以外すべてのパケット送出インタフェースをトリガ対象に含める場合に指定します。

<priority>

- 優先度
  変化させる優先度を、1～254 の 10 進数値で指定します。
  省略時は、254 を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

インタフェースダウントリガを設定します。
<interface>で指定したインタフェースがダウンした場合、トリガを適用します。
<interface>で指定したインタフェースが有効ではないインタフェースであった場合はトリガは動作しません。また、同一インタフェースに重複してトリガが設定された場合はすべてを適用します。
<interface>がリモートインタフェースである場合、ケーブル抜け、同期はずれ、または PVC 状態確認手順によって通信不可と判断された該当インタフェースに設定されたトリガを適用します。
トリガが適用された場合、VRRP グループの現在の優先度から<priority>で指定した値を減算した優先度の VRRP ルータとして動作します。
<priority>で優先度を減算すると 1 以下になる場合は、優先度 1 の VRRP ルータとして動作します。

[未設定時]

インタフェースダウントリガは設定されないものとみなされます。

5.7.7 lan vrrp group trigger route

[機能]

ルートダウントリガの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] vrrp group <vrrp_number> trigger <trigger_no> route <dst_addr> <interface> [<priority>]

[オプション]

<number>

- lan 定義番号

  lan 定義の通し番号を、10 進数値で指定します。

  省略時は、0 を指定したものとみなされます。

<vrrp_number>

- VRRP グループ定義番号

  LAN インタフェースに対する VRRP グループ定義の通し番号を、0〜1 の 10 進数値で指定します。

<trigger_no>

- トリガ定義番号

  VRRP グループに対するトリガ定義の通し番号を、10 進数値で指定します。

範囲	機種
0〜127	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B
0〜49	Si-R180

<dst_addr>

トリガを適用する経路を指定します。

- IPv4 アドレス/マスクビット数 (またはマスク値)

  あて先または中継先ネットワークの IPv4 アドレスとマスクビット数の組み合わせを指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。

  以下に、有効な記述形式を示します。

  - IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
  - IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)

  設定値として、0.0.0.0 は指定できません。

- default

  経路としてデフォルトルートを指定します。

<interface>

トリガを適用する経路のパケット送出インタフェースを指定します。

- インタフェース名

  lan または、rmt インタフェースを以下の範囲で指定します。

範囲	機種
lan0～lan19 rmt0～rmt999	Si-R570
lan0～lan19 rmt0～rmt499	Si-R370
lan0～lan19 rmt0～rmt99	Si-R260B　Si-R240　Si-R220B
lan0～lan9 rmt0～rmt49	Si-R180

- any

  パケット送出インタフェースを特定しない場合に指定します。

<priority>

- 優先度

  変化させる優先度を、1～254 の 10 進数値で指定します。

  省略時は、254 を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ルートダウントリガを設定します。
<dst_addr>で指定したあて先のパケットを<interface>で指定したインタフェースに送出する経路がルーティングテーブルに存在しない場合、トリガを適用します。
<interface>が any である場合は、送出先インタフェースに関係なくあて先の経路が存在していればトリガは適用となりません。
トリガが適用された場合、VRRP グループの現在の優先度から<priority>で指定した値を減算した優先度の VRRP ルータとして動作します。
<priority>で優先度を減算すると 1 以下になる場合は、優先度 1 の VRRP ルータとして動作します。
なお、VRRP グループが設定された LAN インタフェースがダウンした場合はこの限りではありません (自装置の VRRP グループは仮想ルータとして無効な状態となります)。

[未設定時]

ルートダウントリガは設定されないものとみなされます。

5.7.8 lan vrrp group trigger node

[機能]

ノードダウントリガの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] vrrp group <vrrp_number> trigger <trigger_no> node <dst_addr> <interface> [<priority> [<resend_time> [<time_out> [<normal_interval> [error_interval>]]]]]

[オプション]

<number>

- lan 定義番号

  lan 定義の通し番号を、10 進数値で指定します。

  省略時は、0 を指定したものとみなされます。

<vrrp_number>

- VRRP グループ定義番号

  LAN インタフェースに対する VRRP グループ定義の通し番号を、0〜1 の 10 進数値で指定します。

<trigger_no>

- トリガ定義番号

  VRRP グループに対するトリガ定義の通し番号を、10 進数値で指定します。

範囲	機種
0〜127	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B
0〜49	Si-R180

<dst_addr>

- ICMP ECHO パケットのあて先 IP アドレス

  ICMP ECHO パケットのあて先 IP アドレスを指定します。

  指定可能な範囲は以下のとおりです。

  1.0.0.1 〜 126.255.255.254

  128.0.0.1 〜 191.255.255.254

  192.0.0.1 〜 223.255.255.254

<interface>

ICMP ECHO パケットを送出するインタフェースを指定します。

- インタフェース名

  rmt インタフェースを以下の範囲で指定します。

範囲	機種
rmt0～rmt999	Si-R570
rmt0～rmt499	Si-R370
rmt0～rmt99	Si-R260B　Si-R240　Si-R220B
rmt0～rmt49	Si-R180

- any
  パケット送出インタフェースを特定しない場合に指定します。

<priority>

- 優先度
  変化させる優先度を、1～254 の 10 進数値で指定します。
  省略時は、254 を指定したものとみなされます。

<resend_time>

- ICMP ECHO パケットの再送間隔
  ICMP ECHO パケットの再送間隔を、1 秒～60 秒の範囲で指定します。
  単位は、m(分)、s(秒) のどれかを指定します。
  省略時は、5 秒を指定したものとみなされます。

<time_out>

- ICMP ECHO のタイムアウト時間
  ICMP ECHO のタイムアウト時間を、<resend_time>+1 秒～240 秒の範囲で指定します。
  単位は、m(分)、s(秒) のどれかを指定します。
  省略時は、<resend_time>× 3+1 秒を指定したものとみなされます。

<normal_interval>

- ICMP ECHO パケットの正常時送信間隔
  ICMP ECHO パケットの正常時送信間隔を、<time_out>+1 秒～255 秒の範囲で指定します。単位は、m(分)、s(秒) のどれかを指定します。
  省略時は、<time_out>+1 秒を指定したものとみなされます。

<error_interval>

- ICMP ECHO パケットの異常時送信間隔
  ICMP ECHO パケットの異常時送信間隔を、1 秒～255 秒の範囲で指定します。
  単位は、m(分)、s(秒) のどれかを指定します。
  省略時は、30 秒を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ノードダウントリガを設定します。
<dst_addr>で指定したあて先に ICMP ECHO パケットを<interface>で指定したインタフェースから送出し、<time_out>時間応答がない場合、トリガを適用します。<interface>が any である場合、送出先インタフェースは経路情報に依存します。
トリガが適用された場合、VRRP グループの現在の優先度から<priority>で指定した値を減算した優先度の VRRP ルータとして動作します。

<priority>で優先度を減算すると 1 以下になる場合は、優先度 1 の VRRP ルータとして動作します。
なお、VRRP グループが設定された LAN インタフェースがダウンした場合はこの限りではありません (自装置の VRRP グループは仮想ルータとして無効な状態となります)。

[注意]

<dst_addr>にはブロードキャストアドレス、マルチキャストアドレスを指定しないでください。
指定した場合は正常に動作しません。
優先度を"master"に設定した VRRP グループにノードダウントリガを設定した場合は正常に動作しません。
ノードダウントリガを設定する場合は優先度を"master"以外にしてください。ノードダウントリガで送信される ICMP ECHO パケットの送信元 IP アドレスは VRRP グループが設定された LAN のインタフェースアドレスとなりますので、ICMP ECHO 応答パケットの経路に注意してください。
ノードダウントリガでは定期的にパケットが送信されますので異常課金に注意してください。

[未設定時]

ノードダウントリガは設定されないものとみなされます。

5.7.9　lan vrrp group action

[機能]

VRRP 状態変化に対するアクションの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] vrrp group <vrrp_number> action <action_no> <state> online lan [<lan_number>]
lan [<number>] vrrp group <vrrp_number> action <action_no> <state> online switch [<switch_number> [port <port_number>]]
lan [<number>] vrrp group <vrrp_number> action <action_no> <state> online remote [<remote_number> [ap <ap_number> [id <id> <password>]]]
lan [<number>] vrrp group <vrrp_number> action <action_no> <state> online access-point <ap_name>
lan [<number>] vrrp group <vrrp_number> action <action_no> <state> online template <template_number> uid <user_id>
lan [<number>] vrrp group <vrrp_number> action <action_no> <state> offline lan [<lan_number>]
lan [<number>] vrrp group <vrrp_number> action <action_no> <state> offline switch [<switch_number> [port <port_number>]]
lan [<number>] vrrp group <vrrp_number> action <action_no> <state> offline remote [<remote_number> [ap <ap_number>]]
lan [<number>] vrrp group <vrrp_number> action <action_no> <state> offline access-point <ap_name>
lan [<number>] vrrp group <vrrp_number> action <action_no> <state> offline template interface <interface_name>
lan [<number>] vrrp group <vrrp_number> action <action_no> <state> offline template <template_number> [uid <user_id>]
lan [<number>] vrrp group <vrrp_number> action <action_no> <state> diallock remote [<remote_number>]
lan [<number>] vrrp group <vrrp_number> action <action_no> <state> dialreject remote [<remote_number>]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<vrrp_number>

- VRRP グループ定義番号
  LAN インタフェースに対する VRRP グループ定義の通し番号を、0～1 の 10 進数値で指定します。

<action_no>

- アクション定義番号
  VRRP グループが<state>で指定された状態へ変化した場合のアクション定義通し番号を 10 進数値で指定します。

範囲	機種
0〜49	Si-R570
0〜29	Si-R370
0〜19	Si-R260B Si-R240 Si-R220B
0〜9	Si-R180

<state>

アクションを適用する状態を指定します。

- master
  適用する状態をマスタ状態とします。
- backup
  適用する状態をバックアップまたは、イニシャル状態とします。

online, offline, diallock, dialreject

アクションを指定します。

- online
  <state>に装置リセット以外の要因で状態遷移した場合に対象を online にします。
  master と設定されている場合はマスタ状態からバックアップまたは、イニシャル状態へ遷移した場合に online を適用します。
  backup と設定されている場合はバックアップまたは、イニシャル状態からマスタ状態へ遷移した場合に online を適用します。
- offline
  <state>に装置リセット以外の要因で状態遷移した場合に対象を offline にします。
  master と設定されている場合はマスタ状態からバックアップまたは、イニシャル状態へ遷移した場合に offline を適用します。
  backup と設定されている場合はバックアップまたは、イニシャル状態からマスタ状態へ遷移した場合に offline を適用します。
- diallock
  <state>で指定した状態の間、指定された相手ネットワークへの自動発信を抑止します。
- dialreject
  <state>で指定した状態の間、指定された相手ネットワークからの自動着信を抑止します。

lan, access-point, template interface, template, remote

アクション適用対象の種別を指定します。

- lan
  適用対象を指定された lan とします。
- switch
  適用対象を指定されたスイッチポートとします。
- access-point
  適用対象を接続先名で指定された接続先とします。
- template interface
  適用対象をテンプレート着信で接続している指定されたインタフェースの相手ネットワークとします。
- template
  適用対象を指定されたテンプレート定義によるテンプレートの接続とします。
- remote
  適用対象を指定された相手ネットワークや接続先とします。

<lan_number>

- lan 定義番号

  lan 定義の通し番号を、10 進数値で指定します。

  複数の lan 定義番号を指定する場合は、", "(カンマ) で区切って指定します。また、範囲指定する場合は、「2-4」のように"-"(ハイフン) を使用して指定します。

  lan 定義番号は、","(カンマ) および"-"(ハイフン) を使用して 5 個まで指定できます。

  省略時は、すべての lan を指定したものとみなされます。

<switch_number>

- スイッチ定義番号

  スイッチ定義の通し番号を、10 進数値で指定します。

  省略時は、0 を指定したものとみなされます。

<port_number>

- スイッチポート番号

  スイッチポートの番号を、10 進数値で指定します。

  複数のスイッチポートを指定する場合は、", "(カンマ) で区切って指定します。また、

  範囲指定する場合は、「2-4」のように"-"(ハイフン) を使用して指定します。

<remote_number> ap <ap_number> id <id> <password>

相手定義番号と接続先定義番号にて接続先を指定します。

省略時は、すべての接続先を指定したものとみなされます。

id <id>および<password>は接続ごとに認証 ID、認証パスワードを変更する場合に指定します。

<remote_number>

- 相手定義番号

  相手ネットワークの通し番号を、10 進数値で指定します。

  省略時は、すべての相手ネットワークを指定したものとみなされます。

範囲	機種
0～999	Si-R570
0～499	Si-R370
0～99	Si-R260B　Si-R240　Si-R220B
0～49	Si-R180

複数の相手定義番号を指定する場合は、", "(カンマ) で区切って指定します。また、範囲指定する場合は、「2-4」のように"-"(ハイフン) を使用して指定します。

相手定義番号は、","(カンマ) および"-"(ハイフン) を使用して 5 個まで指定できます。

ap <ap_number>

- 接続先定義番号

  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B Si-R240 Si-R220B
0〜49	Si-R180

複数の接続先定義番号を指定する場合は、", "(カンマ) で区切って指定します。また、範囲指定する場合は、「2-4」のように"-"(ハイフン) を使用して指定します。
接続先定義番号は、","(カンマ) および"-"(ハイフン) を使用して 5 個まで指定できます。

id <id>

- 送信認証 ID
  0x21,0x23〜0x7e の文字で構成される 64 文字以内の ASCII 文字列を指定します。
  <remote_number>、<ap_number>で複数の接続先を指定していない場合に指定できます。

<password>

- 送信認証パスワード
  0x21,0x23〜0x7e の文字で構成される 64 文字以内の ASCII 文字列を指定します。
  <remote_number>、<ap_number>で複数の接続先を指定していない場合に指定できます。

<ap_name>

- 接続先名
  0x21,0x23〜0x7e の文字で構成される 8 文字以内の ASCII 文字列を指定します。

<template_number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。

範囲	機種
0〜5	Si-R570 Si-R370
0〜2	Si-R240 Si-R220B
0〜1	Si-R260B Si-R180

<user_id>

- ユーザ ID
  0x21,0x23〜0x7e の文字で構成される 145 文字以内の ASCII 文字列を指定します。
  online のオプションとして指定する場合は動的 VPN サーバに登録しているユーザ ID を設定します。
  offline の場合は template を利用している接続がユーザ ID と一致するユーザによるものであれば切断します。省略時は、ユーザ ID を特定しないものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

VRRP 状態変化に対するアクションを設定します。
<action>が diallock または dialreject の場合は、<state>が示す状態の間自働発信または自働着信を抑止します。構成定義にて自働発信または自働着信と設定された相手ネットワーク以外を指定しても機能しません。
<action>が online または offline の場合は、<state>が示す状態へ遷移した場合に online または offline を適用します。
アクション適用対象が常時接続であれば offline により閉塞状態となり、online で閉塞状態解除となります。
アクション適用対象が ISDN(回線交換)/PPPoE 接続であれば offline により回線を切断し、online で発信します。
テンプレートによる接続の場合はアクション適用時に接続があれば offline により回線を切断します。
なお、online および offline の動作は運用コマンドの online および offline と同様です。

[未設定時]

VRRP 状態変化に対するアクションは設定されないものとみなされます。

5.7.10 lan vrrp group vaddr icmp

[機能]

仮想 IP アドレスあて ICMP ECHO パケット受信動作の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] vrrp group <vrrp_number> vaddr icmp <mode> [<src>]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<vrrp_number>

- VRRP グループ定義番号
  LAN インタフェースに対する VRRP グループ定義の通し番号を、0〜1 の 10 進数値で指定します。

<mode>

仮想 IP アドレスあて ICMP ECHO パケットを受理するか破棄するかを指定します。

- accept
  仮想 IP アドレスあて ICMP ECHO パケットを受理する場合に指定します。
  受理すると指定しても ICMP ECHO 以外の ICMP パケットは破棄します。
- discard
  仮想 IP アドレスあて ICMP ECHO パケットを破棄する場合に指定します。

<src>

仮想 IP アドレスあて ICMP ECHO を受理すると指定した場合に応答パケット送信元 IP アドレスを指定します。
<mode>に discard を指定した場合は、<src>を指定することはできません。
省略時は、virtual を指定したものとみなされます。

- virtual
  応答パケット送信元 IP アドレスに仮想 IP アドレスを使用します。
- real
  応答パケット送信元 IP アドレスにインタフェースアドレスを使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

VRRP の仮想 IP あて ICMP ECHO の受信動作を設定します。
受理すると設定した場合であっても VRRP グループの状態がマスタ状態以外である場合は破棄します。

[未設定時]

仮想 IP アドレスあて ICMP ECHO は受理しないものとみなされます。

```
lan <number> vrrp group <vrrp_number> vaddr icmp discard
```

5.8 MPLS 関連情報

5.8.1 lan mpls use

[機能]

MPLS 利用可否の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] mpls use <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- on
  MPLS を利用します。
- off
  MPLS を利用しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

MPLS を利用するかどうかを設定します。

[未設定時]

off が選択されたものとして動作します。

```
lan <number> mpls use off
```

5.8.2　lan mpls distribution

[機能]

ラベル配布プロトコルの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] mpls distribution <protocol>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<protocol>

- ldp
  ラベル配布プロトコルに LDP を使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ラベル配布プロトコルを指定します。

[未設定時]

ldp が選択されたものとして動作します。

```
lan <number> mpls distribution ldp
```

5.8.3 lan mpls ldp hello-timers

[機能]

LDP Hello に関するタイマの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] mpls ldp hello-timers <interval> <holdtime>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<interval>

- Hello 送信間隔のタイマ値
  Hello の送信間隔を、1 秒〜65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。

<holdtime>

- HoldTime のタイマ値
  近隣関係の維持を判定するための HoldTime を、1 秒〜65534 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
- infinity
  近隣関係の維持を判定するための HoldTime を infinity(0xffff:無限) とします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

LDP 近隣関係の維持に用いられる Hello パケットの送信間隔と HoldTime を設定します。
HoldTime の値は interval の値より小さくすることはできません。
HoldTime の値は interval の値の 3 倍以上を設定することを推奨します。

[注意]

HoldTime は近隣関係にある LDP ルータとネゴシエーションし、値の小さい方が採用されますが、送信間隔はネゴシエーションしないため、相手 LSR のタイマ設定と自装置のタイマ設定を一致させておくことを推奨します。

[未設定時]

interval が 5 秒、HoldTime が 15 秒として動作します。

```
lan <number> mpls ldp hello-timers 5s 15s
```

5.8.4　lan mpls ldp keepalive-timers

[機能]

LDP KeepAlive に関するタイマの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] mpls ldp keepalive-timers <interval> <timeout>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<interval>

- KeepAlive 送信間隔のタイマ値
  KeepAlive の送信間隔を、1 秒〜65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。

<timeout>

- KeepAlive タイムアウトのタイマ値
  LDP セッションの維持を判定するためのタイムアウト時間を、1 秒〜65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

LDP セッションの維持に用いられる KeepAlive メッセージの送信間隔とタイムアウトを設定します。
timeout の値は interval の値より小さくすることはできません。
timeout の値は interval の値の 3 倍以上を設定することを推奨します。

[注意]

タイムアウトは近隣関係にある LDP ルータとネゴシエーションし、値の小さい方が採用されますが、送信間隔はタイムアウトのネゴシエーション結果の 3 分の 1 の値とこのコマンドで設定された送信間隔とを比較し、値が小さい方が送信間隔として採用されます。

[未設定時]

interval が 1 分、timeout が 3 分として動作します。

```
lan <number> mpls ldp keepalive-timers 1m 3m
```

5.8.5 lan mpls ldp advertisement

[機能]

LDP ラベル広報方式の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] mpls ldp advertisement <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- dod
  Downstream On Demand を使用します。
- du
  Downstream Unsolicited を使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

LDP のラベル広報方式を指定します。

[未設定時]

du が選択されたものとして動作します。

```
lan <number> mpls ldp advertisement du
```

5.8.6　lan mpls ldp retention

[機能]

LDP ラベル保持方式の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] mpls ldp retention <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- liberal
  Liberal Label Retention Mode を使用します。
- conservative
  Conservative Label Retention Mode を使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

LDP のラベル保持方式を指定します。

[未設定時]

liberal が選択されたものとして動作します。

```
lan <number> mpls ldp retention liberal
```

5.8.7 lan mpls ldp interface-label

[機能]

PHP の無効化

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] mpls ldp interface-label <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- off
  インタフェースの IP アドレスにラベルを割り当てません。
- on
  インタフェースの IP アドレスにラベルを割り当てます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

インタフェースの IP アドレスに対してラベルを割り当てるかどうかを指定します。
割り当てた場合は、インタフェースあての LSP の PHP を無効にすることができます。

[注意]

MPLS トンネル接続機能を使用する場合、自側エンドポイントと IP アドレスが同一のとき、本設定に依らず、PHP 機能は無効となります。

[未設定時]

off が選択されたものとして動作します。

```
lan <number> mpls ldp interface-label off
```

5.8.8　lan mpls ldp ip transport

[機能]

IPv4 Transport Address の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] mpls ldp ip transport <address>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<address>

- LDP セッションの送信元 IPv4 アドレス
  IPv4 アドレスを指定します。以下の範囲で指定してください。

  0.0.0.0
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[動作モード]

構成定義モード (管理者クラス)

[説明]

インタフェース単位で LDP が相手との通信に用いる送信元 IPv4 アドレスを分ける必要がある場合に、本装置に設定された IPv4 アドレスを指定します。
0.0.0.0 を指定した場合は、MPLS 情報の設定の IPv4 Transport Address の設定に従います。

[注意]

インタフェース単位で IPv4 Transport Address を設定する場合は、必ず本装置に存在するアドレスを指定してください。本装置に存在しないアドレスをインタフェースに指定した場合は、そのインタフェースでは LDP を使用できません。

[未設定時]

MPLS 情報の設定の IPv4 Transport Address の設定に従います。

```
lan mpls ldp ip transport 0.0.0.0
```

5.8.9 lan mpls l2-circuit vc

[機能]

EoMPLS の VC 情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] mpls l2-circuit vc <vc_id> <address> [<vc_type>]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<vc_id>

- VC ID の設定
  lan 定義の VC ID を 1〜4294967295 の 10 進数値で指定します。
  VC ID は装置内で一意でなければなりません。

<address>

- 相手装置の IPv4 アドレス
  指定可能な範囲は以下のとおりです。

  1.0.0.1 〜 126.255.255.254
  128.0.0.1 〜 191.255.255.254
  192.0.0.1 〜 223.255.255.254

<vc_type>

- auto
  lan 定義から、ethernet か vlan かを自動的に識別します。
- ethernet
  lan 定義に関係なく VC Type を Ethernet に設定します。
- vlan
  lan 定義に関係なく VC Type を Ethernet VLAN に設定します。

省略時は auto を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

EoMPLS 通信の VC ID、相手装置のアドレス、VC Type の設定をします。
<vc_id> は EoMPLS 通信の相手装置と同じ値を指定します。本装置と相手装置で同じ VC ID を持つインタフェース同士を VC LSP で接続し、EoMPLS 通信を行います。VC ID 装置内で一意になるように設定する必要があります。
<address> は EoMPLS 通信の相手装置の IPv4 アドレスを指定します。相手装置にて指定した IPv4 Transport Address と同じ値を指定してください。EoMPLS 通信を行うためには相手装置のアドレスへの経路情報が必要となります。LDP ラベル広報経路情報の設定で、必要な経路情報を LDP で広報するように設定してください。
<vc_type> は、相手装置で同じ VC ID を持つインタフェースと同じ値を指定します。lan 定義と VC Type の設定の関係、および、EoMPLS 通信時のフレームの処理は以下のようになります。

本装置の設定		LDP の動作	EoMPLS 通信時のフレームの処理			
lan定義	<vc_type> の値	ラベル交換で使用する VC Type の値	lan定義のI/F側から タグなし受信	lan定義のI/F側から タグ付き受信	VC LSP側から タグなし受信	VC LSP側から タグ付き受信
VLAN定義していない lan定義	auto	Ethernet	そのまま転送	そのまま転送	そのまま転送	そのまま転送
	ethernet	Ethernet				
	vlan	Ethernet VLAN				
VLAN定義している lan定義	auto	Ethernet VLAN	--	そのまま転送	タグを挿入して転送	タグを上書きして転送
	ethernet	Ethernet				
	vlan	Ethernet VLAN				

そのまま転送　　：フレームを加工しないで、そのまま同じフレームを転送します。
タグを挿入して転送　：VC LSPから受信しlan定義に出力する際に、VLAN IDの設定、VLANのプライオリティ情報の設定で指定した VLAN タグをフレームに挿入します。
タグを上書きして転送：VC LSPから受信しlan定義に出力する際に、フレームに設定されている VLAN タグを、VLAN IDの設定、VLAN のプライオリティ情報の設定で指定した VLAN タグで上書きします。

[注意]

- 本設定で EoMPLS 通信の設定を行った LAN インタフェースでは、自装置あての通信を含めて、すべての通信が EoMPLS 通信による転送の対象となります。
  このため本設定を行った lan 定義では以下の機能は使用できません。
  - IP 機能
  - IPv6 機能
  - ブリッジ機能 (STP、MAC 学習、MAC フィルタ機能を含みます)
  - VRRP 機能
  - MPLS 機能 (EoMPLS 機能は除きます)
- EoMPLS 通信の相手装置のアドレスが、MPLS LSP トンネルの REMOTE インタフェース設定のトンネルエンドポイントと同じである場合は、REMOTE インタフェースの設定で、MPLS を使用する、LDP Multicast Hello パケットを送信しない、と設定してください。
- EoMPLS 通信を行う場合は、MAC 学習や STP のサポートを行いため、パケットのループが発生する構成は行わないでください。フレームがループし続け通信不可となります。EoMPLS 通信を用いて冗長構成を行う場合は、LAN インタフェース側に、STP などを使用できるスイッチ装置を設置し、フレームがループしないようにしてください。

- VLAN タグが異なる VLAN インタフェース同士で EoMPLS 通信を行い、タグを上書きして転送する構成の場合は、STP パケットの VLAN タグも上書きされるため、STP が正常に動作しない可能性があります。VLAN インタフェース側で STP を使用する場合は、VLAN タグを本装置と相手装置で一致させてください。

[未設定時]

EoMPLS を使用しないものとみなされます。

5.8.10　lan mpls l2-circuit exp

[機能]

EoMPLS 通信時の Exp 値書き換えの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] mpls l2-circuit exp {vlan | <exp>}

[オプション]

<number>

- lan 定義番号

  lan 定義の通し番号を、10 進数値で指定します。

  省略時は、0 を指定したものとみなされます。

vlan

- VLAN タグのプライオリティを使用

  VLAN タグのプライオリティフィールドから値を取り出し、MPLS SHIM ヘッダの Exp フィールドにそのまま格納します。EoMPLS 通信で転送するフレームが VLAN でない場合は、Exp フィールドには 0 が格納されます。

<exp>

- 固定の Exp 値を使用

  書き換える Exp 値を、0〜7 の 10 進数値で設定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

EoMPLS 通信が用いる Exp 値を設定します。

[注意]

VC LSP と Tunnel LSP の両方で同じ Exp 値が格納されます。

[未設定時]

0 が設定されているものとみなされます。

```
lan mpls l2-circuit exp 0
```

5.9 VLAN 関連情報

5.9.1 lan vlan bind

[機能]

VLAN インタフェースの出力先の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] vlan bind [<master_type>] <master_number>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<master_type>

このオペランドは Si-R180 のみ有効なオペランドです。
バインド先の定義種別を以下の中から選択して指定します。省略時は"lan"が指定されたものと扱われます。

- lan
  lan 定義にバインドします。
- switch
  スイッチ定義にバインドします。

<master_number>

出力先の lan 定義番号またはスイッチ定義番号を指定します。

[注意]

- <master_number>に VLAN インタフェースを指定しても動作しません。
- VLAN インタフェースの削除は通常の物理 LAN インタフェースと同様に delete lan コマンドによって行います。
- lan vlan bind が設定されていない LAN インタフェースで VLAN のほかの設定を行っても、無効となります。

Si-R180 の場合は以下に注意してください。

- スイッチポート (SW1～SW4) を利用する LAN インタフェースは必ず VLAN 指定となり、<master_type> に’switch’ を指定してください。
- lan vlan tag vid で指定された VLAN-ID と同じ ID を持つポートが少なくともひとつ設定してください。
- スイッチポートをすべて同一のネットワークとして利用する場合、VLAN ID の設定は不要です。
  その場合、スイッチ情報定義の"switch port vlan"の定義も不要です。
- スイッチポートを利用する場合、Ethernet 上に送出されるパケットの tag の有無は switch 定義で設定された内容に従います。lan vlan vid で VLAN-ID が設定されている場合でも、switch 定義で untag として定義された場合は、tag なしパケットとして Ethernet 上に送出されます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

<master_number>で指定した物理 LAN インタフェースを出力先として、VLAN インタフェースとして動作します。lan vlan bind の定義がある LAN インタフェースは VLAN インタフェースとして動作し、lan vlan bind の定義がない LAN インタフェースは通常の物理 LAN インタフェースとして動作します。
VLAN インタフェースの IP アドレスは、lan ip address コマンドによって指定します。また VLAN 上で動作するサービスの定義は、通常の物理 LAN インタフェースと同様に lan コマンドで行います。

[未設定時]

VLAN として動作しないで、通常の物理 LAN インタフェースとして動作します。

5.9.2 lan vlan tag vid

[機能]

VLAN ID の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] vlan tag vid <vid>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<vid>

VLAN ID を、1〜4094 の 10 進数値で設定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

VLAN ID を設定します。

[未設定時]

<vid>に 1 が設定されたものとみなされます。

```
lan <number> vlan tag vid 1
```

5.9.3　lan vlan tag pri

[機能]

プライオリティ情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] vlan tag pri <priority>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<priority>

プライオリティを、0〜7 の 10 進数値で設定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

VLAN インタフェースのフレーム送出時に、VLAN タグのプライオリティフィールド に格納される値を設定します。

[未設定時]

<priority>に 0 が設定されたものとみなされます。

```
lan <number> vlan tag pri 0
```

5.9.4 lan vlan tag primap

[機能]

VLAN プライオリティマッピングの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] vlan tag primap <count> <proto> <tos> <priority>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- プライオリティマッピング定義番号
  プライオリティマッピング定義の通し番号を、10 進数値で指定します。

範囲	機種
0〜199	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B
0〜99	Si-R180

<proto>

- ip
  IP パケットのプライオリティマッピングを定義します。
- ip6
  IPv6 パケットのプライオリティマッピングを定義します。

<tos>

マッピング対象とする ToS 値 (IP) または Traffic Class 値 (IPv6) を、0〜ff の 16 進数値、または"any"で指定します。複数の値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。TOS/Traffic Class 値は","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
以下に、有効な記述形式を示します。

- 0〜ff の 16 進数値 (例: ff = ff の TOS/Traffic Class 値)
- 16 進数値-16 進数値 (例: 32-64 = 32 から 64 までの TOS/Traffic Class 値)
- 16 進数値- (例: 80- = 80 から ff までの TOS/Traffic Class 値)
- -16 進数値 (例: -7f = 0 から 7f までの TOS/Traffic Class 値)
- 16 進数値,16 進数値,… (例: 10,20,30- = 10 と 20 と 30 以降の TOS/Traffic Class 値)

<priority>

プライオリティを、0〜7 の 10 進数値で設定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IP の ToS 値、および IPv6 の Traffic Class 値から VLAN のプライオリティ値へのマッピングの設定をします。
VLAN プライオリティマッピング定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
200	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
100	Si-R180

[未設定時]

VLAN プライオリティマッピング機能を使用しません。

5.10 MAC アドレス認証関連情報

5.10.1 lan macauth use

[機能]

MAC アドレス認証機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] macauth use <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- on
  MAC アドレス認証機能を使用します。
- off
  MAC アドレス認証機能を使用しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

MAC アドレス認証機能について設定します。
<mode>が on の場合、パケット送信元端末の MAC アドレス認証を行い、認められた MAC アドレスである場合に中継を行い、認められていなければパケット破棄します。
<mode>が off の場合、MAC アドレス認証機能は無効です。

[注意]

MAC アドレス認証を行うために、AAA ユーザ情報、RADIUS 情報を設定しておく必要があります。
また、本コマンドと同時に、lan macauth aaa <group_id> で認証先データベースの指定を行ってください。
<group_id>を指定しておかないと MAC アドレス認証が動作しませんので、必ず設定してください。

[未設定時]

MAC アドレス認証機能を使用しないものとみなされます。

```
lan <number> macauth use off
```

5.10.2　lan macauth expire

[機能]

MAC アドレス認証結果保持時間の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] macauth expire <success_time> <failure_time>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<success_time>

- 認証成功保持時間
  MAC アドレス認証が成功した場合の保持時間を、60 秒～86400 秒の範囲で指定します。
  単位は、s(秒)、m(分)、h(時)、d(日) のどれかを指定します。

<failure_time>

- 認証失敗保持時間
  MAC アドレス認証が失敗した場合の保持時間を、60 秒～86400 秒の範囲で指定します。
  単位は、s(秒)、m(分)、h(時)、d(日) のどれかを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本コマンドは、MAC アドレス認証機能を使用する場合にだけ有効です。
MAC アドレス認証結果の保持時間を設定します。

[未設定時]

MAC アドレス認証結果保持時間として認証成功保持時間 20 分、失敗保持時間 5 分を定義したものとみなされます。

```
lan <number> macauth expire 20m 5m
```

5.10.3 lan macauth aaa

[機能]

MAC アドレス認証先データベースの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] macauth aaa <group_id>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

MAC アドレス認証先データベースのグループ ID を設定します。

[注意]

MAC アドレス認証を行うために、AAA ユーザ情報、RADIUS 情報を設定しておく必要があります。
また、本コマンドで<group_id>を指定しておかないと MAC アドレス認証が動作しませんので、必ず設定してください。

[未設定時]

MAC アドレス認証先データベースを指定していないものとみなされます。

5.10.4　lan macauth security

[機能]

MAC アドレス認証エラー時のセキュリティレベルの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

lan [<number>] macauth security <level>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<level>

- high
  認証エラー時のセキュリティレベルを高くします。
- normal
  認証エラー時のセキュリティレベルを通常とします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

MAC アドレス認証が正常に行えなかった場合 (サーバ無応答、内部資源不足など) のセキュリティ動作について設定します。
<level>が high の場合は、パケット通過を遮断します。<level>が normal の場合は、パケットを通過させます。

[未設定時]

認証エラー時のセキュリィレベルとして high を定義したものとみなされます。

```
lan <number> macauth security high
```

第 6 章　シリアル情報の設定

- serial 定義番号の指定範囲

  本章のコマンド の [オプション] に記載されている<number>(serial 定義番号) に指定する serial 定義の通し番号 (10 進数値) は、機種ごとに以下に示す範囲で指定してください。

範囲	機種
0	Si-R220B

6.1　シリアル共通情報

6.1.1　serial use

[機能]

COM ポート動作モードの設定

[適用機種]

				SI-R 220B	

[入力形式]

serial [<number>] use <mode>

[オプション]

<number>

- serial 定義番号
  serial 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

COM ポートを利用するかどうかを指定します。

- on
  COM ポートを利用する場合に指定します。
- off
  COM ポートを利用しない場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

COM ポートを利用するかどうかを指定します。

[未設定時]

COM ポートを利用しないものとみなされます。

```
serial <number> use off
```

6.1.2 serial speed

[機能]

COM ポート通信速度の設定

[適用機種]

				Si-R 220B	

[入力形式]

serial [<number>] speed <speed>

[オプション]

<number>

- serial 定義番号
  serial 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<speed>

- 通信速度
  9600/19200/38400/57600/115200/230400

[動作モード]

構成定義モード (管理者クラス)

[説明]

COM ポートの通信速度を指定します。

[未設定時]

COM ポートの通信速度が 115200bps とみなされます。

```
serial <number> modem speed 115200
```

6.2　モデム関連情報

6.2.1　serial modem dial

[機能]

ダイヤル方式の設定

[適用機種]

				SR 220B	

[入力形式]

serial [<number>] modem dial <type>

[オプション]

<number>

- serial 定義番号
  serial 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<type>

- tone
  トーン式を使用します。
- pulse
  パルス式を使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

モデムでダイヤルするときにトーン式を使うかパルス式を使うかを設定します。

[未設定時]

モデムでダイヤルするときにトーン式を使用するものとみなされます。

```
serial <number> modem dial tone
```

6.2.2 serial modem tonedetect

[機能]

ダイヤルトーン検出の設定

[適用機種]

				Si-R 220B	

[入力形式]

serial [<number>] modem tonedetect <mode>

[オプション]

<number>

- serial 定義番号
  serial 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- on
  ダイヤルトーンを検出します。
- off
  ダイヤルトーンを検出しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ダイヤルする前にダイヤルトーンを検出するかを設定します。

[未設定時]

ダイヤルする前にダイヤルトーンを検出するものとみなされます。

```
serial <number> modem tonedetect on
```

6.2.3　serial modem speaker mode

[機能]

スピーカモード の設定

[適用機種]

				Si-R 220B	

[入力形式]

serial [<number>] modem speaker mode <mode>

[オプション]

<number>

- serial 定義番号
  serial 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- on
  スピーカを ON にします。
- off
  スピーカを OFF にします。
- dial
  スピーカを呼毎に ON にします。
- setup
  スピーカをダイヤル終了からキャリア検出まで ON にします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

スピーカをどのタイミングでならすかを定義します。

[未設定時]

スピーカを呼毎に ON にするものとみなされます。

```
serial <number> modem speaker mode dial
```

6.2.4 serial modem speaker volume

[機能]

スピーカ音量の設定

[適用機種]

				Si-R 220B	

[入力形式]

serial [<number>] modem speaker volume <mode>

[オプション]

<number>

- serial 定義番号
  serial 定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- high
  スピーカ音量を大に設定します。
- medium
  スピーカ音量を中に設定します。
- low
  スピーカ音量を小に設定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

スピーカの音量を設定します。

[未設定時]

スピーカの音量は中とみなされます。

```
serial <number> modem speaker volume medium
```

第 7 章　相手情報の設定

- 相手定義番号の指定範囲

  本章のコマンド の [オプション] に記載されている<number>(相手定義番号) に指定する相手ネットワークの通し番号 (10 進数値) は、機種ごとに以下に示す範囲で指定してください。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B　Si-R240　Si-R220B
0〜49	Si-R180

- 接続先定義番号の指定範囲

  接続先情報の [オプション] に記載されている<ap_number>(接続先定義番号) に指定する接続先の通し番号 (10 進数値) は、機種ごとに以下に示す範囲で指定してください。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B　Si-R240　Si-R220B
0〜49	Si-R180

7.1　相手共通情報

7.1.1　remote name

[機能]

相手ネットワーク名称の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] name <network_name>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<network_name>

- 相手ネットワーク名
  相手ネットワーク名を、0x21,0x23～0x7e の 8 文字以内の ASCII 文字列で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手ネットワーク名を設定します。

[注意]

すでに同一名称の相手ネットワークが登録されている場合は、異常終了します。

[未設定時]

相手ネットワーク名を設定しないものとみなされます。

7.1.2　remote autodial

[機能]

自動ダイヤル可否の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] autodial <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

自動的にダイヤルするかどうかを指定します。

- enable
  送信すべきパケットが発生した場合に、自動ダイヤルを行います。
- disable
  送信すべきパケットが発生しても、自動ダイヤルを行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

指定した相手に対して、自動的にダイヤルするかどうかを設定します。

[注意]

Si-R570 Si-R370 Si-R220B の場合は以下に注意してください。
wan isdn autodial で<mode>に disable を指定している場合は、自動ダイヤルを行えません。自動ダイヤルを行う場合は、<mode>に enable を指定しておいてください。

[未設定時]

自動ダイヤルを行うものとみなされます。

```
remote <number> autodial enable
```

7.1.3 remote mtu

[機能]

送信パケット最大長 (MTU 値) の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] mtu <mtu>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mtu>

- MTU 値
  MTU 値を、200～1500 の 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

リモートに対して送信するパケットの MTU 値を設定します。
MTU 値を変更すると、このリモートに対して送信するパケットの最大長が変更されます。また、PPP ネゴシエーションで相手 MRU 値、相手 MRRU 値が MTU 値まで小さくなることを許すようになります。

[未設定時]

MTU 値に 1500 を指定したものとみなされます。

```
remote <number> mtu 1500
```

7.1.4　remote shaping

[機能]

シェーピング機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] shaping <mode> [<rate>]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- on
  シェーピングを使用します。
- off
  シェーピングを使用しません。

<rate>

- 最大送出レート
  最大送出レートを、10 進数値と単位文字で指定します。
  10 進数値の末尾に k または m の単位文字を付与することで単位を指定できます。
  単位文字を付与しない場合、単位は Kbps となります。
  単位文字 k を付与した場合、単位は Kbps となります。
  単位文字 m を付与した場合、単位は Mbps となります。
  1Kbps は 1000bps、1Mbps は 1000Kbps です。

範囲	機種
1～1000000 1k～1000000k 1m～1000m	Si-R570
1～100000 1k～100000k 1m～100m	上記以外

[動作モード]

構成定義モード (管理者クラス)

[説明]

シェーピング機能について設定します。
<mode>が on の場合、<rate>で設定したレートに送信を抑制します。回線速度を上回る値を設定した場合は、実質的にシェーピングは機能しません。
<mode>が off の場合、<rate>は設定できません。

[注意]

使用する回線が LAN の場合、シェーピングを使用しないと帯域制御機能は有効に動作しません。

[未設定時]

シェーピングを使用しないものとみなされます。

```
remote <number> shaping off
```

7.2　接続先情報

7.2.1　remote ap name

[機能]

接続先の名称の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] name <ap_name>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_name>

- 接続先名
  接続先名を、0x21,0x23～0x7e の 8 文字以内の ASCII 文字列で指定します。
  ただし、all は接続／切断コマンドで使う予約語であるため、使用しないでください。
  接続先名に all を指定した接続先のみを接続／切断することができなくなります。

[動作モード]

構成定義モード (管理者クラス)

[説明]

接続先名を設定します。

[注意]

接続先の情報をすべて未設定時の値で使用する場合は必ず接続先名を設定してください。すべての値が未設定時値の場合は接続先の情報は削除されます。

[未設定時]

接続先名を設定しないものとみなされます。

7.2.2 remote ap move

[機能]

接続先の優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap move <ap_number> <new_ap_number>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 対象接続先定義番号
  優先順序を変更する接続先定義番号を指定します。

<new_ap_number>

- 移動先接続先定義番号
  対象接続先を移動させる先の接続先定義番号を指定します。
  対象接続先は、ここで指定した接続先の前に移動されます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

接続先の順序を変更します。

7.2.3　remote ap datalink type

[機能]

パケット転送方法の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] datalink type <type>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<type>

パケットの転送方式を指定します。

- physical
  bind 命令 (remote ap datalink bind を参照) によって決定された利用回線のデフォルトの転送方式を提供する場合に指定します。以下に各回線のデフォルトの転送方式を示します。

回線種別	転送方式	Si-R570 Si-R370	Si-R180	Si-R260B	Si-R240	Si-R220B
ISDN	PPP	○	―	―	―	○
HSD	PPP	○	―	―	―	○
FR	RFC2427方式	○	―	―	―	○
ATM	AAL5(RFC1483)	○	―	○	―	―
Ethernet	PPPoE方式	○	○	○	○	○
モデム接続	非同期PPP	―	―	―	―	○
データ通信カード *1)	非同期PPP	―	―	―	○	―

*1) PC カードスロットに挿入したデータ通信カードを利用

- ip
  IP tunnel を使用する場合に指定します。
- ipsec
  IPsec を使用する場合に指定します。
- overlap
  overlap ap として、別 IF からの出力とする場合に指定します。

- mpls
  MPLS LSP を使用する場合に指定します。
- discard
  この接続先利用時にはすべてのパケットが破棄されます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

指定した接続先を利用してパケットを転送する場合の転送方式を設定します。

[未設定時]

転送方式として physical を設定するものとみなされます。

```
remote <number> ap 0 datalink type physical
```

7.2.4　remote ap datalink bind

[機能]

パケット転送回線の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] datalink bind <kind> [<conf_number>]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<kind>

- wan
  wan 定義によって指定される回線を利用する場合に指定します。
  (※ Si-R180 では指定できません)
- lan
  lan 定義によって指定される回線を利用する場合に指定します。
- serial
  serial 定義によって指定される回線を利用する場合に指定します。
  (※ Si-R220B だけ指定できます)
- any
  ISDN を使用するように設定した、すべての wan 定義を指定したものとみなされます。
  (※ Si-R260B Si-R240 Si-R180 では指定できません)

<conf_number>

wan 定義または lan 定義または serial 定義の定義番号を指定します。

- wan 定義の定義番号
  利用する wan 定義の定義番号を、10 進数値で指定します。
  (※ Si-R180 では指定できません)

範囲	機種
0～131	Si-R570
0～15	Si-R370　Si-R260B
0	Si-R240　Si-R220B

- lan 定義の定義番号
  利用する lan の定義番号を、10 進数値で指定します。

範囲	機種
0〜19	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B
0〜9	Si-R180

- serial 定義の定義番号
  serial 定義の定義番号を、10 進数値で指定します。
  (※ Si-R220B だけ指定できます)

範囲	機種
0	Si-R220B

[動作モード]

構成定義モード (管理者クラス)

[説明]

指定した接続先定義を利用してパケットを転送する場合の回線を設定します。
本コマンドは、remote ap datalink type の<type>で physical を指定した場合にだけ有効です。

[未設定時]

Si-R570 Si-R370 Si-R260B Si-R220B の場合は、<kind>に wan を、<conf_number>に 0 を指定するものとみなされます。

```
remote <number> ap 0 datalink bind wan 0
```

Si-R240 Si-R180 の場合は、パケット転送回線を設定しないものとみなされます。

7.2.5　remote ap recovery

[機能]

接続自動復旧モード の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] recovery <mode> <startup>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- auto
  回線障害復旧時に接続を自動復旧します。
- manual
  回線障害発生時に自動的に接続先閉塞状態となり、回線障害が復旧した場合にもオペレータ指示があるまで接続を復旧させません。

<startup>

- up
  装置起動時、および動的定義反映時は接続先閉塞していない状態で動作を開始します。
- down
  装置起動時、および動的定義反映時は接続先閉塞状態で動作を開始し、オペレータからの閉塞状態解除指示を待ちます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

回線障害の復旧時に、接続回復の動作モード を設定します。

[未設定時]

装置起動時、および動的定義反映時に接続先閉塞していない状態で動作を開始し、回線障害発生時でも障害復旧後に接続を自動復旧します。

```
remote <number> ap <ap_number> recovery auto up
```

7.2.6 remote ap ip dns

[機能]

DNS サーバアドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ip dns <dns>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<dns>

- DNS サーバアドレス
  接続先と接続するときに利用する DNS サーバのアドレスを指定します。
  ここでの指定によって、以下のように動作します。

  0.0.0.0 アドレスを自動取得するものとみなされます。

  255.255.255.255
  DNS サーバを使用しないものとみなされます。

  上記以外 設定したアドレスを、相手装置に通知します。
  この場合の設定可能な範囲は以下のとおりです。
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[動作モード]

構成定義モード (管理者クラス)

[説明]

指定した接続先と接続するときに利用する DNS サーバアドレスを設定します。
本コマンドによる設定情報は、以下の 2 つの場合に利用されます。

- ProxyDNS からの利用
  ProxyDNS 機能と併用する場合、接続先と接続中のときは、<dns>で設定したアドレスに対して ProxyDNS から DNS 問い合わせを行います。本コマンドによる設定情報がない場合は、IPCP 機能によって相手ルータから DNS サーバアドレスを取得します。
- 通信相手への DNS サーバアドレス通知
  接続先から IPCP 機能を用いて DNS サーバアドレス通知要求を受けた場合に、<dns>で設定した IP アドレスを通知します。本コマンドによる設定がない場合は通知しません。

[未設定時]

アドレスを自動取得するものとみなされます。

```
remote <number> ap 0 ip dns 0.0.0.0
```

7.2.7 remote ap multiroute pattern

[機能]

マルチルーティングのパケット振り分けパターンの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] multiroute pattern <count> <action> <src_addr>/<mask> <src_port> <dst_addr>/<mask> <dst_port> <protocol> [<tos>]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- パケット振り分けパターン定義番号
  パケット振り分けパターンの優先度を表す番号を、10 進数値で指定します。
  指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つ定義がすでに存在する場合は、既存の定義を変更します。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B Si-R240 Si-R220B
0〜49	Si-R180

<action>

該当するパケットの動作を設定します。

- use
  該当するパケットは、この ap 定義を利用して送信されます。
- unuse
  該当するパケットは、この ap 定義を利用して送信されません。
- backup
  以降の ap 定義で出力することができない場合に、この ap 定義を利用して送信されます。

<src_addr>/<mask>

対象とする送信元 IP アドレスとマスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)

  対象とする送信元 IP アドレスとマスクビット数の組み合わせを指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。

  - IP アドレス/マスクビット数 (例: 192.168.1.1/24)
  - IP アドレス/マスク値 (例: 192.168.1.1/255.255.255.0)

- any

  すべての送信元 IP アドレスを対象とする場合に指定します。

  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<src_port>

対象とする送信元ポート番号を指定します。

- ポート番号

  対象とする送信元ポート番号を、1〜65535 の 10 進数値で指定します。

  複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。

  ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。

  以下に、有効な記述形式を示します。

  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)

- any

  すべての送信元ポート番号を対象とする場合に指定します。

<dst_addr>/<mask>

対象とするあて先 IP アドレスとマスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)

  対象とするあて先 IP アドレスとマスクビット数の組み合わせを指定します。

  記述形式は、<src_addr>/<mask>と同様です。

- any

  すべてのあて先 IP アドレスを対象とする場合に指定します。

  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<dst_port>

対象とするあて先ポート番号を指定します。

- ポート番号

  対象とするあて先ポート番号を、1〜65535 の 10 進数値で指定します。

  記述形式は、<src_port>と同様です。

- any

  すべてのあて先ポート番号を対象とする場合に指定します。

<protocol>

対象とするプロトコル番号を指定します。

- プロトコル番号
  対象とするプロトコル番号を、1〜255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号を対象とする場合に指定します。

<tos>

対象とする TOS 値を指定します。
省略時は、any を指定したものとみなされます。

- TOS 値
  対象とする TOS 値を、0〜ff の 16 進数値で指定します。
  複数の TOS 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。TOS 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 00〜ff の 16 進数値 (例: ff = ff の TOS 値)
  - TOS 値-TOS 値 (例: 32-64 = 32 から 64 までの TOS 値)
  - TOS 値- (例: 80- = 80 から ff までの TOS 値)
  - -TOS 値 (例: -7f = 0 から 7f までの TOS 値)
  - TOS 値,TOS 値,… (例: 10,20,30- = 10 と 20 と 30 以降の TOS 値)
- any
  すべての TOS 値をフィルタリング対象とする場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

マルチルーティング機能の接続先選択に対するパケットパターンを設定します。
指定したアドレス、ポート番号、プロトコル、TOS 値と一致するパケットを透過または遮断します。設定した優先度順に一致するか調べ、一致した時点で処理が判断され、それ以降の設定は参照されません。
本装置全体で以下の数まで定義できます。

最大定義数	機種
1000	Si-R570
500	Si-R370
100	Si-R260B Si-R240 Si-R220B
50	Si-R180

[未設定時]

すべてのパケットがこの ap 定義を利用して送信可能とみなします。

7.2.8　remote ap multiroute pattern move

[機能]

マルチルーティングのパケット振り分けパターンの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] multiroute pattern move <count> <new_count>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象ルール定義番号
  優先順序を変更するルール定義の番号を指定します。

<new_count>

- 移動先ルール定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0～999	Si-R570
0～499	Si-R370
0～99	Si-R260B　Si-R240　Si-R220B
0～49	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

マルチルーティングのパケット振り分けパターンの優先順序を変更します。

7.2.9 remote ap limit charge

[機能]

課金累計制限の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

remote [<number>] ap [<ap_number>] limit charge <charge>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<charge>

- 課金累計上限
  課金累計の上限金額を、0〜999999 の 10 進数値で指定します。
  0 を指定した場合は、上限を設定しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

指定した接続先に対する課金累計の上限値を設定します。
発信時に、接続先に対する課金累計が指定した上限値を超えていた場合は、この接続先に対する自動発信を行いません。次の優先度の接続先に対して処理を移します。

[未設定時]

課金累計の上限値を設定しないものとみなされます。

```
remote <number> ap <ap_number> limit charge 0
```

7.2.10　remote ap limit time

[機能]

接続時間累計制限の設定

[適用機種]

Si-R 570	Si-R 370		Si-R 240	Si-R 220B	

[入力形式]

remote [<number>] ap [<ap_number>] limit time <time>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<time>

- 接続時間累計上限
  接続時間累計の上限時間を、0 秒～999 時間の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。
  0 秒を指定した場合は、上限を設定しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

指定した接続先に対する接続時間累計の上限値を設定します。
発信時に、この接続先に対する接続時間累計が指定した上限値を超えていた場合は、この接続先に対する自動発信を行いません。次の優先度の接続先に対して処理を移します。

[未設定時]

接続時間累計の上限値を設定しないものとみなされます。

```
remote <number> ap <ap_number> limit time 0s
```

7.2.11 remote ap disconnect time

[機能]

強制切断を行う累計接続時間の設定

[適用機種]

			Si-R 240		

[入力形式]

remote [<number>] ap [<ap_number>] disconnect time <time >

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<time>

- 強制切断を行う累計接続時間
  累計接続時間の上限値を、0 秒～999 時間の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。
  0 秒を指定した場合は、累計接続時間による強制切断を行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

指定した接続先に対する強制切断を行う累計接続時間を設定します。
接続中に、この接続先に対する累計接続時間が指定した上限値を超えていた場合は、切断し、以降の手動および自動発信を行いません。

[注意]

本コマンド はデータ通信カード 接続時に有効です。

[未設定時]

指定した接続先に対する強制切断を行う累計接続時間を設定しないものとみなされます。

```
remote <number> ap <ap_number> disconnect time 0s
```

7.2.12　remote ap disconnect packet

[機能]

強制切断を行う累計パケット数の設定

[適用機種]

Si-R 240

[入力形式]

remote [<number>] ap [<ap_number>] disconnect packet <packet> <algorithm>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<packet>

- 強制切断を行う累計パケット数
  累計パケット数の上限値を 0～1000000000 の範囲で指定します。
  0 を指定すると累計パケット数による強制切断を行いません。

<algorithm>

累計パケット数の計算方法を指定します。

- per128
  累計送受信バイト数 (PPP パケット長) を 128 で割った値を累計パケット数とします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

指定した接続先に対する強制切断を行う累計パケット数を設定します。
接続中に、この接続先に対する累計パケット数が指定した上限値を超えていた場合は、切断し、以降の手動および自動発信を行いません。

[注意]

本コマンドはデータ通信カード接続時に有効です。

[未設定時]

指定した接続先に対する強制切断を行う累計パケット数を設定しないものとみなされます。

```
remote <number> ap <ap_number> disconnect packet 0 per128
```

7.2.13 remote ap ppp auth type

[機能]

認証方法の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

remote [<number>] ap [<ap_number>] ppp auth type <authtype>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<authtype>

認証プロトコルのタイプを指定します。

- off
  認証を要求しない場合に指定します。
- pap
  PAP による認証を要求する場合に指定します。
- chap_md5
  MD5-CHAP による認証を要求する場合に指定します。
- any
  MD5-CHAP または PAP による認証を要求し、実際に利用する認証プロトコルはネゴシエーションによって決定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

接続時に要求する認証プロトコルのタイプを設定します。
ここでの設定は、着信し、かつ CLID 相手判定が行われた場合に有効となります。

[未設定時]

着信時の認証プロトコルに MD5-CHAP または PAP を用います。

```
remote <number> ap 0 ppp auth type any
```

7.2.14　remote ap ppp auth send

[機能]

送信認証情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ppp auth send <id> <password> [encrypted]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<id>

- 認証 ID
  認証 ID を、0x21,0x23～0x7e の文字で構成される 64 文字以内の文字列を指定します。

<password>

- 認証パスワード
  認証パスワードを、0x21,0x23～0x7e の文字で構成される 64 文字以内の文字列を指定します。
  show コマンドで表示される暗号化された認証パスワード文字列を encrypted とともに指定することもできます。その場合、表示された文字列をそのまま正確に入力してください。文字列は 64 文字を超えていてもかまいません。
- 暗号化された認証パスワード
  show コマンドで表示される暗号化された認証パスワードを encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化認証パスワード指定
  <password>に暗号化された認証パスワードを設定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

指定した接続先に接続するときに送信する認証情報 (認証 ID およびパスワード) を設定します。

[注意]

認証 ID およびパスワードが設定されていない場合、接続相手からの認証要求を拒否します。show コマンドでは、暗号化された認証パスワードが encrypted と共に表示されます。

[未設定時]

送信する認証情報を定義しないものとみなされます。

7.2.15　remote ap ppp auth receive

[機能]

受諾認証情報の設定

[適用機種]

Si-R 570	Si-R 370		Si-R 240	Si-R 220B	

[入力形式]

remote [<number>] ap [<ap_number>] ppp auth receive <id> <password> [encrypted]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<id>

- 認証 ID
  認証 ID を、0x21,0x23～0x7e の文字で構成される 64 文字以内の文字列を指定します。

<password>

- 認証パスワード
  認証パスワードを、0x21,0x23～0x7e の文字で構成される 64 文字以内の文字列を指定します。
  show コマンドで表示される暗号化された認証パスワードを encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化認証パスワード指定
  <password>に暗号化された認証パスワードを設定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

認証プロトコル使用時に受諾する、認証情報 (認証 ID および認証パスワード) を設定します。

[注意]

show コマンドでは、暗号化された認証パスワードが encrypted と共に表示されます。

[未設定時]

受諾する認証情報を設定しないものとみなされます。

7.2.16 remote ap ppp mp use

[機能]

発信時の MP 利用の可否の設定

[適用機種]

Si-R 570 | Si-R 370 | | | Si-R 220B | |

[入力形式]

remote [<number>] ap [<ap_number>] ppp mp use <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

MP を利用するかどうかを指定します。

- off
  MP を利用しない場合に指定します。
- on
  MP を利用する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

発信時に MP を利用するかどうかを設定します。
着信時は、CLID 相手判定によって指定した接続先への接続が決定された場合に、MP を利用するかどうかを設定します。

[未設定時]

MP を利用しないものとみなされます。

```
remote <number> ap 0 ppp mp use off
```

7.2.17　remote ap ppp mp bap use

[機能]

発信時の BAP/BACP 利用の可否の設定

[適用機種]

Si-R 570 | Si-R 370 | | | Si-R 220B | |

[入力形式]

remote [<number>] ap [<ap_number>] ppp mp bap use <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

BAP/BACP を利用するかどうかを指定します。

- off
  BAP/BACP を利用しない場合に指定します。
- on
  BAP/BACP を利用する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

MP を利用する場合に BAP/BACP を利用するかどうかを設定します。
着信時は、CLID 相手判定によってこの接続先への接続が決定された場合に、BAP/BACP を利用するかどうかを設定します。

[未設定時]

BAP/BACP を利用しないものとみなされます。

```
remote <number> ap 0 ppp mp bap use off
```

7.2.18 remote ap pppoe acname

[機能]

アクセスコンセントレータ名 (AC-Name) の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] pppoe acname <ac_name>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ac_name>

- アクセスコンセントレータ名
  アクセスコンセントレータ名 (AC-Name) を、0x21,0x23～0x7e のコードで構成される 64 文字以内の ASCII 文字列で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

アクセスコンセントレータ名 (AC-Name) を設定します。

[未設定時]

アクセスコンセントレータ名 (AC-Name) を指定しないものとみなされます。

7.2.19　remote ap pppoe svname

[機能]

サービスネーム (Service-Name) の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] pppoe svname <sv_name>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<sv_name>

- サービスネーム
  サービスネーム (Service-Name) を、0x21,0x23～0x7e のコードで構成される 64 文字以内の ASCII 文字列で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

サービスネーム (Service-Name) を設定します。

[未設定時]

サービスネーム (Service-Name) を指定しないものとみなされます。

7.2.20 remote ap dial number

[機能]

接続先の電話番号の設定

[適用機種]

Si-R 570	Si-R 370		Si-R 240	Si-R 220B	

[入力形式]

remote [<number>] ap [<ap_number>] dial <count> number <dial_number> [<subaddress>]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

ダイヤル定義番号として、以下のどれかを指定します。

- 0
- 1
- 2

<dial_number>

- 相手電話番号
  相手の電話番号を、0〜9 の数字と、*、#、-、(、)、\ の文字で構成される 32 桁以内の ASCII 文字列で指定します。

<subaddress>

- 相手サブアドレス
  相手のサブアドレスを、0x21,0x23〜0x7e の文字で構成される 19 桁以内の ASCII 文字列で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

接続先の電話番号を設定します。

[注意]

Si-R370 Si-R220B は PIAFS 接続に対応しています。PIAFS(64Kbps) 着信時は、<subaddress> で設定した相手サブアドレスは無視されます。

[未設定時]

接続先の電話番号を設定しないものとみなされます。

7.2.21　remote ap dial speed

[機能]

接続先の通信速度の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

remote [<number>] ap [<ap_number>] dial <count> speed <speed> [<carrier>]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

ダイヤル定義番号として、以下のどれかを指定します。

- 0
- 1
- 2

<speed>

通信速度、通信手順を指定します。"PIAFS" および "PIAFS64K" は PIAFS 対応の Si-R370 Si-R220B でだけ指定できます。

- 64K
  同期 PPP 64Kbps の場合に指定します。
- PIAFS
  PIAFS(32Kbps) 接続の場合に指定します。
- PIAFS64K
  PIAFS(64Kbps) 接続の場合に指定します。

<carrier>

通信速度に "PIAFS64K" を指定した場合に通信事業者を指定します。省略時は、"docomo" を指定したものとみなされます。なお、通信速度に "PIAFS64K" 以外を指定した場合は、本パラメタを指定しないでください。

- docomo
  NTT DoCoMo の PIAFS(64Kbps) 接続の場合に指定します。
- ddip
  ウィルコム (旧 DDI Pocket) の PIAFS(64Kbps) 接続の場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

接続先の通信速度および通信手順を設定します。

[未設定時]

通信速度に 64kbps を指定したものとみなされます。

```
remote <number> ap 0 dial <count> speed 64K
```

7.2.22　remote ap called accept

[機能]

接続先からの着信許可の設定

[適用機種]

Si-R 570	Si-R 370		Si-R 240	Si-R 220B	

[入力形式]

remote [<number>] ap <ap_number> called accept <incoming>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<incoming>

着信を許可するかどうかを指定します。

- enable
  着信を許可する場合に指定します。
- disable
  着信を許可しない場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

指定した接続先から送られてきたと判断されたデータに対して、着信を許可するかどうかを設定します。

[未設定時]

着信を許可するものとみなされます。

```
remote <number> ap 0 called accept enable
```

7.2.23 remote ap called clid

[機能]

CLID 相手判断利用の可否の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

remote [<number>] ap <ap_number> called clid <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

着信時に CLID 相手判定をするかどうかを指定します。

- enable
  着信時に CLID 相手判定をする場合に指定します。
- disable
  着信時に CLID 相手判定をしない場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

着信時に、相手電話番号を判定するかどうかを設定します。相手電話番号を判定することを、CLID 相手判定と呼びます。

- 以下の定義の相手電話番号を利用して、着信時に相手を判定します。
  1) remote ap called number による定義が存在する場合は、その定義の相手電話番号。
  2) 1) の定義が存在しないで、remote ap dial number による定義が存在する場合は、その定義の相手電話番号。
- 本コマンド の<mode>で enable を指定した場合に上記の番号が発信者番号として通知されたときは、指定した接続先から着信したものとみなされます。

[未設定時]

着信時に、CLID 相手判定を行うものとみなされます。

```
remote <number> ap 0 called clid enable
```

7.2.24　remote ap called number

[機能]

CLID の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

remote [<number>] ap [<ap_number>] called number <called_number> [<subaddress>]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<called_number>

相手電話番号

- 相手電話番号
  相手の電話番号を、0～9 の数字と、*、#、-、(、)、\ の文字で構成される 32 桁以内の ASCII 文字列で指定します。
- any
  着信時の CLID 相手判定に、"remote ap dial number"で設定した相手電話番号を使用する場合に指定します。

<subaddress>

- 相手サブアドレス
  相手のサブアドレスを、0x21,0x23～0x7e の文字で構成される 19 桁以内の ASCII 文字列で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

CLID 相手判定で、チェックする番号を設定します。

[注意]

Si-R370 Si-R220B は PIAFS 接続に対応しています。PIAFS(64Kbps) 着信時には、<subaddress> で設定した相手サブアドレスは無視されます。

[未設定時]

着信時の CLID 相手判定に、"remote ap dial number"で設定された相手電話番号を使用します。

```
remote <number> ap 0 called number any
```

7.2.25　remote ap connect priority

[機能]

接続優先制御の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

remote [<number>] ap [<ap_number>] connect priority <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- off
  接続優先制御を行いません。
- initiator
  発信接続を優先して接続します。
- responder
  着信接続を優先して接続します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

自装置からの発信接続と相手装置からの着信接続が競合した場合に、どちらの接続を優先して接続するかを設定します。
off を設定した場合は、両方の接続処理が行われます。

[注意]

自装置と接続相手装置の両方で接続優先制御を行う場合は、それぞれ異なる優先方法を選択してください。
同じ優先制御を行うと、接続できない場合があります。

[未設定時]

接続優先制御を行いません。

```
remote <number> ap <ap_number> connect priority off
```

7.2.26 remote ap idle

[機能]

無通信監視タイマの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] idle <time> [<direction>]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<time>

- 無通信監視時間
  無通信監視時間を、0 秒～3600 秒の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。
  0 秒を指定した場合は、監視を行いません。

<direction>

- 省略
  送信パケット、および受信パケットを通信監視の対象とします。
- send
  送信パケットだけを通信監視の対象とします。受信パケットは監視対象とはなりません。
- receive
  受信パケットだけを通信監視の対象とします。送信パケットは監視対象とはなりません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

指定した接続先と接続したときの無通信監視時間を設定します。
<time>で設定された間、監視対象となるパケットがない場合に、無通信として回線を切断します。

[未設定時]

無通信監視を行わないものとみなされます。

```
remote <number> ap <ap_number> idle 0d
```

7.2.27　remote ap step

[機能]

平日昼間時間帯の課金単位時間の設定

[適用機種]

Si-R 570	Si-R 370		Si-R 240	Si-R 220B	

[入力形式]

remote [<number>] ap [<ap_number>] step <time>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<time>

- 課金単位時間
  平日昼間時間帯 (月～金曜日 8:00～19:00) の課金単位時間 (秒) の 10 倍の値を、0～36000 の 10 進数値で指定します (例: 180 秒=1800、16.5 秒=165)。
  0 を指定した場合は、課金単位に応じた接続保持を行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ISDN 回線を利用して通信するときの平日昼間時間帯 (月～金曜日 08:00～19:00) の課金単位時間を設定します。課金単位時間を設定すると、無通信の場合でも接続時間が設定値の整数倍になるまで接続を保持します。

[注意]

課金単位時間を設定する場合、本装置の時刻を正しく設定してください。祝日の料金には対応していません。

[未設定時]

課金単位時間を設定しないものとみなされます。

7.2.28 remote ap step2

[機能]

夜間・休日時間帯の課金単位時間の設定

[適用機種]

Si-R 570	Si-R 370		Si-R 240	Si-R 220B	

[入力形式]

remote [<number>] ap [<ap_number>] step2 <time2>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<time2>

- 課金単位時間
  夜間・休日時間帯 (月～金曜日 19:00～23:00)、土/日曜日 (08:00～23:00) の課金単位時間 (秒) の 10 倍の値を、0～36000 の 10 進数値で指定します (例: 180 秒=1800、16.5 秒=165)。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ISDN 回線を利用して通信するときの夜間・休日時間帯 (月～金曜日 19:00～23:00、土/日曜日 08:00～23:00) の課金単位時間を設定します。課金単位時間を設定すると、無通信の場合でも接続時間が設定値の整数倍になるまで接続を保持します。

[注意]

課金単位時間を設定する場合、本装置の時刻を正しく設定してください。
この設定は、"remote ap step"を設定した場合にだけ有効です。祝日の料金には対応していません。

[未設定時]

課金単位時間を設定していないものとみなされ、"remote ap step"で設定した値が使用されます。

7.2.29　remote ap step3

[機能]

深夜時間帯の課金単位時間の設定

[適用機種]

Si-R 570	Si-R 370		Si-R 240	Si-R 220B	

[入力形式]

remote [<number>] ap [<ap_number>] step3 <time3>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<time3>

- 課金単位時間
  深夜時間帯 (全日 23:00～08:00) の課金単位時間 (秒) の 10 倍の値を、0～36000 の 10 進数値で指定します (例: 180 秒=1800、16.5 秒=165)。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ISDN 回線を利用して通信するときの深夜時間帯 (全日 23:00～08:00) の課金単位時間を設定します。課金単位時間を設定すると、無通信の場合でも接続時間が設定値の整数倍になるまで接続を保持します。

[注意]

課金単位時間を設定する場合、本装置の時刻を正しく設定してください。
この設定は、"remote ap step"を設定した場合にだけ有効です。祝日の料金には対応していません。

[未設定時]

課金単位時間を設定していないものとみなされ、"remote ap step2"で設定した値が使用されます。この設定もない場合は、"remote ap step"で設定した値が使用されます。

7.2.30 remote ap keep

[機能]

回線接続保持機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] keep <keep>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<keep>

回線接続保持の方式を設定します。

- off
  回線接続を保持しません。
- connect
  常時接続機能を使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

回線接続保持の方式を設定します。
"connect"のときには回線接続保持の方式として、常時接続機能による制御を行います。

[未設定時]

回線接続保持機能を使用しないものとみなされます。

```
remote <number> ap 0 keep off
```

7.2.31　remote ap fr dlci

[機能]

フレームリレーの DLCI の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

remote [<number>] ap <ap_number> fr dlci <dlci_number>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<dlci_number>

- DLCI
  自局で使用する DLCI を、16～991 の 10 進数値で指定します。
  なお、設定を削除する場合は、0 を指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

フレームリレーの DLCI(データリンクコネクション識別子) を設定します。
フレームリレーを使用する場合は、本コマンド を必ず実行してください。

[未設定時]

DLCI を設定しないものとみなされます。

7.2.32 remote ap fr cir

[機能]

フレームリレーの CIR の設定

[適用機種]

Si-R 570 | Si-R 370 | | | Si-R 220B | |

[入力形式]

remote [<number>] ap <ap_number> fr cir <cir>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<cir>

- CIR 値
  CIR 値を、0〜アクセス速度/2 で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

フレームリレーの、DLCI ごとの CIR 値 (認定情報速度) を設定します。

[未設定時]

CIR 値として 0 を指定したものとみなされます。

```
remote <number> ap <ap_number> fr cir 0
```

7.2.33　remote ap atm vci

[機能]

VCC の VCI 値の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B

[入力形式]

remote [<number>] ap [<ap_number>] atm vci <vci_value>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<vci_value>

- VCI 値
  VCC の VCI 値を以下の範囲で指定します。
  なお、設定を削除する場合は、0 を指定します。

機種	拡張モジュール	範囲
Si-R570	ATM25M拡張モジュールL2 ATM155M拡張モジュールL2	32～4095 32～2047
	ATM25M拡張モジュールH1 ATM155M拡張モジュールH1	32～1023
Si-R370	ATM25M拡張モジュールL2 ATM155M拡張モジュールL2	32～4095 32～2047
Si-R260B		32～4095

[動作モード]

構成定義モード (管理者クラス)

[説明]

VCC(Virtual Channel Connection) で使用する VCI 値を設定します。
また、拡張モジュール単位で定義可能な VCC 数は以下のとおりです。
装置全体で定義可能な VCC 数は「仕様一覧」のシステム最大値一覧を参照してください。

- Si-R260B および ATM25M 拡張モジュール L2
  20VCC

- ATM155M 拡張モジュール L2
  20VCC
- ATM25M 拡張モジュール H1
  200VCC
- ATM155M 拡張モジュール H1
  200VCC

[未設定時]

VCI 値を設定しないものとみなされます。

7.2.34　remote ap atm rate

[機能]

VCC の VC 速度の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B

[入力形式]

remote [<number>] ap [<ap_number>] atm rate <rate>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<rate>

- VC 速度値
  VCC の速度を以下の範囲で指定します。

機種	拡張モジュール	範囲
Si-R570	ATM25M拡張モジュールL2 ATM155M拡張モジュールL2	64k～ 25m:8k刻み、または50k刻み
	ATM25M拡張モジュールH1	64k～ 25m:8k刻み、または50k刻み
	ATM155M拡張モジュールH1	64k～100m:8k刻み、または50k刻み
Si-R370	ATM25M拡張モジュールL2 ATM155M拡張モジュールL2	64k～ 25m:8k刻み、または50k刻み
Si-R260B		64k～ 25m:8k刻み、または50k刻み

kとmは単位を表し、kはKbpsをmはMbpsを示します。
なお、設定を削除する場合は、0を指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

VCC(Virtual Channel Connection) の VC 速度を設定します。
VC 速度は VCC が属する VPC の VP 速度を超えないように設定します。

[未設定時]

VC 速度を設定しないものとみなされます。

```
remote <number> ap <ap_number> atm rate 0
```

7.2.35　remote ap atm ast

[機能]

VCC のサービスタイプの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B

[入力形式]

remote [<number>] ap [<ap_number>] atm ast cbr
remote [<number>] ap [<ap_number>] atm ast vbr [<scr> [<mbs>]]
remote [<number>] ap [<ap_number>] atm ast ubrp [<mcr>]
remote [<number>] ap [<ap_number>] atm ast gfrp [<gr>]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

cbr

- サービスタイプ CBR
  サービスタイプとして CBR を指定します。

vbr

- サービスタイプ VBR
  サービスタイプとして VBR を指定します。

ubrp

- サービスタイプ UBR+
  サービスタイプとして UBR+を指定します。
  なお、ATM 拡張モジュール H1 では、1-VPC での VP/VC 同時シェーピング時以外に UBR+を指定された場合は、無効となります。

gfrp

- サービスタイプ GFR+
  サービスタイプとして GFR+を指定します。

<scr>

- 平均速度値
  サービスタイプとして VBR を指定したときの平均速度を以下の範囲で指定します。

機種	拡張モジュール	範囲
Si-R570	ATM25M拡張モジュールL2 ATM155M拡張モジュールL2	64k～ 25m:8k刻み、または50k刻み
	ATM25M拡張モジュールH1	64k～ 25m:8k刻み、または50k刻み
	ATM155M拡張モジュールH1	64k～100m:8k刻み、または50k刻み
Si-R370	ATM25M拡張モジュールL2 ATM155M拡張モジュールL2	64k～ 25m:8k刻み、または50k刻み
Si-R260B		64k～ 25m:8k刻み、または50k刻み

kとmは単位を表し、kはKbpsをmはMbpsを示します。
0を指定、または省略時は、装置内部で自動設定されます。

<mbs>

- 最大バースト長

  サービスタイプとして VBR を指定したときの最大バースト長を、1～1400 の 10 進数値で指定します。

  省略時は、0 を指定したものとみなされ、装置内部で自動設定されます。

<mcr>

- 最低速度値

  サービスタイプとして UBR+を指定したときの最低速度を指定します。

機種	拡張モジュール	範囲
Si-R570	ATM25M拡張モジュールL2 ATM155M拡張モジュールL2	64k～ 25m:8k刻み、または50k刻み
	ATM25M拡張モジュールH1	64k～ 25m:8k刻み、または50k刻み
	ATM155M拡張モジュールH1	64k～100m:8k刻み、または50k刻み
Si-R370	ATM25M拡張モジュールL2 ATM155M拡張モジュールL2	64k～ 25m:8k刻み、または50k刻み
Si-R260B		64k～ 25m:8k刻み、または50k刻み

kとmは単位を表し、kはKbpsをmはMbpsを示します。
0を指定、または省略時は、装置内部で自動設定されます。

<gr>

- 保証速度値

  サービスタイプとして GFR+を指定したときの保証速度を指定します。

機種	拡張モジュール	範囲
Si-R570	ATM25M拡張モジュールL2 ATM155M拡張モジュールL2	64k～ 25m:8k刻み、または50k刻み
	ATM25M拡張モジュールH1	64k～ 25m:8k刻み、または50k刻み
	ATM155M拡張モジュールH1	64k～100m:8k刻み、または50k刻み
Si-R370	ATM25M拡張モジュールL2 ATM155M拡張モジュールL2	64k～ 25m:8k刻み、または50k刻み
Si-R260B		64k～ 25m:8k刻み、または50k刻み

kとmは単位を表し、kはKbpsをmはMbpsを示します。
0を指定、または省略時は、装置内部でVC速度の1/10が自動設定されます。
ただし、VC速度の1/10が64Kbps未満になる場合は、64Kbpsに設定されます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

VCC(Virtual Channel Connection) のサービスタイプ (ATM Service Type) を設定します。
<scr> <mcr> <gr> は VC 速度 を超えないように指定します。

[未設定時]

cbr が設定されたものとみなされます。

```
remote <number> ap <ap_number> atm ast cbr
```

7.2.36 remote ap atm oam

[機能]

VCC の OAM(F5) による制御の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B

[入力形式]

remote [<number>] ap [<ap_number>] atm oam <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- on
  以下の OAM(F5) の受信を受け付けます。
  - OAM(F5)-AIS
  - OAM(F5)-RDI
  - OAM(F5)-LPB
- off
  OAM(F5) の受信を受け付けません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

VCC(Virtual Channel Connection) で OAM(F5) の受信を受け付けるかどうかを設定します。
OAM(F5) の受信を受け付ける場合、OAM(F5) の故障通知による VCC の故障検出が可能です。

[未設定時]

OAM(F5) の受信を受け付けないとみなされます。

```
remote <number> ap <ap_number> atm oam off
```

7.2.37　remote ap atm vcwatch

[機能]

ATM 到達性監視の設定

[適用機種]

Si-R 570

[入力形式]

remote [<number>] ap [<ap_number>] atm vcwatch <interval> [<retry>]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<interval>

- 監視間隔
  到達性監視間隔を 3～10 の 10 進数で指定します。単位は秒です。
  0 を指定した場合は設定が削除され、監視は行われません。

<retry>

- 再確認回数
  到達性確認に対する応答がなかった場合の再確認回数を 1～20 の 10 進数値で指定します。
  省略時は、5 を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ATM レイヤ (レイヤ 2) の到達性確認を行うための動作情報を設定します。
監視間隔ごとに ATM の OAM(F5) を利用して到達性確認を行います。
到達性確認に対して応答がなければ監視間隔後に再確認します。
再確認回数連続して応答がない場合は、システムログに記録するとともに SNMP にて異常を通知します。
応答がない間も監視を行い、接続性が再確認できた場合にも、システムログに記録するとともに SNMP にて状態変更を通知します。

[注意]

ATM 到達性監視の設定は、ATM25M 拡張モジュール H1、または ATM155M 拡張モジュール H1 に対してだけ有効です。
到達性確認に対して接続先までの中継装置が応答を返すことがあり、接続先までの到達性が確認できない場合があります。

接続先までの到達性を確認したい場合は、レイヤ 3 での到達性を確認する remote ap sessionwatch コマンドを利用することができます。
本機能使用時には、OAM(F5) の受信を受け付けない設定であっても、OAM(F5) の到達性確認に対する応答は行います。
到達性確認の送信には時間がかかり、50 の VCC に対して 1 秒が必要です。ATM 到達性監視を行う VCC が 150 を超える場合は、50 の VCC あたり 1 秒以上になるように監視間隔を設定してください。監視間隔が短い場合は、誤って到達性がないと認識してしまう場合があります。

[未設定時]

ATM 到達性監視をしないものとみなされます。

```
remote <number> ap <ap_number> atm vcwatch 0
```

7.2.38　remote ap ipsec type

[機能]

IPsec 情報のタイプの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ipsec type <type>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<type>

IPsec 情報のタイプを設定します。

- off
  IPsec を使用しません。
- manual
  IPsec を手動鍵設定で使用します。
- ike
  IPsec 自動鍵交換を使用します。
- dvpn
  動的 VPN で IPsec を使用する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPsec を使用するかどうかを設定します。

- IPsec 情報のタイプに manual を指定する場合、以下の設定も行ってください。
  手動鍵設定を行う場合に、自動鍵設定 (交換) および動的 VPN で使用する定義を行っても使用されません。
  - remote ap ipsec send
  - remote ap ipsec receive
- IPsec 情報のタイプに ike を指定する場合、以下の設定も行ってください。
  自動鍵設定 (交換) を行う場合に、手動鍵設定および動的 VPN で使用する定義を行っても使用されません。

- remote ap ipsec ike
- remote ap ike

- IPsec 情報のタイプに dvpn を指定する場合、以下の設定も行ってください。
  動的 VPN を行う場合に、手動鍵設定で使用する定義を行っても使用されません。
  - remote ap dvpn
  - remote ap ipsec ike
  - remote ap ike
  - dvpn client

IPsec 区間について

IPsec 区間は、tunnel 利用時の自側の tunnel endpoint アドレスと tunnel 利用時の相手側の tunnel endpoint アドレスの定義で指定します。

手動鍵設定の場合、自側の tunnel endpoint アドレスと相手側の tunnel endpoint アドレスの双方を指定してください。

自動鍵設定 (交換) の場合、事前に tunnel endpoint アドレスが決定している時は指定してください。

動的 VPN の場合、自側の tunnel endpoint アドレスのみ指定してください。

相手側の tunnel endpoint アドレスは、動的 VPN 情報交換で相手から通知されたアドレスを使用します。

tunnel endpoint アドレスの設定例

双方の IP アドレスが固定で決まっている場合:

- remote 0 ap 0 tunnel local 192.168.1.1
- remote 0 ap 0 tunnel remote 172.168.1.1

相手側の tunnel endpoint アドレスが不定または動的 VPN である場合:

- remote 0 ap 0 tunnel local 192.168.1.1

自側の tunnel endpoint アドレスが不定である場合:

- remote 0 ap 0 tunnel remote 172.168.1.1

IPsec 対象パケットについて

<number>で設定された相手情報に range 指定があればその範囲の IP パケットが IPsec 対象となります。
range 指定がなければ<number>で設定された相手情報を使用する IP パケットすべてが IPsec 対象となります。
IPsec 情報のタイプに dvpn を指定した場合は、動的 VPN で接続する自側ネットワークの設定で指定したネットワークアドレスのファミリにより自動的に決定します。

[未設定時]

IPsec を使用しないものとみなされます。

```
remote <number> ap <ap_number> ipsec type off
```

7.2.39　remote ap ipsec send spi

[機能]

手動鍵送信用 IPsec 情報のセキュリティパラメタインデックスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ipsec send spi <spi>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<spi>

- セキュリティパラメタインデックス
  手動鍵送信用 IPsec SA のセキュリティパラメタインデックスを、100～ffffffff の範囲の 16 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

手動鍵送信用 IPsec SA を認識する、セキュリティパラメタインデックスの設定を行います。

[注意]

手動鍵送信用 IPsec 情報の SPI 値は同一相手側 tunnel endpoint アドレスで同一の値を指定しないでください。同一の SPI 値を指定した場合、通信できなくなることがあります。

[未設定時]

手動鍵送信用 IPsec 情報の SPI 設定は設定されません。

7.2.40 remote ap ipsec send protocol

[機能]

手動鍵送信用 IPsec 情報のセキュリティプロトコルの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ipsec send protocol <protocol>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<protocol>

手動鍵送信用 IPsec SA のセキュリティプロトコルを指定します。

- none
  セキュリティプロトコル未指定
- esp
  暗号
- ah
  認証

[動作モード]

構成定義モード (管理者クラス)

[説明]

手動鍵送信用 IPsec SA の、セキュリティプロトコルの設定を行います。
認証/暗号アルゴリズム定義、セキュリティプロトコル定義と IPsec SA の関係

auth(認証)	encrypt(暗号)	セキュリティプロトコル	IPsec SA
―	―	esp(暗号)	×
―	―	ah(認証)	×
―	―	―	×
○	―	esp(暗号)	×
○	―	ah(認証)	◎
○	―	―	×
―	○	esp(暗号)	◎
―	○	ah(認証)	×
―	○	―	×
○	○	esp(暗号)	◎ESPinAuth(認証付暗号)
○	○	ah(認証)	◎
○	○	―	×

○:定義あり ―:定義なし ◎:SA作成可 ×:SA作成不可

[未設定時]

手動鍵送信用 IPsec 情報のセキュリティプロトコルは未指定となります。

```
remote <number> ap <ap_number> ipsec send protocol none
```

7.2.41 remote ap ipsec send range

[機能]

手動鍵送信用 IPsec 情報の対象範囲の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ipsec send range <src_addr>/<mask> <dst_addr>/<mask>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<src_addr>/<mask>

IPsec 対象となる送信元 IP アドレス、マスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  IPsec 対象となる送信元 IP アドレスとマスクビット数の組み合わせを指定します。
- any4
  すべての IPv4 アドレスを IPsec 対象に含めます。
  0.0.0.0/0(0.0.0.0/0.0.0.0) と同意。

<dst_addr>/<mask>

IPsec 対象となるあて先 IP アドレス、マスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  IPsec 対象となるあて先 IP アドレスとマスクビット数の組み合わせを指定します。
- any4
  すべての IPv4 アドレスを IPsec 対象に含めます。
  0.0.0.0/0(0.0.0.0/0.0.0.0) と同意。

[動作モード]

構成定義モード (管理者クラス)

[説明]

パケット送信時に IPsec を適用するセッションの範囲を設定します。(Security Policy Database の情報)

[未設定時]

<src_addr>,<dst_addr>共に any4 が設定されたものとして扱います。

```
remote <number> ap <ap_number> ipsec send range any4 any4
```

7.2.42 remote ap ipsec send encrypt

[機能]

手動鍵送信用 IPsec 情報の暗号情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ipsec send encrypt <enc_algo> [<kind> <enc_key> [encrypted]]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<enc_algo>

暗号アルゴリズムを指定します。

- des-cbc
- 3des-cbc
- aes-cbc-128
- aes-cbc-192
- aes-cbc-256
- null
- none

<kind>

鍵種別を指定します。

- hex
  16 進数鍵を使用します。
- text
  文字列鍵を使用します。

<enc_key>

暗号鍵を指定します。

- 暗号化されていない暗号鍵
  <enc_algo>で指定した暗号アルゴリズムが使用する鍵長未満の鍵を指定した場合は、16 進数鍵では鍵長になるまで 0x0 でパディングされます。
  文字列鍵の場合は、0x22(ダブルクォーテーション) を除く [0x20-0x7e] の範囲のコードで構成される ASCII 文字列で指定します。ただし、文字列鍵で 0x20(空白文字) を使用する場合は、文字列鍵を""で囲う必要があります。
  以下に、入力範囲を示します。

鍵種別 暗号アルゴリズム	hex 16進数鍵	text 文字列鍵
des-cbc	1〜16桁	8文字
3des-cbc	1〜48桁	24文字
aes-cbc-128	1〜32桁	16文字
aes-cbc-192	1〜48桁	24文字
aes-cbc-256	1〜64桁	32文字

- 暗号化された暗号鍵

  暗号化された暗号鍵を指定します。

  show コマンドで表示される暗号化された暗号鍵を encrypted と共に指定します。

  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化暗号鍵指定

  <enc_key>に暗号化された暗号鍵を指定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

送信パケットを暗号化するための、暗号アルゴリズムと鍵の設定を行います。
show コマンドでは、暗号化された暗号鍵が encrypted と共に表示されます。
暗号アルゴリズムの"aes-cbc"に続く数字は鍵長を表しています。
数字が大きいほど強固な鍵になりますが、その分処理時間を要します。

- 手動鍵設定としての暗号アルゴリズム

  暗号アルゴリズムが"null"および"none"の場合、暗号鍵は入力できません。

[注意]

- weak key

  手動鍵設定で指定する暗号鍵に、RFC2409 の Appendix A に記載されている weak key を設定した場合、コマンドエラーとなります。

  RFC2409 の Appendix A に記載されている weak key(DES, 3DES だけ)

```
0101010101010101, FEFEFEFEFEFEFEFE, 1F1F1F1FE0E0E0E0, E0E0E0E01F1F1F1F,
01FE01FE01FE01FE, FE01FE01FE01FE01, 1FE01FE00EF10EF1, E01FE01FF10EF10E,
01E001E001F101F1, E001E001F101F101, 1FFE1FFE0EFE0EFE, FE1FFE1FFE0EFE0E,
011F011F010E010E, 1F011F010E010E01, E0FEE0FEF1FEF1FE, FEE0FEE0FEF1FEF1
```

  3des-cbc の場合は、暗号鍵を 16 桁ごとに 3 つの鍵に分割し、どれかの鍵が weak key となるような指定はできません。

[未設定時]

IPsec によるパケット暗号は行われません。

```
remote <number> ap <ap_number> ipsec send encrypt none
```

7.2.43 remote ap ipsec send auth

[機能]

手動鍵送信用 IPsec 情報の認証情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ipsec send auth <auth_algo> [<kind> <auth_key> [encrypted]]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<auth_algo>

認証アルゴリズムを指定します。

- hmac-md5
- hmac-sha1
- none

<kind>

鍵種別を指定します。

- hex
  16 進数鍵を使用します。
- text
  文字列鍵を使用します。

<auth_key>

認証鍵を指定します。

- 暗号化されていない認証鍵
  <auth_algo>で指定した認証アルゴリズムが使用する鍵長未満の鍵を指定した場合は、16 進数鍵では鍵長になるまで 0x0 でパディングされます。
  文字列鍵の場合は、0x22(ダブルクォーテーション) を除く [0x20-0x7e] の範囲のコードで構成される ASCII 文字列で指定します。ただし、文字列鍵で 0x20(空白文字) を使用する場合は、文字列鍵を""で囲う必要があります。
  以下に、入力範囲を示します。

鍵種別 認証アルゴリズム	hex 16進数鍵	text 文字列鍵
hmac-md5 hmac-sha1	1〜32桁 1〜40桁	16文字 20文字

- 暗号化された認証鍵を指定します。
  show コマンドで表示される暗号化された認証鍵を encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化認証鍵指定
  <auth_key>に暗号化された認証鍵を指定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

送信パケットを認証するための、認証アルゴリズムと鍵の設定を行います。
show コマンドでは、暗号化された認証鍵が encrypted と共に表示されます。

- 手動鍵設定としての認証アルゴリズム
  認証アルゴリズムが"none"の場合、認証鍵は入力できません。

[未設定時]

IPsec によるパケット認証は行われません。

```
remote <number> ap <ap_number> ipsec send auth none
```

7.2.44 remote ap ipsec receive spi

[機能]

手動鍵受信用 IPsec 情報のセキュリティパラメタインデックスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ipsec receive spi <spi>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<spi>

- セキュリティパラメタインデックス
  受信用 IPsec SA のセキュリティパラメタインデックスを、100～ffffffff の範囲の 16 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

手動鍵受信用 IPsec SA を認識する、セキュリティパラメタインデックスの設定を行います。

[注意]

手動鍵受信用 IPsec 情報の SPI 値は装置内で同一の値を指定しないでください。
同一の SPI 値を指定した場合、通信できなくなることがあります。

[未設定時]

手動鍵受信用 IPsec 情報の SPI 設定は設定されません。

7.2.45　remote ap ipsec receive protocol

[機能]

手動鍵受信用 IPsec 情報のセキュリティプロトコルの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ipsec receive protocol <protocol>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<protocol>

手動鍵受信用 IPsec SA のセキュリティプロトコルを指定します。

- none
  セキュリティプロトコル未指定
- esp
  暗号
- ah
  認証

[動作モード]

構成定義モード (管理者クラス)

[説明]

手動鍵受信用 IPsec SA の、セキュリティプロトコルの設定を行います。

[未設定時]

手動鍵受信用 IPsec 情報のセキュリティプロトコルは未指定となります。

```
remote <number> ap <ap_number> ipsec send protocol none
```

7.2.46 remote ap ipsec receive range

[機能]

手動鍵受信用 IPsec 情報の対象範囲の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ipsec receive range <dst_addr>/<mask> <src_addr>/<mask>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<dst_addr>/<mask>

IPsec 対象となる相手側 IP アドレス、マスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  IPsec 対象となる相手側 IP アドレスとマスクビット数の組み合わせを指定します。
- any4
  すべての IPv4 アドレスを IPsec 対象に含めます。
  0.0.0.0/0(0.0.0.0/0.0.0.0) と同意。

<src_addr>/<mask>

IPsec 対象となる自側 IP アドレス、マスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  IPsec 対象となる自側 IP アドレスとマスクビット数の組み合わせを指定します。
- any4
  すべての IPv4 アドレスを IPsec 対象に含めます。
  0.0.0.0/0(0.0.0.0/0.0.0.0) と同意。

[動作モード]

構成定義モード (管理者クラス)

[説明]

パケット受信時に IPsec を適用するセッションの範囲を設定します。(Security Policy Database の情報)

[未設定時]

<dst_addr>,<src_addr>共に any4 が設定されたものとして扱います。

```
remote <number> ap <ap_number> ipsec receive range any4 any4
```

7.2.47 remote ap ipsec receive encrypt

[機能]

手動鍵受信用 IPsec 情報の暗号情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ipsec receive encrypt <enc_algo> [<kind> <enc_key> [encrypted]]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<enc_algo>

暗号アルゴリズムを指定します。

- des-cbc
- 3des-cbc
- aes-cbc-128
- aes-cbc-192
- aes-cbc-256
- null
- none

<kind>

鍵種別を指定します。

- hex
  16 進数鍵を使用します。
- text
  文字列鍵を使用します。

<enc_key>

暗号鍵を指定します。

- 暗号化されていない暗号鍵
  <enc_algo>で指定した暗号アルゴリズムが使用する鍵長未満の鍵を指定した場合は、16 進数鍵では鍵長になるまで 0x0 でパディングされます。
  文字列鍵の場合は、0x22(ダブルクォーテーション) を除く [0x20-0x7e] の範囲のコードで構成される ASCII 文字列で指定します。ただし、文字列鍵で 0x20(空白文字) を使用する場合は、文字列鍵を""で囲う必要があります。
  以下に、入力範囲を示します。

鍵種別 暗号アルゴリズム	hex 16進数鍵	text 文字列鍵
des-cbc	1〜16桁	8文字
3des-cbc	1〜48桁	24文字
aes-cbc-128	1〜32桁	16文字
aes-cbc-192	1〜48桁	24文字
aes-cbc-256	1〜64桁	32文字

- 暗号化された暗号鍵

  暗号化された暗号鍵を指定します。

  show コマンドで表示される暗号化された暗号鍵を encrypted と共に指定します。

  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化暗号鍵指定

  <enc_key>に暗号化された暗号鍵を指定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

受信パケットを暗号化するための、暗号アルゴリズムと鍵の設定を行います。
show コマンドでは、暗号化された暗号鍵が encrypted と共に表示されます。
暗号アルゴリズムの"aes-cbc"に続く数字は鍵長を表しています。
数字が大きいほど強固な鍵になりますが、その分処理時間を要します。

- 手動鍵設定としての暗号アルゴリズム

  暗号アルゴリズムが"null"および"none"の場合、暗号鍵は入力できません。

[注意]

- weak key

  手動鍵設定で指定する暗号鍵に、RFC2409 の Appendix A に記載されている weak key を設定した場合、コマンドエラーとなります。

  RFC2409 の Appendix A に記載されている weak key(DES, 3DES だけ)

```
0101010101010101, FEFEFEFEFEFEFEFE, 1F1F1F1FE0E0E0E0, E0E0E0E01F1F1F1F,
01FE01FE01FE01FE, FE01FE01FE01FE01, 1FE01FE00EF10EF1, E01FE01FF10EF10E,
01E001E001F101F1, E001E001F101F101, 1FFE1FFE0EFE0EFE, FE1FFE1FFE0EFE0E,
011F011F010E010E, 1F011F010E010E01, E0FEE0FEF1FEF1FE, FEE0FEE0FEF1FEF1
```

  3des-cbc の場合は、暗号鍵を 16 桁ごとに 3 つの鍵に分割し、どれかの鍵が weak key となるような指定はできません。

[未設定時]

IPsec によるパケット暗号は行われません。

```
remote <number> ap <ap_number> ipsec receive encrypt none
```

7.2.48 remote ap ipsec receive auth

[機能]

手動鍵受信用 IPsec 情報の認証情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ipsec receive auth <auth_algo> [<kind> <auth_key> [encrypted]]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<auth_algo>

認証アルゴリズムを指定します。

- hmac-md5
- hmac-sha1
- none

<kind>

鍵種別を指定します。

- hex
  16 進数鍵を使用します。
- text
  文字列鍵を使用します。

<auth_key>

認証鍵を指定します。

- 暗号化されていない認証鍵
  <auth_algo>で指定した認証アルゴリズムが使用する鍵長未満の鍵を指定した場合は、16 進数鍵では鍵長になるまで 0x0 でパディングされます。
  文字列鍵の場合は、0x22(ダブルクォーテーション) を除く [0x20-0x7e] の範囲のコードで構成される ASCII 文字列で指定します。ただし、文字列鍵で 0x20(空白文字) を使用する場合は、文字列鍵を""で囲う必要があります。以下に、入力範囲を示します。

鍵種別 認証アルゴリズム	hex 16進数鍵	text 文字列鍵
hmac-md5	1〜32桁	16文字
hmac-sha1	1〜40桁	20文字

- 暗号化された認証鍵を指定します。
  show コマンドで表示される暗号化された認証鍵を encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化認証鍵指定
  <auth_key>に暗号化された認証鍵を指定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

送信パケットを認証するための、認証アルゴリズムと鍵の設定を行います。
show コマンドでは、暗号化された認証鍵が encrypted と共に表示されます。

- 手動鍵設定としての認証アルゴリズム

認証アルゴリズムが"none"の場合、認証鍵は入力できません。

[未設定時]

IPsec によるパケット認証は行われません。

```
remote <number> ap <ap_number> ipsec receive auth none
```

7.2.49 remote ap ipsec ike protocol

[機能]

自動鍵交換用 IPsec 情報のセキュリティプロトコルの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike protocol <protocol>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<protocol>

自動鍵交換用 IPsec SA のセキュリティプロトコルを指定します。

- none
  セキュリティプロトコル未指定
- esp
  暗号
- ah
  認証

[動作モード]

構成定義モード (管理者クラス)

[説明]

自動鍵交換用 IPsec SA の、セキュリティプロトコルの設定を行います。

[未設定時]

自動鍵交換用 IPsec 情報のセキュリティプロトコルは未指定となります。

```
remote <number> ap <ap_number> ipsec ike protocol none
```

7.2.50　remote ap ipsec ike encrypt

[機能]

自動鍵交換用 IPsec 情報の暗号情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike encrypt <enc_algo>[,<enc_algo>...]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<enc_algo>

暗号アルゴリズムを指定します。
複数のアルゴリズムを指定することができます。複数定義する時は、アルゴリズムを空白なしでカンマ’,’ で区切ります。

- des-cbc
- 3des-cbc
- aes-cbc-128
- aes-cbc-192
- aes-cbc-256
- null
- none

[動作モード]

構成定義モード (管理者クラス)

[説明]

送受信パケットを暗号化/復号化するための、暗号アルゴリズムの設定を行います。
暗号アルゴリズムを複数指定する場合、指定順序にかかわらず以下の優先順位となります。
暗号アルゴリズムの"aes-cbc"に続く数字は鍵長を表しています。
数字が大きいほど強固な鍵になりますが、その分処理時間を要します。

- aes-cbc-256
- aes-cbc-192
- aes-cbc-128
- 3des-cbc
- des-cbc
- null

[未設定時]

IPsec によるパケット暗号は行われません。

```
remote <number> ap <ap_number> ipsec ike encrypt none
```

7.2.51　remote ap ipsec ike auth

[機能]

自動鍵交換用 IPsec 情報の認証情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike auth <auth_algo>[,<auth_algo>...]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<auth_algo>

認証アルゴリズムを指定します。
複数のアルゴリズムを指定することができます。複数定義する時は、アルゴリズムを空白なしでカンマ’,’ で区切ります。

- hmac-md5
- hmac-sha1
- none

[動作モード]

構成定義モード (管理者クラス)

[説明]

送受信パケットを認証するための、認証アルゴリズムの設定を行います。
認証アルゴリズムを複数指定する場合、指定順序にかかわらず以下の優先順位となります。

- hmac-md5
- hmac-sha1

[未設定時]

IPsec によるパケット認証は行われません。

```
remote <number> ap <ap_number> ipsec ike auth none
```

7.2.52 remote ap ipsec ike pfs

[機能]

自動鍵交換用 IPsec 情報の PFS 使用時の DH(Diffie-Hellman) グループの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike pfs <pfs_group>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<pfs_group>

Diffie-Hellman グループについて指定します。

- modp768
  Diffie-Hellman グループの MODP768(グループ 1)
- modp1024
  Diffie-Hellman グループの MODP1024(グループ 2)
- modp1536
  Diffie-Hellman グループの MODP1536(グループ 5)
- off
  Diffie-Hellman グループを使用しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPsec セッションの鍵素材を保護する、PFS 使用時の DH(Diffie-Hellman) グループの設定を行います。

[未設定時]

PFS による鍵交換データ保護は行いません。セキュア通信を行いたい場合は適切な PFS 使用時の DH グループを設定してください。

```
remote <number> ap <ap_number> ipsec ike pfs off
```

7.2.53　remote ap ipsec ike lifetime

[機能]

自動鍵交換用 IPsec 情報の SA 有効時間の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike lifetime <lifetime>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<lifetime>

- SA 有効時間
  SA 有効時間を、600 秒 (10 分)～86400 秒 (1 日) の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPsec セッションの通信データを保護する、IPsec SA の SA 有効時間 (秒) の設定を行います。

[未設定時]

IPsec SA の有効時間として 8h(8 時間) が設定されたものとして扱います。

```
remote <number> ap <ap_number> ipsec ike lifetime 8h
```

7.2.54 remote ap ipsec ike lifebyte

[機能]

自動鍵交換用 IPsec 情報の SA 有効パケット量の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike lifebyte <lifebyte>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<lifebyte>

- SA 有効パケット量
  IPsec 用 Security Association(SA) 有効パケット量のバイト数を、0 または 2400k〜108000m の範囲で指定します。
  単位は以下の 3 種類です。1k は 1024 バイトで計算されます。

  k: キロバイト (例: 2400k → 2400k)

  m: メガバイト (例: 4m → 4096k)

  g: ギガバイト (例: 1g → 1048576k)

  0 を指定した場合は、lifebyte による IPsec SA の更新を行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPsec セッションの通信データを保護する、IPsec SA の SA 有効パケット量 (キロバイト) の設定を行います。

[未設定時]

SA 有効パケット量に 0 バイトを指定したものとみなされます。

```
remote <number> ap <ap_number> ipsec ike lifebyte 0
```

7.2.55　remote ap ipsec ike newsa initiator

[機能]

自動鍵交換用 IPsec 情報の New SA Initiator(更新時間/更新データ量) の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike newsa initiator <time> [<byte>]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<time>

- Initiator SA 更新時間
  Initiator SA 更新時間を、30 秒～180 秒 (3 分) の範囲で指定します。
  単位は、m(分)、s(秒) のどれかを指定します。

<byte>

- Initiator SA 更新データ量
  Initiator SA 更新データ量を、0 または 120kbyte～230400kbyte の範囲で指定します。
  単位は、k(キロバイト)、m(メガバイト) のどれかを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

自側が Initiator の場合に、IPsec SA の有効時間または SA 有効データ量が満了になる前に、IPsec SA の更新を行うための時間／データ量の設定を行います。
相手側の New SA Responder と同じ時間／データ量にならないように設定してください。
また、SA 有効データ量の設定を行い、更新データ量設定が 0 指定時には有効データ量満了した時点で SA 更新が行われます。

[未設定時]

Initiator SA 更新時間として 90s(90 秒)、データ量として 0k(0kbyte) が設定されたものとして扱います。

```
remote <number> ap <ap_number> ipsec ike newsa initiator 90s 0
```

7.2.56 remote ap ipsec ike newsa responder

[機能]

自動鍵交換用 IPsec 情報の New SA Responder(更新時間/更新データ量) の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike newsa responder <time> [<byte>]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<time>

- Responder SA 更新時間
  Responder SA 更新時間を、30 秒～180 秒 (3 分) の範囲で指定します。
  単位は、m(分)、s(秒) のどれかを指定します。
- off
  Responder 側からの SA 更新は行いません。

<byte>

- Responder SA 更新データ量
  Responder SA 更新データ量を、0 または 120kbyte～230400kbyte の範囲で指定します。
  単位は、k(キロバイト)、m(メガバイト) のどれかを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

自側が Responder の場合に、IPsec SA の有効時間または SA 有効データ量が満了になる前に、IPsec SA の更新を行うための時間／データ量の設定を行います。
相手側の New SA Initiator と同じ時間／データ量にならないように設定してください。
また、SA 有効データ量の設定を行い、更新データ量設定が 0 指定時には有効データ量満了した時点で SA 更新が行われます。更新時間設定が off 指定時には Responder 側からの SA 更新は行いません。

[未設定時]

Responder SA 更新時間として 30s(30 秒)、データ量として 0k(0kbyte) が設定されたものとして扱います。

```
remote <number> ap <ap_number> ipsec ike newsa responder 30s 0
```

7.2.57 remote ap ipsec ike range

[機能]

自動鍵交換用 IPsec 情報の対象範囲の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike range <src_addr>/<mask> <dst_addr>/<mask>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<src_addr>/<mask>

IPsec 対象となる送信元 IP アドレス、マスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  IPsec 対象となる送信元 IP アドレスとマスクビット数の組み合わせを指定します。
- any4
  すべての IPv4 アドレスを IPsec 対象に含めます。
  0.0.0.0/0(0.0.0.0/0.0.0.0) と同意。
- any6
  すべての IPv6 アドレスを IPsec 対象に含めます。
  ::/0 と同意。

<dst_addr>/<mask>

IPsec 対象となるあて先 IP アドレス、マスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  IPsec 対象となるあて先 IP アドレスとマスクビット数の組み合わせを指定します。
- any4
  すべての IPv4 アドレスを IPsec 対象に含めます。
  0.0.0.0/0(0.0.0.0/0.0.0.0) と同意。
- any6
  すべての IPv6 アドレスを IPsec 対象に含めます。
  ::/0 と同意。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPsec を適用するセッションの範囲を設定します。(Security Policy Database の情報)

[未設定時]

<src_addr>,<dst_addr>共に any4 が設定されたものとして扱います。

```
remote <number> ap <ap_number> ipsec ike range any4 any4
```

7.2.58 remote ap ipsec extension-range

[機能]

拡張 IPsec 対象範囲の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ipsec extension-range <count> <src_addr>/<mask> <dst_addr>/<mask>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 拡張 IPsec 対象範囲定義番号
  拡張 IPsec 対象範囲の通し番号を、10 進数値で指定します。
  指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つ拡張 IPsec 対象範囲定義がすでに存在する場合は、既存の定義を変更します。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B Si-R240 Si-R220B
0〜49	Si-R180

<src_addr>/<mask>

IPsec 対象となる送信元 IP アドレス、マスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  IPsec 対象となる送信元 IP アドレスとマスクビット数の組み合わせを指定します。
- any4
  すべての IPv4 アドレスを IPsec 対象に含めます。
  0.0.0.0/0(0.0.0.0/0.0.0.0) と同意。
- any6
  すべての IPv6 アドレスを IPsec 対象に含めます。
  ::/0 と同意。

<dst_addr>/<mask>

IPsec 対象となるあて先 IP アドレス、マスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  IPsec 対象となるあて先 IP アドレスとマスクビット数の組み合わせを指定します。
- any4
  すべての IPv4 アドレスを IPsec 対象に含めます。
  0.0.0.0/0(0.0.0.0/0.0.0.0) と同意。
- any6
  すべての IPv6 アドレスを IPsec 対象に含めます。
  ::/0 と同意。

[動作モード]

構成定義モード (管理者クラス)

[説明]

拡張 IPsec 対象範囲を設定します。
拡張 IPsec 対象範囲定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
1000	Si-R570
500	Si-R370
100	Si-R260B　Si-R240　Si-R220B
50	Si-R180

[注意]

拡張 IPsec 対象範囲設定を行わない場合でも「IPsec 情報の対象範囲の設定」を設定することにより IPsec 通信は可能です。「IPsec 情報の対象範囲の設定」以外の IPsec 対象範囲を指定してください。
拡張 IPsec 対象範囲設定は、IKE ネゴシエーション開始契機になりますが、IKE ネゴシエーション情報としては使用しません。IKE ネゴシエーション情報としての IPsec 対象範囲は「自動鍵交換用 IPsec 情報の対象範囲の設定」をご利用ください。
IPsec の相手となる装置が復号化後に IPsec 対象範囲をチェックする場合は、IPsec 通信が遮断される場合があります。
拡張 IPsec 対象範囲を使用して双方向通信を行う場合は、相手装置側にも同様の設定が必要です。相手装置側に、自側装置と同様の設定が存在しない場合は、片側通信のみ暗号化し折り返しの通信は暗号化されない場合があります。

[未設定時]

拡張 IPsec 対象範囲を設定しないものとみなされます。

7.2.59 remote ap ike port

[機能]

IKE 情報の相手側 IKE ポート番号の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ike port <port>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<port>

- 相手側 IKE ポート番号
  相手側 IKE ポート番号を指定します。(デフォルト: 500 番)

[動作モード]

構成定義モード (管理者クラス)

[説明]

SA 確立のネゴシエーションを行う、相手 IKE サーバのポート番号の設定を行います。

[未設定時]

相手側 IKE ポート番号に標準ポート番号である 500 を指定したものとみなされます。

```
remote <number> ap <ap_number> ike port 500
```

7.2.60　remote ap ike shared key

[機能]

IKE セッション確立時の共有鍵 (Pre-shared key) の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ike shared key <kind> <shared_key> [encrypted]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<kind>

鍵種別を指定します。

- hex
  16 進数鍵を使用します。
- text
  文字列鍵を使用します。
- dynamic
  動的 VPN 機能により配布された共有鍵を使用する場合に指定します。

<shared_key>

共有鍵 (事前共有秘密鍵方式) を指定します。

- 暗号化されていない共有鍵を指定します。
  文字列鍵の場合は、0x22(ダブルクォーテーション) を除く [0x20-0x7e] の範囲のコードで構成される ASCII 文字列で指定します。ただし、文字列鍵で 0x20(空白文字) を使用する場合は、文字列鍵をダブルクォーテーション (") で囲う必要があります。
  以下に、入力範囲を示します。

鍵種別	16進数鍵	文字列鍵
共有鍵	1～256桁	1～128文字

- 暗号化された共有鍵を指定します。
  show コマンドで表示される暗号化された共有鍵を encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化共有鍵指定
  <shared_key>に暗号化された共有鍵を指定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

SA 確立のネゴシエーションのときに接続相手を認証するための、共有鍵の設定を行います。
show コマンドでは、暗号化された共有鍵が encrypted と共に表示されます。
動的 VPN 接続を行う場合に限り、<kind>に dynamic を指定することができます。
dynamic を指定した場合は、共有鍵の指定はできません。

[注意]

dynamic は、IPsec 情報のタイプの設定で dvpn を指定したときだけ有効となります。

[未設定時]

共有鍵が設定されません。IKE により鍵交換を行う場合は必ず設定してください。
動的 VPN 機能を利用して IKE により鍵交換を行う場合は必ず設定してください。

7.2.61　remote ap ike proposal move

[機能]

IKE セッション用 Proposal 定義優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ike proposal move <proposal_number> <new_number>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<proposal_number>

- 移動元の Proposal 定義優先順序を指定します。

<new_number>

- 移動先の Proposal 定義優先順序を指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

<ap_number>で指定した接続先情報の IKE セッション用の Proposal 定義優先順序を変更します。
IKE セッション用 Proposal 定義とネゴシエーションの関係

	ネゴシエーション情報	Proposal	Proposal	...
a	暗号情報	3des-cbc	des-cbc	...
b	認証(ハッシュ)情報	hmac-md5	0	...
c	DHグループ	modp768	modp1024	...
d	SA有効時間	600s	0	...

※ a を複数指定 (<proposal_number>0,1,2 を定義) した場合、ほかの情報は定義しなければ各情報のデフォルト値を採用します。
IKE セッションのネゴシエーションは、Proposal 単位 (a～d を一組) として行います。その中で a～c は相手装置の定義と一致することが条件となります。
自側が Responder の場合は、相手の Proposal が許容できるかを判断するため、自装置の定義は参照されません。

本装置を Aggressive Mode で動作させる時に、IKE セッション用 Proposal 定義を複数設定する場合、DH グループ設定はすべて同じ値を設定してください。
これは、Aggressive Mode が Diffie-Hellman のグループについてネゴシエーションができないためです。
(Initiator が最初の ISAKMP パケットに載せる鍵素材の計算に使用するため、Diffie-Hellman のグループは同じである必要があります)
Aggressive Mode は、相手 (リモート) 情報 tunnel 利用時の自側の tunnel endpoint address を未設定にし、IKE 情報の自装置識別情報を設定します。

7.2.62　remote ap ike proposal encrypt

[機能]

IKE セッション用暗号情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ike proposal [<proposal_number>] encrypt <enc_algo>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<proposal_number>

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。
  省略時は、0 を指定したものとみなされます。

<enc_algo>

暗号アルゴリズムを指定します。

- des-cbc
- 3des-cbc
- aes-cbc-128
- aes-cbc-192
- aes-cbc-256

[動作モード]

構成定義モード (管理者クラス)

[説明]

IKE セッションの送受信パケットを暗号化/復号化するための、暗号アルゴリズムの設定を行います。
コマンドによる定義を行う場合は、必ず設定してください。
IKE セッション用暗号情報設定が未定義ですと IKE が動作しません。

[未設定時]

IKE セッション用暗号情報が設定されません。IKE により鍵交換を行う場合は必ず設定してください。

7.2.63 remote ap ike proposal hash

[機能]

IKE セッション用認証 (ハッシュ) 情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ike proposal [<proposal_number>] hash <hash_algo>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<proposal_number>

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。
  省略時は、0 を指定したものとみなされます。

<hash_algo>

認証 (ハッシュ) アルゴリズムを指定します。

- hmac-md5
- hmac-sha1

[動作モード]

構成定義モード (管理者クラス)

[説明]

IKE セッションのネゴシエーションパケットを認証するための、ハッシュアルゴリズムの設定を行います。

[未設定時]

認証のためのハッシュアルゴリズムに hmac-md5 を指定したものとみなされます。

```
remote <number> ap <ap_number> ike proposal <count> hash hmac-md5
```

7.2.64　remote ap ike proposal pfs

[機能]

IKE セッション用 DH(Diffie-Hellman) グループの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ike proposal [<proposal_number>] pfs <pfs_group>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<proposal_number>

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。
  省略時は、0 を指定したものとみなされます。

<pfs_group>

Diffie-Hellman グループについて指定します。

- modp768
  MODP768(グループ 1) の Diffie-Hellman グループ
- modp1024
  MODP1024(グループ 2) の Diffie-Hellman グループ
- modp1536
  MODP1536(グループ 5) の Diffie-Hellman グループ

[動作モード]

構成定義モード (管理者クラス)

[説明]

IKE セッションのネゴシエーションパケットを保護するための、DH(Diffie-Hellman) グループの設定を行います。

[未設定時]

DH グループに modp768 を指定したものとみなされます。

```
remote <number> ap <ap_number> ike proposal <count> pfs modp768
```

7.2.65 remote ap ike proposal lifetime

[機能]

IKE 情報の SA 有効時間の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ike proposal [<proposal_number>] lifetime <lifetime>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<proposal_number>

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。
  省略時は、0 を指定したものとみなされます。

<lifetime>

- SA 有効時間
  SA 有効時間を、600 秒 (10 分)〜86400 秒 (1 日) の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IKE セッションのネゴシエーションパケットを保護するための、SA 有効時間 (秒) の設定を行います。

[未設定時]

IKE SA の有効時間として 24h(24 時間) が設定されたものとして扱われます。

```
remote <number> ap <ap_number> ike proposal <count> lifetime 24h
```

7.2.66　remote ap ike retry

[機能]

IKE 情報の初回再送時間および再送回数の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ike retry <time> <count>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<time>

- 初回再送時間
  初回再送時間を、1 秒～60 秒 (1 分) の範囲で指定します。
  単位は、m(分)、s(秒) のどちらかを指定します。

<count>

- 再送回数
  再送回数を、1～10 の範囲で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IKE セッションのネゴシエーションパケットに対する初回再送時間および再送回数の設定を行います。

[未設定時]

初回再送時間に 10 秒、再送回数に 3 回を設定したものとみなされます。

```
remote <number> ap <ap_number> ike retry 10s 3
```

7.2.67 remote ap ike idtype

[機能]

IKE 情報の送信 ID タイプの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ike idtype <id_type>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<id_type>

ネゴシエーションの送信 ID タイプを指定します。

- fqdn
  省略なしドメイン名
- user_fqdn
  省略なしユーザ識別名

[動作モード]

構成定義モード (管理者クラス)

[説明]

IKE セッションを確立する、ネゴシエーションの ID タイプの設定を行います。
IKE セッション確立のネゴシエーションパケットの ID payload に使用されます。

[未設定時]

IKE セッション確立のネゴシエーションパケットの ID タイプとして FQDN が設定されたものとして扱われます。

```
remote <number> ap <ap_number> ike idtype fqdn
```

7.2.68　remote ap ike name local

[機能]

IKE 情報の自装置識別情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ike name local <name>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<name>

- 自装置識別情報
  自装置を識別する名前を指定します。
  指定範囲は、1～64 文字です。
  識別情報は、0x22(ダブルクォーテーション) を除く [0x21-0x7e] の範囲のコードで構成される ASCII 文字列で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IKE セッションを確立する、自装置の IP アドレスが不定の場合に識別情報の設定を行います。
ISAKMP SA のネゴシエーション交換モードについては、remote ap ike mode を参照してください。

[未設定時]

IKE セッション用自装置識別情報が設定されません。Aggressive Mode により鍵交換を行う場合は必ず設定してください。

7.2.69 remote ap ike name remote

[機能]

IKE 情報の相手装置識別情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ike name remote <name>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<name>

- 相手装置識別情報
  相手装置を識別する名前を指定します。
  指定範囲は、1～64 文字です。
  名前は、0x22(ダブルクォーテーション) を除く [0x21-0x7e] の範囲のコードで構成される ASCII 文字列で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IKE セッションを確立する、相手装置の IP アドレスが不定の場合に識別情報の設定を行います。
ISAKMP SA のネゴシエーション交換モードについては、remote ap ike mode を参照してください。

[未設定時]

IKE セッション用相手装置識別情報が設定されません。
装置識別情報により共有鍵認証を行う場合は、必ず設定してください。

7.2.70　remote ap ike release

[機能]

IPsec/IKE 情報の解放動作の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ike release <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

IPsec/IKE の SA 情報の解放動作設定を指定します。

- on
  回線切断時に解放処理を行います。
- off
  解放処理は行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

自動鍵設定で作成された SA 情報の解放動作設定を行います。
on を指定した場合は、回線切断時に自動鍵設定が使用している SA 情報の解放動作を行います。
off を指定した場合は、回線切断時に自動鍵設定が使用している SA 情報の解放動作を行いません。

[注意]

本コマンドは、以下の回線切断動作時に有効です。

- ISDN(回線交換) を使用した時の回線切断時 (※ Si-R260B Si-R240 Si-R180 を除く)
- PPPoE を使用した時の切断時
- モデムを使用した時の切断時 (※ Si-R220B のみ)
- データ通信カードを使用した時の切断時 (※ Si-R240 のみ)

[未設定時]

回線切断時に IKE SA 情報の解放を行うものとみなされます。

```
remote <number> ap <ap_number> ike release on
```

7.2.71　remote ap ike initial

[機能]

IKE ネゴシエーション開始動作の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ike initial <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

IKE ネゴシエーション開始動作を指定します。

- forward
  IPsec 対象パケットの送信を契機として、IPsec/IKE SA の確立動作を開始します。
- connect
  対象回線の接続または IPsec 対象パケットの送信を契機として、IPsec/IKE SA の確立動作を開始します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IKE ネゴシエーションを開始する契機を設定します。
<mode>に connect を指定した場合、回線接続または IPsec 対象パケットの送信を契機として、IKE ネゴシエーションを開始し、IPsec/IKE SA の確立を行います。

[注意]

本コマンドは、以下の回線接続時に有効です。

- ISDN(回線交換) を使用した時 (※ Si-R260B Si-R240 Si-R180 を除く)
- PPPoE を使用した時
- モデムを使用した時 (※ Si-R220B のみ)
- データ通信カードを使用した時 (※ Si-R240 のみ)

[未設定時]

IPsec 対象パケットの送信を契機として、IPsec/IKE SA の確立を行うものとみなされます。

```
remote <number> ap <ap_number> ike initial forward
```

7.2.72　remote ap ike sessionwatch

[機能]

IKE セッション監視の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ike sessionwatch <address> [<normal_interval> [<abnormal_interval> [<timeout>]]]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<address>

- ICMP ECHO パケットのあて先 IP アドレス
  ICMP ECHO パケットのあて先 IP アドレスを指定します。
  IPsec 対象範囲に含まれる IP アドレスを以下の範囲で指定してください。

  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  また、0.0.0.0 を指定した場合は IKE セッションを監視しないものとみなされます。

<normal_interval>

- ICMP ECHO パケットの正常時送信間隔
  ICMP ECHO パケットの正常時送信間隔を、1 秒～60 秒 (1 分) の範囲で指定します。
  単位は、m(分)、s(秒) のどちらかを指定します。
  省略時は、10 秒を指定したものとみなされます。

<abnormal_interval>

- ICMP ECHO パケットの異常時送信間隔
  ICMP ECHO パケットの異常時送信間隔を、60 秒～600 秒 (10 分) の範囲で指定します。
  単位は、m(分)、s(秒) のどちらかを指定します。
  省略時は、180 秒 (3 分) を指定したものとみなされます。

<timeout>

- ICMP ECHO パケットのタイムアウト時間
  ICMP ECHO パケットのタイムアウト時間を、5 秒～180 秒 (3 分) の範囲で指定します。単位は、m(分)、s(秒) のどちらかを指定します。
  省略時は、5 秒を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IKE セッションの生存確認を行うための動作情報を設定します。
指定したあて先 IP アドレスに対して ICMP ECHO パケットの送受信で生存確認を行います。
あて先 IP アドレスは、IPv4 アドレスのみ指定可能です。
ICMP ECHO パケットの応答が正常に受信できている間は正常時送信間隔で監視を行いますが、ICMP ECHO パケットの応答が受信できなくなると、障害発生とみなし監視先に関連する IPsec /IKE SA を解放し、異常時送信間隔で監視を行います。
ICMP ECHO パケットの応答が受信できた時を復旧とみなし、監視先に関連する IPsec/IKE SA の確立を行い、正常送信間隔での監視に戻ります。
ICMP ECHO パケットのタイムアウト時間は、回線品質が悪い時や高負荷状態により ICMP ECHO パケットの応答が遅延するような状況のときに有効です。

[未設定時]

IKE セッションの生存を監視しないものとみなされます。

```
remote <number> ap <ap_number> ike sessionwatch 0.0.0.0 10s 3m 5s
```

7.2.73　remote ap ike mode

[機能]

IKE 情報の交換モードの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ike mode <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- IKE ネゴシエーションの交換モード
  IKE ネゴシエーションの交換モードを指定します。

  auto ： IKE 情報の交換モードを tunnel endpoint address および IKE 情報装置識別情報の設定によって自動判別します。

  aggressive ：
  IKE 情報の交換モードとして Aggressive Mode を使用します。

  main ： IKE 情報の交換モードとして Main Mode を使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IKE セッションを確立する、IKE ネゴシエーション交換モードの設定を行います。
交換モード、tunnel endpoint address、装置識別情報の設定により、以下の表のように動作します。

tunnel endpoint address の設定	name の設定	mode の設定		
		aggressive	main	auto
tunnel local ○ tunnel remote ○	name local ○ name remote ×	Aggressive (Initiator)	Main	Main
	name local × name remote ○	Aggressive (Responder)	Main	Main
	name local ○ name remote ○	Aggressive*1	Main	Main
	name local × name remote ×	動作しない	Main	Main
tunnel local × tunnel remote ○	name local ○ name remote ×	Aggressive (Initiator)	動作しない	Aggressive (Initiator)
	name local × name remote ○	動作しない	動作しない	動作しない
	name local ○ name remote ○	Aggressive (Initiator)	動作しない	Aggressive (Initiator)
	name local × name remote ×	動作しない	動作しない	動作しない
tunnel local ○ tunnel remote ×	name local ○ name remote ×	動作しない	動作しない	動作しない
	name local × name remote ○	Aggressive (Responder)	動作しない	Aggressive (Responder)
	name local ○ name remote ○	Aggressive (Responder)	動作しない	Aggressive (Responder)
	name local × name remote ×	動作しない	動作しない	動作しない

○：設定あり　×：設定なし
※tunnel local/remoteが設定なしの場合は、name、modeの設定に関係なくすべて動作しません。
*1 初期動作としてInitiator、Responder両方の動作が可能です。

[未設定時]

IKE 情報の交換モードとして自動判別を行うものとみなされます。

```
remote <number> ap <ap_number> ike mode auto
```

7.2.74　remote ap ike bind

[機能]

利用 IKE 情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ike bind <kind> [<conf_number>]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<kind>

- 利用する接続先定義番号指定の有無
  利用する IKE 情報が設定されている接続先定義番号を指定するかを決定します。

  self ：　同一接続先情報の IKE 定義を利用します。

  ap ：　<conf_number>で指定された接続先情報の IKE 定義を利用します。

<conf_number>

- 接続先情報定義番号
  利用する IKE 定義がされている接続先情報定義番号として 0 以上の 10 進数値を指定します。利用できる接続先情報は同一の相手情報定義内の接続先情報である必要があります。<kind>が self の場合は設定できません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

利用する IKE 定義の接続先情報を設定します。
利用する IKE 定義に指定する接続先情報番号には、有効な IKE 定義が存在する必要があります。
有効な IKE 定義が存在しない場合、<ap_number>の接続先情報は利用できません。
利用する接続先情報の IKE 定義が有効な場合、利用する接続先情報定義は以下のとおりです。

- remote ap ike port
- remote ap ike shared key
- remote ap ike proposal encrypt
- remote ap ike proposal hash
- remote ap ike proposal pfs

- remote ap ike proposal lifetime
- remote ap ike retry
- remote ap ike idtype
- remote ap ike name local
- remote ap ike name remote
- remote ap ike release
- remote ap ike initial
- remote ap ike sessionwatch
- remote ap tunnel local
- remote ap tunnel remote

[注意]

<conf_number>は、設定している接続先情報定義番号と同一の接続先情報定義番号は設定できません。

[未設定時]

利用する IKE 定義として同一接続先情報の IKE 定義を使用するとみなされます。

```
remote <remote_number> ap <ap_number> ike bind self
```

7.2.75　remote ap ike nat-traversal use

[機能]

IKE 情報の NAT トラバーサル利用可否の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] ike nat-traversal use <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

NAT トラバーサルを利用するかどうかを指定します。

- off
  NAT トラバーサルを利用しない場合に指定します。
- on
  NAT トラバーサルを利用する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IKE ネゴシエーションパケットおよび IPsec パケットを NAT トラバーサルするための設定を行います。

[注意]

NAT トラバーサル機能を利用するときは、以下の点に注意してください。

- IKE を行う双方の装置で設定してください。片方の装置での利用や NAT トラバーサルのバージョンが異なると、NAT トラバーサルはできません。
  NAT トラバーサルは、以下の RFC、Internet Draft のバージョンをサポートします。

  “ Negotiation of NAT-Traversal in the IKE ”

  RFC3947
  draft-ietf-ipsec-nat-t-ike-03
  draft-ietf-ipsec-nat-t-ike-02

  “ UDP Encapsulation of IPsec ESP Packets ”

  RFC3948

- IPsec トンネルに存在する NAT 装置の変換テーブルが解放されると、NAT トラバーサルは動作できなくなります。変換テーブルを保持するために、接続先監視機能と併用することを推奨します。
- 自動鍵交換用 IPsec 情報の暗号アルゴリズムを設定し、自動鍵交換用 IPsec 情報のセキュリティプロトコルを暗号 (esp) を指定してください。

  暗号アルゴリズムおよびセキュリティプロトコルが暗号でない場合は動作しません。
- 自側トンネルエンドポイントアドレス、および相手側エンドポイントアドレスに IPv4 アドレスを設定してください。IPv6 アドレスを設定した場合は動作しません。
- IPsec 情報のタイプに IKE を指定してください。動的 VPN(dvpn) および手動鍵 (manual) を設定した場合は動作しません。

[未設定時]

IKE 情報の NAT トラバーサル利用に off を指定したものとみなされます。

```
remote <number> ap <ap_number> ike nat-traversal use off
```

7.2.76　remote ap dvpn client

[機能]

動的 VPN 接続で使用するクライアント情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] dvpn client <conf_number>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<conf_number>

動的 VPN クライアント定義の定義番号を指定します。

- 動的 VPN クライアント定義の定義番号
  利用する動的 VPN クライアント定義の定義番号を、10 進数値で指定します。

範囲	機種
0～5	Si-R570　Si-R370
0～2	Si-R240　Si-R220B
0～1	Si-R260B　Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN 接続で使用するクライアント情報を設定します。
動的 VPN 機能を利用する場合は、本コマンドを必ず実行してください。

[未設定時]

動的 VPN 接続で使用するクライアント情報を設定しないものとみなされます。

7.2.77 remote ap dvpn remotenet

[機能]

動的 VPN で接続する相手側ネットワークの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] dvpn remotenet <count> <address>/<mask> [<invite_mode>]

[オプション]

<number>

- 相手定義番号

  相手ネットワークの通し番号を、10 進数値で指定します。

  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号

  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。

  省略時は、0 を指定したものとみなされます。

<count>

- プレフィックス定義番号

  プレフィックスの定義番号を、0 から 19 までの 10 進数値で指定します。

  指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つプレフィックス定義がすでに存在する場合は、既存の定義を変更します。

<address>/<mask>

- 相手側ネットワーク

  相手側ネットワークを IPv4 アドレス/マスクビット数 (またはマスク値) または IPv6 アドレスとプレフィックス長で指定します。

  IPv4: IPv4 アドレスとマスクビット数の組み合わせで指定します。
  マスク値は、最上位ビットから 1 で連続した値にしてください。
  デフォルトルートを設定する場合は、0.0.0.0/0(0.0.0.0/0.0.0.0) を指定します。

  IPv6: IPv6 アドレスとプレフィックスの組み合わせで指定します。
  リンクローカルアドレスは指定できません。
  デフォルトルートを設定する場合は、::/0 を指定します。

<invite_mode>

動的 VPN の接続契機となる IPv4/IPv6 パケットの検出条件の設定で invite 条件に一致した場合にテンプレートを使用して接続要求を発行するかどうかを指定します。
省略時は、off を指定したものとみなされます。

- off

  テンプレートを使用して接続要求を発行しません。

- on

  テンプレートを使用して接続要求を発行します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN 接続する場合の相手側ネットワークを IPv4 アドレス/マスクビット数 (またはマスク値) または IPv6 アドレスとプレフィックス長を指定します。
<invite_mode>は、相手側ネットワークに対してテンプレートを使用して接続要求するかどうかを指定します。接続先から動的 VPN 接続をする時は、off を指定してください。

[未設定時]

動的 VPN で接続する相手側ネットワークを設定しないものとみなされます。
本コマンドを省略する場合は、動的 VPN で接続する相手側ユーザ ID の設定を必ず実行してください。

7.2.78 remote ap dvpn remoteid

[機能]

動的 VPN で接続する相手側ユーザ ID の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] dvpn remoteid <id>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<id>

- 相手側ユーザ ID
  相手側ユーザ ID となる ID を、50 文字以内の ASCII 文字列で指定します。
  指定可能な範囲は以下のとおりです。

文字	範囲
半角アルファベット	a～z, A～Z
半角数値	0～9
半角記号	'-', '_', '.'

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN 接続する場合の相手側ユーザ ID を指定します。
本コマンドで指定した相手側ユーザ ID は、動的 VPN 接続要求を受信した時に接続先を特定する条件として使用されます。
また、回線接続契機などによる自装置から動的 VPN 接続要求を発行する時の相手側ユーザ ID としても使用されます。

[未設定時]

動的 VPN で接続する相手側ユーザ ID を設定しないものとみなされます。
本コマンドを省略する場合は、動的 VPN で接続する相手側ネットワークの設定を必ず実行してください。

7.2.79　remote ap tunnel local

[機能]

トンネル利用時の自側のトンネルエンドポイントアドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] tunnel local <address>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<address>

- 自側のトンネルエンドポイントアドレス
  自側のトンネルエンドポイントとなる IPv4 アドレスまたは IPv6 アドレスを指定します。本装置に設定されている IP アドレスを指定してください。
  指定可能な範囲は以下のとおりです。

  IPv4: 1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  IPv6: ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

  IPv6 DHCP クライアントが取得したプレフィックスを使用する場合は上位を"dhcp@インタフェース名"の形式で指定し、下位 80bit 分を IPv6 アドレス形式で指定します。インタフェース名には、rmt インタフェースを以下の範囲で指定します。

範囲	機種
rmt0～rmt999	Si-R570
rmt0～rmt499	Si-R370
rmt0～rmt99	Si-R260B　Si-R240　Si-R220B
rmt0～rmt49	Si-R180

例) rmt0 で動作する IPv6 DHCP クライアントが取得した IPv6 プレフィックスを使用する場合の設定例

```
dhcp@rmt0::
dhcp@rmt0::1:2:3:4
```

[動作モード]

構成定義モード (管理者クラス)

[説明]

指定した接続先定義にトンネル利用が設定されている場合に、そのトンネルの自側エンドポイントアドレスを設定します。
トンネルを利用して通信を行う場合は、本コマンドを必ず実行してください。

[注意]

動的 VPN 機能を利用した構成で IPv6 DHCP クライアントが取得したプレフィックスを使用する場合、プレフィックスが割り当てられるインタフェースと同じ値になるように指定してください。

[未設定時]

自側のトンネルエンドポイントアドレスを設定しないものとみなされます。

7.2.80　remote ap tunnel remote

[機能]

トンネル利用時の相手側のトンネルエンドポイントアドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] tunnel remote <address>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<address>

- 相手側のトンネルエンドポイントアドレス
  相手側のトンネルエンドポイントとなる IPv4 アドレスまたは IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  IPv4:　1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  IPv6:　::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

[動作モード]

構成定義モード (管理者クラス)

[説明]

指定した接続先定義にトンネル利用が設定されている場合に、そのトンネルの相手側エンドポイントアドレスを設定します。
トンネルを利用して通信を行う場合は、本コマンドを必ず実行してください。

[未設定時]

相手側のトンネルエンドポイントアドレスを設定しないものとみなされます。

7.2.81 remote ap overlap to

[機能]

overlap ap の実際の送出先の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] overlap to <kind> <conf_number>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<kind>

- lan
  実際の送出先を lan 定義とする場合に指定します。
- remote
  実際の送出先を remote 定義とする場合に指定します。

<conf_number>

lan 定義、remote 定義の定義番号を指定します。

- lan 定義の定義番号
  利用する lan の定義番号を、10 進数値で指定します。

範囲	機種
0〜19	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B
0〜9	Si-R180

- remote 定義の定義番号
  利用する remote の定義番号を、10 進数値で指定します。
  ただし、<number>と同じ値は指定できません。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B Si-R240 Si-R220B
0〜49	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

指定した接続先定義を利用してパケットを転送する場合の定義を設定します。
本コマンドは、remote ap datalink type の<type>で overlap を指定した場合にだけ有効です。

[未設定時]

パケット転送先を設定しないものとみなされます。

7.2.82 remote ap overlap nexthop

[機能]

overlap ap の転送先 IPv4 ルータの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] overlap nexthop <address>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<address>

- 転送先となる IPv4 ルータの IP アドレスを指定します。
  以下の範囲で指定してください。

  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[動作モード]

構成定義モード (管理者クラス)

[説明]

overlap ap 機能を利用して lan にパケットを転送する場合の、転送先 IPv4 ルータの IP アドレスを指定します。
本コマンドは、remote ap datalink type の<type>で overlap を指定し、remote ap overlap to の<kind>で lan を指定した場合にだけ有効です。

[未設定時]

IPv4 転送を行わないものとみなされます。

7.2.83　remote ap overlap nexthop6

[機能]

overlap ap の転送先 IPv6 ルータの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] overlap nexthop6 <address>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<address>

- 転送先となる IPv6 ルータの IP アドレスを指定します。
  以下の範囲で指定してください。

  ::2 〜 feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

[動作モード]

構成定義モード (管理者クラス)

[説明]

overlap ap 機能を利用して lan にパケットを転送する場合の、転送先 IPv6 ルータの IP アドレスを指定します。
本コマンドは、remote ap datalink type の<type>で overlap を指定し、remote ap overlap to の<kind>で lan を指定した場合にだけ有効です。

[未設定時]

IPv6 転送を行わないものとみなされます。

7.2.84 remote ap sessionwatch address

[機能]

接続先監視のアドレス設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] sessionwatch address <source> <destination>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<source>

- ICMP ECHO パケットの送信元 IP アドレス
  ICMP ECHO パケットの送信元 IP アドレスを指定します。装置に設定されている自側 IPv4/IPv6 アドレスのどれかを指定してください。
  指定可能な範囲は以下のとおりです。

  IPv4: 1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  IPv6: ::2 ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<destination>

- ICMP ECHO パケットのあて先 IP アドレス
  監視対象となる IPv4/IPv6 アドレスを指定します。
  <source>と同じプロトコルアドレスで指定してください。
  指定可能な範囲は以下のとおりです。

  IPv4: 1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  IPv6: ::2 ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

[動作モード]

構成定義モード (管理者クラス)

[説明]

接続先の生存確認を行うための動作情報を設定します。
指定したあて先 IP アドレスに対して ICMP ECHO パケットの送受信で生存確認を行います。

[注意]

以下の場合では、監視を行いません。

- ISDN 回線を利用する接続先で、常時接続機能を利用していない場合。
- PPPoE 回線を利用する接続先で、常時接続機能を利用していない場合。

また、IPsec/IKE を利用する接続先で、IKE セッション監視の設定 (remote ap ike sessionwatch) が同時に設定されている場合は、IKE セッション監視は動作しないで、接続先監視機能だけが動作します。

[未設定時]

接続先監視機能を利用しないものとみなされます。

7.2.85 remote ap sessionwatch interval

[機能]

接続先監視の各種インターバル設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] sessionwatch interval <normal> <error> <timeout> [<retry>]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<normal>

- ICMP ECHO パケットの正常時送信間隔
  ICMP ECHO パケットの正常時送信間隔を、1 秒～60 秒 (1 分) の範囲で指定します。
  単位は、m(分)、s(秒) のどちらかを指定します。

<error>

- ICMP ECHO パケットの異常時送信間隔
  ICMP ECHO パケットの異常時送信間隔を、60 秒～600 秒 (10 分) の範囲で指定します。
  単位は、m(分)、s(秒) のどちらかを指定します。

<timeout>

- 監視タイムアウト
  監視失敗とみなすまでのタイムアウト時間を、5 秒～180 秒 (3 分) の範囲で指定します。
  単位は、m(分)、s(秒) のどちらかを指定します。

<retry>

- ICMP ECHO パケットの再送間隔
  ICMP ECHO パケットの正常時送信に対して応答がない時の ICMP ECHO パケットの再送間隔を、1 秒～<timeout>-1 秒の範囲で指定します。
  単位は、m(分)、s(秒) のどちらかを指定します。
  省略時は、1s が指定されたものとして動作します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

接続先の生存確認を行うための動作情報を設定します。
指定したあて先 IP アドレスに対して ICMP ECHO パケットの送受信で生存確認を行います。
ICMP ECHO パケットの応答が正常に受信できている間は正常時送信間隔で監視を行いますが、ICMP ECHO パケットの応答が受信できなくなると、障害発生とみなし、異常時送信間隔で監視を行います。
ICMP ECHO パケットの応答が受信できた時を復旧とみなし、正常送信間隔での監視に戻ります。

[注意]

以下の場合では、監視を行いません。

- ISDN 回線を利用する接続先で、常時接続機能を利用していない場合。
- PPPoE 回線を利用する接続先で、常時接続機能を利用していない場合。

また、IPsec/IKE を利用する接続先で、IKE セッション監視の設定 (remote ap ike sessionwatch) が同時に設定されている場合は、IKE セッション監視は動作しないで、接続先監視機能だけが動作します。

[未設定時]

正常時送信間隔 10 秒、異常時送信間隔 1 分、監視タイムアウト 5 秒、再送間隔 1 秒が指定されたものとして動作します。

```
remote <number> ap <ap_number> sessionwatch interval 10s 1m 5s 1s
```

7.2.86 remote ap sessionwatch ttl

[機能]

接続先監視の TTL/HopLimit 値設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] sessionwatch ttl <send_ttl>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<send_ttl>

- 送信 TTL / HopLimit 値
  ICMP ECHO パケットを送信する時の IPv4 TTL/IPv6 HopLimit 値を、1〜255 の範囲で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

接続先の生存確認を行うための動作情報を設定します。
ICMP ECHO パケットの TTL/HopLimit 値を指定された値で送信します。

[注意]

以下の場合では、監視を行いません。

- ISDN 回線を利用する接続先で、常時接続機能を利用していない場合。
- PPPoE 回線を利用する接続先で、常時接続機能を利用していない場合。

また、IPsec/IKE を利用する接続先で、IKE セッション監視の設定 (remote ap ike sessionwatch) が同時に設定されている場合は、IKE セッション監視は動作しないで、接続先監視機能だけが動作します。

[未設定時]

送信 TTL/HopLimit 値に 255 が指定されたものとして動作します。

```
remote <number> ap <ap_number> sessionwatch ttl 255
```

7.2.87　remote ap sessionwatch mode

[機能]

接続先監視の動作モード設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] sessionwatch mode <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

監視方式を指定します。

- always
  常時監視を行います。
- idleonly
  無通信状態 (送信がない、または受信がない状態) に限り監視を行います。

[動作モード]

構成定義モード (管理者クラス)

[説明]

接続先の生存確認を行うための動作情報を設定します。
ICMP ECHO パケットによる監視を行う期間を指定します。

[注意]

以下の場合では、監視を行いません。

- ISDN 回線を利用する接続先で、常時接続機能を利用していない場合。
- PPPoE 回線を利用する接続先で、常時接続機能を利用していない場合。

また、IPsec/IKE を利用する接続先で、IKE セッション監視の設定 (remote ap ike sessionwatch) が同時に設定されている場合は、IKE セッション監視は動作しないで、接続先監視機能だけが動作します。

[未設定時]

常時監視が指定されたものとして動作します。

```
remote <number> ap <ap_number> sessionwatch mode always
```

7.2.88　remote ap sessionwatch recovery

[機能]

接続先監視の復旧タイミング設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] sessionwatch recovery <count>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 応答受信回数
  異常状態から正常状態へ復旧するまでの連続応答受信回数を 1～100 の範囲で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

接続先の生存確認を行うための動作情報を設定します。
異常状態から正常状態へ復旧するために必要な連続応答受信回数を設定します。これにより、回線状態が不安定な場合のインタフェースダウン／アップのばたつきを防ぎます。
連続応答待ち状態での ICMP ECHO パケット送信間隔は、正常時送信間隔を使用します。
本装置起動後を含め、回線接続直後に通信可能な状態であっても、必要な回数の応答を受信するまで通信可能にはなりませんので、ご注意ください。

[注意]

以下の場合では、監視を行いません。

- ISDN 回線を利用する接続先で、常時接続機能を利用していない場合。
- PPPoE 回線を利用する接続先で、常時接続機能を利用していない場合。

また、IPsec/IKE を利用する接続先で、IKE セッション監視の設定 (remote ap ike sessionwatch) が同時に設定されている場合は、IKE セッション監視は動作しないで、接続先監視機能だけが動作します。

[未設定時]

連続応答受信回数に 1 が指定されたものとして動作します。

```
remote <number> ap <ap_number> sessionwatch recovery 1
```

7.2.89　remote ap sessionwatch error-wait

[機能]

接続先監視の異常時送信開始待ち時間設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] sessionwatch error-wait <time>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<time>

- 異常時送信開始待ち時間
  異常時 ICMP ECHO パケットの送信開始待ち時間を、0 秒〜86400 秒 (1 日) の範囲で指定します。0 秒が指定された場合は待ち合わせをしません。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

接続先の生存確認を行うための動作情報を設定します。
正常状態から異常状態に遷移した場合に、最初の ICMP ECHO パケットを送信するまでの待ち時間を設定します。

[注意]

以下の場合では、監視を行いません。

- ISDN 回線を利用する接続先で、常時接続機能を利用していない場合。
- PPPoE 回線を利用する接続先で、常時接続機能を利用していない場合。

また、IPsec/IKE を利用する接続先で、IKE セッション監視の設定 (remote ap ike sessionwatch) が同時に設定されている場合は、IKE セッション監視は動作しないで、接続先監視機能だけが動作します。

[未設定時]

```
remote <number> ap <ap_number> sessionwatch error-wait 0s
```

7.2.90 remote ap mpls to

[機能]

MPLS LSP の送出先の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] mpls to <kind> <conf_number>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<kind>

- lan
  MPLS LSP の送出先を lan 定義とする場合に指定します。
- remote
  MPLS LSP の送出先を remote 定義とする場合に指定します。

<conf_number>

lan 定義、remote 定義の定義番号を指定します。

- lan 定義の定義番号
  利用する lan の定義番号を、10 進数値で指定します。

範囲	機種
0〜19	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B
0〜9	Si-R180

- remote 定義の定義番号
  利用する remote の定義番号を、10 進数値で指定します。
  ただし、<number>と同じ値は指定できません。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B Si-R240 Si-R220B
0〜49	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

指定した接続先定義を利用してパケットを転送する場合の定義を設定します。
本コマンドは、remote ap datalink type の<type>で mpls を指定した場合にだけ有効です。

[未設定時]

MPLS LSP を設定しないものとみなされます。

7.2.91 remote ap mpls nexthop

[機能]

MPLS LSP の次ホップのラベルスイッチルータの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ap [<ap_number>] mpls nexthop <address>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<address>

- 次ホップのラベルスイッチルータの IP アドレスを指定します。
  以下の範囲で指定してください。

  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[動作モード]

構成定義モード (管理者クラス)

[説明]

MPLS LSP を利用して lan にパケットを転送する場合の、次ホップのラベルスイッチルータの IP アドレスを指定します。
本コマンドは、remote ap datalink type の<type>で mpls を指定し、remote ap mpls to の<kind>で lan を指定した場合にだけ有効です。

[未設定時]

lan で MPLS LSP を使用しないものとみなされます。

7.3　PPP 関連情報

7.3.1　remote ppp compress

[機能]

データ圧縮機能の設定

[適用機種]

Si-R 570	Si-R 370		Si-R 240	Si-R 220B	

[入力形式]

remote [<number>] ppp compress <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- off
  データ圧縮機能を使用しない場合に指定します。
- on
  データ圧縮機能を使用する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

データ圧縮機能を使用するかどうか設定します。

[注意]

MP を使用する場合、受信順序制御 (remote ppp mp order を参照) を有効にしてください。MP を使用し、かつ受信順序制御を使用しないと定義している場合、ヒストリ機能 (高圧縮のための機能) を使用できません。

[未設定時]

データ圧縮機能を使用しないものとみなされます。

```
remote <number> ppp compress off
```

7.3.2 remote ppp mp start

[機能]

MP 利用時の初期接続リンク数の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

remote [<number>] ppp mp start <link>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<link>

- MP 利用時の初期接続リンク数
  MP 利用時の初期接続リンク数を指定します。

範囲	機種
1〜23	Si-R570 Si-R370
1〜2	Si-R220B

[動作モード]

構成定義モード (管理者クラス)

[説明]

MP 利用時の初期接続リンク数を設定します。
MP 利用時に自装置から発信する場合、最初から接続を試みるリンク数を設定します。なお、発信に失敗した場合、再試行は行いません。また、最大接続リンク数の設定値を超えて接続は実施しません。

[注意]

以下の条件に一致した場合は、ここで指定したチャネル数まで増加しません。

- 接続に失敗した場合
- 最大接続リンク数の設定値より大きい値を設定した場合

また、初期接続のリンク増加時は、最初に接続を行った電話番号に対して発信します。

[未設定時]

初期接続リンク数として 1 を指定したものとみなされます。

```
remote <number> ppp mp start 1
```

7.3.3　remote ppp mp max

[機能]

MP の最大接続リンク数の設定

[適用機種]

Si-R 570 | Si-R 370

[入力形式]

remote [<number>] ppp mp max <link>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<link>

- MP 利用時の最大接続リンク数
  MP 利用時の最大接続リンク数を 2〜23 の範囲で指定します。

[注意]

接続先回線が複数の場合は、以下のどちらかを行ってください。

- 自局電話番号の設定および BAP 有効化。
- 代表取り扱いサービスの契約。

[動作モード]

構成定義モード (管理者クラス)

[説明]

MP を利用した時の最大接続リンク数を設定します。

[未設定時]

最大接続リンク数として 2 を指定したものとみなされます。

```
remote <number> ppp mp max 2
```

7.3.4 remote ppp mp divide

[機能]

MP 通信時の最小分割長の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

remote [<number>] ppp mp divide <length>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<length>

- default
  最小分割長を 256byte、最小分割単位を 128byte として動作します。
- 最小分割長
  最小分割長を 1〜1524 の範囲で指定します。この値は最小分割単位としても利用されます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

複数チャネルでの MP 通信時の、送信フレームの最小分割長を指定します。
ここで指定した長さ以上の送信フレームは、余り部分を除き、最小分割単位以上となるように均等に分割して送信されます。

[未設定時]

最小分割長として default を指定したものとみなされます。

```
remote <number> ppp mp divide default
```

7.3.5　remote ppp mp traffic use

[機能]

自動チャネル数制御の可否の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

remote [<number>] ppp mp traffic use <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- on
  スループット BOD の機能を使用します。
- off
  スループット BOD の機能を使用しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

スループット BOD 機能を使用するかどうかを設定します。

[未設定時]

スループット BOD 機能を使用しないとみなされます。

```
remote <number> ppp mp traffic use off
```

7.3.6 remote ppp mp traffic increase

[機能]

リンク増加閾値の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

remote [<number>] ppp mp traffic increase <traffic> <time>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<traffic>

- 回線増加閾値
  単位時間当たりのチャネル利用率を、0〜100 の 10 進数値で指定します。
  以下に、回線増加閾値の計算式を示します。
  チャネル利用率 (%) = 転送バイト量 ÷ 転送可能バイト数 × 100

<time>

- 増加猶予時間
  トラフィックが回線増加閾値を超え続けた場合に、発信するまでの猶予時間を
  0 秒〜3600 秒の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

スループット BOD 機能使用時のリンク増加閾値を設定します。
スループット BOD 機能を使用する場合は、本コマンド を必ず設定してください。

[注意]

指定した増加猶予時間の間、チャネル利用率が回線増加閾値を超え続けた場合にチャネル増加のための発信が行われます。

[未設定時]

回線増加閾値および猶予時間を設定しないものとみなされます。

7.3.7　remote ppp mp traffic decrease

[機能]

リンク減少閾値の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

remote [<number>] ppp mp traffic decrease <traffic> <time>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<traffic>

- 回線減少閾値
  単位時間当たりのチャネル利用率を、0〜100 の 10 進数値で指定します。
  以下に、回線減少閾値の計算式を示します。
  チャネル利用率 (%) = 転送バイト量 ÷ 転送可能バイト数 × 100

<time>

- 減少猶予時間
  トラフィックが回線減少閾値を超え続けた場合に、切断するまでの猶予時間を
  0 秒〜3600 秒の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

スループット BOD 利用時のリンク減少閾値を設定します。
スループット BOD 機能を使用する場合は、本コマンド を必ず設定してください。

[注意]

設定された減少猶予時間の間、チャネル利用率が回線減少閾値を下回り続けた場合にチャネル減少が行われます。

[未設定時]

回線減少閾値および猶予時間を設定しないものとみなされます。

7.3.8 remote ppp mp order

[機能]

受信パケット順序制御の有無の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

remote [<number>] ppp mp order <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- off
  順序制御をしない場合に指定します。
- on
  順序制御をする場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

MP 受信パケットの順序制御を行うかどうか設定します。

[注意]

以下に、MP 受信パケットの順序制御が無効になっていると動作に影響が出る機能を示します。

- ブリッジ機能
  順序に依存するプロトコルをブリッジによって通信する場合、通信が停止することがあります。
- VJ ヘッダ圧縮機能
  設定にかかわらず、常に VJ ヘッダ圧縮を使用しません。
- IP ヘッダ圧縮機能
  設定にかかわらず、常に IP ヘッダ圧縮を使用しません。
- データ圧縮機能
  LZS アルゴリズムで、ヒストリ機能 (高効率圧縮の機能) を使用しません。

[未設定時]

MP 受信パケットの順序制御をしないものとみなされます。

```
remote <number> ppp mp order off
```

7.3.9　remote ppp ipcp vjcomp

[機能]

VJ-Compression の利用の有無の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ppp ipcp vjcomp <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- enable
  VJ ヘッダ圧縮を使用する場合に指定します。
- disable
  VJ ヘッダ圧縮を使用しない場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

VJ ヘッダ圧縮機能 (VJCOMP) を使用するかどうかを設定します。VJ ヘッダ圧縮機能は、RFC1144 に準拠しています。

[注意]

Si-R570 Si-R370 Si-R220B の場合は以下に注意してください。
MP を使用する場合は、remote ppp mp order の<mode>に on を指定して、受信順序制御を使用してください。
MP を使用するにもかかわらず受信順序制御を使用しないと定義している場合、VJ ヘッダ圧縮機能は無条件に無効となります。

[未設定時]

VJ ヘッダ圧縮機能を使用するものとみなされます。

```
remote <number> ppp ipcp vjcomp enable
```

7.3.10 remote ppp ipcp iphc

[機能]

IPv4 の IP ヘッダ圧縮 (IPHC) の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ppp ipcp iphc <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- enable
  IP ヘッダ圧縮を使用する場合に指定します。
- disable
  IP ヘッダ圧縮を使用しない場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv4 で、IP ヘッダ圧縮 (IPHC) を使用するかどうかを設定します。IP ヘッダ圧縮機能は、圧縮方法が RFC2507/RFC2508 に、ネゴシエーション方法が RFC2509 に準拠しています。

[注意]

Si-R570 Si-R370 Si-R220B の場合は以下に注意してください。
MP を使用する場合は、remote ppp mp order の<mode>に on を指定して、受信順序制御を使用してください。
MP を使用するにもかかわらず受信順序制御を使用しないと定義している場合、IP ヘッダ圧縮機能は無条件に無効となります。

[未設定時]

IP ヘッダ圧縮機能を使用しないものとみなされます。

```
remote <number> ppp ipcp iphc disable
```

7.3.11　remote ppp ipv6cp iphc

[機能]

IPv6 の IP ヘッダ圧縮 (IPHC) の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ppp ipv6cp iphc <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- enable
  IP ヘッダ圧縮を使用する場合に指定します。
- disable
  IP ヘッダ圧縮を使用しない場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv6 で、IP ヘッダ圧縮 (IPHC) の使用するかどうかを設定します。IP ヘッダ圧縮機能は、圧縮方法が RFC2507/RFC2508 に、ネゴシエーション方法が RFC2509 に準拠しています。

[注意]

Si-R570 Si-R370 Si-R220B の場合は以下に注意してください。
MP を使用する場合は、remote ppp mp order の<mode>に on を指定して、受信順序制御を使用してください。
MP を使用するにもかかわらず受信順序制御を使用しないと定義している場合、IP ヘッダ圧縮機能は無条件に無効となります。

[未設定時]

IPv6 ヘッダ圧縮機能を使用しないものとみなされます。

```
remote <number> ppp ipv6cp iphc disable
```

7.4 IP 関連情報

7.4.1 remote ip address local

[機能]

自側 IP アドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip address local <address>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<address>

- 自側 IP アドレス
  相手ネットワークでの自側 IP アドレスを指定します。
  自側 IP アドレスの指定可能な範囲は以下のとおりです。

  0.0.0.0
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  0.0.0.0 を指定した場合は、設定を削除します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手ネットワークでの自側 IP アドレスを設定します。

[未設定時]

IP アドレスなし (unnumbered) として動作します。

7.4.2　remote ip address remote

[機能]

相手側 IP アドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip address remote <address>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<address>

- 相手側 IP アドレス
  相手ネットワークでの相手側 IP アドレスを指定します。
  相手側 IP アドレスの指定可能な範囲は以下のとおりです。

  0.0.0.0
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  0.0.0.0 を指定した場合は、設定を削除します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手ネットワークでの相手側 IP アドレスを設定します。

[未設定時]

相手装置のアドレスが任意のアドレスであるものとして扱います。相手装置にアドレスがない場合、IP アドレスを割り当てません。

7.4.3 remote ip route

[機能]

IPv4 スタティック経路情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip route <count> <address>/<mask> [<metric> [<distance>]]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- スタティック経路情報定義番号
  スタティック経路情報の定義番号を、10 進数値で指定します。

範囲	機種
0〜1999	Si-R570
0〜1249	Si-R370
0〜255	Si-R260B Si-R240 Si-R220B
0〜127	Si-R180

<address>/<mask>

- IPv4 アドレス/マスクビット数 (またはマスク値)
  あて先ネットワークを IPv4 アドレスとマスクビット数の組み合わせで指定します。
  マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
  - IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
  - IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)
- default
  あて先ネットワークとしてデフォルトルートを設定する場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<metric>

- RIP メトリック値
  このスタティック経路情報を RIP に再配布するときのメトリック値を、1〜15 の 10 進数値で指定します。
  省略時は、1 を指定したものとみなされます。

<distance>

- 優先度
  このスタティック経路情報の優先度を、0〜254 の 10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。
  省略時は、0 を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv4 スタティック経路 (静的経路) 情報を設定します。
RIP メトリック値は、スタティック経路情報を RIP に再配布するときのメトリック値を設定します。RIP に再配布したときは、設定した RIP メトリック値+1 のメトリック値で RIP テーブルに登録されます。
優先度は、同じあて先への経路情報が複数ある場合、優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。各ダイナミックルーティングプロトコルの優先度については、routemanage ip distance コマンドを参照してください。
優先度に 0 が設定されているときは、routemanage interface floating コマンドでのフローティング設定に応じてフローティング動作が切り替わります。優先度に 1 以上が設定されているときは、常にフローティング動作します。
フローティング動作する場合、remote インタフェースが通信可能な状態 (リンクアップなど) であれば、スタティック経路情報をルーティングテーブルに追加します。通信不可能な状態 (リンクダウンなど) であれば、ルーティングテーブルから削除します。
フローティング動作しない場合は、インタフェースの状態にかかわらず常にスタティック経路情報をルーティングテーブルに追加します。
以下に、各設定値とフローティング動作の関係を示します。

<distance> 設定値	インタフェース経路の フローティング設定	スタティック経路の フローティング動作
0(省略値)	使用しない	しない
0(省略値)	使用する	する
1以上	使用しない	する
1以上	使用する	する

以下のような用途でスタティック経路情報を使用する場合、フローティング動作するとなるように設定してください。

- IP ルーティングおよびダイナミックルーティングでの広報で、スタティック経路の出口インタフェースで異常が発生した場合、ルーティングテーブルよりスタティック経路を削除します。
- あて先が同じ経路をダイナミックルーティングで受信した場合、優先度関係により経路を決定します。

複数のスタティック経路情報で ECMP 機能を使用するときは、あて先、RIP メトリック値、優先度がそれぞれ同じとなるようにスタティック経路情報を設定します。また、ECMP 機能を使用する場合は、routemanage ip ecmp mode コマンドで ECMP を使用するように設定します。
ECMP となるスタティック経路情報は、同じあて先への経路情報ごとに装置全体で 4 個まで定義できます。
IPv4 スタティック経路情報は、本装置全体で以下の数まで定義できます。

最大定義数	機種
2000	Si-R570
1250	Si-R370
256	Si-R260B　Si-R240　Si-R220B
128	Si-R180

[注意]

同じあて先へのスタティック経路情報を複数設定する場合、以下の点に注意してください。

- 優先度が 0 のスタティック経路情報と、優先度が 0 または 1 以上のスタティック経路情報は同時に設定できません。
- 優先度が同じで、RIP メトリック値が違うスタティック経路情報は同時に設定できません。

[未設定時]

IPv4 スタティック経路情報を使用しないものとみなされます。

7.4.4　remote ip rip use

[機能]

RIP 基本情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip rip use <send> <receive> <metric> [<ignore> [<password>]]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<send>

RIP の送信について指定します。

- v1
  RIPv1(Unicast または Broadcast) を送信します。
  自側 IP アドレスが設定されている場合は Unicast で送信します。設定されていない場合 (unnumbered) は Broadcast で送信します。
- v2
  RIPv2(Unicast または Broadcast) を送信します。
  自側 IP アドレスが設定されている場合は Unicast で送信します。設定されていない場合 (unnumbered) は Broadcast で送信します。
- v2m
  RIPv2(Multicast) を送信します。
- off
  RIP を送信しません。

<receive>

RIP の受信について指定します。

- v1
  RIPv1 を受信します。
- v2
  RIPv1, RIPv2 を受信します。
- off
  RIP を受信しません。

<metric>

- 加算メトリック値
  RIP パケット送信時の加算メトリック値を、0〜16 の 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<ignore>

自装置に<password>を設定していないときに、パスワード付きの RIPv2 パケットを受信したときの破棄の動作を指定します。
省略時は、off を指定したものとみなされます。

- on
  受信した RIPv2 パケットを破棄します。
- off
  受信した RIPv2 パケットを破棄しません。

<password>

- RIPv2 パスワード
  <send>または<receive>に v2 を指定した場合のパスワードを、0x21,0x23〜0x7e のコードで構成される 16 文字以内の ASCII 文字列で指定します。
  省略時は、パスワードなしとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP の基本的な動作を設定します。
<metric>は、RIP パケットを送信する際に加算するメトリック値を設定します。
RIP(IPv4) を使用するインタフェースは、本装置全体で以下の数まで定義できます。

最大定義数	機種
220	Si-R570
120	Si-R370 Si-R260B Si-R240 Si-R220B
50	Si-R180

[注意]

remote mtu コマンドを使用し、MTU 値を 576 よりも小さい値を設定すると、RIPv1(Broadcast), RIPv2(Broadcast) パケットを送信しない場合があります。MTU 値は 576 以上を設定してください。
NAT との併用はできません。
Si-R570 Si-R370 Si-R240 Si-R220B の場合は以下に注意してください。
ISDN またはフレームリレー (従量課金) の場合、RIP 情報を送信すると、思わぬ課金 (定期発信または長時間接続) が発生します。

[未設定時]

RIP 機能を使用しないものとみなされます。

```
remote <number> ip rip use off off 0 off
```

7.4.5　remote ip rip filter act

[機能]

RIP フィルタ動作の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip rip filter <count> act <action> <direction>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜799	Si-R570
0〜399	Si-R370　Si-R260B　Si-R240　Si-R220B
0〜199	Si-R180

<action>

フィルタリング条件に一致した場合の動作を指定します。

- pass
  該当する経路情報を透過します。
- reject
  該当する経路情報を遮断します。

<direction>

フィルタリングを行う方向を指定します。

- in
  受信時にフィルタリングを行います。
- out
  送信時にフィルタリングを行います。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP での経路情報送受信時に、フィルタリング条件に一致した経路情報を通過 (pass) させるか遮断 (reject) させるかを設定します。フィルタリング条件は優先度順に検索し、条件に一致した経路情報があった時点でフィルタリングが行われ、それ以降の条件は参照されません。全条件に不一致の経路情報は遮断されます。
フィルタリング条件は、remote ip rip filter route コマンド を使用し経路情報を設定します。
<count>は、指定値が順番にソート されてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。
RIP フィルタは、本装置全体で以下の数まで定義できます。

最大定義数	機種
800	Si-R570
400	Si-R370 Si-R260B Si-R240 Si-R220B
200	Si-R180

[注意]

フィルタリング条件が設定されていない場合、本コマンド の設定は無効となります。

[未設定時]

RIP フィルタを使用しないものとみなされ、すべての RIP の経路情報が透過します。

7.4.6　remote ip rip filter move

[機能]

RIP フィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip rip filter move <count> <new_count>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0〜799	Si-R570
0〜399	Si-R370　Si-R260B　Si-R240　Si-R220B
0〜199	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP フィルタの優先順序を変更します。
<new_count>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、<new_count>は順番にソートされてリナンバリングされます。

7.4.7 remote ip rip filter route

[機能]

RIP フィルタの経路情報設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip rip filter <count> route <address>/<mask> [<prefix_match>]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜799	Si-R570
0〜399	Si-R370 Si-R260B Si-R240 Si-R220B
0〜199	Si-R180

<address>/<mask>

- IPv4 アドレス/マスクビット数 (またはマスク値)
  フィルタリング対象とする経路情報を、IPv4 アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
  - IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
  - IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)
- any
  すべての経路情報をフィルタリング対象とする場合に指定します。
- default
  デフォルトルートをフィルタリング対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<prefix_match>

経路情報 (IPv4 アドレス/マスク) の検索条件を指定します。
省略時は、exact を指定したものとみなされます。
<address>/<mask>に"any"または"default"を指定した場合は、<prefix_match>は指定できません。

- exact
  指定した<address>/<mask>と経路情報の IPv4 アドレス/マスクを比較し、一致した場合に、フィルタリング対象とします。

- inexact

  指定した<address>と経路情報の IPv4 アドレスを比較し、<mask>まで一致した場合、フィルタリング対象とします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

フィルタリング条件として経路情報を設定します。

[未設定時]

フィルタリング条件が設定されていないものとみなされます。

7.4.8 remote ip rip filter set metric

[機能]

RIP フィルタのメトリック設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip rip filter <count> set metric <metric>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜799	Si-R570
0〜399	Si-R370 Si-R260B Si-R240 Si-R220B
0〜199	Si-R180

<metric>

- メトリック値
  メトリック値を、0〜16 の 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

フィルタリング条件に一致した経路情報のメトリック値を変更します。
<metric>に 1〜16 を設定した場合、メトリック値は設定した値に変更されます。また、この場合、remote ip rip use コマンドで設定した加算メトリック値は加算されません。0 を指定した場合、メトリック値の変更は行われません。

[注意]

フィルタリング条件が設定されていない場合、本コマンドの設定は無効となります。
フィルタリング条件の"any"と一致した場合、本コマンドの設定は無効となります。

[未設定時]

フィルタリング条件に一致した経路情報のメトリック値を変更しないものとみなされます。

7.4.9　remote ip ospf use

[機能]

OSPF 利用可否の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip ospf use <mode> [<area_number>]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- off
  OSPF を利用しません。
- on
  OSPF を利用します。

<area_number>

- エリア定義番号
  OSPF を利用する場合は、エリアの定義番号を指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜9	Si-R570
0〜3	Si-R370
0〜2	Si-R260B　Si-R240　Si-R220B
0〜1	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

OSPF を利用するかどうかと、インタフェースが属するエリアの定義番号を設定します。
OSPF を使用するインタフェースは、本装置全体で以下の数まで定義できます。

最大定義数	機種
100	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
50	Si-R180

[注意]

OSPF の利用は、"ospf ip area id"を設定した場合にだけ有効です。
Unnumbered インタフェースの場合、OSPF は動作しません。

[未設定時]

OSPF を使用しないものとみなされます。

```
remote <number> ip ospf use off
```

7.4.10　remote ip ospf cost

[機能]

OSPF 出力コストの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip ospf cost <cost>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<cost>

- 出力コスト
  出力コストを、1～65535 で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

OSPF 出力コストを設定します。

[未設定時]

OSPF 出力コストに 10 が設定されているものとみなされます。

```
remote <number> ip ospf cost 10
```

7.4.11 remote ip ospf hello

[機能]

OSPF Hello パケット送信間隔の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip ospf hello <hello_interval>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<hello_interval>

- Hello パケット送信間隔
  Hello パケットの送信間隔時間を、1 秒〜65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、1s〜65535s、1m〜1092m、1h〜18h です。

[動作モード]

構成定義モード (管理者クラス)

[説明]

OSPF 隣接関係の維持に用いられる Hello パケットの送信間隔を設定します。
hello_interval の値は OSPF 隣接ルータ間で同じ値を設定します。

[注意]

OSPF 隣接ルータ間で異なる Hello パケットの送信間隔を設定した場合、ルーティングが行えません。

[未設定時]

Hello パケット送信間隔に 10 秒が設定されているものとみなされます。

```
remote <number> ip ospf hello 10s
```

7.4.12　remote ip ospf dead

[機能]

OSPF 隣接ルータ停止確認間隔の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip ospf dead <dead_interval>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<dead_interval>

- 隣接ルータ停止確認間隔
  隣接ルータ停止確認の間隔時間を、1 秒〜65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、1s〜65535s、1m〜1092m、1h〜18h です。

[動作モード]

構成定義モード (管理者クラス)

[説明]

OSPF 隣接関係の維持に用いられる隣接ルータ停止確認間隔を設定します。
隣接ルータ停止確認間隔の間に Hello パケットを受信しなかった場合は、そのルータとの隣接関係は解除されます。
dead_interval の値は OSPF 隣接ルータ間で同じ値を設定します。
dead_interval の値は Hello パケット送信間隔よりも大きな値を設定する必要があります。
Hello パケット送信間隔の 4 倍を設定することを推奨します。

[注意]

OSPF 隣接ルータ間で異なる隣接ルータ停止確認間隔を設定した場合、ルーティングが行えません。

[未設定時]

隣接ルータ停止確認間隔に 40 秒が設定されているものとみなされます。

```
remote <number> ip ospf dead 40s
```

7.4.13 remote ip ospf retrans

[機能]

OSPF パケット再送間隔の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip ospf retrans <retransmit_interval>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<retransmit_interval>

- パケット再送間隔
  パケットの再送間隔を、3 秒〜65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、3s〜65535s、1m〜1092m、1h〜18h です。

[動作モード]

構成定義モード (管理者クラス)

[説明]

OSPF パケットを再送する間隔を設定します。

[未設定時]

OSPF パケットの再送間隔に 5 秒が設定されているものとみなされます。

```
remote <number> ip ospf retrans 5s
```

7.4.14　remote ip ospf delay

[機能]

OSPF LSU パケット送信遅延時間の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip ospf delay <transmit_delay>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<transmit_delay>

- LSU パケット送信遅延時間
  LSU パケットを送信する場合の遅延時間を、1 秒～65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、1s～65535s、1m～1092m、1h～18h です。

[動作モード]

構成定義モード (管理者クラス)

[説明]

LSU(Link State Update) パケットの送信遅延時間を設定します。
LSU パケットでは、LSA(Link State Advertisement) を作成してからの経過時間に<transmit_delay>の値を加算して広報します。

[注意]

一般的な装置では、作成してからの経過時間が 1 時間となった LSA を破棄します。このため、LSU 送信遅延時間に 1 時間以上を設定した場合は、正しくルーティングできない場合があります。

[未設定時]

LSU パケット送信遅延時間に 1 秒が設定されているものとみなされます。

```
remote <number> ip ospf delay 1s
```

7.4.15 remote ip ospf auth type

[機能]

OSPF パケット認証方式の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip ospf auth type <authtype>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<authtype>

パケット認証方式を指定します。

- off
  認証を行いません。
- text
  テキスト認証を使用します。
- md5
  MD5 認証を使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

OSPF パケットに対する認証方式を設定します。

[注意]

テキスト認証の使用は、"remote ip ospf auth textkey"を設定した場合にだけ有効です。
MD5 認証の使用は、"remote ip ospf auth md5key"を設定した場合にだけ有効です。

[未設定時]

OSPF パケット認証を使用しないものとみなされます。

```
remote <number> ip ospf auth type off
```

7.4.16　remote ip ospf auth textkey

[機能]

OSPF テキスト認証鍵の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip ospf auth textkey <kind> <key> [encrypted]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<kind>

鍵種別を指定します。

- text
  文字列鍵を使用します。
- hex
  16 進数鍵を使用します。

<key>

- テキスト認証鍵
  文字列鍵の場合は、0x21,0x23～0x7e のコードで構成される 8 文字以内の ASCII 文字列で指定します。
  16 進数鍵の場合は、16 桁以内の 16 進数値で指定します。16 桁未満の値を指定したときは左詰めで設定され、残りは 16 桁になるまで 0x0 でパディングされます。
- 暗号化されたテキスト認証鍵
  show コマンドで表示される暗号化されたテキスト認証鍵を encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化テキスト認証鍵指定
  <key>に暗号化されたテキスト認証鍵を指定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

テキスト認証で使用する鍵を設定します。
show コマンドでは、暗号化されたテキスト認証鍵が encrypted と共に表示されます。

[未設定時]

テキスト認証鍵が設定されていないものとみなされます。

7.4.17 remote ip ospf auth md5key

[機能]

OSPF MD5 認証鍵情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip ospf auth md5key <key_id> <key> [encrypted]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<key_id>

- MD5 認証鍵 ID
  MD5 認証鍵 ID を、1〜255 で指定します。
- 暗号化された MD5 認証鍵 ID
  show コマンドで表示される暗号化された MD5 認証鍵 ID を encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

<key>

- MD5 認証鍵
  MD5 認証鍵を、0x21,0x23〜0x7e のコードで構成される 16 文字以内の ASCII 文字列で指定します。
- 暗号化された MD5 認証鍵
  show コマンドで表示される暗号化された MD5 認証鍵を encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化 MD5 認証鍵情報指定
  <key_id>と<key>に暗号化された MD5 認証鍵 ID と MD5 認証鍵を指定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

MD5 認証で使用する鍵情報 (MD5 認証鍵 ID、MD5 認証鍵) を設定します。show コマンドでは、暗号化された MD5 認証鍵 ID と MD5 認証鍵が encrypted と共に表示されます。
show remote [<number>] ip ospf auth md5key を実行すると、暗号化していない MD5 認証鍵 ID と MD5 認証鍵が表示されます。

[未設定時]

MD5 認証で使用する鍵情報が設定されていないものとみなされます。

7.4.18　remote ip ospf passive

[機能]

OSPF パケット送信抑止の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip ospf passive <interface_type>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<interface_type>

- on
  パケットの送信を抑止します。
- off
  パケットの送信を抑止しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

OSPF パケット送信の抑止を設定します。

[未設定時]

OSPF パケットの送信は抑止しないものとみなされます。

```
remote <number> ip ospf passive off
```

7.4.19 remote ip ospf multicast

[機能]

OSPF 送信方法の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip ospf multicast <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

OSPF パケットをマルチキャストで送信するかどうかを指定します。

- on
  マルチキャストで送信します。
- off
  ユニキャストで送信します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

OSPF パケットは、通常はマルチキャストで送信します。マルチキャストでは受信できない相手装置と接続する場合、off を設定することでユニキャストで送信します。

[未設定時]

マルチキャストで送信するものとみなされます。

```
remote <number> ip ospf multicast on
```

7.4.20　remote ip ospf checkmtu

[機能]

OSPF パケットの MTU 値確認抑止の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip ospf checkmtu <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

OSPF パケットの MTU 値の確認を抑止するかどうかを指定します。

- on
  MTU 値の確認を行います。
- off
  MTU 値の確認を行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

OSPF パケットの MTU 値は、通常、同一値であることを確認します。ただし、相手装置仕様により、MTU 値の不整合が回避できない場合、off を設定することで確認を抑止することができます。

[注意]

MTU 値の確認設定を off とする場合は、相手装置の送信するパケットの長さが自装置の MTU サイズ以下である必要があります。相手装置の仕様が確認できる場合だけご使用ください。

[未設定時]

OSPF パケットの MTU 値の確認を行うものとみなされます。

```
remote <number> ip ospf checkmtu on
```

7.4.21 remote ip nat mode

[機能]

アドレス変換の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip nat mode <mode> [<address> <addr_number> [<time>]]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

アドレス変換 (NAT) を使用するかどうかを設定します。

- off
  NAT を使用しません。
- nat
  NAT を使用します。
- multi
  マルチ NAT を使用します。
- static
  静的 NAT だけを使用します。

以下のパラメタは、<mode>に nat または multi または static を設定した場合に有効です。

<address>

- 先頭グローバル IP アドレス
  動的変換に使用するグローバル IP アドレスの先頭アドレスを指定します。
- any
  グローバル IP アドレスの先頭アドレスとして IPCP ネゴシエーションの結果を使用します。

<addr_number>

- グローバル IP アドレスの個数
  動的アドレス変換に使用するグローバル IP アドレスの個数を、1〜16 の 10 進数値で指定します。
  <address>に any を指定した場合は、1 を指定してください。

<time>

- 割当時間
  割り当てられた変換テーブルを解放するための無通信監視時間を、0 秒〜86400 秒 (1 日) の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。
  0 秒を指定した場合は、変換テーブル解放のための監視を行いません。
  省略時は、5 分を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手ネットワークに対するアドレス変換 (NAT) の動作を設定します。

[未設定時]

アドレス変換は使用しないものとみなされます。

```
remote <number> ip nat mode off
```

7.4.22 remote ip nat static

[機能]

静的アドレス変換の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip nat static <count> <private_addr> <private_port> <global_addr> <global_port> [<protocol>]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 静的アドレス変換定義番号
  静的アドレス変換定義番号を、10 進数値で指定します。

範囲	機種
0〜499	Si-R570
0〜299	Si-R370
0〜199	Si-R260B Si-R240 Si-R220B
0〜63	Si-R180

<private_addr>

- プライベート IP アドレス
  静的アドレス変換の対象となるプライベート側の IP アドレスを指定します。

<private_port>

- プライベートポート番号
  静的アドレス変換の対象となるプライベート側のポート番号を、1〜65535 の 10 進数値で指定します。
  グローバルポート番号に複数ポート番号を指定した場合は、変換後の複数ポートの先頭ポート番号を指定します。
- any
  すべてのプライベートポート番号に対して有効な設定となります。

<global_addr>

- グローバル IP アドレス
  静的アドレス変換の対象となるグローバル側の IP アドレスを指定します。
  範囲指定する場合は、「172.16.0.2-172.16.0.254」のように"-"(ハイフン) を使用して指定します。なお、アドレスの範囲指定は一組だけ指定可能です。

- any

  remote ip nat mode コマンドで<address>に any を指定した場合は IPCP ネゴシエーションの結果をグローバル側の IP アドレスとして用います。

  remote ip nat mode コマンドで<address>に any 以外を指定した場合は指定したアドレスをグローバル側の IP アドレスとして用います。

<global_port>

- グローバルポート番号

  静的アドレス変換の対象となるグローバル側のポート番号を、1〜65535 の 10 進数値で指定します。

  範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。

  なお、ポート番号の範囲指定は一組だけ指定可能です。

- any

  すべてのグローバルポート番号に対して有効な設定となります。

<protocol>

- プロトコル番号

  静的アドレス変換の対象となるプロトコル番号を指定します。

  省略時は、any を指定したものとみなされます。

- any

  すべてのプロトコル番号に対して有効な設定となります。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手ネットワークに対する静的アドレス変換を設定します。
静的アドレス変換の対象となるパケットは、プロトコル番号<protocol>のプライベート側の IP アドレス <private_addr> とポート番号 <private_port>、グローバル側の IP アドレス<global_addr>とポート番号 <global_port>の指定内容により交換されます。
静的アドレス変換は、本装置全体で以下の数まで定義できます。

最大定義数	機種
500	Si-R570
300	Si-R370
200	Si-R260B　Si-R240　Si-R220B
64	Si-R180

[未設定時]

静的アドレス変換は設定されません。

7.4.23 remote ip nat static default

[機能]

テーブルに一致しないパケットの扱いの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip nat static default <action>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<action>

すべての NAT テーブルにも一致しなかったパケットをどう扱うかを指定します。

- pass
  該当するパケットの IP アドレスやポート番号を変換しないで透過させます。
- reject
  該当するパケットを破棄します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

すべての NAT テーブルに一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

すべての NAT テーブルにも一致しないパケットは破棄します。

```
remote <number> ip nat static default reject
```

7.4.24　remote ip nat rule

[機能]

アドレス変換ルールの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip nat rule <count> ftp <server_addr> <server_port> [<check>]
remote [<number>] ip nat rule <count> dns <server_addr> <server_port> [<check>]
remote [<number>] ip nat rule <count> irc <server_addr> <server_port>
remote [<number>] ip nat rule <count> sip <server_addr> <server_port>
remote [<number>] ip nat rule <count> mldt <server_addr> <server_port>
remote [<number>] ip nat rule <count> ipbs <server_addr> <server_port>
remote [<number>] ip nat rule <count> dch <server_addr> <server_port>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 変換ルール番号
  変換ルール番号を、0～31 の 10 進数値で指定します。

ftp, irc, dns, sip, mldt, ipbs, dch

変換ルールの対象となるアプリケーションを指定します。

<server_addr>

- IP アドレス
  NAT に割り当てたグローバルアドレス以外のアドレスを指定します。ここで指定したアドレスを変換ルールの対象とします。
- any
  すべての IP アドレスを変換ルールの対象とします。
  any を指定した場合は、グローバル側とプライベート側の両方のアプリケーションサーバに対応します。
- global
  NAT に割り当てたグローバルアドレス以外のすべてのアドレスを変換ルールの対象とします。
  global を指定した場合は、グローバル側のアプリケーションサーバに対応します。
- local
  NAT に割り当てたグローバルアドレスを変換ルールの対象とします。
  local を指定した場合は、プライベート側のアプリケーションサーバに対応します。
- off
  指定したアプリケーションに対する変換ルールを無効にします。

<server_port>

アプリケーションサーバで待ち受けるポート番号を指定します。

- ポート番号

  アプリケーションサーバで待ち受けるポート番号を、1〜65535 の 10 進数値で指定します。

  範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。

  なお、ポート番号の範囲指定は一組だけ指定可能です。

<check>

- on

  アプリケーションに ftp を指定した場合、ftp サーバのデータ転送用 IP アドレスおよびポート番号のチェックを行います。

  アプリケーションに dns を指定した場合、グローバル側にサーバが存在するときだけ有効となります。DNS の応答の UDP パケットのソース IP アドレスおよびソースポート番号が問い合わせの UDP パケットのディスティネーション IP アドレスおよびディスティネーションポート番号と同一かどうかチェックします。

  省略時は、on を指定したものとみなされます。

- off

  アプリケーションに ftp を指定した場合、ftp サーバのデータ転送用 IP アドレスおよびポート番号のチェックを行いません。

  アプリケーションに dns を指定した場合、IP アドレスおよびポート番号のチェックを行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手ネットワークに対するアドレス変換ルールを設定します。
指定 IP アドレス、指定ポート番号で動作する指定アプリケーションに対応するサーバに対するアドレス変換の特殊対応の設定を行います。
アドレス変換ルールは、本装置全体で 32 個まで定義できます。

[未設定時]

アドレス変換ルールは設定されません。

7.4.25　remote ip nat wellknown

[機能]

ポート番号変換の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip nat wellknown <count> <port> <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

ポート番号変換定義番号を、0～99 の 10 進数値で指定します。

<port>

- プライベートポート番号
  プライベートポート番号を、1～65535 の 10 進数値で指定します。
  範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。
  以下に、有効な記述形式を示します。
  - 1～65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
- any
  すべてのプライベートポート番号を対象とする場合に指定します。

<mode>

- on
  well-known ポート番号とみなし、変換を行いません。
- off
  well-known ポート番号とみなさず、変換を行います。

[動作モード]

構成定義モード (管理者クラス)

[説明]

プライベートポート番号の変換を行うかどうかの設定をします。プライベートポート番号がどの設定にもあてはまらない場合は、未設定時と同様にプライベートポート番号の変換を行います。
ポート番号変換の設定は本装置全体で 100 個まで定義できます。

[未設定時]

以下のポート番号についてはポート番号の変換を行いません。
1～1024(本来の well-known ポート番号) 28800～28830(Microsoft Internet Gaming Zone)

```
 1558(StreamWorks)
 8000(StreamWorks)
  118(Diablo)
  116(Diablo)
 6112(Battle.net)
 6799(NETSTORM)
 6800(NETSTORM)
 9000(HEAVY GEAR)
 7070(Real Player)
 7000(VDO Live Video)
 6667(IRC)
 7648(CU-SeeMe)
 7649(CU-SeeMe)
40027(SurfV)
40026(SurfV)
 1638(DARK REIGN)
```

7.4.26　remote ip nat destination

[機能]

あて先変換の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip nat destination <count> <private_addr> <global_addr>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- あて先変換定義番号
  あて先変換の優先度を表す番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜499	Si-R570
0〜299	Si-R370
0〜199	Si-R260B　Si-R240　Si-R220B
0〜63	Si-R180

<private_addr>

- プライベート IP アドレス
  あて先変換の対象となるプライベート側の IP アドレスを指定します。

<global_addr>

- グローバル IP アドレス
  あて先変換の対象となるグローバル側の IP アドレスを指定します。
  範囲指定する場合は、「172.16.0.2-172.16.0.254」のように"-"(ハイフン) を使用して指定します。なお、アドレスの範囲指定は一組だけ指定可能です。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手ネットワークに対するあて先変換を設定します。
あて先変換の対象となるパケットは、プライベート側の IP アドレス<private_addr> とグローバル側の IP アドレス<global_addr>の指定内容により交換されます。
あて先変換は、本装置全体で以下の数まで定義できます。

最大定義数	機種
500	Si-R570
300	Si-R370
200	Si-R260B　Si-R240　Si-R220B
64	Si-R180

[未設定時]

あて先変換は設定されません。

7.4.27　remote ip nat appli

[機能]

アプリ対応の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip nat appli <function> <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<function>

設定する機能を指定します。

- ftp
  FTP に対する設定を行います。
- sip
  SIP に対する設定を行います。
- h323
  H.323 に対する設定を行います。
- dns
  DNS に対する設定を行います。
- snmp
  SNMP Trap に対する設定を行います。
- irc
  IRC に対する設定を行います。
- ntdomain
  NT ドメインログオンに対する設定を行います。
- stream
  各種ストリーミングに対する設定を行います。
  CU-SeeMe、RealPlayer、VDO Live、Stream Works、SurfV が含まれます。
- game
  各種オンラインゲームに対する設定を行います。
  DIABLO(Battle.net)、NETSTORM、信長の野望 (KOEI)、AGE of EMPIRES が含まれます。

<mode>

- on
  アプリ対応を有効にします。
- off
  アプリ対応を無効にします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

各アプリケーションに対する特殊対応を有効にするかどうかを設定します。

[注意]

このコマンドは、アプリケーションに対するデフォルトの特殊対応動作を設定するものです。
ここで機能を無効に設定した場合でも、rule コマンドで指定されたものは有効になります。

[未設定時]

すべてのアプリ対応を有効にするとみなされます。

```
remote <number> ip nat appli ftp on
remote <number> ip nat appli sip on
remote <number> ip nat appli h323 on
remote <number> ip nat appli dns on
remote <number> ip nat appli snmp on
remote <number> ip nat appli irc on
remote <number> ip nat appli ntdomain on
remote <number> ip nat appli stream on
remote <number> ip nat appli game on
```

7.4.28　remote ip filter

[機能]

IP フィルタの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip filter <count> <action> acl <acl_count> [<direction>]
remote [<number>] ip filter <count> <action> <src_addr>/<mask> <src_port> <dst_addr>/<mask> <dst_port> <protocol> <tcpconnect> [<tos> [<direction> [<icmptype> [<icmpcode>]]]]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す番号を、10 進数値で指定します。
  指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つフィルタリング定義がすでに存在する場合は、既存の定義を変更します。

範囲	機種
0〜999	Si-R570　Si-R370
0〜199	Si-R260B　Si-R240　Si-R220B
0〜63	Si-R180

<action>

フィルタリング対象に該当するパケットを透過するかどうかを設定します。

- pass
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。
- restrict
  該当するパケットを、回線が接続されていれば透過し、切断されていれば遮断します。

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、そのフィルタ定義は無効となり、無視されます。
  IP フィルタでは、ACL の以下の定義を使用します。
  - ip
    ip 値が設定されていない場合、そのフィルタ定義は無効となり、無視されます。

- tcp

  ip の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。

- udp

  ip の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp

  ip の<protocol>値が 1 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip の<protocol>値が 1 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B Si-R240 Si-R220B
0〜149	Si-R180

<src_addr>/<mask>

フィルタリング対象とする送信元 IP アドレスとマスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)

  フィルタリング対象とする送信元 IP アドレスとマスクビット数の組み合わせを指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。

  以下に、有効な記述形式を示します。

  - IP アドレス/マスクビット数 (例: 192.168.1.1/24)
  - IP アドレス/マスク値 (例: 192.168.1.1/255.255.255.0)

- any

  すべての送信元 IP アドレスをフィルタリング対象とする場合に指定します。

  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<src_port>

フィルタリング対象とする送信元ポート番号を指定します。

- ポート番号

  フィルタリング対象とする送信元ポート番号を、1〜65535 の 10 進数値で指定します。

  複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、

  <dst_port>合わせて 10 個まで指定できます。

  以下に、有効な記述形式を示します。

  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)

- ポート番号- (例: 1- = 1 から 65535 までのポート)
- -ポート番号 (例: -1000 = 1 から 1000 までのポート)
- ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)

- any
  すべての送信元ポート番号をフィルタリング対象とする場合に指定します。

<dst_addr>/<mask>

フィルタリング対象とするあて先 IP アドレスとマスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  フィルタリング対象とするあて先 IP アドレスとマスクビット数の組み合わせを指定します。
  記述形式は、<src_addr>/<mask>と同様です。
- any
  すべてのあて先 IP アドレスをフィルタリング対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<dst_port>

フィルタリング対象とするあて先ポート番号を指定します。

- ポート番号
  フィルタリング対象とするあて先ポート番号を、1～65535 の 10 進数値で指定します。
  記述形式は、<src_port>と同様です。
- any
  すべてのあて先ポート番号をフィルタリング対象とする場合に指定します。

<protocol>

フィルタリング対象とするプロトコル番号を指定します。

- プロトコル番号
  フィルタリング対象とするプロトコル番号を、1～255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号をフィルタリング対象とする場合に指定します。

<tcpconnect>

- yes
  TCP プロトコルでコネクション接続要求をフィルタリング対象に含めます。
- no
  TCP プロトコルでコネクション接続要求をフィルタリング対象に含めません。

<tos>

フィルタリング対象とする TOS 値を指定します。
省略時は、any を指定したものとみなされます。

- TOS 値
  フィルタリング対象とする TOS 値を、0～ff の 16 進数値で指定します。
  複数の TOS 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。TOS 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。

- 00～ff の 16 進数値 (例: ff = ff の TOS 値)
- TOS 値-TOS 値 (例: 32-64 = 32 から 64 までの TOS 値)
- TOS 値- (例: 80- = 80 から ff までの TOS 値)
- -TOS 値 (例: -7f = 0 から 7f までの TOS 値)
- TOS 値,TOS 値,… (例: 10,20,30- = 10 と 20 と 30 以降の TOS 値)

- any
  すべての TOS 値をフィルタリング対象とする場合に指定します。

<direction>

フィルタリングする方向を指定します。
省略時は、any を指定したものとみなされます。

- any
  入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。
- in
  入力パケットだけをフィルタリング対象とする場合に指定します。
- out
  出力パケットだけをフィルタリング対象とする場合に指定します。
- reverse
  入力パケットと出力パケットの両方をフィルタリング対象とします。
  ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。
  - 送信元 IP アドレス/マスクとあて先 IP アドレス/マスク
  - 送信元ポート番号とあて先ポート番号

<icmptype>

フィルタリング対象とする ICMP TYPE を指定します。

- ICMP TYPE
  フィルタリング対象とする送信元 ICMP TYPE を、0～255 の 10 進数値で指定します。
  複数の ICMP TYPE を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「8-30」のように"-"(ハイフン) を使用して指定します。
  ICMP TYPE は、","(カンマ) および"-"(ハイフン) を使用して、10 個まで指定できます。以下に、有効な記述形式を示します。
  - 0～255 の 10 進数値 (例: 8 = ICMP TYPE 8)
  - ICMP TYPE-ICMP TYPE (例: 2-8 = 2 から 8 までの ICMP TYPE)
  - ICMP TYPE- (例: 8- = 8 から 255 までの ICMP TYPE)
  - -ICMP TYPE (例: -200 = 0 から 200 までの ICMP TYPE)
  - ICMP TYPE,ICMP TYPE,… (例: 0,8,30- = 0 と 8 と 30 以降の ICMP TYPE)
- any
  すべての ICMP TYPE をフィルタリング対象とする場合に指定します。

<icmpcode>

フィルタリング対象とする ICMP CODE を指定します。

- ICMP CODE

  フィルタリング対象とする送信元 ICMP CODE を、0〜255 の 10 進数値で指定します。

  複数の ICMP CODE を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「8-30」のように"-"(ハイフン) を使用して指定します。

  ICMP CODE は、","(カンマ) および"-"(ハイフン) を使用して、10 個まで指定できます。

  以下に、有効な記述形式を示します。

  - 0〜255 の 10 進数値 (例: 8 = ICMP CODE 8)
  - ICMP CODE-ICMP CODE (例: 2-8 = 2 から 8 までの ICMP CODE)
  - ICMP CODE- (例: 8- = 8 から 255 までの ICMP CODE)
  - -ICMP CODE (例: -200 = 0 から 200 までの ICMP CODE)
  - ICMP CODE,ICMP CODE,… (例: 0,8,30- = 0 と 8 と 30 以降の ICMP CODE)

- any

  すべての ICMP CODE をフィルタリング対象とする場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手ネットワークに対する IP フィルタを設定します。
IP フィルタは、指定したアドレス、ポート番号、プロトコル、TOS 値と ICMP TYPE, ICMP CODE と一致するパケットを透過または遮断します。設定した優先度順に一致するか調べ、一致した時点でフィルタリングされ、それ以降の設定は参照されません。
IP フィルタリングの旧定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
1000	Si-R570　Si-R370
200	Si-R260B　Si-R240　Si-R220B
64	Si-R180

また、ACL 参照定義は、ほかの ACL 参照定義 (IP フィルタ、帯域制御 (WFQ) など) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B　Si-R240　Si-R220B
450	Si-R180

旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

[注意]

<direction>に reverse を指定した場合は、入力パケットは IP アドレス/マスクとポート番号だけを逆転した条件でフィルタリングされます。このため、<tcpconnect>を有効にしている場合は、入力パケットに対しても、TCP プロトコルのコネクション接続要求がフィルタリング対象に含まれます。

[未設定時]

IP フィルタを設定しないものとみなされ、すべてのパケットが透過します。

7.4.29　remote ip filter move

[機能]

IP フィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip filter move <count> <new_count>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義の番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0〜999	Si-R570　Si-R370
0〜199	Si-R260B　Si-R240　Si-R220B
0〜63	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

IP フィルタの優先順序を変更します。
旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

7.4.30 remote ip filter default

[機能]

どの IP フィルタテーブルにも不一致時の動作の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip filter default <action> [<time>]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<action>

どの IP フィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- pass
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。
- restrict
  該当するパケットを、回線が接続されていれば透過し、切断されていれば遮断します。
- spi
  該当するパケットに対して SPI を動作させます。

<time>

- 割当時間
  action に spi を指定したときに、接続に割り当てられたテーブルを解放するための無通信監視時間を、0 秒〜86400 秒 (1 日) の範囲で指定します。単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。
  0 秒を指定した場合は、変換テーブル解放のための監視を行いません。
  省略時は、5 分を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

どの IP フィルタテーブルに一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

どの IP フィルタテーブルにも一致しないパケットは透過します。

```
remote <number> ip filter default pass
```

7.4.31　remote ip tos

[機能]

TOS 値書き換え条件の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip tos <count> acl <acl_count> <new_tos>
remote [<number>] ip tos <count> <src_addr>/<mask> <src_port> <dst_addr>/<mask> <dst_port> <protocol> <tos> <new_tos>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- TOS 値書き換え定義番号
  TOS 値書き換え条件の優先度を表す定義番号を、10 進数値で指定します。
  指定した値は、設定完了時に順方向にソートされてリナンバリングされます。
  また、指定した定義番号と同じ値を持つ TOS 値書き換え定義がすでに存在する場合は、既存定義の値を変更します。

範囲	機種
0〜499	Si-R570　Si-R370
0〜99	Si-R260B　Si-R240　Si-R220B
0〜31	Si-R180

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、その TOS 値書き換え定義は無効となり、無視されます。
  TOS 値書き換えでは、ACL の以下の定義を使用します。
  - ip
    ip 値が設定されていない場合、その TOS 値書き換え定義は無効となり、無視されます。
  - tcp
    ip の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。

- udp

  ip の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp

  ip の<protocol>値が 1 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip の<protocol>値が 1 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B Si-R240 Si-R220B
0〜149	Si-R180

<src_addr>/<mask>

- IP アドレス/マスクビット数 (またはマスク値)

  TOS 値書き換え対象となる送信元 IP アドレスとマスクビット数の組み合わせを指定します。マスク値は最上位ビットから 1 で連続した値にしてください。

  以下に、有効な記述形式を示します。

  - IP アドレス/マスクビット数 (例: 192.168.1.1/24)
  - IP アドレス/マスク値 (例: 192.168.1.1/255.255.255.0)

- any

  すべての送信元 IP アドレスを TOS 値書き換えの対象とする場合に指定します。

  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<src_port>

TOS 値書き換え対象となる送信元ポート番号を指定します。

- ポート番号

  TOS 値書き換え対象となる送信元ポート番号を、1〜65535 の 10 進数値で指定します。複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、

  <dst_port>合わせて 10 個まで指定できます。

  以下に、有効な記述形式を示します。

  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)

- any

  すべてのポート番号を対象とする場合に指定します。

<dst_addr>/<mask>

TOS 値書き換え対象となるあて先 IP アドレス、マスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  TOS 値書き換え対象となるあて先 IP アドレスとマスクビット数の組み合わせを指定します。
  記述形式は、<src_addr>/<mask>と同様です。
- any
  すべてのあて先 IP アドレスを TOS 値書き換えの対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<dst_port>

TOS 値書き換え対象となるあて先ポート番号を指定します。

- ポート番号
  TOS 値書き換え対象となるあて先ポート番号を、1～65535 の 10 進数値で指定します。
  記述形式は、<src_port>と同様です。
- any
  すべてのポート番号を対象とする場合に指定します。

<protocol>

TOS 値書き換え対象となるプロトコル番号を指定します。

- プロトコル番号
  TOS 値書き換え対象となるプロトコル番号を、1～255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号を TOS 値書き換え対象とする場合に指定します。

<tos>

- TOS 値
  書き換え対象となる TOS 値を、0～ff の 16 進数値で指定します。
  複数の TOS 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。
  TOS 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 00～ff の 16 進数値 (例: ff = ff の TOS 値)
  - TOS 値-TOS 値 (例: 32-64 = 32 から 64 までの TOS 値)
  - TOS 値- (例: 80- = 80 から ff までの TOS 値)
  - -TOS 値 (例: -7f = 0 から 7f までの TOS 値)
  - TOS 値,TOS 値,… (例: 10,20,30- = 10 と 20 と 30 以降の TOS 値)
- any
  すべての TOS 値を、TOS 値書き換えの対象とする場合に指定します。

<new_tos>

- TOS 値
  書き換える TOS 値を、0～ff の 16 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

TOS 値書き換え条件を設定します。
条件に一致したパケットの TOS 値を、指定した TOS 値に書き換えます。
TOS 値書き換えの旧定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
500	Si-R570 Si-R370
100	Si-R260B Si-R240 Si-R220B
32	Si-R180

また、ACL 参照定義は、ほかの ACL 参照定義 (IP フィルタ、帯域制御 (WFQ) など) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B Si-R240 Si-R220B
450	Si-R180

旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

[未設定時]

TOS 値書き換えを行わないものとみなされます。

7.4.32　remote ip tos move

[機能]

TOS 値書き換え条件の優先度の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip tos move <count> <new_count>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象 TOS 値書き換え定義番号
  優先順序を変更する前の TOS 値書き換え定義番号を指定します。

<new_count>

- 移動先 TOS 値書き換え定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0～499	Si-R570　Si-R370
0～99	Si-R260B　Si-R240　Si-R220B
0～31	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

TOS 値書き換え条件の優先度を変更します。
旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

7.4.33 remote ip priority

[機能]

帯域制御の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip priority <count> acl <acl_count> <width>
remote [<number>] ip priority <count> <src_addr>/<mask> <src_port> <dst_addr>/<mask> <dst_port> <protocol> <tos> <width>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 帯域制御定義番号
  帯域制御定義番号を、10 進数値で指定します。

範囲	機種
0～999	Si-R570
0～499	Si-R370
0～99	Si-R260B Si-R240 Si-R220B
0～63	Si-R180

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、その定義は無効となり、無視されます。
  帯域制御では、ACL の以下の定義を使用します。

  - ip
    ip 値が設定されていない場合、その定義は無効となり、無視されます。
  - tcp
    ip の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。
  - udp
    ip の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp
  ip の<protocol>値が 1 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 1 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B　Si-R240　Si-R220B
0〜149	Si-R180

<src_addr>/<mask>

帯域制御の対象となる送信元 IP アドレス、マスクビット数を指定します。

- 送信元 IP アドレス/マスクビット数 (またはマスク値)
  帯域制御の対象となる送信元 IP アドレスとマスクビット数の組み合わせを指定します。
  マスク値は、最上位ビットから 1 で連続した値にしてください。
  以下に、有効な記述形式を示します。
  - IP アドレス/マスクビット数 (例: 192.168.1.1/24)
  - IP アドレス/マスク値 (例: 192.168.1.1/255.255.255.0)
- any
  すべての IP アドレスを帯域制御の対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<src_port>

帯域制御の対象となる送信元ポート番号を指定します。

- ポート番号
  帯域制御の対象となる送信元ポート番号を、1〜65535 の 10 進数値で指定します。
  複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。
  ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)
- any
  すべてのポート番号を対象とする場合に指定します。

<dst_addr>/<mask>

帯域制御の対象となるあて先 IP アドレス、マスクビット数を指定します。

- あて先 IP アドレス/マスクビット数 (またはマスク値)
  帯域制御の対象となるあて先 IP アドレスとマスクビット数の組み合わせを指定します。
  記述形式は<src_addr>/<mask>と同様です。
- any
  すべての IP アドレスを帯域制御の対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<dst_port>

帯域制御の対象となるあて先ポート番号を指定します。

- ポート番号
  帯域制御の対象となるあて先ポート番号を、1～65535 の 10 進数値で指定します。
  記述形式は<src_port>と同様です。
- any
  すべてのポート番号を対象とする場合に指定します。

<protocol>

帯域制御の対象となるプロトコル番号を指定します。

- プロトコル番号
  帯域制御の対象となるプロトコル番号を、1～255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号を帯域制御の対象とする場合に指定します。

<tos>

- TOS 値
  帯域制御の対象となる TOS 値を、0～ff の 16 進数値で指定します。
  複数の TOS 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。
  TOS 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 00～ff の 16 進数値 (例: ff = ff の TOS 値)
  - TOS 値-TOS 値 (例: 32-64 = 32 から 64 までの TOS 値)
  - TOS 値- (例: 80- = 80 から ff までの TOS 値)
  - -TOS 値 (例: -7f = 0 から 7f までの TOS 値)
  - TOS 値,TOS 値,… (例: 10,20,30- = 10 と 20 と 30 以降の TOS 値)
- any
  すべての TOS 値を、帯域制御の対象とする場合に指定します。

<width>

- express
  最優先データとして扱います。
- besteffort
  非優先 (ベストエフォート) として扱います。
- 帯域
  1〜99 の 10 進数値で指定した場合、それぞれ指定した値の比で帯域を割り当てます。たとえば、同じ相手ネットワーク中の定義が 3 つあり、それぞれ<width>の値が 30、30、60 であった場合、帯域として 25%、25%、50%が割り当てられます。なお、1〜99 を指定した定義のそれぞれの合計値が 100 未満の場合、残った帯域は定義に一致しないデータ用の帯域となります。
  「数字 + "kbps"(,"mbps")」で指定した場合、指定した帯域をそのまま割り当てます。1kbps〜100000kbps または、1mbps〜100mbps の範囲で指定します。全定義の帯域の
  合計が回線速度を超えた場合は、それぞれ指定した値の比で帯域を割り当てます。
  指定した値の合計値が回線速度に達しない場合、残った帯域は定義に一致しないデータ用の帯域となります。
  「"share" + 数字」で指定した場合、数字で指定した帯域制御定義番号で定義された帯域を共有します。この場合、指定する数字は自分自身の帯域制御定義番号より小さい、すでに定義されてあるもの指定しなければなりません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

帯域制御を設定します。任意のプロトコル、アドレス、ポート、TOS 値を指定して、割り当てる帯域を指定します。
帯域制御の旧定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
1000	Si-R570
500	Si-R370
100	Si-R260B　Si-R240　Si-R220B
64	Si-R180

また、ACL 参照定義は、ほかの ACL 参照定義 (IP フィルタ、帯域制御 (WFQ) など) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B　Si-R240　Si-R220B
450	Si-R180

旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

[注意]

使用する回線が LAN の場合、シェーピングを使用しないと帯域制御機能は有効に動作しません。
使用する回線が ATM の場合、適切な VC 速度を設定しないと帯域制御機能は有効に動作しません。

[未設定時]

帯域制御を行わないものとみなされます。

7.4.34　remote ip clp

[機能]

IPv4 CLP 値の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B

[入力形式]

remote [<number>] ip clp <count> <mode> acl <acl_count>
remote [<number>] ip clp <count> <mode> <src_addr>/<mask> <src_port> <dst_addr>/<mask> <dst_port> <protocol> [<tos>]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- CLP 値設定条件定義番号
  CLP 値設定の優先度を表す番号を、10 進数値で指定します。
  指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つ CLP 値設定条件定義がすでに存在する場合は、既存の定義を変更します。

範囲	機種
0～1999	Si-R570
0～99	Si-R370　Si-R260B

<mode>

- on
  条件と一致する場合に、CLP 値を 1 に設定します。
- off
  条件と一致する場合に、CLP 値を 0 に設定します。

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。指定した<acl_count>の ACL が定義されていない場合、その CLP 値設定定義は無効となり、無視されます。
  CLP 値設定では、ACL の以下の定義を使用します。
  - ip
    ip 値が設定されていない場合、そのフィルタ定義は無効となり、無視されます。
  - tcp
    ip の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。

- udp

  ip の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp

  ip の<protocol>値が 1 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip の<protocol>値が 1 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B

<src_addr>/<mask>

CLP 値設定対象となる送信元 IP アドレス、マスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)

  CLP 値設定対象となる送信元 IP アドレスとマスクビット数の組み合わせを指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。

  以下に、有効な記述形式を示します。

  - IP アドレス/マスクビット数 (例: 192.168.1.1/24)
  - IP アドレス/マスク値 (例: 192.168.1.1/255.255.255.0)

- any

  すべての IP アドレスを対象とする場合に指定します。

  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<src_port>

CLP 値設定対象となる送信元ポート番号を指定します。

- ポート番号

  CLP 値設定対象となる送信元ポート番号を、1〜65535 の 10 進数値で指定します。

  複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。

  以下に、有効な記述形式を示します。

  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)

- any

  すべてのポート番号を対象とする場合に指定します。

<dst_addr>/<mask>

CLP 値設定対象となる送信先 IP アドレス、マスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  CLP 値設定対象となる送信先 IP アドレスとマスクビット数の組み合わせを指定します。
  記述形式は、<src_addr>/<mask>と同様です。
- any
  すべての IP アドレスを対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<dst_port>

CLP 値設定対象となる送信先ポート番号を指定します。

- ポート番号
  CLP 値設定対象となる送信先ポート番号を、1～65535 の 10 進数値で指定します。
  記述形式は、<src_port>と同様です。
- any
  すべてのポート番号を対象とする場合に指定します。

<protocol>

CLP 値設定対象となるプロトコル番号を指定します。

- プロトコル番号
  CLP 値設定対象となるプロトコル番号を、1～255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号を CLP 値設定対象とする場合に指定します。

<tos>

CLP 値書き換え対象となる TOS 値を指定します。
省略時は、any を指定したものとみなされます。

- TOS 値
  CLP 値設定対象の TOS 値を、0～ff の 16 進数値で指定します。
  複数の TOS 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、"-"(ハイフン) を使用して指定します。
  TOS 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 00～ff の 16 進数値 (例: ff = ff の TOS 値)
  - TOS 値-TOS 値 (例: 32-64 = 32 から 64 までの TOS 値)
  - TOS 値- (例: 80- = 80 から ff までの TOS 値)
  - -TOS 値 (例: -7f = 0 から 7f までの TOS 値)
  - TOS 値,TOS 値,… (例: 10,20,30- = 10 と 20 と 30 以降の TOS 値)
- any
  すべての TOS 値を対象とする場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手ネットワークに対する CLP 値設定条件を設定します。
CLP 値設定条件は、IPv4 の旧定義は本装置全体で以下の数まで定義できます。

最大定義数	機種
2000	Si-R570
100	Si-R370　Si-R260B

また、ACL 参照定義はほかの ACL 参照定義 (IP フィルタなど) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B

[注意]

ATM にだけ有効です。
また、従来定義と ACL 定義が混在した場合は、ACL 定義から並べ替えられます。

[未設定時]

IPv4 CLP 値設定は行わないとみなされます。
また、CLP 値設定を行わない場合は、常に CLP 値は 0 となります。

7.4.35　remote ip clp move

[機能]

IPv4 CLP 値設定条件優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B

[入力形式]

remote [<number>] ip clp move <count> <new_count>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象 CLP 値設定条件定義番号
  優先順序を変更する CLP 値設定条件定義の番号を指定します。

<new_count>

- 移動先 CLP 値設定条件定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0～1999	Si-R570
0～99	Si-R370　Si-R260B

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv4 CLP 値設定条件優先順序を変更します。
また、従来定義と ACL 定義が混在した場合は、ACL 定義から並べ替えられます。

7.4.36 remote ip in-policy

[機能]

Ingress ポリシールーティングの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip in-policy <in-policy_number> policy-group <policy-group_number>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<in-policy_number>

- Ingress ポリシールーティング定義番号
  この I/F での Ingress ポリシールーティング定義の通し番号を、10 進数値で指定します。
  本定義は、ほかのポリシーグループ参照定義を含めて本装置全体で
  以下の数まで定義できます。

最大定義数	機種
2000	Si-R570
1000	Si-R370
200	Si-R260B Si-R240 Si-R220B
100	Si-R180

<policy-group_number>

- ポリシーグループ番号
  参照するポリシーグループ番号を、10 進数値で指定します。
  IPv4 Ingress ポリシールーティングでは、ポリシーグループで指定された ACL の以下の定義を使用します。

  - ip
    ip 値が設定されていない場合、その定義は無効となり、無視されます。
  - tcp
    ip の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。
  - udp
    ip の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp

  ip の<protocol>値が 1 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip の<protocol>値が 1 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B　Si-R220B
0〜49	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

Ingress ポリシールーティングに使用するポリシーグループを指定します。

[注意]

Ingress ポリシールーティングを行う場合は、必ずポリシーグループ指定を行う必要があります。
また、定義されている全ポリシーグループと不一致の場合は、アドレスによる経路探索が行われます。

[未設定時]

Ingress ポリシールーティングを設定しないとみなされます。

7.4.37 remote ip in-policy move

[機能]

Ingress ポリシールーティングの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip in-policy move <count> <new_count>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象 Ingress ポリシールーティング定義番号
  優先順序を変更するフィルタリング定義の番号を指定します。

<new_count>

- 移動先 Ingress ポリシールーティング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

Ingress ポリシールーティングの優先順序を変更します。

7.4.38　remote ip msschange

[機能]

MSS 書き換えの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip msschange <mss>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mss>

- MSS 値
  MSS の書き換え値を、0 または 160～1460 の 10 進数値で指定します。
  0 を指定した場合は、MSS を書き換えません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

MSS 書き換え機能を利用する場合の、書き換え値を設定します。

[未設定時]

MSS 書き換え機能を利用しないものとみなされます。

```
remote <number> ip msschange 0
```

7.4.39 remote ip multicast mode

[機能]

マルチキャストインタフェースの定義

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip multicast mode <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

マルチキャスト定義の動作を指定します。

- off
  マルチキャストパケットを中継しません。
- static
  スタティックルーティングのみで動作します。
- pimdm
  PIM-DM として動作します。
- pimsm
  PIM-SM として動作します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

<number>で指定したインタフェースのマルチキャスト・ルーティングプロトコルを有効化し、マルチキャストパケットを中継します。

[注意]

複数インタフェースで異なるプロトコルが選択された場合は、最初に見つかったインタフェースのプロトコルが有効になります。

[未設定時]

マルチキャストパケットを中継しません。

```
remote <number> ip multicast mode off
```

7.4.40　remote ip multicast ttl threshold

[機能]

マルチキャストインタフェースの TTL しきい値の定義

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip multicast ttl threshold <threshold>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<threshold>

- TTL しきい値
  マルチキャストパケットを中継するインタフェースの TTL の
  しきい値を 1～255 の 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

TTL が<threshold>で指定したしきい値以上のマルチキャストパケットだけ中継します。

[注意]

PIM-SM の PIM Register パケットによりカプセル化されるマルチキャスト・パケットは、出力先インタフェースの TTL しきい値の設定によらずに出力されます。

[未設定時]

1 になります。

```
remote <number> ip multicast ttl threshold 1
```

7.4.41 remote ip multicast pim preference

[機能]

マルチキャストインタフェースの PIM プリファレンス値の定義

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip multicast pim preference <preference>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<preference>

- プリファレンス値
  マルチキャストパケットを中継するインタフェースの PIM プリファレンス値を 1〜65535 の 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

マルチキャスト・パケットの配送経路が重複したばあいには、プリファレンス値の小さい経路で配送されます。

[注意]

PIM Assert 発行時には Assert 対象となるパケットの発信元へのユニキャスト経路を参照し、発信元へ向かうインタフェースのプリファレンス値を Assert メッセージに格納します。Assert メッセージが出力されるインタフェースのプリファレンス値が格納されるわけではありません。

[未設定時]

1024 になります。

```
remote <number> ip multicast pim preference 1024
```

7.4.42　remote ip multicast pim upstream type

[機能]

上流ルータの種類によるマルチキャストパケット転送許可設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip multicast pim upstream type <type>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<type>

- pim
  上流ルータが PIM ルータのときだけ、マルチキャストパケットを転送します。
- any
  上流ルータが PIM ルータでない場合でも、マルチキャストパケットを転送します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本装置より上流にルータが存在し、そのルータを経由してマルチキャストパケットが転送されてくる場合、どの種類のルータからのマルチキャストパケット転送を許可するかを指定します。
上流ルータが PIM ルータでない場合 (マルチキャストパケットをスタティック経路によって転送するルータであった場合) に転送を許可したい場合は <type> に any を指定することで転送を可能にします。

[注意]

受信インタフェースと同一の IP セグメントから送信された (直接接続されたホストからの) マルチキャストパケットについては、本コマンドの指定にかかわらず転送が行われます。

[未設定時]

上流ルータが PIM ルータのときだけ、マルチキャストパケットを転送します。

```
remote <number> ip multicast pim upstream type pim
```

7.4.43 remote ip dvpn

[機能]

動的 VPN の接続契機となる IPv4 パケットの検出条件の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip dvpn <count> invite acl <acl_count> <invite_mask> <template_number>
remote [<number>] ip dvpn <count> ignore acl <acl_count>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 接続契機条件定義番号
  接続契機条件の優先度を表す番号を、10 進数値で指定します。
  指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つ接続契機条件定義がすでに存在する場合は、既存の定義を変更します。

範囲	機種
0〜9000	Si-R570
0〜4500	Si-R370
0〜900	Si-R260B Si-R240 Si-R220B
0〜450	Si-R180

invite

条件に一致した場合に接続要求を発行します。

ignore

条件に一致した場合に接続要求を発行しません。

<acl_count>

- ACL 定義番号
  接続契機パケットを検出するための ACL 定義番号を指定します。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B Si-R240 Si-R220B
0〜149	Si-R180

<invite_mask>

接続要求を発行する際の相手ネットワークマスクビット数を、0～32 の 10 数数値で指定します。

<template_number>

動的 VPN 接続に利用するテンプレート定義の定義番号を指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN 接続を利用する場合の、接続契機 IPv4 パケットの検出条件を設定します。

[未設定時]

すべての IPv4 パケットを動的 VPN 接続契機としません。

7.4.44 remote ip dvpn move

[機能]

動的 VPN の接続契機検出条件の優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip dvpn move <count> <new_count>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 接続契機条件定義番号
  優先順序を変更する接続契機条件定義の番号を指定します。

<new_count>

- 移動先接続契機条件定義番号
  <count>に対する新しい順序を 10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0〜9000	Si-R570
0〜4500	Si-R370
0〜900	Si-R260B Si-R240 Si-R220B
0〜450	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN 接続契機パケット検出条件の優先順序の変更します。

7.4.45　remote ip exp

[機能]

Exp 値書き換え条件の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip exp <count> acl <acl_count> <exp>
remote [<number>] ip exp <count> <src_addr>/<mask> <src_port> <dst_addr>/<mask> <dst_port> <protocol> <tos> <exp>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- Exp 書き換え条件定義番号
  Exp 書き換えの優先度を表す番号を、10 進数値で指定します。
  指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つ Exp 書き換え条件定義がすでに存在する場合は、既存の定義を変更します。

範囲	機種
0～499	Si-R570　Si-R370
0～99	Si-R260B　Si-R240　Si-R220B
0～31	Si-R180

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。

範囲	機種
0～2999	Si-R570
0～1499	Si-R370
0～299	Si-R260B　Si-R240　Si-R220B
0～149	Si-R180

<src_addr>/<mask>

Exp 値書き換え対象となる送信元 IP アドレス、マスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  Exp 値書き換え対象となる送信元 IP アドレスとマスクビット数の組み合わせを指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。
  以下に、有効な記述形式を示します。
  - IP アドレス/マスクビット数 (例: 192.168.1.1/24)
  - IP アドレス/マスク値 (例: 192.168.1.1/255.255.255.0)
- any
  すべての IP アドレスを対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<src_port>

Exp 値書き換え対象となる送信元ポート番号を指定します。

- ポート番号
  Exp 値書き換え対象となる送信元ポート番号を、1〜65535 の 10 進数値で指定します。
  複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、
  <dst_port>合わせて 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)
- any
  すべてのポート番号を対象とする場合に指定します。

<dst_addr>/<mask>

Exp 値書き換え対象となる送信先 IP アドレス、マスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  Exp 値書き換え対象となる送信先 IP アドレスとマスクビット数の組み合わせを指定します。
  記述形式は、<src_addr>/<mask>と同様です。
- any
  すべての IP アドレスを対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<dst_port>

Exp 値書き換え対象となる送信先ポート番号を指定します。

- ポート番号
  Exp 値書き換え対象となる送信先ポート番号を、1〜65535 の 10 進数値で指定します。
  記述形式は、<src_port>と同様です。
- any
  すべてのポート番号を対象とする場合に指定します。

<protocol>

Exp 値書き換え対象となるプロトコル番号を指定します。

- プロトコル番号

  Exp 値書き換え対象となるプロトコル番号を、1〜255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。

- any

  すべてのプロトコル番号を Exp 値書き換え対象とする場合に指定します。

<tos>

Exp 値書き換え対象となる TOS 値を指定します。

- TOS 値

  Exp 値書き換え対象の TOS 値を、0〜ff の 16 進数値で指定します。

  複数の TOS 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、"-"(ハイフン) を使用して指定します。

  TOS 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。

  以下に、有効な記述形式を示します。

  - 00〜ff の 16 進数値 (例: ff = ff の TOS 値)
  - TOS 値-TOS 値 (例: 32-64 = 32 から 64 までの TOS 値)
  - TOS 値- (例: 80- = 80 から ff までの TOS 値)
  - -TOS 値 (例: -7f = 0 から 7f までの TOS 値)
  - TOS 値,TOS 値,… (例: 10,20,30- = 10 と 20 と 30 以降の TOS 値)

- any

  すべての TOS 値を対象とする場合に指定します。

<exp>

- Exp 値

  書き換える Exp 値を、0〜7 の 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手ネットワークに対する Exp 書き換え条件を設定します。
Exp 書き換え条件の旧定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
500	Si-R570　Si-R370
100	Si-R260B　Si-R240　Si-R220B
32	Si-R180

また、ACL 参照定義は、ほかの ACL 参照定義 (IP フィルタ、帯域制御 (WFQ) など) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B　Si-R240　Si-R220B
450	Si-R180

旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

[注意]

remote ap datalink type mpls の ap を使用する場合にだけ有効です。

[未設定時]

Exp 値書き換えは行わないとみなされます。

7.4.46　remote ip exp move

[機能]

Exp 値書き換え条件優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip exp move <count> <new_count>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象 Exp 書き換え条件定義番号
  優先順序を変更する Exp 書き換え条件定義の番号を指定します。

<new_count>

- 移動先 Exp 書き換え条件定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0～499	Si-R570　Si-R370
0～99	Si-R260B　Si-R240　Si-R220B
0～31	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

Exp 値を書き換えの条件優先順序を変更します。
旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

7.4.47 remote ip ids use

[機能]

IDS の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip ids use <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- off
  IDS を利用しません。
- on
  IDS を利用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

このインタフェースで、IPv4 パケットに対して IDS を利用するかどうかを設定します。

[注意]

なし

[未設定時]

IPv4 パケットに対して IDS を利用しないものとみなされます。

```
remote <number> ip ids use off
```

7.5　IPv6 関連情報

7.5.1　remote ip6 use

[機能]

IPv6 機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 use <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

IPv6 パケットの送受信を行うかどうか指定します。

- on
  このインタフェースで、IPv6 パケットの送受信を行います。
- off
  このインタフェースで、IPv6 パケットの送受信を行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

このインタフェースで、IPv6 機能を利用するかどうかを設定します。

[未設定時]

IPv6 機能を利用しないものとみなされます。

```
remote <number> ip6 use off
```

7.5.2 remote ip6 ifid

[機能]

IPv6 インタフェース ID の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 ifid <interfaceID>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<interfaceID>

このインタフェースで利用する ID を指定します。

- auto
  本装置が持つ MAC アドレスから、EUI-64 形式の ID を自動生成する場合に指定します。
- インタフェース ID
  このインタフェースで利用する ID を、16 進数値で指定します。4 桁ずつ":"(コロン) で区切ってください。なお、各フィールドの先頭の 0 は省略できます (例: 2a0:c9ff:fe84:759)。

通常は auto を指定してください。特定のインタフェース ID を指定する場合は、同一の link 上でホストと衝突しない値を指定してください。

[動作モード]

構成定義モード (管理者クラス)

[説明]

このインタフェースで利用する、インタフェース ID を設定します。

[未設定時]

インタフェース ID を自動生成するものとみなされます。

```
remote <number> ip6 ifid auto
```

7.5.3　remote ip6 address

[機能]

IPv6 アドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 address [<count>] <address>/<prefixlen> <valid> <preferred> [<flags>]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- IPv6 アドレス定義番号
  IPv6 アドレスの定義番号を、0〜3 の 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<address>/<prefixlen>

- IPv6 アドレス/プレフィックス長
  IPv6 アドレスとプレフィックス長を指定します。リンクローカルアドレスは指定できません。
  IPv6 DHCP クライアントが取得したプレフィックスを使用する場合は上位を"dhcp@インタフェース名"の形式で指定し、下位 80bit 分を IPv6 アドレス形式で指定します。インタフェース名には、rmt インタフェースを以下の範囲で指定します。

範囲	機種
rmt0〜rmt999	Si-R570
rmt0〜rmt499	Si-R370
rmt0〜rmt99	Si-R260B　Si-R240　Si-R220B
rmt0〜rmt49	Si-R180

例)　rmt0 で動作する IPv6 DHCP クライアントが取得した IPv6 プレフィックスを使用する場合の設定例

```
dhcp@rmt0::/64
dhcp@rmt0::1:2:3:4/64
```

プレフィックス長には 64 を指定してください。

<valid>

- valid lifetime の時間
  このインタフェースから RA(Router Advertisement メッセージ) を送信するときに、このプレフィックスに対する valid lifetime を、0 秒〜365 日の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。
  <address>/<prefixlen>に IPv6 DHCP クライアントが取得したプレフィックスを使用する指定をした場合は、IPv6 DHCP クライアントが取得した valid lifetime と比較して短い方が有効になります。

- infinity

  このインタフェースから RA を送信するときに、このプレフィックスに対する valid lifetime を無限とする場合に指定します。

<preferred>

- preferred lifetime の時間

  このインタフェースから RA を送信する場合に、このプレフィックスに対する preferred lifetime を、0 秒〜365 日の範囲で指定します。

  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。

  <preferred>は、<valid>よりも短い時間となるように設定してください。<preferred>が<valid>よりも大きい場合、<valid>と同じ時間として扱われます。

  <address>/<prefixlen>に IPv6 DHCP クライアントが取得したプレフィックスを使用する指定をした場合は、IPv6 DHCP クライアントが取得した preferred lifetime と比較して短い方が有効になります。

- infinity

  このインタフェースから RA を送信する場合に、このプレフィックスに対する preferred lifetime を無限とします。

<flags>

- RA Prefix Information に付与されるフラグ

  このインタフェースから RA を送出する場合に、この prefix に対する flags フィールドの値を 16 進数値で設定します。

  省略時は、c0 を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

このインタフェースの IPv6 アドレスを設定します。
<address>の指定で、<prefixlen>以降がすべて 0 の場合は、指定した値は IPv6 プレフィックスであると判断されます。この IPv6 プレフィックスとインタフェース ID によって、IPv6 アドレスが生成されます。

[注意]

IPv6 DHCP クライアントが取得したプレフィックスと設定値の重なる部分で、0 以外の値がある場合は、IPv6 アドレスは割り当てられません。

```
<-IPv6 DHCPクライアントが取得したプレフィックス->
                                <---------------ユーザ設定値(80bit)---------------------->
| ////////////                                                                          |
                                <------------>
                                設定値が重なる部分
```

例) IPv6 DHCP クライアントが 2001:db8:1000:5555::/64 を取得した場合

設定内容	利用されるアドレス
dhcp@rmt0:0:100::1/64	2001:db8:1000:5555:100::1/64
dhcp@rmt0:100:200::1/64	無効

[未設定時]

Link local アドレス以外の IPv6 アドレスを設定しないものとみなされます。

7.5.4　remote ip6 ra mode

[機能]

Router Advertisement の動作の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 ra mode <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- off
  RA の送信を行いません。
  定期送信、および host からの RS に対する RA の送信を行いません。
- send
  RA の送信を行います。
  定期送信、および host からの RS に対する RA の送信を行います。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RA(Router Advertisement メッセージ) を送信するかどうかを設定します。

[未設定時]

RA の送信を行わないものとみなされます。

```
remote <number> ip6 ra mode off
```

7.5.5 remote ip6 ra interval

[機能]

Router Advertisement メッセージ送信間隔の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 ra interval <max> <min> <lifetime>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<max>

- 最大送信間隔

RA を定期送信する場合の最大送信間隔 (秒) を、4〜1800 の 10 進数値で設定します。

<min>

- 最小送信間隔
  RA を定期送信する場合の最小送信間隔 (秒) を、3〜<max>× 3/4 の 10 進数値で設定します。

<lifetime>

- Router Lifetime の値
  送信する RA の Router Lifetime の値を、0 または<max>〜9000 の 10 進数値で設定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RA の送信間隔、および RA の Router Lifetime の値の設定を行います。RA は<min>〜<max>でランダムに決定された間隔で定期送信されます。

[未設定時]

最大送信間隔に 600 秒、最小送信間隔に 200 秒、Router Lifetime の値に 1800 が設定されたものとみなされます。

```
remote <number> ip6 ra interval 600 200 1800
```

7.5.6　remote ip6 ra mtu

[機能]

Router Advertisement メッセージに含める MTU option の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 ra mtu <mtu>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mtu>

- MTU option の内容
  RA に含める MTU option の値を、0 または 1280～1500 の 10 進数値で設定します。
  0 を指定した場合は、RA に MTU option を含めません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RA に含める MTU option の値を設定します。

[未設定時]

送信する RA に MTU option を含めないものとみなされます。

```
remote <number> ip6 ra mtu 0
```

7.5.7 remote ip6 ra reachabletime

[機能]

Router Advertisement メッセージに含める Reachable Time の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 ra reachabletime <time>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<time>

- Reachable Time の値
  RA に含める Reachable Time の値を、0〜3600000 の 10 進数値で設定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RA に含める Reachable Time の値を設定します。

[未設定時]

Reachable Time の値として 0 が設定されたものとみなされます。

```
remote <number> ip6 ra reachabletime 0
```

7.5.8　remote ip6 ra retranstimer

[機能]

Router Advertisement メッセージに含める Retrans Timer の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 ra retranstimer <time>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<time>

- Retrans Timer の値
  RA に含める Retrans Timer の値を、0～4294967295 の 10 進数値で設定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RA に含める Retrans Timer の値を設定します。

[未設定時]

Retrans Timer の値として 0 が設定されたものとみなされます。

```
remote <number> ip6 ra retranstimer 0
```

7.5.9 remote ip6 ra curhoplimit

[機能]

Router Advertisement メッセージに含める Cur Hop Limit の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 ra curhoplimit <CurHopLimit>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<CurHopLimit>

- Cur Hop Limit の値
  RA に含める Cur Hop Limit の値を、0〜255 の 10 進数値で設定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RA に含める Cur Hop Limit の値を設定します。

[未設定時]

Cur Hop Limit の値として 64 が設定されたものとみなされます。

```
remote <number> ip6 ra curhoplimit 64
```

7.5.10　remote ip6 ra flags

[機能]

Router Advertisement メッセージに含める flags field の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 ra flags <flags>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<flags>

- flags field の値
  RA に含める flags field の値を、00〜ff の 16 進数値で設定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RA に含める flags field の値を設定します。

[未設定時]

flags field の値として 00 が設定されたものとみなされます。

```
remote <number> ip6 ra flags 00
```

7.5.11 remote ip6 route

[機能]

IPv6 スタティック経路情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 route <count> <address>/<prefixlen> [<metric> [<distance>]]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- スタティック経路情報定義番号
  スタティック経路情報の定義番号を、10 進数値で指定します。

範囲	機種
0〜1999	Si-R570
0〜1249	Si-R370
0〜255	Si-R260B Si-R240 Si-R220B
0〜127	Si-R180

<address>/<prefixlen>

- IPv6 アドレス/プレフィックス
  あて先ネットワークを IPv6 アドレスとプレフィックスの組み合わせで指定します。
  リンクローカルアドレスは指定できません。
- default
  あて先ネットワークとしてデフォルトルートを設定する場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<metric>

- メトリック値
  このスタティック経路情報を RIP に再配布するときのメトリック値を、1〜15 の 10 進数値で指定します。
  省略時は、1 を指定したものとみなされます。

<distance>

- 優先度
  このスタティック経路情報の優先度を、0〜254 の 10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。
  省略時は、0 を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv6 スタティック経路 (静的経路) 情報を設定します。
RIP メトリック値は、スタティック経路情報を RIP に再配布するときのメトリック値を設定します。RIP に再配布したときは、設定した RIP メトリック値+1 のメトリック値で RIP テーブルに登録されます。
優先度は、同じあて先への経路情報が複数ある場合、優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。各ダイナミックルーティングプロトコルの優先度については、routemanage ip6 distance コマンドを参照してください。
優先度に 0 が設定されているときは、routemanage interface floating コマンドでのフローティング設定に応じてフローティング動作が切り替わります。優先度に 1 以上が設定されているときは、常にフローティング動作します。
フローティング動作する場合、remote インタフェースが通信可能な状態 (リンクアップなど) であれば、スタティック経路情報をルーティングテーブルに追加します。通信不可能な状態 (リンクダウンなど) であれば、ルーティングテーブルから削除します。
フローティング動作しない場合は、インタフェースの状態にかかわらず常にスタティック経路情報をルーティングテーブルに追加します。
以下に、各設定値とフローティング動作の関係を示します。

<distance> 設定値	インタフェース経路の フローティング設定	スタティック経路の フローティング動作
0(省略値)	使用しない	しない
0(省略値)	使用する	する
1以上	使用しない	する
1以上	使用する	する

以下のような用途でスタティック経路情報を使用する場合、フローティング動作するとなるように設定してください。

- IP ルーティングおよびダイナミックルーティングでの広報で、スタティック経路の出口インタフェースで異常が発生した場合、ルーティングテーブルよりスタティック経路を削除します。
- あて先が同じ経路をダイナミックルーティングで受信した場合、優先度関係により経路を決定します。

IPv6 スタティック経路情報は、本装置全体で以下の数まで定義できます。

最大定義数	機種
2000	Si-R570
1250	Si-R370
256	Si-R260B　Si-R240　Si-R220B
128	Si-R180

[注意]

同じあて先へのスタティック経路情報を複数設定する場合、以下の点に注意してください。

- 優先度が 0 のスタティック経路情報と、優先度が 0 または 1 以上のスタティック経路情報は同時に設定できません。
- 優先度が同じスタティック経路情報は同時に設定できません。

[未設定時]

IPv6 スタティック経路情報を使用しないものとみなされます。

7.5.12　remote ip6 rip use

[機能]

IPv6 RIP 基本情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 rip use <send> <receive> [<metric>]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<send>

RIP(IPv6) パケットを送信するかどうか指定します。

- on
  RIP(IPv6) パケットを送信します。
- off
  RIP(IPv6) パケットを送信しません。

<receive>

RIP(IPv6) パケットを受信するかどうか指定します。

- on
  RIP(IPv6) パケットを受信します。
- off
  RIP(IPv6) パケットを受信しません。

<metric>

- 加算メトリック値
  RIP(IPv6) パケット送信時の加算メトリック値を、0～16 の 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP(IPv6) の基本的な動作を設定します。
<metric>は、RIP(IPv6) パケットを送信する際に加算するメトリック値を設定します。
RIP(IPv6) を使用するインタフェースは、本装置全体で以下の数まで定義できます。

最大定義数	機種
220	Si-R570　Si-R370
120	Si-R260B　Si-R240　Si-R220B
58	Si-R180

[注意]

Si-R570 Si-R370 Si-R240 Si-R220B の場合は以下に注意してください。
ISDN またはフレームリレー (従量課金) の場合、RIP 情報を送信すると、思わぬ課金 (定期発信または長時間接続) が発生します。

[未設定時]

RIP(IPv6) 機能を使用しないものとみなされます。

```
remote <number> ip6 rip use off off 0
```

7.5.13　remote ip6 rip site-local

[機能]

IPv6 RIP site-local プレフィックス送受信の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 rip site-local <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

site-local プレフィックスを送受信するかどうかを指定します。

- on
  site-local プレフィックスを送受信します。
- off
  site-local プレフィックスを送受信しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP(IPv6) で site-local プレフィックスを送受信するかどうかを設定します。

[未設定時]

site-local プレフィックスを送受信するものとみなされます。

```
remote <number> ip6 rip site-local on
```

7.5.14 remote ip6 rip aggregate

[機能]

IPv6 RIP の集約経路の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 rip aggregate <count> <address>/<prefixlen> <rejectroute>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 集約経路定義番号
  集約経路の定義番号を、0〜3 の 10 進数値で指定します。

<address>/<prefixlen>

- IPv6 アドレス/プレフィックス長
  集約経路のあて先ネットワークを IPv6 アドレスとプレフィックス長の組み合わせで指定します。
- default
  集約経路としてデフォルトルートを設定する場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<rejectroute>

- on
  集約経路に対する reject 経路を設定します。
- off
  集約経路に対する reject 経路を設定しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP(IPv6) の集約経路の設定を行います。
集約経路が設定された場合は、設定された集約経路に含まれる個々の経路は広報されず、集約経路だけを広報します。また、集約経路と等しいネットワークに対する経路情報を持たない場合は、実際に持たないあて先に対するパケットを破棄するために、設定された集約経路に対する reject 経路を設定することもできます。
集約経路情報のメトリック値は、集約された経路のメトリック値に関係なく 1 として広報され、remote ip6 rip use および、remote ip6 rip filter set metric で広報するメトリック値を変更することができます。
同一 remote 定義内に同一の集約経路は設定できません。

[未設定時]

RIP(IPv6) で経路集約しないものとみなされます。

7.5.15　remote ip6 rip filter act

[機能]

IPv6 RIP フィルタ動作の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 rip filter <count> act <action> <direction>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜399	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
0〜199	Si-R180

<action>

フィルタリング条件に一致した場合の動作を指定します。

- pass
  該当する経路情報を透過します。
- reject
  該当する経路情報を遮断します。

<direction>

フィルタリングを行う方向を指定します。

- in
  受信時にフィルタリングを行います。
- out
  送信時にフィルタリングを行います。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP(IPv6) での経路情報送受信時に、フィルタリング条件に一致した経路情報を通過 (pass) させるか遮断 (reject) させるかを設定します。フィルタリング条件は優先度順に検索し、条件に一致した経路情報があった時点でフィルタリングが行われ、それ以降の条件は参照されません。全条件に不一致の経路情報は遮断されます。
フィルタリング条件は、remote ip6 rip filter route コマンドを使用し経路情報を設定します。
<count>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。
RIP フィルタ (IPv6) は、本装置全体で以下の数まで定義できます。

最大定義数	機種
400	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B
200	Si-R180

[注意]

フィルタリング条件が設定されていない場合、本コマンドの設定は無効となります。

[未設定時]

RIP(IPv6) フィルタを使用しないものとみなされ、すべての RIP(IPv6) の経路情報が透過します。

7.5.16　remote ip6 rip filter move

[機能]

IPv6 RIP フィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 rip filter move <count> <new_count>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0〜399	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
0〜199	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP(IPv6) フィルタの優先順序を変更します。
<new_count>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、<new_count>は順番にソートされてリナンバリングされます。

7.5.17 remote ip6 rip filter route

[機能]

IPv6 RIP フィルタの経路情報設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 rip filter <count> route <address>/<prefixlen> [<prefix_match>]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜399	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B
0〜199	Si-R180

<address>/<prefixlen>

- IPv6 アドレス/プレフィックス長
  フィルタリング対象とする経路情報を、IPv6 アドレスとプレフィックス長の組み合わせで指定します。
- any
  すべての経路情報をフィルタリング対象とする場合に指定します。
- default
  デフォルトルートをフィルタリング対象とする場合に指定します。

<prefix_match>

経路情報の検索条件を指定します。
省略時は、exact を指定したものとみなされます。
<address>/<prefixlen>に"any"または"default"を指定した場合は、<prefix_match>は指定できません。

- exact
  指定した<address>/<prefixlen>と経路情報の IPv6 アドレス/プレフィックス長を比較し、一致した場合に、フィルタリング対象とします。
- inexact
  指定した<address>と経路情報の IPv6 アドレスを比較し、<prefixlen>まで一致した場合、フィルタリング対象とします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

フィルタリング条件として経路情報を設定します。

[未設定時]

フィルタリング条件が設定されていないものとみなされます。

7.5.18 remote ip6 rip filter set metric

[機能]

IPv6 RIP フィルタのメトリック設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 rip filter <count> set metric <metric>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜399	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B
0〜199	Si-R180

<metric>

- メトリック値
  メトリック値を、0〜16 の 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

フィルタリング条件に一致した経路情報のメトリック値を変更します。
<metric>に 1〜16 を設定した場合、メトリック値は設定した値に変更されます。この場合、remote ip6 rip use コマンドで設定した加算メトリック値は加算されません。0 を指定した場合、メトリック値の変更は行われません。

[注意]

フィルタリング条件が設定されていない場合、本コマンドの設定は無効となります。
フィルタリング条件の"any"と一致した場合、本コマンドの設定は無効となります。

[未設定時]

フィルタリング条件に一致した経路情報のメトリック値を変更しないものとみなされます。

7.5.19　remote ip6 filter

[機能]

IPv6 フィルタの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 filter <count> <action> acl <acl_count> [<direction>]
remote [<number>] ip6 filter <count> <action> <src_addr>/<prefixlen> <src_port> <dst_addr>/<prefixlen> <dst_port> <protocol> <tcpconnect> [<trafficclass> [<direction> [<icmptype> [<icmpcode>]]]]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す番号を、10 進数値で指定します。
  指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つフィルタリング定義がすでに存在する場合は、既存の定義を変更します。

範囲	機種
0〜999	Si-R570　Si-R370
0〜199	Si-R260B　Si-R240　Si-R220B
0〜63	Si-R180

<action>

フィルタリング対象に該当するパケットを透過するかどうかを設定します。

- pass
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。
- restrict
  該当するパケットを、回線が接続されていれば透過し、切断されていれば遮断します。

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、そのフィルタ定義は無効となり、無視されます。IPv6 フィルタでは、ACL の以下の定義を使用します。
  - ip6
    ip6 値が設定されていない場合、そのフィルタ定義は無効となり、無視されます。

- tcp
  ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。
- udp
  ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。
- icmp
  ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B Si-R240 Si-R220B
0〜149	Si-R180

<src_addr>/<prefixlen>

フィルタリング対象とする送信元 IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長
  フィルタリング対象とする送信元 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- any
  すべての送信元 IPv6 アドレスをフィルタリング対象とする場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<src_port>

フィルタリング対象とする送信元ポート番号を指定します。

- ポート番号
  フィルタリング対象とする送信元ポート番号を、1〜65535 の 10 進数値で指定します。
  複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)
- any
  すべての送信元ポート番号をフィルタリング対象とする場合に指定します。

<dst_addr>/<prefixlen>

フィルタリング対象とするあて先 IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長
  フィルタリング対象とするあて先 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- any
  すべてのあて先 IPv6 アドレスをフィルタリング対象とする場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<dst_port>

フィルタリング対象とするあて先ポート番号を指定します。

- ポート番号
  フィルタリング対象とするあて先ポート番号を、1〜65535 の 10 進数値で指定します。
  記述形式は、<src_port>と同様です。
- any
  すべてのあて先ポート番号をフィルタリング対象とする場合に指定します。

<protocol>

フィルタリング対象とするプロトコル番号を指定します。

- プロトコル番号
  フィルタリング対象とするプロトコル番号を、0〜254 の 10 進数値で指定します。
- any
  すべてのプロトコルをフィルタリング対象とします。

<tcpconnect>

- yes
  TCP プロトコルでコネクション接続要求をフィルタリング対象に含めます。
- no
  TCP プロトコルでコネクション接続要求をフィルタリング対象に含めません。

<trafficclass>

- フィルタリング対象 Traffic Class 値
  フィルタリング対象となる Traffic Class フィールドの値を 0-ff までの 16 進数値、または、"-"を使用して表現される 16 進数値の範囲を指定します。
  Traffic Class 値の指定は、"," を区切として 10 個まで設定可能です。
  複数の Traffic Class 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。
  Traffic Class 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 00〜ff の 16 進数値 (例: ff = ff の Traffic Class 値)
  - Traffic Class 値-Traffic Class 値 (例: 32-64 = 32 から 64 までの Traffic Class 値)
  - Traffic Class 値- (例: 80- = 80 から ff までの Traffic Class 値)
  - -Traffic Class 値 (例: -7f = 0 から 7f までの Traffic Class 値)
  - Traffic Class 値,Traffic Class 値,… (例: 10,20,30- = 10 と 20 と 30 以降の Traffic Class 値)
- any
  すべての Traffic Class 値をフィルタリング対象とします。省略時は any として扱われます。

<direction>

フィルタリングする方向を指定します。
省略時は、any を指定したものとみなされます。

- any
  入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。
- in
  入力パケットのみをフィルタリング対象とする場合に指定します。
- out
  出力パケットのみをフィルタリング対象とする場合に指定します。
- reverse
  入力パケットと出力パケットの両方をフィルタリング対象とします。
  ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。
  - 送信元 IP アドレス/プレフィックス長とあて先 IP アドレス/プレフィックス長
  - 送信元ポート番号とあて先ポート番号

<icmptype>

フィルタリングする ICMPv6 メッセージタイプ番号を指定します。

- フィルタリング対象 icmptype 値
  フィルタリング対象となる icmptype フィールドの値を 0-255 までの 10 進数値、または、"-"を使用して表現される 10 進数値の範囲を指定します。
  icmptype 値の指定は、"," を区切として 10 個まで設定可能です。
  記述形式は、<src_port>と同様です。
- any
  すべての icmptype 値をフィルタリング対象とします。省略時は any として扱われます。

<icmpcode>

フィルタリングする ICMPv6 メッセージコード番号を指定します。
icmpcode 指定時は、icmptype も指定する必要があります。

- フィルタリング対象 icmpcode 値
  フィルタリング対象となる icmpcode フィールドの値を 0-255 までの 10 進数値、または、"-"を使用して表現される 10 進数値の範囲を指定します。
  icmptype 値の指定は、"," を区切として 10 個まで設定可能です。
  記述形式は、<src_port>と同様です。
- any
  すべての icmpcode 値をフィルタリング対象とします。省略時は any として扱われます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手ネットワークに対する IPv6 フィルタを設定します。
各パラメタに設定された値によって、動作が変化する場合があります。以下に説明します。

- <protocol>に指定した値によって、IPv6 拡張ヘッダの扱いが以下のように変化します。

- any を指定した場合は、0 個以上の IPv6 拡張ヘッダを含む、あらゆる upper-layer protocol(upper-layer protocol なしを含む) に一致します。
- 以下の IPv6 拡張ヘッダの値を指定した場合は、その拡張ヘッダが付与されている、あらゆる upper-layer protocol(upper-layerprotocol なしを含む) のパケットが一致します。

0　Hop-by-Hop Options Header

43　Routing Header

44　Fragment Header

60　Destination Options Header

- 以下の値を指定した場合は、0 個以上の IPv6 拡張ヘッダ (AH、ESP、IPComp を除く) を含む、upper-layer protocol ヘッダが付与されていないパケットが一致します。

59　no next header

- その他の値が設定されている場合は、upper-layer protocol ヘッダの protocol 番号に等しい値であるパケットが一致します。この場合、AH、ESP、IPComp を除くすべての IPv6 拡張ヘッダは無視されます。パケット中に AH、ESP が設定されている場合は、それ以降の拡張ヘッダおよび upper-layer protocol ヘッダの解釈は行いません。

● <src_port>、<dst_port>に指定した値によって、<protocol>の扱いが以下のように変化します。

- <protocol>に any を指定し、かつ<src_port>、<dst_port>のどちらか、または両方を指定している場合、TCP および UDP パケットの該当ポート番号を持つパケットのみが一致します。
- <protocol>に TCP(6) または UDP(17) を指定し、かつ<src_port>、<dst_port>のどちらか、または両方を指定している場合、指定プロトコルの該当ポート番号を持つパケットのみが一致します。
- <protocol>に TCP(6) または UDP(17) 以外を指定し、かつ<src_port>、<dst_port>のどちらか、または両方を指定している場合、あらゆるパケットが一致しません。

● <icmptype>、<icmpcode>に指定した値によって、<protocol>の扱いが以下のように変化します。

- <protocol>に any を指定し、かつ<icmptype>、<icmpcode>を指定している場合、ICMPv6 パケットの該当 type/code 番号を持つパケットのみが一致します。
- <protocol>に ICMPv6(58) を指定し、かつ<icmptype>、<icmpcode>を指定している場合、指定プロトコルの該当 type/code 番号を持つパケットのみが一致します。
- <protocol>に ICMPv6(58) 以外を指定し、かつ<icmptype>、<icmpcode>を指定している場合、あらゆるパケットが一致しません。

● <tcpconnect>の扱いを以下に示します。

- <protocol>に any を指定した場合、TCP パケットのときにこの設定値が適用されます。
- <protocol>に TCP(6) を指定した場合、常にこの設定値が適用されます。
- <protocol>に any または TCP(6) 以外を指定した場合、この設定値は適用されません。

IPv6 フィルタリングの旧定義は、本装置全体で次の数まで定義できます。

最大定義数	機種
1000	Si-R570　Si-R370
200	Si-R260B　Si-R240　Si-R220B
64	Si-R180

また、ACL 参照定義は、ほかの ACL 参照定義 (IP フィルタ、帯域制御 (WFQ) など) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B Si-R240 Si-R220B
450	Si-R180

旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

[未設定時]

IPv6 フィルタを設定しないものとみなされ、すべてのパケットが透過します。

7.5.20　remote ip6 filter move

[機能]

IPv6 フィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 filter move <count> <new_count>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義の番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0〜999	Si-R570　Si-R370
0〜199	Si-R260B　Si-R240　Si-R220B
0〜63	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv6 フィルタの優先順序を変更します。旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

7.5.21 remote ip6 filter default

[機能]

どの IP フィルタテーブルにも不一致時の動作の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 filter default <action> [<time>]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<action>

どの IPv6 フィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- pass
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。
- restrict
  該当するパケットを、回線が接続されていれば透過し、切断されていれば遮断します。
- spi
  該当するパケットに対して SPI を動作させます。

<time>

- 割当時間
  action に spi を指定したときに接続に割り当てられたテーブルを解放するための無通信監視時間を、0 秒〜86400 秒 (1 日) の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。
  0 秒を指定した場合は、変換テーブル解放のための監視を行いません。
  省略時は、5 分を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

どの IPv6 フィルタテーブルにも一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

どの IPv6 フィルタテーブルにも一致しないパケットは透過します。

```
remote <number> ip6 filter default pass
```

7.5.22　remote ip6 trafficclass

[機能]

Traffic Class 値書き換え条件の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 trafficclass <count> acl <acl_count> <new_trafficclass>
remote [<number>] ip6 trafficclass <count> <src_addr>/<prefixlen> <src_port> <dst_addr>/<prefixlen> <dst_port> <protocol> <trafficclass> <new_trafficclass>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- Traffic Class 値書き換え定義番号
  Traffic Class 値書き換え条件の優先度を表す定義番号を、10 進数値で指定します。
  指定した値は、設定完了時に順方向にソートされてリナンバリングされます。
  また、指定した定義番号と同じ値を持つ Traffic Class 値書き換え定義がすでに存在する場合は、既存定義の値を変更します。

範囲	機種
0〜499	Si-R570　Si-R370
0〜99	Si-R260B　Si-R240　Si-R220B
0〜31	Si-R180

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、その定義は無効となり、無視されます。
  Traffic Class 書き換えでは、ACL の以下の定義を使用します。
  - ip6
    ip6 値が設定されていない場合、その定義は無効となり、無視されます。
  - tcp
    ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip6 の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。
  - udp
    ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip6 の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp
  ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B Si-R240 Si-R220B
0〜149	Si-R180

<src_addr>/<prefixlen>

書き換え対象とする送信元 IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長
  書き換え対象とする送信元 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- any
  すべての送信元 IPv6 アドレスを書き換え対象とする場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<src_port>

書き換え対象とする送信元ポート番号を指定します。

- ポート番号
  書き換え対象とする送信元ポート番号を、1〜65535 の 10 進数値で指定します。
  複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。
  ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)
- any
  すべての送信元ポート番号を書き換え対象とする場合に指定します。

<dst_addr>/<prefixlen>

書き換え対象とするあて先 IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長
  書き換え対象とするあて先 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- any
  すべてのあて先 IPv6 アドレスを書き換え対象とする場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<dst_port>

書き換え対象とするあて先ポート番号を指定します。

- ポート番号
  書き換え対象とするあて先ポート番号を、1〜65535 の 10 進数値で指定します。
  記述形式は、<src_port>と同様です。
- any
  すべてのあて先ポート番号を書き換え対象とする場合に指定します。

<protocol>

書き換え対象とするプロトコル番号を指定します。

- プロトコル番号
  書き換え対象とするプロトコル番号を、0〜254 の 10 進数値で指定します。
- any
  すべてのプロトコルを書き換え対象とします。

<trafficclass>

- Traffic Class 値
  書き換え対象となる Traffic Class フィールドの値を 0-ff までの 16 進数値、または、"-"を使用して表現される 16 進数値の範囲を指定します。
  Traffic Class 値の指定は、"," を区切として 10 個まで設定可能です。
  複数の Traffic Class 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。
  Traffic Class 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 00〜ff の 16 進数値 (例: ff = ff の Traffic Class 値)
  - Traffic Class 値-Traffic Class 値 (例: 32-64 = 32 から 64 までの Traffic Class 値)
  - Traffic Class 値- (例: 80- = 80 から ff までの Traffic Class 値)
  - -Traffic Class 値 (例: -7f = 0 から 7f までの Traffic Class 値)
  - Traffic Class 値,Traffic Class 値,… (例: 10,20,30- = 10 と 20 と 30 以降の Traffic Class 値)
- any
  すべての Traffic Class 値を書き換え対象とします。

<new_trafficclass>

- Traffic Class 値
  書き換える Traffic Class 値を、0〜ff の 16 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

Traffic Class 値書き換え条件を設定します。
条件に一致したパケットの Traffic Class 値を、指定した Traffic Class 値に書き換えます。
Traffic Class 値書き換えの旧定義は、本装置全体で次の数まで定義できます。

最大定義数	機種
500	Si-R570 Si-R370
100	Si-R260B Si-R240 Si-R220B
32	Si-R180

また、ACL 参照定義は、ほかの ACL 参照定義 (IP フィルタ、帯域制御 (WFQ) など) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B Si-R240 Si-R220B
450	Si-R180

旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

[未設定時]

Traffic Class 値書き換えを行わないものとみなされます。

7.5.23　remote ip6 trafficclass move

[機能]

Traffic Class 値書き換え条件の優先度の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 trafficclass move <count> <new_count>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象 Traffic Class 値書き換え定義番号
  優先順序を変更する前の Traffic Class 値書き換え定義番号を指定します。

<new_count>

- 移動先 Traffic Class 値書き換え定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0〜499	Si-R570　Si-R370
0〜99	Si-R260B　Si-R240　Si-R220B
0〜31	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

Traffic Class 値書き換え条件の優先度を変更します。
旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

7.5.24 remote ip6 priority

[機能]

IPv6 プロトコル帯域制御の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 priority <count> acl <acl_count> <width>
remote [<number>] ip6 priority <count> <src_addr>/<prefixlen> <src_port> <dst_addr>/<prefixlen> <dst_port> <protocol> <trafficclass> <width>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 帯域制御定義番号
  帯域制御定義番号を、10 進数値で指定します。

範囲	機種
0～999	Si-R570
0～499	Si-R370
0～99	Si-R260B Si-R240 Si-R220B
0～63	Si-R180

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、その定義は無効となり、無視されます。
  IPv6 プロトコル帯域制御では、ACL の以下の定義を使用します。

  - ip6
    ip6 値が設定されていない場合、その定義は無効となり、無視されます。
  - tcp
    ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip6 の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。
  - udp
    ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip6 の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp
  ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B　Si-R240　Si-R220B
0〜149	Si-R180

<src_addr>/<prefixlen>

帯域制御の対象とする送信元 IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長
  帯域制御の対象とする送信元 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- any
  すべての送信元 IPv6 アドレスを帯域制御の対象とする場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<src_port>

帯域制御の対象とする送信元ポート番号を指定します。

- ポート番号
  帯域制御の対象となる送信元ポート番号を、1〜65535 の 10 進数値で指定します。
  複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。
  ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、
  <dst_port>合わせて 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)
- any
  すべてのポート番号を対象とする場合に指定します。

<dst_addr>/<prefixlen>

帯域制御の対象とするあて先 IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長
  帯域制御の対象とするあて先 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- any
  すべてのあて先 IPv6 アドレスを帯域制御の対象とする場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<dst_port>

帯域制御の対象とするあて先ポート番号を指定します。

- ポート番号
  帯域制御の対象となるあて先ポート番号を、1〜65535 の 10 進数値で指定します。
  記述形式は<src_port>と同様です。
- any
  すべてのポート番号を対象とする場合に指定します。

<protocol>

帯域制御の対象とするプロトコル番号を指定します。

- プロトコル番号
  帯域制御の対象となるプロトコル番号を、0〜254 の 10 進数値で指定します (例: ICMPv6:58、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号をフィルタリング対象とする場合に指定します。

<trafficclass>

- 帯域制御対象 Traffic Class 値
  帯域制御の対象となる Traffic Class フィールドの値を 0-ff までの 16 進数値、または、"-"を使用して表現される 16 進数値の範囲を指定します。
  Traffic Class 値の指定は、"," を区切として 10 個まで設定可能です。
  複数の Traffic Class 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。
  Traffic Class 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 00〜ff の 16 進数値 (例: ff = ff の Traffic Class 値)
  - Traffic Class 値-Traffic Class 値 (例: 32-64 = 32 から 64 までの Traffic Class 値)
  - Traffic Class 値- (例: 80- = 80 から ff までの Traffic Class 値)
  - -Traffic Class 値 (例: -7f = 0 から 7f までの Traffic Class 値)
  - Traffic Class 値,Traffic Class 値,… (例: 10,20,30- = 10 と 20 と 30 以降の Traffic Class 値)
- any
  すべての Traffic Class 値を、帯域制御の対象とします。省略時は any として扱われます。

<width>

- express
  最優先データとして扱います。
- besteffort
  非優先 (ベストエフォート) として扱います。
- 帯域
  1〜99 の 10 進数値で指定した場合、それぞれ指定した値の比で帯域を割り当てます。たとえば、同じ相手ネットワーク中の定義が 3 つあり、それぞれ<width>の値が 30、30、60 であった場合、帯域として 25%、25%、50%が割り当てられます。なお、1〜99 を指定した定義のそれぞれの合計値が 100 未満の場合、残った帯域は定義に一致しないデータ用の帯域となります。
  「数字 + "kbps"(,"mbps")」で指定した場合、指定した帯域をそのまま割り当てます。1kbps〜100000kbps または、1mbps〜100mbps の範囲で指定します。全定義の帯域の合計が回線速度を超えた場合は、それぞれ指定した値の比で帯域を割り当てます。

指定した値の合計値が回線速度に達しない場合、残った帯域は定義に一致しないデータ用の帯域となります。

「"share" + 数字」で指定した場合、数字で指定した帯域制御定義番号で定義された帯域を共有します。この場合、指定する数字は自分自身の帯域制御定義番号より小さい、すでに定義されてあるもの指定しなければなりません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv6 プロトコル帯域制御を設定します。任意のプロトコル、アドレス、ポート、トラフィッククラスを指定して、割り当てる帯域を指定します。
IPv6 プロトコル帯域制御の旧定義は、本装置全体で次の数まで定義できます。

最大定義数	機種
1000	Si-R570
500	Si-R370
100	Si-R260B　Si-R240　Si-R220B
64	Si-R180

また、ACL 参照定義は、ほかの ACL 参照定義 (IP フィルタ、帯域制御 (WFQ) など) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B　Si-R240　Si-R220B
450	Si-R180

旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

[注意]

使用する回線が LAN の場合、シェーピングを使用しないと帯域制御機能は有効に動作しません。
使用する回線が ATM の場合、適切な VC 速度を設定しないと帯域制御機能は有効に動作しません。

[未設定時]

IPv6 プロトコル帯域制御を行わないものとみなされます。

7.5.25 remote ip6 in-policy

[機能]

Ingress ポリシールーティングの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 in-policy <in-policy_number> policy-group <policy-group_number>

[オプション]

<number>

- 相手定義番号

  相手ネットワークの通し番号を、10 進数値で指定します。

  省略時は、0 を指定したものとみなされます。

<in-policy_number>

- Ingress ポリシールーティング定義番号

  この I/F での Ingress ポリシールーティング定義の通し番号を、10 進数値で指定します。

  本定義は、ほかのポリシーグループ参照定義を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
2000	Si-R570
1000	Si-R370
200	Si-R260B Si-R240 Si-R220B
100	Si-R180

<policy-group_number>

- ポリシーグループ番号

  参照するポリシーグループ番号を、10 進数値で指定します。

  IPv6 Ingress ポリシールーティングでは、ポリシーグループで指定された ACL の以下の定義を使用します。

  - ip6

    ip6 値が設定されていない場合、その定義は無効となり、無視されます。

  - tcp

    ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。

    また、ip6 の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。

  - udp

    ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。

    また、ip6 の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp

  ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B　Si-R220B
0〜49	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

Ingress ポリシールーティングに使用するポリシーグループを指定します。

[注意]

Ingress ポリシールーティングを行う場合は、必ずポリシーグループ指定を行う必要があります。
また、定義されている全ポリシーグループと不一致の場合は、アドレスによる経路探索が行われます。

[未設定時]

Ingress ポリシールーティングを設定しないとみなされます。

7.5.26 remote ip6 in-policy move

[機能]

Ingress ポリシールーティングの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 in-policy move <count> <new_count>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象 Ingress ポリシールーティング定義番号
  優先順序を変更するフィルタリング定義の番号を指定します。

<new_count>

- 移動先 Ingress ポリシールーティング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

Ingress ポリシールーティングの優先順序を変更します。

7.5.27　remote ip6 dhcp service

[機能]

IPv6 DHCP 機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 dhcp service <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

IPv6 DHCP 機能のモードを指定します。

- off
  IPv6 DHCP 機能を使用しません。
- client
  IPv6 DHCP クライアント機能を使用します。
- server
  IPv6 DHCP サーバ機能を使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv6 DHCP 機能情報を設定します。

[未設定時]

IPv6 DHCP 機能を使用しないものとみなされます。

```
remote <number> ip6 dhcp service off
```

7.5.28 remote ip6 dhcp duid

[機能]

IPv6 DHCP の DUID 設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 dhcp duid <kind> [<duid>]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<kind>

- auto
  DUID を自動生成する場合に指定します。
- hex
  16 進数で DUID を指定します。
- text
  文字列で DUID を指定します。

<duid>

- DUID
  0x21,0x23～0x7e の 130 文字以内の ASCII 文字列、または 260 桁以内の 16 進数で指定します。
  <kind>が auto の場合は、指定できません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv6 DHCP サーバ／クライアントの DUID を指定します。

例)

```
remote ip6 dhcp duid auto
remote ip6 dhcp duid hex 2105afffe66437d
remote ip6 dhcp duid text Fujitsu
```

auto の場合は、DUID-LL フォーマットにより DUID を自動生成します。

[未設定時]

DUID を自動生成するものとみなされます。

```
remote <number> ip6 dhcp duid auto
```

7.5.29　remote ip6 dhcp client option pd

[機能]

IPv6 DHCP クライアントのプレフィックス要求の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 dhcp client option pd <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- on
  プレフィックスを要求します。
- off
  プレフィックスを要求しません。
- troan
  draft-troan-dhcpv6-opt-prefix-delegation-01 に準拠した方式でプレフィックスを要求します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv6 DHCP クライアント機能を使用する場合に、サーバにプレフィックスを要求するかどうかを設定します。
<mode>に on を設定した場合は、RFC3315、3633 に準拠したオプション番号を使用します。
<mode>に troan に設定した場合は、DNS サーバオプションのオプション番号に 25 番を使用し、PD オプションのオプション番号に 30 番を使用してプレフィックスの要求を行います。

[未設定時]

プレフィックスを要求するものとみなされます。

```
remote <number> ip6 dhcp client option pd on
```

7.5.30 remote ip6 dhcp client option dns

[機能]

IPv6 DHCP クライアントの DNS サーバアドレス要求の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 dhcp client option dns <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- on
  DNS サーバアドレスを要求します。
- off
  DNS サーバアドレスを要求しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv6 DHCP クライアント機能を使用する場合に、サーバに DNS サーバアドレスを要求するかどうかを設定します。

[未設定時]

DNS サーバアドレスを要求するものとみなされます。

```
remote <number> ip6 dhcp client option dns on
```

7.5.31　remote ip6 dhcp client iaid

[機能]

IPv6 DHCP クライアントの IAID 設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 dhcp client iaid <iaid>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<iaid>

- auto
  IAID を自動生成する場合に指定します。
- IAID を指定
  IAID を指定する場合の設定可能範囲は、1～4294967295 です。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv6 DHCP クライアントの IAID を指定します。
auto を指定した場合は、インタフェース番号が IAID として使用されます。

[未設定時]

IAID を自動生成するものとみなされます。

```
remote <number> ip6 dhcp client iaid auto
```

7.5.32 remote ip6 dhcp client route

[機能]

IPv6 DHCP クライアントのリジェクト経路設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 dhcp client route <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- blackhole
  DHCP クライアントで取得したプレフィックスを、リジェクト経路として登録します。
  リジェクト経路あての送信者に対して、応答しません。
- reject
  DHCP クライアントで取得したプレフィックスを、リジェクト経路として登録します。
  リジェクト経路あての送信者に対して、ICMP の unreach でエラー報告を行います。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv6 DHCP クライアントで取得したプレフィックスをリジェクト経路として登録します。
<mode>が reject の場合は、リジェクト経路あての送信者に対して、ICMP の unreach でエラー報告を行います。blackhole の場合は、応答しません。

[未設定時]

blackhole を設定するものとみなされます。

```
remote <number> ip6 dhcp client route blackhole
```

7.5.33　remote ip6 dhcp server preference

[機能]

IPv6 DHCP サーバのプリファレンス値設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 dhcp server preference <preference>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<preference>

- プリファレンス値
  IPv6 DHCP サーバの優先度を、0〜255 の 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv6 DHCP サーバのプリファレンス値を指定します。
プリファレンス値は、Advertise メッセージの Preference オプションで使用され、255 が最優先の値になります。

[未設定時]

プリファレンス値 0 を設定するものとみなされます。

```
remote <number> ip6 dhcp server preference 0
```

7.5.34 remote ip6 dhcp server info dns

[機能]

IPv6 DHCP サーバの DNS サーバアドレス配布情報設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 dhcp server info dns <dns1> [<dns2>]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<dns1>

- DNS サーバ IPv6 アドレス
  IPv6 DHCP クライアントに配布する、DNS サーバの IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<dns2>

- セカンダリ DNS サーバ IPv6 アドレス
  IPv6 DHCP クライアントに配布する、セカンダリ DNS サーバの IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv6 DHCP サーバ機能を使用する場合に、配布する DNS サーバアドレス情報の設定をします。

7.5.35　remote ip6 dhcp server info prefix

[機能]

IPv6 DHCP サーバのプレフィックス配布情報設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 dhcp server info prefix <prefix>/<prefixlen> <valid> <preferred> <routeset>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<prefix>/<prefixlen>

配布するプレフィックス、プレフィックス長を指定します。

- プレフィックス
  配布するプレフィックスを指定します。
  指定可能な範囲は以下のとおりです。

  ::2 〜 fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: 〜 feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

- プレフィックス長
  配布プレフィックス長として、48〜64 の範囲の 10 進数値を指定します。

<valid>

- valid lifetime
  このインタフェースから配布するプレフィックスに対する valid lifetime を、0 秒〜365 日の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。
- infinity
  このインタフェースから配布するプレフィックスに対する valid lifetime を、無限とする場合に指定します。

<preferred>

- preferred lifetime
  このインタフェースから配布するプレフィックスに対する preferred lifetime を、0 秒〜365 日の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。
  <preferred>は、<valid>よりも短い時間となるように設定してください。<preferred>が<valid>よりも大きい場合、<valid>と同じ時間として扱われます。
- infinity
  このインタフェースから配布するプレフィックスに対する preferred lifetime を無限とします。

<routeset>

- on
  配布プレフィックスへの経路を自動登録します。
- off
  配布プレフィックスへの経路を自動登録しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv6 DHCP サーバ機能を使用する場合に、プレフィックス配布情報を設定します。
プレフィックスを配布する場合は、配布プレフィックス、プレフィックス長、Preferred Lifetime、Valid Lifetime、経路登録を指定して登録します。
<routeset>を on にした場合は、プレフィックス配布と同時にクライアントへの経路を追加します。

7.5.36　remote ip6 dvpn

[機能]

動的 VPN の接続契機となる IPv6 パケットの検出条件の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 dvpn <count> invite acl <acl_count> <invite_mask> <template_number>
remote [<number>] ip6 dvpn <count> ignore acl <acl_count>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 接続契機条件定義番号
  接続契機条件の優先度を表す番号を、10 進数値で指定します。
  指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つ接続契機条件定義がすでに存在する場合は、既存の定義を変更します。

範囲	機種
0～9000	Si-R570
0～4500	Si-R370
0～900	Si-R260B　Si-R240　Si-R220B
0～450	Si-R180

invite

条件に一致した場合に接続要求を発行します。

ignore

条件に一致した場合に接続要求を発行しません。

<acl_count>

- ACL 定義番号
  接続契機パケットを検出するための ACL 定義番号を指定します。

範囲	機種
0～2999	Si-R570
0～1499	Si-R370
0～299	Si-R260B　Si-R240　Si-R220B
0～149	Si-R180

<invite_mask>

接続要求を発行する際の相手ネットワークマスクビット数を、0〜128 の 10 数数値で指定します。

<template_number>

動的 VPN 接続に利用するテンプレート定義の定義番号を指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN 接続を利用する場合の、接続契機 IPv6 パケットの検出条件を設定します。

[未設定時]

すべての IPv6 パケットを動的 VPN 接続契機としません。

7.5.37　remote ip6 dvpn move

[機能]

動的 VPN の接続契機検出条件の優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 dvpn move <count> <new_count>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 接続契機条件定義番号
  優先順序を変更する接続契機条件定義の番号を指定します。

<new_count>

- 移動先接続契機条件定義番号
  <count>に対する新しい順序を 10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0～9000	Si-R570
0～4500	Si-R370
0～900	Si-R260B　Si-R240　Si-R220B
0～450	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN 接続契機パケット検出条件の優先順序の変更します。

7.5.38 remote ip6 exp

[機能]

Exp 値書き換え条件の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 exp <count> acl <acl_count> <exp>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- Exp 書き換え条件定義番号
  Exp 書き換えの優先度を表す番号を、10 進数値で指定します。
  指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つ Exp 書き換え条件定義がすでに存在する場合は、既存の定義を変更します。

範囲	機種
0〜499	Si-R570 Si-R370
0〜99	Si-R260B Si-R240 Si-R220B
0〜31	Si-R180

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B Si-R240 Si-R220B
0〜149	Si-R180

<exp>

- Exp 値
  書き換える Exp 値を、0〜7 の 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手ネットワークに対する Exp 書き換え条件を設定します。
ACL 参照定義は、ほかの ACL 参照定義 (IP フィルタ、帯域制御 (WFQ) など) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B　Si-R240　Si-R220B
450	Si-R180

[注意]

remote ap datalink type mpls の ap を使用する場合にだけ有効です。

[未設定時]

Exp 値書き換えは行わないとみなされます。

7.5.39 remote ip6 exp move

[機能]

Exp 値書き換え条件優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] ip6 exp move <count> <new_count>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象 Exp 書き換え条件定義番号
  優先順序を変更する Exp 書き換え条件定義の番号を指定します。

<new_count>

- 移動先 Exp 書き換え条件定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0～499	Si-R570 Si-R370
0～99	Si-R260B Si-R240 Si-R220B
0～31	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

Exp 値を書き換えの条件優先順序を変更します。

7.5.40　remote ip6 clp

[機能]

IPv6 CLP の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B

[入力形式]

remote [<number>] ip6 clp <count> <mode> acl <acl_count>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- CLP 値設定条件定義番号
  CLP 値設定の優先度を表す番号を、10 進数値で指定します。
  指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つ CLP 値設定条件定義がすでに存在する場合は、既存の定義を変更します。

範囲	機種
0～1999	Si-R570
0～99	Si-R370　Si-R260B

<mode>

- on
  条件と一致する場合に、CLP 値を 1 に設定します。
- off
  条件と一致する場合に、CLP 値を 0 に設定します。

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、その CLP 設定定義は無効となり、無視されます。
  IPv6 CLP 設定では、ACL の以下の定義を使用します。
  - ip6
    ip6 値が設定されていない場合、そのフィルタ定義は無効となり、無視されます。
  - tcp
    ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。

- udp

  ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp

  ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手ネットワークに対する CLP 値設定条件を設定します。
ACL 参照定義はほかの ACL 参照定義 (IP フィルタなど) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B

[注意]

ATM にだけ有効です。

[未設定時]

IPv6 CLP 値設定は行わないとみなされます。
また、CLP 値設定を行わない場合は、常に CLP 値は 0 となります。

7.5.41　remote ip6 clp move

[機能]

IPv6 CLP 値設定条件優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B

[入力形式]

remote [<number>] ip clp move <count> <new_count>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象 CLP 値設定条件定義番号
  優先順序を変更する CLP 値設定条件定義の番号を指定します。

<new_count>

- 移動先 CLP 値設定条件定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0～1999	Si-R570
0～99	Si-R370　Si-R260B

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv6 CLP 値設定条件優先順序を変更します。

7.6 ブリッジ関連情報

7.6.1 remote bridge use

[機能]

ブリッジ機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] bridge use <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

ブリッジを使用するかどうかを指定します。

- on
  ブリッジを使用する場合に指定します。
- off
  ブリッジを使用しない場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ブリッジを使用するかどうかを設定します。
ブリッジを使用する場合、IP および IPv6 のパケット以外をすべてブリッジします。
ただし、接続先との接続時に BCP のネゴシエーションを行い、ネゴシエーションが成功した場合にブリッジデータの送受信が可能となります。

[注意]

IP および IPv6 以外のネットワークプロトコル (IPX など) をルーティングしているネットワークでブリッジを使用する場合は、ブリッジによって中継されることでネットワークがダウンすることがあります。ルーティングと併用する場合は、ルーティングによって転送するプロトコルをフィルタリングするよう設定してください。

[未設定時]

ブリッジを使用しないものとみなされます。

```
remote <number> bridge use off
```

7.6.2　remote bridge group

[機能]

ブリッジグループ識別子の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] bridge group <group_id>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<group_id>

- グループ識別子
  グループ識別子を 10 進数値で指定します。

範囲	機種
0〜19	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
0〜7	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

ブリッジのグループ識別子を設定します。

[未設定時]

グループ識別子に 0 を指定したものとみなされます。

```
remote <number> bridge group 0
```

7.6.3 remote bridge static

[機能]

静的学習テーブル情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] bridge static <count> <mac>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 静的学習テーブル定義番号
  指定した定義番号と同じ値を持つ定義がすでに存在する場合は、既存の設定に対する修正をみなされます。

範囲	機種
0〜399	Si-R570 Si-R370
0〜199	Si-R260B Si-R240 Si-R220B Si-R180

<mac>

静的な定義として学習テーブルに追加する MAC アドレスを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

学習テーブルに指定された MAC アドレスを静的な学習テーブル情報として追加します。

7.6.4　remote bridge stp use

[機能]

STP モードの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] bridge stp use <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- on
  STP を使用する場合に指定します。
- off
  STP を使用しない場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

スパニングツリーアルゴリズムで経路制御を行うかどうかを設定します。
本コマンドは、ブリッジを使用している場合にだけ有効です。

[注意]

ブリッジグループ 0 以外のブリッジグループでは STP は動作しません。

[未設定時]

STP を使用しないものとみなされます。

```
remote <number> bridge stp use off
```

7.6.5 remote bridge stp cost

[機能]

パスコストの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] bridge stp cost <path_cost>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<path_cost>

接続先と通信する場合のパスコストを指定します。
通常は auto を指定してください。ただし、ブリッジネットワークを構築するうえで、優先ブリッジ決定のために任意のパスコストを指定することができます。

- auto
  インタフェースの速度に応じて、パスコストが自動決定されます。
  以下に、本パラメタ指定時のパスコストを示します。

回線種別	パスコスト	備考
Ethernet(1Gbps) Ethernet(100Mbps) Ethernet(10Mbps)	100 100 100	
HSD(64kbps) HSD(128kbps) HSD(192kbps) * HSD(256kbps) * HSD(384kbps) * HSD(512kbps) * HSD(768kbps) * HSD(1Mbps) * HSD(1.5Mbps) * FR(64kbps) FR(128kbps) FR(256kbps) * FR(384kbps) * FR(512kbps) * FR(768kbps) * FR(1Mbps) * FR(1.5Mbps) * ISDN MODEM	15620 7810 1000 1000 1000 1000 1000 667 667 16000 8500 1100 1100 1100 1100 680 680 16000 16000	*：192kbps～1.5Mbpsは PRIの場合
IPトンネル	16000	
その他 1Mbps>=速度 1.5Mbps>=速度>1Mbps 4Mbps>=速度>1.5Mbps 6Mbps>=速度>4Mbps 10Mbps>=速度>6Mbps 16Mbps>=速度>10Mbps 20Mbps>=速度>16Mbps 25Mbps>=速度>20Mbps 40Mbps>=速度>25Mbps 80Mbps>=速度>40Mbps 速度>80Mbps	 1000 667 250 167 100 62 50 40 25 12 10	

- パスコスト
  パスコストを、1～65535 の 10 進数値で指定します。
  値が小さいほど、優先度が高くなります。

[動作モード]

構成定義モード (管理者クラス)

[説明]

スパニングツリーアルゴリズムで使用するパスコストを設定します。
本コマンドは、STP を使用する場合にだけ有効です。

[未設定時]

パスコストを自動決定するとみなされます。

```
remote <number> bridge stp cost auto
```

7.6.6 remote bridge stp priority

[機能]

インタフェース優先度の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] bridge stp priority <port_priority>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<port_priority>

- インタフェース優先度
  インタフェースごとの優先度を、0〜255 の 10 進数値で指定します。
  値が小さいほど、優先度が高くなります。

[動作モード]

構成定義モード (管理者クラス)

[説明]

スパニングツリーアルゴリズムで使用する、インタフェースごとの優先度を設定します。
通常、設定する必要はありません。
本コマンドは、STP を使用する場合にだけ有効です。
本コマンドを設定しない場合は、<number>で指定したインタフェースが優先となり、remote 定義で定義されたインタフェースが非優先となります。lan 定義内で定義されたインタフェースでは、定義番号のもっとも小さいものが優先されます。

[未設定時]

インタフェース優先度に 128 が設定されたものとみなされます。

```
remote <number> bridge stp priority 128
```

7.6.7　remote bridge filter

[機能]

MAC フィルタの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] bridge filter <count> <action> acl <acl_count> [direction]
remote [<number>] bridge filter <count> <action> <src_mac>
<dst_mac> <format> [<value> [<vlan_analyze>]]

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す番号を、10 進数値で指定します。
  指定した値は、設定完了時に順方向にソートされリナンバリングされます。
  指定した定義番号と同じ値を持つ定義がすでに存在する場合は、既存の設定に対する修正とみなされます。指定した値を持つ定義が存在しない場合は、追加とみなされます。

範囲	機種
0～255	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
0～127	Si-R180

<action>

フィルタリング対象に該当するフレームを透過するかどうかを指定します。

- pass
  該当するフレームを透過します。
- reject
  該当するフレームを遮断します。
- restrict
  該当するフレームを、回線が接続されていれば透過し、切断されていれば遮断します。

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、そのフィルタ定義は無効となり、無視されます。
  MAC フィルタでは、ACL の以下の定義を使用します。
  - mac
    mac 値が設定されていない場合、そのフィルタ定義は無効となり、無視されます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B Si-R240 Si-R220B
0〜143	Si-R180

<direction>

フィルタリングする方向を指定します。
ACL を利用した定義でのみ指定可能です。
省略時は、any を指定したものとみなされます。

- any
  入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。
- in
  入力パケットだけをフィルタリング対象とする場合に指定します。
- out
  出力パケットだけをフィルタリング対象とする場合に指定します。
- reverse
  入力パケットと出力パケットの両方をフィルタリング対象とします。
  ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。
  - 送信元 MAC アドレスとあて先 MAC アドレス

<src_mac>

フィルタリング対象とする送信元 MAC アドレスを指定します。

- any
  すべての MAC アドレスを対象とする場合に指定します。
- bcast
  ブロードキャスト MAC アドレスを対象とする場合に指定します。
- mcast
  マルチキャスト MAC アドレスを対象とする場合に指定します。
- 上記以外
  対象とする MAC アドレスを指定します。フィルタリング対象とする送信元 MAC アドレスを、xx:xx:xx:xx:xx:xx(xx は 2 桁の 16 進数値) の形式で指定します。

<dec_mac>

フィルタリング対象とするあて先 MAC アドレスを指定します。

- any
  すべての MAC アドレスを対象とする場合に指定します。
- bcast
  ブロードキャスト MAC アドレスを対象とする場合に指定します。
- mcast
  マルチキャスト MAC アドレスを対象とする場合に指定します。
- 上記以外
  対象とする MAC アドレスを指定します。フィルタリング対象とする送信元 MAC アドレスを、xx:xx:xx:xx:xx:xx(xx は 2 桁の 16 進数値) の形式で指定します。

<format> <value>

- llc
  <value>の値と LSAP が一致する LLC 形式フレームを対象とする場合に指定します。<value>には、0～ffff の 16 進数値を指定します。
- ether
  <value>の値とタイプが一致する Ethernet 形式フレームを対象とする場合に指定します。<value>には、5dd～ffff の 16 進数値を指定します。
- any
  すべてのフレームを対象とする場合に指定します。<value>は、指定不要です。

<vlan_analyze>

VLAN タグ付きフレームに対してタグの解析を行うかどうかを指定します。
<value>を指定したときだけ指定可能です。
省略時は、off を指定したものとみなされます。

- on
  VLAN タグ付きフレームの場合に VLAN タグを解析してフィルタリング処理を行います。VLAN タグ付きフレームの場合は、タグの長さ分ずれた位置にある LLC 形式フレームの LSAP や Ethernet 形式フレームのタイプに対してフィルタリング処理を行います。
- off
  VLAN タグ付きフレームの場合に VLAN タグを解析しないでフィルタリング処理を行います。VLAN タグ付きフレームの場合でもタグの長さ分ずらさずにそのままフィルタリング処理を行うため、VLAN タグの TPID が、<value>との比較対象になります。

[動作モード]

構成定義モード (管理者クラス)

[説明]

MAC フィルタを設定します。
本コマンドは、ブリッジ機能を使用する場合にだけ有効です。
指定した条件に一致するフレームを、指定した<action>に従って遮断または通過させます。MAC フィルタは、本装置全体で以下の数まで定義できます。

最大定義数	機種
256	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
128	Si-R180

また、ACL 参照定義は、ほかの ACL 参照定義 (IP フィルタ、帯域制御 (WFQ) など) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B　Si-R240　Si-R220B
432	Si-R180

旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

[注意]

IP および IPv6 以外のネットワークプロトコル (IPX など) をルーティングしているネットワークでブリッジを使用する場合は、ブリッジによって中継されることでネットワークがダウンすることがあります。ルーティングと併用する場合は、ルーティングによって転送するプロトコルをフィルタリングするよう設定してください。

[未設定時]

MAC フィルタを設定しないものとみなされ、すべてのフレームが透過します。

7.6.8　remote bridge filter move

[機能]

MAC フィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] bridge filter move <count> <new_count>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象フィルタリング定義番号
  優先順序を変更する前のフィルタリング定義の番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0〜255	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
0〜127	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

MAC フィルタの優先順序を変更します。
旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

7.6.9 remote bridge priority

[機能]

帯域制御の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] bridge priority <count> acl <acl_count> <width>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 帯域制御定義番号
  帯域制御定義番号を、10 進数値で指定します。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B Si-R240 Si-R220B
0〜63	Si-R180

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、その定義は無効となり、無視されます。
  帯域制御では、ACL の以下の定義を使用します。

  - mac
    mac 値が設定されていない場合、その定義は無効となり、無視されます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B Si-R240 Si-R220B
0〜143	Si-R180

<width>

- express
  最優先データとして扱います。
- besteffort
  非優先 (ベストエフォート) として扱います。
- 帯域
  1〜99 の 10 進数値で指定した場合、それぞれ指定した値の比で帯域を割り当てます。たとえば、同じ相手ネットワーク中の定義が 3 つあり、それぞれ<width>の値が 30、30、60 であった場合、帯域として 25%、25%、50%が割り当てられます。なお、1〜99 を指定した定義のそれぞれの合計値が 100 未満の場合、残った帯域は定義に一致しないデータ用の帯域となります。
  「数字 + "kbps"(,"mbps")」で指定した場合、指定した帯域をそのまま割り当てます。1kbps〜100000kbps または、1mbps〜100mbps の範囲で指定します。全定義の帯域の合計が回線速度を超えた場合は、それぞれ指定した値の比で帯域を割り当てます。指定した値の合計値が回線速度に達しない場合、残った帯域は定義に一致しないデータ用の帯域となります。
  「"share" + 数字」で指定した場合、数字で指定した帯域制御定義番号で定義された帯域を共有します。この場合、指定する数字は自分自身の帯域制御定義番号より小さい、すでに定義されているものを指定しなければなりません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

帯域制御を設定します。任意の ACL 番号を指定して、割り当てる帯域を指定します。
ACL 参照定義は、ほかの ACL 参照定義 (IP フィルタ、帯域制御 (WFQ) など) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B　Si-R240　Si-R220B
432	Si-R180

[注意]

使用する回線が LAN の場合、シェーピングを使用しないと帯域制御機能は有効に動作しません。
使用する回線が ATM の場合、適切な VC 速度を設定しないと帯域制御機能は有効に動作しません。

[未設定時]

帯域制御を行わないものとみなされます。

7.7 MPLS 関連情報

7.7.1 remote mpls use

[機能]

MPLS 機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] mpls use <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- on
  MPLS を利用します。
- off
  MPLS を利用しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

MPLS を利用するかどうかを設定します。

[未設定時]

off が選択されたものとして動作します。

```
remote <number> mpls use off
```

7.7.2　remote mpls distribution

[機能]

ラベル配布プロトコルの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] mpls distribution <protocol>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<protocol>

- ldp
  ラベル配布プロトコルに LDP を使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ラベル配布プロトコルを指定します。

[未設定時]

ldp が選択されたものとして動作します。

```
remote <number> mpls distribution ldp
```

7.7.3 remote mpls ldp hello-timers

[機能]

LDP Hello に関するタイマの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] mpls ldp hello-timers <interval> <holdtime>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<interval>

- Hello 送信間隔のタイマ値
  Hello の送信間隔を、1 秒〜65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。

<holdtime>

- HoldTime のタイマ値
  近隣関係の維持を判定するための HoldTime を、1 秒〜65534 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
- infinity
  近隣関係の維持を判定するための HoldTime を infinity(0xffff:無限) とします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

LDP 近隣関係の維持に用いられる Hello パケットの送信間隔と HoldTime を設定します。
HoldTime の値は interval の値より小さくすることはできません。
HoldTime の値は interval の値の 3 倍以上を設定することを推奨します。

[注意]

HoldTime は近隣関係にある LDP ルータとネゴシエーションし、値の小さい方が採用されますが、送信間隔はネゴシエーションしないため、相手 LSR のタイマ設定と自装置のタイマ設定を一致させておくことを推奨します。

[未設定時]

interval が 5 秒、HoldTime が 15 秒として動作します。

```
remote <number> mpls ldp hello-timers 5s 15s
```

7.7.4　remote mpls ldp keepalive-timers

[機能]

LDP KeepAlive に関するタイマの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] mpls ldp keepalive-timers <interval> <timeout>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<interval>

- KeepAlive 送信間隔のタイマ値
  KeepAlive の送信間隔を、1 秒〜65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。

<timeout>

- KeepAlive タイムアウトのタイマ値
  LDP セッションの維持を判定するためのタイムアウト時間を、1 秒〜65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

LDP セッションの維持に用いられる KeepAlive メッセージの送信間隔とタイムアウトを設定します。
timeout の値は interval の値より小さくすることはできません。
timeout の値は interval の値の 3 倍以上を設定することを推奨します。

[注意]

タイムアウトは近隣関係にある LDP ルータとネゴシエーションし、値の小さい方が採用されますが、送信間隔はタイムアウトのネゴシエーション結果の 3 分の 1 の値とこのコマンドで設定された送信間隔とを比較し、値が小さい方が送信間隔として採用されます。

[未設定時]

interval が 1 分、timeout が 3 分として動作します。

```
remote <number> mpls ldp keepalive-timers 1m 3m
```

7.7.5 remote mpls ldp advertisement

[機能]

LDP ラベル広報方式の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] mpls ldp advertisement <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- dod
  Downstream On Demand を使用します。
- du
  Downstream Unsolicited を使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

LDP のラベル広報方式を指定します。

[未設定時]

du が選択されたものとして動作します。

```
remote <number> mpls ldp advertisement du
```

7.7.6　remote mpls ldp retention

[機能]

LDP ラベル保持方式の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] mpls ldp retention <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- liberal
  Liberal Label Retention Mode を使用します。
- conservative
  Conservative Label Retention Mode を使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

LDP のラベル保持方式を指定します。

[未設定時]

liberal が選択されたものとして動作します。

```
remote <number> mpls ldp retention liberal
```

7.7.7 remote mpls ldp interface-label

[機能]

PHP の無効化

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] mpls ldp interface-label <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- off
  インタフェースの IP アドレスにラベルを割り当てません。
- on
  インタフェースの IP アドレスにラベルを割り当てます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

インタフェースの IP アドレスに対してラベルを割り当てるかどうかを指定します。
割り当てた場合は、インタフェースあての LSP の PHP を無効にすることができます。

[注意]

MPLS トンネル接続機能を使用する場合、自側エンドポイントと IP アドレスが同一のとき、本設定に依らず、PHP 機能は無効となります。

[未設定時]

off が選択されたものとして動作します。

```
remote <number> mpls ldp interface-label off
```

7.7.8　remote mpls ldp ip transport

[機能]

IPv4 Transport Address の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] mpls ldp ip transport <address>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<address>

- LDP セッションの送信元 IPv4 アドレス
  IPv4 アドレスを指定します。以下の範囲で指定してください。

  0.0.0.0
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[動作モード]

構成定義モード (管理者クラス)

[説明]

インタフェース単位で LDP が相手装置との通信に用いる送信元 IPv4 アドレスを分ける必要がある場合に、本装置に設定された IPv4 アドレスを指定します。
0.0.0.0 を指定した場合は、MPLS 情報の設定の IPv4 Transport Address の設定に従います。

[注意]

インタフェース単位で IPv4 Transport Address を設定する場合は、必ず本装置に存在するアドレスを指定してください。本装置に存在しないアドレスをインタフェースに指定した場合は、そのインタフェースでは LDP を使用できません。

[未設定時]

MPLS 情報の設定の IPv4 Transport Address の設定に従います。

```
remote mpls ldp ip transport 0.0.0.0
```

7.7.9 remote mpls ldp multicast-hello

[機能]

Multicast Hello の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

remote [<number>] mpls ldp multicast-hello <mode>

[オプション]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- off
  LDP Multicast Hello パケットを送信しません。
- on
  LDP Multicast Hello パケットを送信します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

LDP Multicast Hello を送出するかしないかを設定します。off に設定すると、Multicast Hello を送出しません。
本設定は、MPLS LSP トンネルを使用する REMOTE インタフェースの設定で、トンネルエンドポイントに指定した装置が EoMPLS 通信の相手装置となる場合に off に設定します。

[注意]

MPLS LSP トンネルを使用する REMOTE インタフェースのトンネルエンドポイントに指定した装置が EoMPLS 通信の相手装置となる場合は、本設定を必ず off に設定してください。
off に指定しない場合は、VC ラベルを交換できない通常の LDP セッションが確立してしまうため、EoMPLS 通信で用いる VC LSP ができず、EoMPLS 通信を行う事ができません。
それ以外の場合では必ず on に設定してください。off に設定した場合は LDP の隣接関係が構築できず、LDP のセッションが確立できなくなります。

[未設定時]

on が設定されているものとみなされます。

```
remote mpls ldp multicast-hello on
```

第 8 章　着信デフォルト情報の設定

8.1 発信者番号 (CLID) で相手が判別できないときの着信動作情報

8.1.1 answer accept

[機能]

発信者番号非通知または発信者番号非登録相手からの着信動作の設定

[適用機種]

Si-R 570	Si-R 370		Si-R 240	Si-R 220B	

[入力形式]

answer accept <mode>

[オプション]

<mode>

- enable
  着信を受け付けます。
- disable
  着信を受け付けません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

発信者番号 (CLID) が通知されない着信、または remote ap called number で設定したどの番号とも一致しない着信について、着信を許可するかどうかを設定します。

[未設定時]

着信を受け付けないものとみなされます。

```
answer accept disable
```

8.1.2　answer ppp auth type

[機能]

着信認証方式の設定

[適用機種]

Si-R 570	Si-R 370		Si-R 240	Si-R 220B	

[入力形式]

answer ppp auth type <authtype>

[オプション]

<authtype>

着信時の認証について指定します。

- off
  着信時の認証を行いません。
- pap
  着信時の認証プロトコルに PAP を使用します。
- chap_md5
  着信時の認証プロトコルに MD5-CHAP を使用します。
- any
  着信時の認証プロトコルに MD5-CHAP または PAP を使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

着信時の認証方式を設定します。

[未設定時]

着信時の認証プロトコルに MD5-CHAP または PAP を用います。

```
answer ppp auth type any
```

8.1.3 answer ppp auth receive add

[機能]

受諾認証情報の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

answer ppp auth receive add <id> <password> [encrypted]

[オプション]

<id>

- 受諾認証 ID
  受諾認証 ID を、0x21,0x23～0x7e のコードで構成される 64 文字以内の ASCII 文字列で指定します。

<password>

- 受諾認証パスワード
  受諾認証パスワードを、0x21,0x23～0x7e のコードで構成される 64 文字以内の文字列で指定します。
- 暗号化された受諾認証パスワード
  show コマンドで表示される暗号化された受諾認証パスワードを encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

<encrypted>

- 暗号化受諾認証パスワード
  <password>に暗号化された受諾認証パスワードを設定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手情報の設定に受諾認証情報の設定がない場合に利用される受諾認証情報を設定します。
この情報は、発信者番号 (CLID) で相手が判別できた場合に利用されます。

[注意]

発信者番号 (CLID) で相手が判別できなかった場合は、この情報は利用されません。
show コマンドでは、暗号化された受諾認証パスワードが encrypted と共に表示されます。

[未設定時]

受諾認証 ID は定義されません。

8.1.4　answer ppp mp use

[機能]

着信時の MP 利用可否の設定

[適用機種]

Si-R 570 | Si-R 370 | | | Si-R 220B | |

[入力形式]

answer ppp mp use <mode>

[オプション]

<mode>

MP を利用するかどうかを指定します。

- off
  MP を利用しない場合に指定します。
- on
  MP を利用する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

発信者番号 (CLID) で相手が判別できない着信について、MP を利用するかどうかを設定します。

[未設定時]

MP を利用しないものとみなされます。

```
answer ppp mp use off
```

8.1.5 answer ppp mp bap use

[機能]

着信時の BAP/BACP 利用可否の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

answer ppp mp bap use <mode>

[オプション]

<mode>

BAP/BACP を利用するかどうかを指定します。

- off
  BAP/BACP を利用しない場合に指定します。
- on
  BAP/BACP を利用する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

発信者番号 (CLID) で相手が判別できない着信について、BAP/BACP を利用するかどうかを設定します。

[未設定時]

BAP/BACP を利用しないものとみなされます。

```
answer ppp mp bap use off
```

第 9 章　テンプレート情報の設定

- テンプレート定義番号の指定範囲

  本章のコマンドの [オプション] に記載されている<number>(テンプレート定義番号) に指定する通し番号 (10 進数値) は、機種ごとに以下に示す範囲で指定してください。

範囲	機種
0〜5	Si-R570　Si-R370
0〜2	Si-R220B
0〜1	Si-R260B　Si-R240　Si-R180

9.1 テンプレート共通情報

9.1.1 template name

[機能]

テンプレート名称の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] name <template_name>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<template_name>

- テンプレート名
  テンプレート名を、0x21,0x23～0x7e の 8 文字以内の ASCII 文字列で指定します。
  ただし、all は切断コマンドで使う予約語であるため、使用しないでください。
  テンプレート名に all を指定したテンプレートのみを切断することができなくなります。

[動作モード]

構成定義モード (管理者クラス)

[説明]

テンプレート名を設定します。

[注意]

すでに同一名称のテンプレートが登録されている場合は、異常終了します。

[未設定時]

テンプレート名を設定しないものとみなされます。

9.1.2　template mtu

[機能]

送信パケット最大長 (MTU 値) の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] mtu <mtu>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mtu>

- MTU 値
  MTU 値を、200～1500 の 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

テンプレート着信で使用する rmt インタフェースに対して送信するパケットの MTU 値を設定します。MTU 値を変更すると、rmt インタフェースに対して送信するパケットの最大長が変更されます。また、PPP ネゴシエーションで相手 MRU 値、相手 MRRU 値が MTU 値まで小さくなることを許すようになります。

[未設定時]

MTU 値に 1500 を指定したものとみなされます。

```
template <number> mtu 1500
```

9.1.3 template idle

[機能]

無通信監視タイマの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] idle <time> [<direction>]

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<time>

- 無通信監視時間
  無通信監視時間を、0 秒～14400 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  0 秒を指定した場合は、監視を行いません。

<direction>

- 省略
  送信パケット、および受信パケットを通信監視の対象とします。
- send
  送信パケットのみを通信監視の対象とします。受信パケットは監視対象とはなりません。
- receive
  受信パケットのみを通信監視の対象とします。送信パケットは監視対象とはなりません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

指定した接続先と接続したときの無通信監視時間を設定します。
<time>で設定された間、監視対象となるパケットがない場合に、無通信として回線を切断します。

[注意]

パケット転送方法に ipsec を指定した場合、無通信監視時間に 1 秒以上 10 秒未満の範囲で指定した時に 10 秒として監視を行います。ただし、未設定時では動的 VPN 機能を使用した場合のみ 10 秒として監視を行います。
また、パケット転送方法に ipsec を指定した場合、<direction>の設定は無視されます。

[未設定時]

無通信監視を行わないものとみなされます。

```
template [<number>] idle 0d
```

9.1.4 template interface pool

[機能]

テンプレート着信で使用する rmt インタフェースの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] interface pool <start> <num>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<start>

- 開始 rmt インタフェース番号
  テンプレート着信で使用する開始 rmt インタフェース番号を 10 進数値で指定します。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B Si-R240 Si-R220B
0〜49	Si-R180

<num>

- インタフェース数
  テンプレート着信で使用する rmt インタフェース数を、10 進数値で指定します。

最大インタフェース数	機種
1000	Si-R570
500	Si-R370
100	Si-R260B Si-R240 Si-R220B
50	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

テンプレート着信で使用する rmt インタフェースを設定します。

[注意]

テンプレート着信用に予約した rmt インタフェース番号に該当する remote 定義番号には一切設定をしないでください。
定義が存在する場合は、該当する remote 定義を削除してから予約を行ってください。予約した範囲に該当する remote 定義が存在した場合は、テンプレート着信は無効になります。

[未設定時]

テンプレート着信で使用する rmt インタフェースが存在しないとみなされます。
(テンプレート着信は機能しません。)

9.1.5 template aaa

[機能]

参照する AAA 情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] aaa <group_id>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<group_id>

- unuse
  AAA 情報を使用しません。
- AAA のグループ ID
  AAA のグループ ID を、10 進数値で指定します。

範囲	機種
0〜9	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

テンプレート着信で認証および着信を行う場合に参照する AAA のグループ ID を指定します。

[未設定時]

AAA 情報を参照しないものとみなされます。

9.1.6　template datalink type

[機能]

パケット転送方法の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] datalink type <type>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<type>

パケットの転送方式を指定します。

- physical
  bind 命令 (template ap datalink bind を参照) によって決定された利用回線のデフォルトの転送方式を提供する場合に指定します。以下に各回線のデフォルトの転送方式を示します。
  (※ Si-R260B Si-R240 Si-R180 では指定できません)

回線種別	転送方式	Si-R570 Si-R370 Si-R220B	Si-R260B Si-R240 Si-R180
ISDN	PPP	○	―

- ipsec
  IPsec を使用する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

テンプレート着信で使用する rmt インタフェースを利用してパケットを転送する場合の転送方式を設定します。

[未設定時]

転送方式として physical を設定するものとみなされます。

```
template <number> datalink type physical
```

Si-R260B Si-R240 Si-R180 の場合は、パケット転送方式を設定しないものとみなされます。

9.1.7 template datalink bind

[機能]

テンプレート着信で使用する回線の設定

[適用機種]

Si-R 570 | Si-R 370 | | | Si-R 220B | |

[入力形式]

template [<number>] datalink bind <kind> [<conf_number>]

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<kind>

- wan
  wan 定義によって指定される回線を利用する場合に指定します。
- any
  ISDN を使用するように設定した、すべての wan 定義を指定したものとみなされます。

<conf_number>

wan 定義の定義番号を指定します。

- wan 定義の定義番号
  利用する wan 定義の定義番号を、10 進数値で指定します。

範囲	機種
0〜131	Si-R570
0〜15	Si-R370
0	Si-R220B

[動作モード]

構成定義モード (管理者クラス)

[説明]

テンプレート着信で使用する回線を設定します。

[未設定時]

<kind>に wan を、<conf_number>に 0 を指定するものとみなされます。

```
template <number> datalink bind wan 0
```

9.1.8　template combine use

[機能]

テンプレートが利用する機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] combine use <function>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<function>

テンプレートが利用する機能を指定します。

- dvpn
  動的 VPN 機能を利用する場合に指定します。
- aaa
  不特定相手着信機能を利用する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

テンプレートが利用する機能を指定します。

[未設定時]

不特定相手着信機能の利用を指定したものとみなされます。

```
template <number> combine use aaa
```

9.1.9 template tunnel local

[機能]

トンネル利用時の自側のトンネルエンドポイントアドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] tunnel local <address>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<address>

- 自側のトンネルエンドポイントアドレス
  自側のトンネルエンドポイントとなる IPv4 アドレスまたは IPv6 アドレスを指定します。本装置に設定されている IP アドレスを指定してください。
  指定可能な範囲は以下のとおりです。

  IPv4: 1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  IPv6: ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

  IPv6 DHCP クライアントが取得したプレフィックスを使用する場合は上位を"dhcp@インタフェース名"の形式で指定し、下位 80bit 分を IPv6 アドレス形式で指定します。インタフェース名には、rmt インタフェースを以下の範囲で指定します。

範囲	機種
rmt0～rmt999	Si-R570
rmt0～rmt499	Si-R370
rmt0～rmt99	Si-R260B Si-R240 Si-R220B
rmt0～rmt49	Si-R180

例) rmt0 で動作する IPv6 DHCP クライアントが取得した IPv6 プレフィックスを使用する場合の設定例

```
dhcp@rmt0::
dhcp@rmt0::1:2:3:4
```

[動作モード]

構成定義モード (管理者クラス)

[説明]

指定したテンプレート着信定義にトンネル利用が設定されている場合に、そのトンネルの自側エンドポイントアドレスを設定します。
IPsec を利用して通信を行う場合は、本コマンドを必ず実行してください。

[注意]

IPsec/IKE の AAA または RADIUS を利用した構成の場合では、IPv6 DHCP クライアントが取得したプレフィックスは使用できません。
また、トンネルの自側エンドポイントアドレスは一意になるように指定してください。
動的 VPN 機能を利用した構成で IPv6 DHCP クライアントが取得したプレフィックスを使用する場合、プレフィックスが割り当てられるインタフェースと同じ値になるように指定してください。

[未設定時]

自側のトンネルエンドポイントアドレスを設定しないものとみなされます。

9.1.10 template sessionwatch address

[機能]

接続先監視アドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] sessionwatch address <source>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<source>

- ICMP ECHO パケットの送信元 IP アドレス
  ICMP ECHO パケットの送信元 IP アドレスを指定します。装置に設定されている自側 IPv4/IPv6 アドレスのどれかを指定してください。
  指定可能な範囲は以下のとおりです。

  IPv4: 1.0.0.1 〜 126.255.255.254
  128.0.0.1 〜 191.255.255.254
  192.0.0.1 〜 223.255.255.254

  IPv6: ::2 〜 feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

  IPv6 DHCP クライアントが取得したプレフィックスを使用する場合は上位を"dhcp@インタフェース名"の形式で指定し、下位 80bit 分を IPv6 アドレス形式で指定します。インタフェース名には、rmt インタフェースを以下の範囲で指定します。

範囲	機種
rmt0〜rmt999	Si-R570
rmt0〜rmt499	Si-R370
rmt0〜rmt99	Si-R260B Si-R240 Si-R220B
rmt0〜rmt49	Si-R180

例) rmt0 で動作する IPv6 DHCP クライアントが取得した IPv6 プレフィックスを使用する場合の設定例

```
dhcp@rmt0::
dhcp@rmt0::1:2:3:4
```

[動作モード]

構成定義モード (管理者クラス)

[説明]

テンプレートを利用した機能で接続先の生存確認を行うための接続先監視アドレスを設定します。
ICMP ECHO パケットの送受信で生存確認を行う際に指定した送信元 IP アドレスを使用します。
ICMP ECHO パケットのあて先 IP アドレスについては以下のアドレスを使用します。
パケットの転送方式 (template datalink type)

- ipsec
  テンプレートが利用する機能 (template combine use)
  - dvpn
    動的 VPN 情報交換で通知された接続先監視アドレス
  - aaa
    AAA または RADIUS に設定された接続先監視アドレス
- physical
  監視を行いません。

[注意]

以下の場合では、監視を行いません。

- RADIUS サーバに接続先監視アドレスを登録していない場合。
- AAA 情報に接続先監視アドレスを設定していない場合。
- 動的 VPN 接続で接続相手と双方の接続先監視アドレスが交換できない場合。

また、IPsec/IKE の AAA または RADIUS を利用した構成の場合では、IPv6 DHCP クライアントが取得したプレフィックスは使用できません。
動的 VPN 機能を利用した構成で IPv6 DHCP クライアントが取得したプレフィックスを使用する場合、プレフィックスが割り当てられるインタフェースと同じ値になるように指定してください。

[未設定時]

接続先監視アドレスを設定しないものとみなされます。

9.1.11 template sessionwatch interval

[機能]

接続先監視のインターバル設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] sessionwatch interval <normal>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<normal>

- ICMP ECHO パケットの正常時送信間隔
  ICMP ECHO パケットの正常時送信間隔を、1 秒～60 秒 (1 分) の範囲で指定します。
  単位は、m(分)、s(秒) のどちらかを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

接続先の生存確認を行うための動作情報を設定します。
指定したあて先 IP アドレスに対して ICMP ECHO パケットの送受信で生存確認を行います。
ICMP ECHO パケットの応答が正常に受信できている間は正常時送信間隔で監視を行います。
接続先監視のパラメタは以下のとおりに決定します。

- 正常時送信間隔：ICMP ECHO パケットの応答が正常に受信されている状態で、次に ICMP ECHO パケットを送信する間隔を、1 秒～60 秒の 10 進数値で指定します。省略時は、無通信監視タイマの 1/2 を正常時送信間隔として動作します。
  ※無通信監視時間が 10 秒未満で指定された場合は 5 秒とします。
- タイムアウト：正常時送信間隔と同等
- リトライ間隔：2 秒
- 監視モード：無通信時監視を実施します。

接続先監視と無通信監視タイマの動作は以下のとおりです。

<table>
<tr><td rowspan="2"></td><td rowspan="2">利用機能</td><td colspan="2">接続先監視あり</td><td rowspan="2">接続先監視なし</td></tr>
<tr><td>正常時送信間隔あり</td><td>正常時送信間隔なし</td></tr>
<tr><td rowspan="2">無通信監視タイマあり</td><td>動的VPN</td><td rowspan="2">正常時送信間隔は設定値でその他は無通信監視タイマの設定値で動作する</td><td rowspan="2">無通信監視タイマの設定値で動作する</td><td rowspan="2">無通信監視タイマの設定値で無通信監視タイマのみ動作する</td></tr>
<tr><td>RADIUSまたはAAA</td></tr>
<tr><td rowspan="2">無通信監視タイマなし</td><td>動的VPN</td><td>正常時送信間隔は設定値でその他は無通信監視タイマが10秒で設定されたものとみなし接続先監視が視が動作する</td><td>無通信監視タイマが10秒で設定されたものとみなし接続先監視が動作する</td><td>無通信監視タイマが10秒で設定されたものとみなし無通信監視タイマのみ動作する</td></tr>
<tr><td>RADIUSまたはAAA</td><td>正常時送信間隔は設定値でその他は無通信監視タイマが10秒で設定されたものとみなし接続先監視のみ動作する</td><td>無通信監視タイマが10秒で設定されたものとみなし接続先監視のみ動作する</td><td>動作しない</td></tr>
</table>

[未設定時]

接続先監視のインターバルを設定しないものとみなされます。

9.2 PPP 関連情報

9.2.1 template ppp auth type

[機能]

認証方法の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

template [<number>] ppp auth type <authtype>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<authtype>

認証プロトコルのタイプを指定します。

- pap
  PAP による認証を要求する場合に指定します。
- chap_md5
  MD5-CHAP による認証を要求する場合に指定します。
- any
  MD5-CHAP または PAP による認証を要求し、実際に利用する認証プロトコルはネゴシエーションによって決定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

着信時の認証方式を設定します。

[未設定時]

着信時の認証プロトコルに MD5-CHAP または PAP を用います。

```
template <number> ppp auth type any
```

9.2.2　template ppp compress

[機能]

データ圧縮機能の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

template [<number>] ppp compress <mode>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- off
  データ圧縮機能を使用しない場合に指定します。
- on
  データ圧縮機能を使用する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

データ圧縮機能を使用するかどうか設定します。

[未設定時]

データ圧縮機能を使用しないものとみなされます。

```
template <number> ppp compress off
```

9.2.3 template ppp ipcp vjcomp

[機能]

VJ-Compression の利用の有無の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

template [<number>] ppp ipcp vjcomp <mode>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- enable
  VJ ヘッダ圧縮を使用する場合に指定します。
- disable
  VJ ヘッダ圧縮を使用しない場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

VJ ヘッダ圧縮機能 (VJCOMP) を使用するかどうかを設定します。VJ ヘッダ圧縮機能は、RFC1144 に準拠しています。

[未設定時]

VJ ヘッダ圧縮機能を使用するものとみなされます。

```
template <number> ppp ipcp vjcomp enable
```

9.2.4　template ppp ipcp iphc

[機能]

IPv4 の IP ヘッダ圧縮 (IPHC) の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

template [<number>] ppp ipcp iphc <mode>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- enable
  IP ヘッダ圧縮を使用する場合に指定します。
- disable
  IP ヘッダ圧縮を使用しない場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv4 で、IP ヘッダ圧縮 (IPHC) を使用するかどうかを設定します。IP ヘッダ圧縮機能は、圧縮方法が RFC2507/RFC2508 に、ネゴシエーション方法が RFC2509 に準拠しています。

[未設定時]

IP ヘッダ圧縮機能を使用しないものとみなされます。

```
template <number> ppp ipcp iphc disable
```

9.2.5 template ppp ipv6cp iphc

[機能]

IPv6 の IP ヘッダ圧縮 (IPHC) の設定

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

template [<number>] ppp ipv6cp iphc <mode>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- enable
  IP ヘッダ圧縮を使用する場合に指定します。
- disable
  IP ヘッダ圧縮を使用しない場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv6 で、IP ヘッダ圧縮 (IPHC) の使用するかどうかを設定します。IP ヘッダ圧縮機能は、圧縮方法が RFC2507/RFC2508 に、ネゴシエーション方法が RFC2509 に準拠しています。

[未設定時]

IPv6 ヘッダ圧縮機能を使用しないものとみなされます。

```
template <number> ppp ipv6cp iphc disable
```

9.3　IP 関連情報

9.3.1　template ip dns

[機能]

DNS サーバアドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip dns <dns>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<dns>

- DNS サーバアドレス
  接続先と接続するときに利用する DNS サーバのアドレスを指定します。
  ここで設定したアドレスを、相手装置に通知します。

  0.0.0.0　アドレスを相手装置に通知しません。
  上記以外　設定したアドレスを、相手装置に通知します。

  設定可能な範囲は以下のとおりです。

  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[動作モード]

構成定義モード (管理者クラス)

[説明]

指定した接続先と接続するときに利用する DNS サーバアドレスを設定します。
本コマンドによる設定情報は、以下の場合に利用されます。

- 通信相手への DNS サーバアドレス通知
  接続先から IPCP 機能を用いて DNS サーバアドレス通知要求を受けた場合に、<dns>で設定した IP アドレスを通知します。本コマンドによる設定がない場合は通知しません。

[未設定時]

DNS サーバアドレスがないものとみなされます。

```
template <number> ip dns 0.0.0.0
```

9.3.2 template ip address remote-pool

[機能]

相手に割り当てる IP アドレス範囲の設定

[適用機種]

Si-R 570 | Si-R 370 | | | Si-R 220B | |

[入力形式]

template [<number>] ip address remote-pool <start> <num>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<start>

- 割り当て先頭アドレス
  割り当てる IP アドレスの先頭アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  1.0.0.1 〜 126.255.255.254
  128.0.0.1 〜 191.255.255.254
  192.0.0.1 〜 223.255.255.254

<num>

- 割り当てアドレス数

最大アドレス数	機種
50	Si-R570 Si-R370 Si-R220B

[動作モード]

構成定義モード (管理者クラス)

[説明]

着信相手に対して、割り当てる IP アドレスの範囲を指定します。

[未設定時]

割り当てる IP アドレス範囲を設定しないものとみなされます。

9.3.3　template ip nat mode

[機能]

アドレス変換の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip nat mode <mode> [<address> <addr_number> [<time>]]

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

アドレス変換 (NAT) を使用するかどうかを設定します。

- off
  NAT を使用しません。
- nat
  NAT を使用します。
- multi
  マルチ NAT を使用します。
- static
  静的 NAT だけを使用します。

以下のパラメタは、<mode>に nat または multi または static を設定した場合に有効です。

<address>

- 先頭グローバル IP アドレス
  動的変換に使用するグローバル IP アドレスの先頭アドレスを指定します。
- any
  グローバル IP アドレスの先頭アドレスとして IPCP ネゴシエーションの結果を使用します。

<addr_number>

- グローバル IP アドレスの個数
  動的アドレス変換に使用するグローバル IP アドレスの個数を、1～16 の 10 進数値で指定します。
  <address>に any を指定した場合は、1 を指定してください。

<time>

- 割当時間
  割り当てられた変換テーブルを解放するための無通信監視時間を、0 秒～86400 秒 (1 日) の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。
  0 秒を指定した場合は、変換テーブル解放のための監視を行いません。
  省略時は、5 分を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手ネットワークに対するアドレス変換 (NAT) の動作を設定します。

[未設定時]

アドレス変換は使用しないものとみなされます。

```
template <number> ip nat mode off
```

9.3.4　template ip nat static

[機能]

静的アドレス変換の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip nat static <count> <private_addr> <private_port>
<global_addr> <global_port> [<protocol>]

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 静的アドレス変換定義番号
  静的アドレス変換定義番号を、10 進数値で指定します。

範囲	機種
0〜499	Si-R570
0〜299	Si-R370
0〜199	Si-R260B　Si-R240　Si-R220B
0〜63	Si-R180

<private_addr>

- プライベート IP アドレス
  静的アドレス変換の対象となるプライベート側の IP アドレスを指定します。

<private_port>

- プライベートポート番号
  静的アドレス変換の対象となるプライベート側のポート番号を、1〜65535 の 10 進数値で指定します。
  グローバルポート番号に複数ポート番号を指定した場合は、変換後の複数ポートの先頭ポート番号を指定します。
- any
  すべてのプライベートポート番号に対して有効な設定となります。

<global_addr>

- グローバル IP アドレス
  静的アドレス変換の対象となるグローバル側の IP アドレスを指定します。
  範囲指定する場合は、「172.16.0.2-172.16.0.254」のように"-"(ハイフン) を使用して指定します。なお、アドレスの範囲指定は一組だけ指定可能です。

- any

  template ip nat mode コマンドで<address>に any を指定した場合は IPCP ネゴシエーションの結果をグローバル側の IP アドレスとして用います。

  template ip nat mode コマンドで<address>に any 以外を指定した場合は指定したアドレスをグローバル側の IP アドレスとして用います。

<global_port>

- グローバルポート番号

  静的アドレス変換の対象となるグローバル側のポート番号を、1〜65535 の 10 進数値で指定します。

  範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。

  なお、ポート番号の範囲指定は一組だけ指定可能です。

- any

  すべてのグローバルポート番号に対して有効な設定となります。

<protocol>

- プロトコル番号

  静的アドレス変換の対象となるプロトコル番号を指定します。

  省略時は、any を指定したものとみなされます。

- any

  すべてのプロトコル番号に対して有効な設定となります。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手ネットワークに対する静的アドレス変換を設定します。
静的アドレス変換の対象となるパケットは、プロトコル番号<protocol>のプライベート側の IP アドレス <private_addr> とポート番号 <private_port>、グローバル側の IP アドレス<global_addr>とポート番号 <global_port>の指定内容により交換されます。
静的アドレス変換は、本装置全体で以下の数まで定義できます。

最大定義数	機種
500	Si-R570
300	Si-R370
200	Si-R260B Si-R240 Si-R220B
64	Si-R180

[未設定時]

静的アドレス変換は設定されません。

9.3.5　template ip nat static default

[機能]

テーブルに一致しないパケットの扱いの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip nat static default <action>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通番として 0 以上の 10 進数値を指定します。省略時は 0 と認識します。

<action>

すべての NAT テーブルにも一致しなかったパケットをどう扱うかを指定します。

- pass
  該当するパケットの IP アドレスやポート番号を変換しないで透過させます。
- reject
  該当するパケットを破棄します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

すべての NAT テーブルに一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

すべての NAT テーブルにも一致しないパケットは破棄します。

```
template <number> ip nat static default reject
```

9.3.6 template ip nat rule

[機能]

アドレス変換ルールの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip nat rule <count> ftp <server_addr> <server_port> [<check>]
template [<number>] ip nat rule <count> dns <server_addr> <server_port> [<check>]
template [<number>] ip nat rule <count> irc <server_addr> <server_port>
template [<number>] ip nat rule <count> sip <server_addr> <server_port>
template [<number>] ip nat rule <count> mldt <server_addr> <server_port>
template [<number>] ip nat rule <count> ipbs <server_addr> <server_port>
template [<number>] ip nat rule <count> dch <server_addr> <server_port>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 変換ルール番号
  変換ルール番号を、0～31 の 10 進数値で指定します。

ftp, irc, dns, sip, mldt, ipbs, dch

変換ルールの対象となるアプリケーションを指定します。

<server_addr>

- IP アドレス
  NAT に割り当てたグローバルアドレス以外のアドレスを指定します。ここで指定したアドレスを変換ルールの対象とします。
- any
  すべての IP アドレスを変換ルールの対象とします。
  any を指定した場合は、グローバル側とプライベート側の両方のアプリケーションサーバに対応します。
- global
  NAT に割り当てたグローバルアドレス以外のすべてのアドレスを変換ルールの対象とします。
  global を指定した場合は、グローバル側のアプリケーションサーバに対応します。
- local
  NAT に割り当てたグローバルアドレスを変換ルールの対象とします。
  local を指定した場合は、プライベート側のアプリケーションサーバに対応します。
- off
  指定したアプリケーションに対する変換ルールを無効にします。

<server_port>

アプリケーションサーバで待ち受けるポート番号を指定します。

- ポート番号

  アプリケーションサーバで待ち受けるポート番号を、1～65535 の 10 進数値で指定します。

  範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。

  なお、ポート番号の範囲指定は一組だけ指定可能です。

<check>

- on

  アプリケーションに ftp を指定した場合、ftp サーバのデータ転送用 IP アドレスおよびポート番号のチェックを行います。

  アプリケーションに dns を指定した場合、グローバル側にサーバが存在するときだけ有効となります。DNS の応答の UDP パケットのソース IP アドレスおよびソースポート番号が問い合わせの UDP パケットのディスティネーション IP アドレスおよびディスティネーションポート番号と同一かどうかチェックします。

  省略時は、on を指定したものとみなされます。

- off

  アプリケーションに ftp を指定した場合、ftp サーバのデータ転送用 IP アドレスおよびポート番号のチェックを行いません。

  アプリケーションに dns を指定した場合、IP アドレスおよびポート番号のチェックを行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手ネットワークに対するアドレス変換ルールを設定します。
指定 IP アドレス、指定ポート番号で動作する指定アプリケーションに対応するサーバに対するアドレス変換の特殊対応の設定を行います。
アドレス変換ルールは、本装置全体で 32 個まで定義できます。

[未設定時]

アドレス変換ルールは設定されません。

9.3.7 template ip nat wellknown

[機能]

ポート番号変換の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip nat wellknown <count> <port> <mode>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

ポート番号変換定義番号を、0〜99 の 10 進数値で指定します。

<port>

- プライベートポート番号
  プライベートポート番号を、1〜65535 の 10 進数値で指定します。
  範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。
  以下に、有効な記述形式を示します。
  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
- any
  すべてのプライベートポート番号を対象とする場合に指定します。

<mode>

- on
  well-known ポート番号とみなし、変換を行いません。
- off
  well-known ポート番号とみなさず、変換を行います。

[動作モード]

構成定義モード (管理者クラス)

[説明]

プライベートポート番号の変換を行うかどうかの設定をします。プライベートポート番号がどの設定にもあてはまらない場合は、未設定時と同様にプライベートポート番号の変換を行います。
ポート番号変換の設定は本装置全体で 100 個まで定義できます。

[未設定時]

以下のポート番号についてはポート番号の変換を行いません。
1～1024(本来の well-known ポート番号)
28800～28830(Microsoft Internet Gaming Zone)

```
 1558(StreamWorks)
 8000(StreamWorks)
  118(Diablo)
  116(Diablo)
 6112(Battle.net)
 6799(NETSTORM)
 6800(NETSTORM)
 9000(HEAVY GEAR)
 7070(Real Player)
 7000(VDO Live Video)
 6667(IRC)
 7648(CU-SeeMe)
 7649(CU-SeeMe)
40027(SurfV)
40026(SurfV)
 1638(DARK REIGN)
```

9.3.8 template ip nat destination

[機能]

あて先変換の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip nat destination <count> <private_addr> <global_addr>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- あて先変換定義番号
  あて先変換の優先度を表す番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜499	Si-R570
0〜299	Si-R370
0〜199	Si-R260B Si-R240 Si-R220B
0〜63	Si-R180

<private_addr>

- プライベート IP アドレス
  あて先変換の対象となるプライベート側の IP アドレスを指定します。

<global_addr>

- グローバル IP アドレス
  あて先変換の対象となるグローバル側の IP アドレスを指定します。
  範囲指定する場合は、「172.16.0.2-172.16.0.254」のように"-"(ハイフン) を使用して指定します。なお、アドレスの範囲指定は一組だけ指定可能です。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手ネットワークに対するあて先変換を設定します。
あて先変換の対象となるパケットは、プライベート側の IP アドレス<private_addr> とグローバル側の IP アドレス<global_addr>の指定内容により交換されます。
あて先変換は、本装置全体で以下の数まで定義できます。

最大定義数	機種
500	Si-R570
300	Si-R370
200	Si-R260B　Si-R240　Si-R220B
64	Si-R180

[未設定時]

あて先変換は設定されません。

9.3.9 template ip nat appli

[機能]

アプリ対応の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip nat appli <function> <mode>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<function>

設定する機能を指定します。

- ftp
  FTP に対する設定を行います。
- sip
  SIP に対する設定を行います。
- h323
  H.323 に対する設定を行います。
- dns
  DNS に対する設定を行います。
- snmp
  SNMP Trap に対する設定を行います。
- irc
  IRC に対する設定を行います。
- ntdomain
  NT ドメインログオンに対する設定を行います。
- stream
  各種ストリーミングに対する設定を行います。
  CU-SeeMe、RealPlayer、VDO Live、Stream Works、SurfV が含まれます。
- game
  各種オンラインゲームに対する設定を行います。
  DIABLO(Battle.net)、NETSTORM、信長の野望 (KOEI)、AGE of EMPIRES が含まれます。

<mode>

- on
  アプリ対応を有効にします。
- off
  アプリ対応を無効にします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

各アプリケーションに対する特殊対応を有効にするかどうかを設定します。

[注意]

このコマンドは、アプリケーションに対するデフォルトの特殊対応動作を設定するものです。
ここで機能を無効に設定した場合でも、rule コマンドで指定されたものは有効になります。

[未設定時]

すべてのアプリ対応を有効にするとみなされます。

```
template [<number>] ip nat appli ftp on
template [<number>] ip nat appli sip on
template [<number>] ip nat appli h323 on
template [<number>] ip nat appli dns on
template [<number>] ip nat appli snmp on
template [<number>] ip nat appli irc on
template [<number>] ip nat appli ntdomain on
template [<number>] ip nat appli stream on
template [<number>] ip nat appli game on
```

9.3.10 template ip filter

[機能]

IP フィルタの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip filter <count> <action> acl <acl_count> [<direction>]
template [<number>] ip filter <count> <action> <src_addr>/<mask> <src_port> <dst_addr>/<mask> <dst_port> <protocol> <tcpconnect> [<tos> [<direction> [<icmptype> [<icmpcode>]]]]

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す番号を、10 進数値で指定します。
  指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つフィルタリング定義がすでに存在する場合は、既存の定義を変更します。

範囲	機種
0〜999	Si-R570 Si-R370
0〜199	Si-R260B Si-R240 Si-R220B
0〜63	Si-R180

<action>

フィルタリング対象に該当するパケットを透過するかどうかを設定します。

- pass
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、そのフィルタ定義は無効となり、無視されます。
  IP フィルタでは、ACL の以下の定義を使用します。
  - ip
    ip 値が設定されていない場合、そのフィルタ定義は無効となり、無視されます。

- tcp

  ip の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。

- udp

  ip の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp

  ip の<protocol>値が 1 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip の<protocol>値が 1 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B　Si-R240　Si-R220B
0〜149	Si-R180

<src_addr>/<mask>

フィルタリング対象とする送信元 IP アドレスとマスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)

  フィルタリング対象とする送信元 IP アドレスとマスクビット数の組み合わせを指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。

  以下に、有効な記述形式を示します。

  - IP アドレス/マスクビット数 (例: 192.168.1.1/24)
  - IP アドレス/マスク値 (例: 192.168.1.1/255.255.255.0)

- any

  すべての送信元 IP アドレスをフィルタリング対象とする場合に指定します。

  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<src_port>

フィルタリング対象とする送信元ポート番号を指定します。

- ポート番号

  フィルタリング対象とする送信元ポート番号を、1〜65535 の 10 進数値で指定します。

  複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。

  ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、

  <dst_port>合わせて 10 個まで指定できます。

  以下に、有効な記述形式を示します。

  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)

- ポート番号- (例: 1- = 1 から 65535 までのポート)
- -ポート番号 (例: -1000 = 1 から 1000 までのポート)
- ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)

- any
  すべての送信元ポート番号をフィルタリング対象とする場合に指定します。

<dst_addr>/<mask>

フィルタリング対象とするあて先 IP アドレスとマスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  フィルタリング対象とするあて先 IP アドレスとマスクビット数の組み合わせを指定します。
  記述形式は、<src_addr>/<mask>と同様です。
- any
  すべてのあて先 IP アドレスをフィルタリング対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<dst_port>

フィルタリング対象とするあて先ポート番号を指定します。

- ポート番号
  フィルタリング対象とするあて先ポート番号を、1～65535 の 10 進数値で指定します。
  記述形式は、<src_port>と同様です。
- any
  すべてのあて先ポート番号をフィルタリング対象とする場合に指定します。

<protocol>

フィルタリング対象とするプロトコル番号を指定します。

- プロトコル番号
  フィルタリング対象とするプロトコル番号を、1～255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号をフィルタリング対象とする場合に指定します。

<tcpconnect>

- yes
  TCP プロトコルでコネクション接続要求をフィルタリング対象に含めます。
- no
  TCP プロトコルでコネクション接続要求をフィルタリング対象に含めません。

<tos>

フィルタリング対象とする TOS 値を指定します。
省略時は、any を指定したものとみなされます。

- TOS 値
  フィルタリング対象とする TOS 値を、0～ff の 16 進数値で指定します。
  複数の TOS 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。
  TOS 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。

- 00～ff の 16 進数値 (例: ff = ff の TOS 値)
- TOS 値-TOS 値 (例: 32-64 = 32 から 64 までの TOS 値)
- TOS 値- (例: 80- = 80 から ff までの TOS 値)
- -TOS 値 (例: -7f = 0 から 7f までの TOS 値)
- TOS 値,TOS 値,… (例: 10,20,30- = 10 と 20 と 30 以降の TOS 値)

- any
  すべての TOS 値をフィルタリング対象とする場合に指定します。

<direction>

フィルタリングする方向を指定します。
省略時は、any を指定したものとみなされます。

- any
  入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。
- in
  入力パケットのみをフィルタリング対象とする場合に指定します。
- out
  出力パケットのみをフィルタリング対象とする場合に指定します。
- reverse
  入力パケットと出力パケットの両方をフィルタリング対象とします。
  ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。
  - 送信元 IP アドレス/マスクとあて先 IP アドレス/マスク
  - 送信元ポート番号とあて先ポート番号

<icmptype>

フィルタリング対象とする ICMP TYPE を指定します。

- ICMP TYPE
  フィルタリング対象とする送信元 ICMP TYPE を、0～255 の 10 進数値で指定します。複数の ICMP TYPE を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「8-30」のように"-"(ハイフン) を使用して指定します。
  ICMP TYPE は、","(カンマ) および"-"(ハイフン) を使用して、10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 0～255 の 10 進数値 (例: 8 = ICMP TYPE 8)
  - ICMP TYPE-ICMP TYPE (例: 2-8 = 2 から 8 までの ICMP TYPE)
  - ICMP TYPE- (例: 8- = 8 から 255 までの ICMP TYPE)
  - -ICMP TYPE (例: -200 = 0 から 200 までの ICMP TYPE)
  - ICMP TYPE,ICMP TYPE,… (例: 0,8,30- = 0 と 8 と 30 以降の ICMP TYPE)
- any
  すべての ICMP TYPE をフィルタリング対象とする場合に指定します。

<icmpcode>

フィルタリング対象とする ICMP CODE を指定します。

- ICMP CODE

  フィルタリング対象とする送信元 ICMP CODE を、0〜255 の 10 進数値で指定します。

  複数の ICMP CODE を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「8-30」のように"-"(ハイフン) を使用して指定します。

  ICMP CODE は、","(カンマ) および"-"(ハイフン) を使用して、10 個まで指定できます。

  以下に、有効な記述形式を示します。

  - 0〜255 の 10 進数値 (例: 8 = ICMP CODE 8)
  - ICMP CODE-ICMP CODE (例: 2-8 = 2 から 8 までの ICMP CODE)
  - ICMP CODE- (例: 8- = 8 から 255 までの ICMP CODE)
  - -ICMP CODE (例: -200 = 0 から 200 までの ICMP CODE)
  - ICMP CODE,ICMP CODE,… (例: 0,8,30- = 0 と 8 と 30 以降の ICMP CODE)

- any

  すべての ICMP CODE をフィルタリング対象とする場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手ネットワークに対する IP フィルタを設定します。
IP フィルタは、指定したアドレス、ポート番号、プロトコル、TOS 値と ICMP TYPE, ICMP CODE と一致するパケットを透過または遮断します。設定した優先度順に一致するか調べ、一致した時点でフィルタリングされ、それ以降の設定は参照されません。
IP フィルタリングの旧定義は、本装置全体で次の数まで定義できます。

最大定義数	機種
1000	Si-R570 Si-R370
200	Si-R260B Si-R240 Si-R220B
64	Si-R180

また、ACL 参照定義は、ほかの ACL 参照定義 (IP フィルタ、帯域制御 (WFQ) など) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B Si-R240 Si-R220B
450	Si-R180

旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

[注意]

<direction>に reverse を指定した場合は、入力パケットは IP アドレス/マスクとポート番号のみを逆転した条件でフィルタリングされます。このため、<tcpconnect>を有効にしている場合は、入力パケットに対しても、TCP プロトコルのコネクション接続要求がフィルタリング対象に含まれます。
定義数の計算は「テンプレート情報で設定した定義数 x テンプレートで使用する rmt インタフェース数」で計算されますので、それを含めて装置最大定義数の範囲に収まるように定義してください。
装置最大定義数を超えた場合は資源不足により、該当機能が動作しない場合があります。

[未設定時]

IP フィルタを設定しないものとみなされます。

9.3.11 template ip filter move

[機能]

IP フィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip filter move <count> <new_count>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義の番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0〜999	Si-R570 Si-R370
0〜199	Si-R260B Si-R240 Si-R220B
0〜63	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

IP フィルタの優先順序を変更します。
旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

9.3.12　template ip filter default

[機能]

どの IP フィルタテーブルにも不一致時の動作の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip filter default <action> [<time>]

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<action>

どの IP フィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- pass
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。
- spi
  該当するパケットに対して SPI を動作させます。

<time>

- 割当時間
  action に spi を指定したときに、接続に割り当てられたテーブルを解放するための無通信監視時間を、0 秒〜86400 秒 (1 日) の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。
  0 秒を指定した場合は、変換テーブル解放のための監視を行いません。
  省略時は、5 分を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

どの IP フィルタテーブルに一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

どの IP フィルタテーブルにも一致しないパケットは透過します。

```
template <number> ip filter default pass
```

9.3.13 template ip tos

[機能]

TOS 値書き換え条件の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip tos <count> acl <acl_count> <new_tos>
template [<number>] ip tos <count> <src_addr>/<mask> <src_port> <dst_addr>/<mask> <dst_port> <protocol> <tos> <new_tos>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- TOS 値書き換え定義番号
  TOS 値書き換え条件の優先度を表す定義番号を、10 進数値で指定します。
  指定した値は、設定完了時に順方向にソートされてリナンバリングされます。
  また、指定した定義番号と同じ値を持つ TOS 値書き換え定義がすでに存在する場合は、既存定義の値を変更します。

範囲	機種
0〜499	Si-R570 Si-R370
0〜99	Si-R260B Si-R240 Si-R220B
0〜31	Si-R180

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、その TOS 値書き換え定義は無効となり、無視されます。
  TOS 値書き換えでは、ACL の以下の定義を使用します。
  - ip
    ip 値が設定されていない場合、その TOS 値書き換え定義は無効となり、無視されます。
  - tcp
    ip の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。

- udp

  ip の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp

  ip の<protocol>値が 1 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip の<protocol>値が 1 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B　Si-R240　Si-R220B
0〜149	Si-R180

<src_addr>/<mask>

- IP アドレス/マスクビット数 (またはマスク値)

  TOS 値書き換え対象となる送信元 IP アドレスとマスクビット数の組み合わせを指定します。マスク値は最上位ビットから 1 で連続した値にしてください。

  以下に、有効な記述形式を示します。

  - IP アドレス/マスクビット数 (例: 192.168.1.1/24)
  - IP アドレス/マスク値 (例: 192.168.1.1/255.255.255.0)

- any

  すべての送信元 IP アドレスを TOS 値書き換えの対象とする場合に指定します。

  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<src_port>

TOS 値書き換え対象となる送信元ポート番号を指定します。

- ポート番号

  TOS 値書き換え対象となる送信元ポート番号を、1〜65535 の 10 進数値で指定します。

  複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。

  ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。

  以下に、有効な記述形式を示します。

  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)

- any

  すべてのポート番号を対象とする場合に指定します。

<dst_addr>/<mask>

TOS 値書き換え対象となるあて先 IP アドレス、マスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  TOS 値書き換え対象となるあて先 IP アドレスとマスクビット数の組み合わせを指定します。
  記述形式は、<src_addr>/<mask>と同様です。
- any
  すべてのあて先 IP アドレスを TOS 値書き換えの対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<dst_port>

TOS 値書き換え対象となるあて先ポート番号を指定します。

- ポート番号
  TOS 値書き換え対象となるあて先ポート番号を、1〜65535 の 10 進数値で指定します。
  記述形式は、<src_port>と同様です。
- any
  すべてのポート番号を対象とする場合に指定します。

<protocol>

TOS 値書き換え対象となるプロトコル番号を指定します。

- プロトコル番号
  TOS 値書き換え対象となるプロトコル番号を、1〜255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号を TOS 値書き換え対象とする場合に指定します。

<tos>

- TOS 値
  書き換え対象となる TOS 値を、0〜ff の 16 進数値で指定します。
  複数の TOS 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。
  TOS 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 00〜ff の 16 進数値 (例: ff = ff の TOS 値)
  - TOS 値-TOS 値 (例: 32-64 = 32 から 64 までの TOS 値)
  - TOS 値- (例: 80- = 80 から ff までの TOS 値)
  - -TOS 値 (例: -7f = 0 から 7f までの TOS 値)
  - TOS 値,TOS 値,… (例: 10,20,30- = 10 と 20 と 30 以降の TOS 値)
- any
  すべての TOS 値を、TOS 値書き換えの対象とする場合に指定します。

<new_tos>

- TOS 値
  書き換える TOS 値を、0〜ff の 16 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

TOS 値書き換え条件を設定します。
条件に一致したパケットの TOS 値を、指定した TOS 値に書き換えます。
TOS 値書き換えの旧定義は、本装置全体で次の数まで定義できます。

最大定義数	機種
500	Si-R570　Si-R370
100	Si-R260B　Si-R240　Si-R220B
32	Si-R180

また、ACL 参照定義は、ほかの ACL 参照定義 (IP フィルタ、帯域制御 (WFQ) など) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B　Si-R240　Si-R220B
450	Si-R180

旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

[注意]

定義数の計算は「テンプレート情報で設定した定義数 x テンプレートで使用する rmt インタフェース数」で計算されますので、それを含めて装置最大定義数の範囲に収まるように定義してください。
装置最大定義数を超えた場合は資源不足により、該当機能が動作しない場合があります。

[未設定時]

TOS 値書き換えを行わないものとみなされます。

9.3.14 template ip tos move

[機能]

TOS 値書き換え条件の優先度の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip tos move <count> <new_count>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象 TOS 値書き換え定義番号
  優先順序を変更する前の TOS 値書き換え定義番号を指定します。

<new_count>

- 移動先 TOS 値書き換え定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0〜499	Si-R570 Si-R370
0〜99	Si-R260B Si-R240 Si-R220B
0〜31	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

TOS 値書き換え条件の優先度を変更します。
旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

9.3.15　template ip priority

[機能]

帯域制御の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip priority <count> acl <acl_count> <width>
template [<number>] ip priority <count> <src_addr>/<mask> <src_port> <dst_addr>/<mask> <dst_port> <protocol> <tos> <width>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 帯域制御定義番号
  帯域制御定義番号を、10 進数値で指定します。

範囲	機種
0～999	Si-R570
0～499	Si-R370
0～99	Si-R260B　Si-R240　Si-R220B
0～63	Si-R180

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、その定義は無効となり、無視されます。
  帯域制御では、ACL の以下の定義を使用します。

  - ip
    ip 値が設定されていない場合、その定義は無効となり、無視されます。
  - tcp
    ip の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。
  - udp
    ip の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp
  ip の<protocol>値が 1 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 1 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B Si-R240 Si-R220B
0〜149	Si-R180

<src_addr>/<mask>

帯域制御の対象となる送信元 IP アドレス、マスクビット数を指定します。

- 送信元 IP アドレス/マスクビット数 (またはマスク値)
  帯域制御の対象となる送信元 IP アドレスとマスクビット数の組み合わせを指定します。
  マスク値は、最上位ビットから 1 で連続した値にしてください。
  以下に、有効な記述形式を示します。
  - IP アドレス/マスクビット数 (例: 192.168.1.1/24)
  - IP アドレス/マスク値 (例: 192.168.1.1/255.255.255.0)
- any
  すべての IP アドレスを帯域制御の対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<src_port>

帯域制御の対象となる送信元ポート番号を指定します。

- ポート番号
  帯域制御の対象となる送信元ポート番号を、1〜65535 の 10 進数値で指定します。
  複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。
  ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、
  <dst_port>合わせて 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)
- any
  すべてのポート番号を対象とする場合に指定します。

<dst_addr>/<mask>

帯域制御の対象となるあて先 IP アドレス、マスクビット数を指定します。

- あて先 IP アドレス/マスクビット数 (またはマスク値)
  帯域制御の対象となるあて先 IP アドレスとマスクビット数の組み合わせを指定します。
  記述形式は<src_addr>/<mask>と同様です。
- any
  すべての IP アドレスを帯域制御の対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<dst_port>

帯域制御の対象となるあて先ポート番号を指定します。

- ポート番号
  帯域制御の対象となるあて先ポート番号を、1～65535 の 10 進数値で指定します。
  記述形式は<src_port>と同様です。
- any
  すべてのポート番号を対象とする場合に指定します。

<protocol>

帯域制御の対象となるプロトコル番号を指定します。

- プロトコル番号
  帯域制御の対象となるプロトコル番号を、1～255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号を帯域制御の対象とする場合に指定します。

<tos>

- TOS 値
  帯域制御の対象となる TOS 値を、0～ff の 16 進数値で指定します。
  複数の TOS 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。
  TOS 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 00～ff の 16 進数値 (例: ff = ff の TOS 値)
  - TOS 値-TOS 値 (例: 32-64 = 32 から 64 までの TOS 値)
  - TOS 値- (例: 80- = 80 から ff までの TOS 値)
  - -TOS 値 (例: -7f = 0 から 7f までの TOS 値)
  - TOS 値,TOS 値,… (例: 10,20,30- = 10 と 20 と 30 以降の TOS 値)
- any
  すべての TOS 値を、帯域制御の対象とする場合に指定します。

<width>

- express
  最優先データとして扱います。
- besteffort
  非優先 (ベストエフォート) として扱います。
- 帯域
  1〜99 の 10 進数値で指定した場合、それぞれ指定した値の比で帯域を割り当てます。たとえば、同じ相手ネットワーク中の定義が 3 つあり、それぞれ<width>の値が 30、30、60 であった場合、帯域として 25%、25%、50%が割り当てられます。なお、1〜99 を指定した定義のそれぞれの合計値が 100 未満の場合、残った帯域は定義に一致しないデータ用の帯域となります。
  「数字 + "kbps"(,"mbps")」で指定した場合、指定した帯域をそのまま割り当てます。1kbps〜100000kbps または、1mbps〜100mbps の範囲で指定します。全定義の帯域の合計が回線速度を超えた場合は、それぞれ指定した値の比で帯域を割り当てます。
  指定した値の合計値が回線速度に達しない場合、残った帯域は定義に一致しないデータ用の帯域となります。
  「"share" + 数字」で指定した場合、数字で指定した帯域制御定義番号で定義された帯域を共有します。この場合、指定する数字は自分自身の帯域制御定義番号より小さい、すでに定義されてあるもの指定しなければなりません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

帯域制御を設定します。任意のプロトコル、アドレス、ポート、TOS 値を指定して、割り当てる帯域を指定します。
帯域制御の旧定義は、本装置全体で次の数まで定義できます。

最大定義数	機種
1000	Si-R570
500	Si-R370
100	Si-R260B Si-R240 Si-R220B
64	Si-R180

また、ACL 参照定義は、ほかの ACL 参照定義 (IP フィルタ、帯域制御 (WFQ) など) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B Si-R240 Si-R220B
450	Si-R180

旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

[注意]

ISDN、専用線、フレームリレー以外の回線上で帯域制御機能を使用する場合は、シェーピングを使用しないと帯域制御は有効に動作しません。
定義数の計算は「テンプレート情報で設定した定義数 x テンプレートで使用する rmt インタフェース数」で計算されますので、それを含めて装置最大定義数の範囲に収まるように定義してください。
装置最大定義数を超えた場合は資源不足により、該当機能が動作しない場合があります。

[未設定時]

帯域制御を行わないものとみなされます。

9.3.16 template ip msschange

[機能]

MSS 書き換えの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip msschange <mss>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mss>

- MSS 値
  MSS の書き換え値を、0 または 160～1460 の 10 進数値で指定します。
  0 を指定した場合は、MSS を書き換えません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

MSS 書き換え機能を利用する場合の、書き換え値を設定します。

[未設定時]

MSS 書き換え機能を利用しないものとみなされます。

```
template <number> ip msschange 0
```

9.3.17　template ip ids use

[機能]

IDS の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip ids use <mode>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- off
  IDS を利用しません。
- on
  IDS を利用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IDS を設定します。

[注意]

なし

[未設定時]

IPv4 パケットに対して IDS を利用しないものとみなされます。

```
template <number> ip ids use off
```

9.3.18 template ip in-policy

[機能]

Ingress ポリシールーティングの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip in-policy <in-policy_number> policy-group <policy-group_number>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<in-policy_number>

- Ingress ポリシールーティング定義番号
  この I/F での Ingress ポリシールーティング定義の通し番号を、10 進数値で指定します。
  本定義は、ほかのポリシーグループ参照定義を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
2000	Si-R570
1000	Si-R370
200	Si-R260B Si-R240 Si-R220B
100	Si-R180

<policy-group_number>

- ポリシーグループ番号
  参照するポリシーグループ番号を、10 進数値で指定します。
  IPv4 Ingress ポリシールーティングでは、ポリシーグループで指定された ACL の以下の定義を使用します。

  - ip
    ip 値が設定されていない場合、その定義は無効となり、無視されます。
  - tcp
    ip の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。
  - udp
    ip の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp

  ip の<protocol>値が 1 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip の<protocol>値が 1 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B　Si-R220B
0〜49	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

Ingress ポリシールーティングに使用するポリシーグループを指定します。

[注意]

Ingress ポリシールーティングを行う場合は、必ずポリシーグループ指定を行う必要があります。
また、定義されている全ポリシーグループと不一致の場合は、アドレスによる経路探索が行われます。

[未設定時]

Ingress ポリシールーティングを設定しないとみなされます。

9.3.19 template ip in-policy move

[機能]

Ingress ポリシールーティングの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip in-policy move <count> <new_count>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象 Ingress ポリシールーティング定義番号
  優先順序を変更するフィルタリング定義の番号を指定します。

<new_count>

- 移動先 Ingress ポリシールーティング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

Ingress ポリシールーティングの優先順序を変更します。

9.4　IPv6 関連情報

9.4.1　template ip6 use

[機能]

IPv6 機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip6 use <mode>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

IPv6 パケットの送受信を行うかどうか指定します。

- on
  テンプレート着信で使用する rmt インタフェースで、IPv6 パケットの送受信を行います。
- off
  テンプレート着信で使用する rmt インタフェースで、IPv6 パケットの送受信を行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

テンプレート着信で使用する rmt インタフェースで、IPv6 機能を利用するかどうかを設定します。

[未設定時]

IPv6 機能を利用しないものとみなされます。

```
template <number> ip6 use off
```

9.4.2 template ip6 ifid

[機能]

IPv6 インタフェース ID の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip6 ifid <interfaceID>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<interfaceID>

テンプレート着信で使用する rmt インタフェースで利用する ID を指定します。

- auto
  本装置が持つ MAC アドレスから、EUI-64 形式の ID を自動生成する場合に指定します。
- インタフェース ID
  rmt インタフェースで利用する ID を、16 進数値で指定します。4 桁ずつ":"(コロン) で区切ってください。なお、各フィールドの先頭の 0 は省略できます (例: 2a0:c9ff:fe84:759)。

通常は auto を指定してください。特定のインタフェース ID を指定する場合は、同一の link 上でホストと衝突しない値を指定してください。

[動作モード]

構成定義モード (管理者クラス)

[説明]

テンプレート着信で使用する rmt インタフェースで利用する、インタフェース ID を設定します。

[未設定時]

インタフェース ID を自動生成するものとみなされます。

```
template <number> ip6 ifid auto
```

9.4.3　template ip6 filter

[機能]

IPv6 フィルタの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip6 filter <count> <action> acl <acl_count> [<direction>]
template [<number>] ip6 filter <count> <action> <src_addr>/<prefixlen> <src_port> <dst_addr>/<prefixlen> <dst_port> <protocol> <tcpconnect> [<trafficclass> [<direction> [<icmptype> [<icmpcode>]]]]

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す番号を、10 進数値で指定します。
  指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つフィルタリング定義がすでに存在する場合は、既存の定義を変更します。

範囲	機種
0〜999	Si-R570　Si-R370
0〜199	Si-R260B　Si-R240　Si-R220B
0〜63	Si-R180

<action>

フィルタリング対象に該当するパケットを透過するかどうかを設定します。

- pass
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、そのフィルタ定義は無効となり、無視されます。IPv6 フィルタでは、ACL の以下の定義を使用します。
  - ip6
    ip6 値が設定されていない場合、そのフィルタ定義は無効となり、無視されます。

- tcp

  ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip6 の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。

- udp

  ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip6 の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp

  ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B Si-R240 Si-R220B
0〜149	Si-R180

<src_addr>/<prefixlen>

フィルタリング対象とする送信元 IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長

  フィルタリング対象とする送信元 IPv6 アドレスとプレフィックス長の組み合わせを指定します。

- any

  すべての送信元 IPv6 アドレスをフィルタリング対象とする場合に指定します。

  ::/0 を指定するのと同じ意味になります。

<src_port>

フィルタリング対象とする送信元ポート番号を指定します。

- ポート番号

  フィルタリング対象とする送信元ポート番号を、1〜65535 の 10 進数値で指定します。複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。

  以下に、有効な記述形式を示します。

  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)

- any

  すべての送信元ポート番号をフィルタリング対象とする場合に指定します。

<dst_addr>/<prefixlen>

フィルタリング対象とするあて先 IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長
  フィルタリング対象とするあて先 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- any
  すべてのあて先 IPv6 アドレスをフィルタリング対象とする場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<dst_port>

フィルタリング対象とするあて先ポート番号を指定します。

- ポート番号
  フィルタリング対象とするあて先ポート番号を、1〜65535 の 10 進数値で指定します。
  記述形式は、<src_port>と同様です。
- any
  すべてのあて先ポート番号をフィルタリング対象とする場合に指定します。

<protocol>

フィルタリング対象とするプロトコル番号を指定します。

- プロトコル番号
  フィルタリング対象とするプロトコル番号を、0〜254 の 10 進数値で指定します。
- any
  すべてのプロトコルをフィルタリング対象とします。

<tcpconnect>

- yes
  TCP プロトコルでコネクション接続要求をフィルタリング対象に含めます。
- no
  TCP プロトコルでコネクション接続要求をフィルタリング対象に含めません。

<trafficclass>

- フィルタリング対象 Traffic Class 値
  フィルタリング対象となる Traffic Class フィールドの値を 0-ff までの 16 進数値、または、"-"を使用して表現される 16 進数値の範囲を指定します。
  Traffic Class 値の指定は、"," を区切として 10 個まで設定可能です。
  複数の Traffic Class 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。
  Traffic Class 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。以下に、有効な記述形式を示します。
  - 00〜ff の 16 進数値 (例: ff = ff の Traffic Class 値)
  - Traffic Class 値-Traffic Class 値 (例: 32-64 = 32 から 64 までの Traffic Class 値)
  - Traffic Class 値- (例: 80- = 80 から ff までの Traffic Class 値)
  - -Traffic Class 値 (例: -7f = 0 から 7f までの Traffic Class 値)
  - Traffic Class 値,Traffic Class 値,… (例: 10,20,30- = 10 と 20 と 30 以降の Traffic Class 値)
- any
  すべての Traffic Class 値をフィルタリング対象とします。省略時は any として扱われます。

<direction>

フィルタリングする方向を指定します。
省略時は、any を指定したものとみなされます。

- any
  入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。
- in
  入力パケットのみをフィルタリング対象とする場合に指定します。
- out
  出力パケットのみをフィルタリング対象とする場合に指定します。
- reverse
  入力パケットと出力パケットの両方をフィルタリング対象とします。
  ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。
  - 送信元 IP アドレス/プレフィックス長とあて先 IP アドレス/プレフィックス長
  - 送信元ポート番号とあて先ポート番号

<icmptype>

フィルタリングする ICMPv6 メッセージタイプ番号を指定します。

- フィルタリング対象 icmptype 値
  フィルタリング対象となる icmptype フィールドの値を 0-255 までの 10 進数値、または、"-"を使用して表現される 10 進数値の範囲を指定します。
  icmptype 値の指定は、"," を区切として 10 個まで設定可能です。
  記述形式は、<src_port>と同様です。
- any
  すべての icmptype 値をフィルタリング対象とします。省略時は any として扱われます。

<icmpcode>

フィルタリングする ICMPv6 メッセージコード番号を指定します。
icmpcode 指定時は、icmptype も指定する必要があります。

- フィルタリング対象 icmpcode 値
  フィルタリング対象となる icmpcode フィールドの値を 0-255 までの 10 進数値、または、"-"を使用して表現される 10 進数値の範囲を指定します。
  icmptype 値の指定は、"," を区切として 10 個まで設定可能です。
  記述形式は、<src_port>と同様です。
- any
  すべての icmpcode 値をフィルタリング対象とします。省略時は any として扱われます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手ネットワークに対する IPv6 フィルタを設定します。
各パラメタに設定された値によって、動作が変化する場合があります。以下に説明します。

- <protocol>に指定した値によって、IPv6 拡張ヘッダの扱いが以下のように変化します。

- any を指定した場合は、0 個以上の IPv6 拡張ヘッダを含む、あらゆる upper-layer protocol(upper-layer protocol なしを含む) に一致します。
- 以下の IPv6 拡張ヘッダの値を指定した場合は、その拡張ヘッダが付与されている、あらゆる upper-layer protocol(upper-layerprotocol なしを含む) のパケットが一致します。

0　Hop-by-Hop Options Header

43　Routing Header

44　Fragment Header

60　Destination Options Header

- 以下の値を指定した場合は、0 個以上の IPv6 拡張ヘッダ (AH、ESP、IPComp を除く) を含む、upper-layer protocol ヘッダが付与されていないパケットが一致します。

59　no next header

- その他の値が設定されている場合は、upper-layer protocol ヘッダの protocol 番号に等しい値であるパケットが一致します。この場合、AH、ESP、IPComp を除くすべての IPv6 拡張ヘッダは無視されます。パケット中に AH、ESP が設定されている場合は、それ以降の拡張ヘッダおよび upper-layer protocol ヘッダの解釈は行いません。

● <src_port>、<dst_port>に指定した値によって、<protocol>の扱いが以下のように変化します。

- <protocol>に any を指定し、かつ<src_port>、<dst_port>のどちらか、または両方を指定している場合、TCP および UDP パケットの該当ポート番号を持つパケットのみが一致します。
- <protocol>に TCP(6) または UDP(17) を指定し、かつ<src_port>、<dst_port>のどちらか、または両方を指定している場合、指定プロトコルの該当ポート番号を持つパケットのみが一致します。
- <protocol>に TCP(6) または UDP(17) 以外を指定し、かつ<src_port>、<dst_port>のどちらか、または両方を指定している場合、あらゆるパケットが一致しません。

● <icmptype>、<icmpcode>に指定した値によって、<protocol>の扱いが以下のように変化します。

- <protocol>に any を指定し、かつ<icmptype>、<icmpcode>を指定している場合、ICMPv6 パケットの該当 type/code 番号を持つパケットのみが一致します。
- <protocol>に ICMPv6(58) を指定し、かつ<icmptype>、<icmpcode>を指定している場合、指定プロトコルの該当 type/code 番号を持つパケットのみが一致します。
- <protocol>に ICMPv6(58) 以外を指定し、かつ<icmptype>、<icmpcode>を指定している場合、あらゆるパケットが一致しません。

● <tcpconnect>の扱いを以下に示します。

- <protocol>に any を指定した場合、TCP パケットのときにこの設定値が適用されます。
- <protocol>に TCP(6) を指定した場合、常にこの設定値が適用されます。
- <protocol>に any または TCP(6) 以外を指定した場合、この設定値は適用されません。

IPv6 フィルタリングの旧定義は、本装置全体で次の数まで定義できます。

最大定義数	機種
1000	Si-R570　Si-R370
200	Si-R260B　Si-R240　Si-R220B
64	Si-R180

また、ACL 参照定義は、ほかの ACL 参照定義 (IP フィルタ、帯域制御 (WFQ) など) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B Si-R240 Si-R220B
450	Si-R180

旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

[注意]

定義数の計算は「テンプレート情報で設定した定義数 x テンプレートで使用する rmt インタフェース数」で計算されますので、それを含めて装置最大定義数の範囲に収まるように定義してください。
装置最大定義数を超えた場合は資源不足により、該当機能が動作しない場合があります。

[未設定時]

IPv6 フィルタを設定しないものとみなされ、すべてのパケットが透過します。

9.4.4　template ip6 filter move

[機能]

IPv6 フィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip6 filter move <count> <new_count>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義の番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0〜999	Si-R570　Si-R370
0〜199	Si-R260B　Si-R240　Si-R220B
0〜63	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv6 フィルタの優先順序を変更します。
旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

9.4.5 template ip6 filter default

[機能]

どの IP フィルタテーブルにも不一致時の動作の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip6 filter default <action> [<time>]

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<action>

どの IPv6 フィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- pass
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。
- spi
  該当するパケットに対して SPI を動作させます。

<time>

- 割当時間
  action に spi を指定したときに接続に割り当てられたテーブルを解放するための無通信監視時間を、0 秒〜86400 秒 (1 日) の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。
  0 秒を指定した場合は、変換テーブル解放のための監視を行いません。
  省略時は、5 分を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

どの IPv6 フィルタテーブルにも一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

どの IPv6 フィルタテーブルにも一致しないパケットは透過します。

```
template <number> ip6 filter default pass
```

9.4.6　template ip6 trafficclass

[機能]

トラフィッククラス値書き換え条件の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip6 trafficclass <count> acl <acl_count> <new_trafficclass>
template [<number>] ip6 trafficclass <count> <src_addr>/<prefixlen> <src_port> <dst_addr>/<prefixlen> <dst_port> <protocol> <trafficclass> <new_trafficclass>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- Traffic Class 値書き換え定義番号
  Traffic Class 値書き換え条件の優先度を表す定義番号を、10 進数値で指定します。
  指定した値は、設定完了時に順方向にソートされてリナンバリングされます。
  また、指定した定義番号と同じ値を持つ Traffic Class 値書き換え定義がすでに存在する場合は、既存定義の値を変更します。

範囲	機種
0〜499	Si-R570　Si-R370
0〜99	Si-R260B　Si-R240　Si-R220B
0〜31	Si-R180

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、その定義は無効となり、無視されます。
  Traffic Class 書き換えでは、ACL の以下の定義を使用します。
  - ip6
    ip6 値が設定されていない場合、その定義は無効となり、無視されます。
  - tcp
    ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip6 の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。
  - udp
    ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip6 の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp
  ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B Si-R240 Si-R220B
0〜149	Si-R180

<src_addr>/<prefixlen>

書き換え対象とする送信元 IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長
  書き換え対象とする送信元 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- any
  すべての送信元 IPv6 アドレスを書き換え対象とする場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<src_port>

書き換え対象とする送信元ポート番号を指定します。

- ポート番号
  書き換え対象とする送信元ポート番号を、1〜65535 の 10 進数値で指定します。
  複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、
  <dst_port>合わせて 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)
- any
  すべての送信元ポート番号を書き換え対象とする場合に指定します。

<dst_addr>/<prefixlen>

書き換え対象とするあて先 IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長
  書き換え対象とするあて先 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- any
  すべてのあて先 IPv6 アドレスを書き換え対象とする場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<dst_port>

書き換え対象とするあて先ポート番号を指定します。

- ポート番号
  書き換え対象とするあて先ポート番号を、1～65535 の 10 進数値で指定します。
  記述形式は、<src_port>と同様です。
- any
  すべてのあて先ポート番号を書き換え対象とする場合に指定します。

<protocol>

書き換え対象とするプロトコル番号を指定します。

- プロトコル番号
  書き換え対象とするプロトコル番号を、0～254 の 10 進数値で指定します。
- any
  すべてのプロトコルを書き換え対象とします。

<trafficclass>

- Traffic Class 値
  書き換え対象となる Traffic Class フィールドの値を 0-ff までの 16 進数値、または、"-"を使用して表現される 16 進数値の範囲を指定します。
  Traffic Class 値の指定は、"," を区切として 10 個まで設定可能です。
  複数の Traffic Class 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。
  Traffic Class 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 00～ff の 16 進数値 (例: ff = ff の Traffic Class 値)
  - Traffic Class 値-Traffic Class 値 (例: 32-64 = 32 から 64 までの Traffic Class 値)
  - Traffic Class 値- (例: 80- = 80 から ff までの Traffic Class 値)
  - -Traffic Class 値 (例: -7f = 0 から 7f までの Traffic Class 値)
  - Traffic Class 値,Traffic Class 値,… (例: 10,20,30- = 10 と 20 と 30 以降の Traffic Class 値)
- any
  すべての Traffic Class 値を書き換え対象とします。

<new_trafficclass>

- Traffic Class 値
  書き換える Traffic Class 値を、0～ff の 16 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

Traffic Class 値書き換え条件を設定します。
条件に一致したパケットの Traffic Class 値を、指定した Traffic Class 値に書き換えます。
Traffic Class 値書き換えの旧定義は、本装置全体で次の数まで定義できます。

最大定義数	機種
500	Si-R570 Si-R370
100	Si-R260B Si-R240 Si-R220B
32	Si-R180

また、ACL 参照定義は、ほかの ACL 参照定義 (IP フィルタ、帯域制御 (WFQ) など) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B Si-R240 Si-R220B
450	Si-R180

旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

[注意]

定義数の計算は「テンプレート情報で設定した定義数 x テンプレートで使用する rmt インタフェース数」で計算されますので、それを含めて装置最大定義数の範囲に収まるように定義してください。
装置最大定義数を超えた場合は資源不足により、該当機能が動作しない場合があります。

[未設定時]

Traffic Class 値書き換えを行わないものとみなされます。

9.4.7　template ip6 trafficclass move

[機能]

Traffic Class 値書き換え条件の優先度の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip6 trafficclass move <count> <new_count>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象 Traffic Class 値書き換え定義番号
  優先順序を変更する前の Traffic Class 値書き換え定義番号を指定します。

<new_count>

- 移動先 Traffic Class 値書き換え定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0〜499	Si-R570　Si-R370
0〜99	Si-R260B　Si-R240　Si-R220B
0〜31	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

Traffic Class 値書き換え条件の優先度を変更します。
旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

9.4.8 template ip6 priority

[機能]

IPv6 プロトコル帯域制御の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip6 priority <count> acl <acl_count> <width>
template [<number>] ip6 priority <count> <src_addr>/<prefixlen> <src_port> <dst_addr>/<prefixlen> <dst_port> <protocol> <trafficclass> <width>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 帯域制御定義番号
  帯域制御定義番号を、10 進数値で指定します。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B Si-R240 Si-R220B
0〜63	Si-R180

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、その定義は無効となり、無視されます。IPv6 プロトコル帯域制御では、ACL の以下の定義を使用します。

  - ip6
    ip6 値が設定されていない場合、その定義は無効となり、無視されます。
  - tcp
    ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip6 の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。
  - udp
    ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip6 の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp
  ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B　Si-R240　Si-R220B
0〜149	Si-R180

<src_addr>/<prefixlen>

帯域制御の対象とする送信元 IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長
  帯域制御の対象とする送信元 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- any
  すべての送信元 IPv6 アドレスを帯域制御の対象とする場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<src_port>

帯域制御の対象とする送信元ポート番号を指定します。

- ポート番号
  帯域制御の対象となる送信元ポート番号を、1〜65535 の 10 進数値で指定します。
  複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、
  <dst_port>合わせて 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)
- any
  すべてのポート番号を対象とする場合に指定します。

<dst_addr>/<prefixlen>

帯域制御の対象とするあて先 IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長
  帯域制御の対象とするあて先 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- any
  すべてのあて先 IPv6 アドレスを帯域制御の対象とする場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<dst_port>

帯域制御の対象とするあて先ポート番号を指定します。

- ポート番号
  帯域制御の対象となるあて先ポート番号を、1〜65535 の 10 進数値で指定します。
  記述形式は<src_port>と同様です。
- any
  すべてのポート番号を対象とする場合に指定します。

<protocol>

帯域制御の対象とするプロトコル番号を指定します。

- プロトコル番号
  帯域制御の対象となるプロトコル番号を、0〜254 の 10 進数値で指定します (例: TCP:6、UDP:17、ICMPv6:58 など)。
- any
  すべてのプロトコル番号をフィルタリング対象とする場合に指定します。

<trafficclass>

- 帯域制御対象 Traffic Class 値
  帯域制御の対象となる Traffic Class フィールドの値を 0-ff までの 16 進数値、または、"-"を使用して表現される 16 進数値の範囲を指定します。
  Traffic Class 値の指定は、"," を区切として 10 個まで設定可能です。
  複数の Traffic Class 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。
  Traffic Class 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 00〜ff の 16 進数値 (例: ff = ff の Traffic Class 値)
  - Traffic Class 値-Traffic Class 値 (例: 32-64 = 32 から 64 までの Traffic Class 値)
  - Traffic Class 値- (例: 80- = 80 から ff までの Traffic Class 値)
  - -Traffic Class 値 (例: -7f = 0 から 7f までの Traffic Class 値)
  - Traffic Class 値,Traffic Class 値,… (例: 10,20,30- = 10 と 20 と 30 以降の Traffic Class 値)
- any
  すべての Traffic Class 値を、帯域制御の対象とします。省略時は any として扱われます。

<width>

- express
  最優先データとして扱います。
- besteffort
  非優先 (ベストエフォート) として扱います。
- 帯域
  1〜99 の 10 進数値で指定した場合、それぞれ指定した値の比で帯域を割り当てます。たとえば、同じ相手ネットワーク中の定義が 3 つあり、それぞれ<width>の値が 30、30、60 であった場合、帯域として 25%、25%、50%が割り当てられます。なお、1〜99 を指定した定義のそれぞれの合計値が 100 未満の場合、残った帯域は定義に一致しないデータ用の帯域となります。
  「数字 + "kbps"(,"mbps")」で指定した場合、指定した帯域をそのまま割り当てます。1kbps〜100000kbps または、1mbps〜100mbps の範囲で指定します。全定義の帯域の合計が回線速度を超えた場合は、それぞれ指定した値の比で帯域を割り当てます。

指定した値の合計値が回線速度に達しない場合、残った帯域は定義に一致しないデータ用の帯域となります。

「"share" + 数字」で指定した場合、数字で指定した帯域制御定義番号で定義された帯域を共有します。この場合、指定する数字は自分自身の帯域制御定義番号より小さい、すでに定義されてあるもの指定しなければなりません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv6 プロトコル帯域制御を設定します。任意のプロトコル、アドレス、ポート、トラフィッククラスを指定して、割り当てる帯域を指定します。
IPv6 プロトコル帯域制御の旧定義は、本装置全体で次の数まで定義できます。

最大定義数	機種
1000	Si-R570
500	Si-R370
100	Si-R260B　Si-R240　Si-R220B
64	Si-R180

また、ACL 参照定義は、ほかの ACL 参照定義 (IP フィルタ、帯域制御 (WFQ) など) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B　Si-R240　Si-R220B
450	Si-R180

旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

[注意]

ISDN、専用線、フレームリレー以外の回線上で帯域制御機能を使用する場合は、シェーピングを使用しないと帯域制御は有効に動作しません。
定義数の計算は「テンプレート情報で設定した定義数 x テンプレートで使用する rmt インタフェース数」で計算されますので、それを含めて装置最大定義数の範囲に収まるように定義してください。
装置最大定義数を超えた場合は資源不足により、該当機能が動作しない場合があります。

[未設定時]

IPv6 プロトコル帯域制御を行わないものとみなされます。

9.4.9 template ip6 in-policy

[機能]

Ingress ポリシールーティングの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip6 in-policy <in-policy_number> policy-group <policy-group_number>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<in-policy_number>

- Ingress ポリシールーティング定義番号
  この I/F での Ingress ポリシールーティング定義の通し番号を、10 進数値で指定します。
  本定義は、ほかのポリシーグループ参照定義を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
2000	Si-R570
1000	Si-R370
200	Si-R260B Si-R240 & tbl220b;
100	Si-R180

<policy-group_number>

- ポリシーグループ番号
  参照するポリシーグループ番号を、10 進数値で指定します。
  IPv6 Ingress ポリシールーティングでは、ポリシーグループで指定された ACL の以下の定義を使用します。

  - ip6
    ip6 値が設定されていない場合、その定義は無効となり、無視されます。
  - tcp
    ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip6 の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。
  - udp
    ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。
    また、ip6 の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp

  ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B　Si-R220B
0〜49	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

Ingress ポリシールーティングに使用するポリシーグループを指定します。

[注意]

Ingress ポリシールーティングを行う場合は、必ずポリシーグループ指定を行う必要があります。
また、定義されている全ポリシーグループと不一致の場合は、アドレスによる経路探索が行われます。

[未設定時]

Ingress ポリシールーティングを設定しないとみなされます。

9.4.10 template ip6 in-policy move

[機能]

Ingress ポリシールーティングの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ip6 in-policy move <count> <new_count>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 対象 Ingress ポリシールーティング定義番号
  優先順序を変更するフィルタリング定義の番号を指定します。

<new_count>

- 移動先 Ingress ポリシールーティング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

Ingress ポリシールーティングの優先順序を変更します。

9.5　動的 VPN 関連情報

9.5.1　template dvpn client

[機能]

動的 VPN 接続で使用するクライアント情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] dvpn client <conf_number>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<conf_number>

動的 VPN クライアント定義の定義番号を指定します。

- 動的 VPN クライアント定義の定義番号
  利用する動的 VPN クライアント定義の定義番号を、10 進数値で指定します。

範囲	機種
0〜5	Si-R570　Si-R370
0〜2	Si-R240　Si-R220B
0〜1	Si-R260B　Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN 接続で使用するクライアント情報を設定します。
動的 VPN 機能を利用する場合は、本コマンドまたは以下のコマンドを必ず実行してください。
template dvpn server address
template dvpn ua
template dvpn domain
template dvpn localnet
template dvpn interface

[注意]

本コマンドおよび上記のコマンドを設定した場合は、本コマンドが有効となります。
この場合、本コマンドを除く template dvpn コマンドはすべて無効となります。
また、本コマンドで指定したクライアント情報の設定が不足していた場合でも上記のコマンドは有効にはなりません。

[未設定時]

動的 VPN 接続で使用するクライアント情報を設定しないものとみなされます。

9.5.2　template dvpn server address

[機能]

動的 VPN サーバのアドレス、ポート番号の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] dvpn server <count> address <address> [<port>]
template [<number>] dvpn server <count> address <fqdn> [<port>]

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 動的 VPN サーバ定義番号
  動的 VPN サーバの定義番号を、0 から 1 までの 10 進数値で指定します。

<address>

- 動的 VPN サーバの IP アドレス
  動的 VPN サーバとなる IPv4 アドレスまたは IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  IPv4:　1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  IPv6:　::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<fqdn>

- 動的 VPN サーバの FQDN
  動的 VPN サーバの FQDN を、0x21,0x23～0x7e の 80 文字以内の ASCII 文字列で指定します。なお、RFC1034 では英数字、"-"(ハイフン)、"."(ピリオド) で
  ドメイン名をつけることを推奨しています。

<port>

- 動的 VPN サーバのポート番号
  動的 VPN サーバが要求を受信するポート番号を、1～65535 の 10 進数値で指定します。
  省略時は 5070 が指定されたものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN サーバのアドレス、ポート番号を設定します。
アドレスは、IP アドレスまたは、FQDN で指定します。
動的 VPN 接続で使用するクライアント情報を参照しないで動的 VPN 機能を利用する場合は、本コマンドを必ず実行してください。

[注意]

動的 VPN サーバの IP アドレスを複数設定したときは一番小さい動的 VPN サーバ定義番号に設定したものをプライマリ動的 VPN サーバとして扱います。

[未設定時]

動的 VPN サーバのアドレス、ポート番号を設定しないものとみなされます。

9.5.3　template dvpn server auth

[機能]

動的 VPN サーバの認証情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] dvpn server <count> auth <id> <password> [encrypted]

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 動的 VPN サーバ定義番号
  動的 VPN サーバの定義番号を、0 から 1 までの 10 進数値で指定します。

<id>

- 認証 ID
  認証 ID を、0x21,0x23～0x7e の文字で構成される 50 文字以内の文字列を指定します。

<password>

- 認証パスワード
  認証パスワードを、0x21,0x23～0x7e の文字で構成される 50 文字以内の文字列を指定します。
  show コマンドで表示される暗号化された認証パスワード文字列を encrypted とともに指定することもできます。その場合、表示された文字列をそのまま正確に入力してください。文字列は 50 文字を超えていてもかまいません。
- 暗号化された認証パスワード
  show コマンドで表示される暗号化された認証パスワードを encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化認証パスワード指定
  <password>に暗号化された認証パスワードを設定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN サーバへ自装置情報を登録する時に使用する認証情報 (認証 ID およびパスワード) を設定します。
show コマンドでは、暗号化された認証パスワードが encrypted と共に表示されます。

[未設定時]

使用する認証情報を設定しないものとみなされます。

9.5.4 template dvpn expire register

[機能]

動的 VPN の情報有効期間の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] dvpn expire register <time>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<time>

- 情報有効期間
  動的 VPN サーバに登録する自装置の有効期間を 90 秒～86400 秒の範囲で指定します。単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  省略時は 1h が指定されたものとみなします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN サーバに登録する自装置情報の有効期間を設定します。

[未設定時]

情報有効期間に 1h を指定したものとみなされます。

```
template <number> dvpn expire register 1h
```

9.5.5　template dvpn expire session

[機能]

動的 VPN のセッション更新間隔の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] dvpn expire session <time>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<time>

- セッション更新間隔
  確立した動的 VPN セッションを更新する時間を 90 秒～3600 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  省略時は 5m が指定されたものとみなします。
- off
  確立した動的 VPN セッションの更新は行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

確立した動的 VPN セッションの更新間隔を設定します。

[未設定時]

セッション更新間隔に 5m を指定したものとみなされます。

```
template <number> dvpn expire session 5m
```

9.5.6 template dvpn ua

[機能]

動的 VPN クライアントのアドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] dvpn ua <address>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<address>

- 動的 VPN クライアントの IP アドレス
  動的 VPN クライアントとなる IPv4 アドレスまたは IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  IPv4: 1.0.0.1 〜 126.255.255.254
  128.0.0.1 〜 191.255.255.254
  192.0.0.1 〜 223.255.255.254

  IPv6: ::2 〜 fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: 〜 feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

IPv6 DHCP クライアントが取得したプレフィックスを使用する場合は上位を"dhcp@インタフェース名"の形式で指定し、下位 80bit 分を IPv6 アドレス形式で指定します。インタフェース名には、rmt インタフェースを以下の範囲で指定します。

範囲	機種
rmt0〜rmt999	Si-R570
rmt0〜rmt499	Si-R370
rmt0〜rmt99	Si-R260B Si-R240 Si-R220B
rmt0〜rmt49	Si-R180

例) rmt0 で動作する IPv6 DHCP クライアントが取得した IPv6 プレフィックスを使用する場合の設定例

```
dhcp@rmt0::
dhcp@rmt0::1:2:3:4
```

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN クライアントのアドレスを設定します。
動的 VPN 接続で使用するクライアント情報を参照しないで動的 VPN 機能を利用する場合は、本コマンドを必ず実行してください。

[注意]

動的 VPN クライアントのアドレスに IPv6 DHCP クライアントが取得したプレフィックスを使用する場合、プレフィックスが割り当てられるインタフェースと同じ値になるように指定してください。

[未設定時]

動的 VPN クライアントのアドレスを設定しないものとみなされます。

9.5.7 template dvpn domain

[機能]

動的 VPN ドメイン名の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] dvpn domain <domain>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<domain>

- ドメイン名
  動的 VPN サーバに登録する動的 VPN ドメイン名を、0x21,0x23〜0x7e の 80 文字以内の ASCII 文字列で指定します。なお、RFC1034 では英数字、"-"(ハイフン)、"." (ピリオド) でドメイン名をつけることを推奨しています。

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN ドメイン名を指定します。動的 VPN ドメイン名は、動的 VPN サーバに登録する自側ユーザ ID の一部として使用されます。
動的 VPN 接続で使用するクライアント情報を参照しないで動的 VPN 機能を利用する場合は、本コマンドを必ず実行してください。

[未設定時]

動的 VPN サーバに登録する動的 VPN ドメイン名を設定しないものとみなされます。

9.5.8　template dvpn localnet

[機能]

動的 VPN で接続する自側ネットワークの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] dvpn localnet <count> <address>/<mask> [<register>]

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- プレフィックス定義番号
  プレフィックスの定義番号を、0 から 19 までの 10 進数値で指定します。
  指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つプレフィックス定義がすでに存在する場合は、既存の定義を変更します。

<address>/<mask>

- 自側ネットワーク
  自側ネットワークを IPv4 アドレス/マスクビット数 (またはマスク値) または IPv6 アドレスとプレフィックス長で指定します。

  IPv4:　IPv4 アドレスとマスクビット数の組み合わせで指定します。
  マスク値は、最上位ビットから 1 で連続した値にしてください。
  デフォルトルートを設定する場合は、0.0.0.0/0(0.0.0.0/0.0.0.0) を指定します。

  IPv6:　IPv6 アドレスとプレフィックスの組み合わせで指定します。
  リンクローカルアドレスは指定できません。
  デフォルトルートを設定する場合は、::/0 を指定します。
  IPv6 DHCP クライアントが取得したプレフィックスを使用する場合は上位を"dhcp@インタフェース名"の形式で指定し、下位 80bit 分を IPv6 アドレス形式で指定します。インタフェース名には、rmt インタフェースを以下の範囲で指定します。

範囲	機種
rmt0～rmt999	Si-R570
rmt0～rmt499	Si-R370
rmt0～rmt99	Si-R260B　Si-R240　Si-R220B
rmt0～rmt49	Si-R180

rmt0 で動作する IPv6 DHCP クライアントが取得した IPv6 プレフィックスを使用する場合の設定例

```
dhcp@rmt0::/64
dhcp@rmt0::1:2:3:4/64
```

プレフィックス長には 64 を指定してください。

<register>

- on
  自側ユーザ ID を生成して動的 VPN サーバに登録します。
- off
  自側ユーザ ID を生成せず動的 VPN サーバに登録しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN で接続する自側ネットワークを IPv4 アドレス/マスクビット数 (またはマスク値) または IPv6 アドレスとプレフィックス長と自側ユーザ ID を生成して動的 VPN サーバに登録するかどうかを指定します。
自側ユーザ ID を生成して動的 VPN サーバに登録すると指定した場合、通信パケット契機で動的 VPN 接続をすることができます。通常は、動的 VPN サーバに登録するにしてください。
自側ユーザ ID は、自側ネットワークとドメイン名を結合して以下のように生成されます。

例) 自側ネットワークに 192.168.1.0/24(2001:db8:1111:1::/64)、ドメイン名に example.com を指定した場合

```
IPsecIKE)c0a80100/24@example.com
IPsecIKE)20010db81111000100000000000000000/64@example.com
```

動的 VPN 接続で使用するクライアント情報を参照しないで動的 VPN 機能を利用する場合は、本コマンドを必ず実行してください。

[注意]

自側ネットワーク設定の 0 番目の定義は、IKE ネゴシエーションに使用します。よって、相手装置の自側ネットワーク設定の 0 番目定義のアドレスファミリと一致するように設定してください。
動的 VPN で接続する自側ネットワークを異るアドレスファミリで設定した場合、拡張 IPsec 対象範囲として 1 定義分使用されます。
拡張 IPsec 対象範囲機能未対応版数 (V30) の装置と動的 VPN 接続を行う場合、動的 VPN で接続する自側ネットワークに異るアドレスファミリの設定を行わないでください。
自側ネットワークに IPv6 DHCP クライアントが取得したプレフィックスを使用する場合、プレフィックスが割り当てられるインタフェースと同じ値になるように指定してください。
自側ネットワークは、本コマンドおよび dvpn client localnet コマンドで重複しないように指定してください。

[未設定時]

動的 VPN で接続する自側ネットワークを設定しないものとみなされます。

9.5.9　template dvpn localid

[機能]

動的 VPN サーバに登録する自側ユーザ ID の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] dvpn localid <id>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<id>

- 自側ユーザ ID
  自側ユーザ ID となる ID を、50 文字以内の ASCII 文字列で指定します。
  指定可能な範囲は以下のとおりです。

文字	範囲
半角アルファベット	a〜z, A〜Z
半角数値	0〜9
半角記号	'-', '_', '.'

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN サーバに登録する自側ユーザ ID を指定します。
本コマンドで指定した自側ユーザ ID は、ドメイン名と結合して以下のように生成されて動的 VPN サーバに登録されます。

例)　template dvpn localid shisya、template dvpn domain example.com と指定した場合

```
shisya@example.com
```

動的 VPN 接続で使用するクライアント情報を参照しないでオペレータの指示で動的 VPN 接続を行いたい場合に指定してください。

[未設定時]

動的 VPN サーバに登録する自側ユーザ ID を設定しないものとみなされます。

9.5.10 template dvpn interface

[機能]

VPN 通信で利用するインタフェースの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] dvpn interface <kind> <conf_number> [<nexthop>]

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<kind>

- lan
  lan 定義によって指定される回線を利用する場合に指定します。
- rmt
  rmt 定義によって指定される回線を利用する場合に指定します。

<conf_number>

lan 定義または rmt 定義の定義番号を指定します。

- lan 定義の定義番号
  利用する lan の定義番号を、10 進数値で指定します。

範囲	機種
0〜19	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B
0〜9	Si-R180

- rmt 定義の定義番号
  利用する rmt の定義番号を、10 進数値で指定します。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B Si-R240 Si-R220B
0〜49	Si-R180

<nexthop>

<kind>に lan を指定した場合で、相手 IPsec トンネル IP アドレスに対する経路を設定する場合に利用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN として接続される IPsec トンネルが通信に利用するインタフェースを設定します。
動的 VPN 接続で使用するクライアント情報を参照しないで動的 VPN 機能を利用する場合は、本コマンドを必ず実行してください。

[未設定時]

VPN 通信で利用するインタフェースを設定しないものとみなされます。

9.5.11 template dvpn global

[機能]

VPN 通信の終端グローバルアドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] dvpn global <address>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<address>

相手装置に通知する VPN 終端グローバルアドレスを以下の範囲で指定します。

1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手装置に通知する VPN 終端グローバルアドレスを指定します。
この設定は、template dvpn interface コマンドで指定されたインタフェースで NAT 機能を使用している場合にのみ参照されます。

[未設定時]

template dvpn interface コマンドで lan を指定した場合は、指定された lan インタフェースに設定されたアドレスが利用されます。
template dvpn interface コマンドで remote を指定した場合は、指定された rmt インタフェースに設定されたアドレス、または PPP により割り当てられたアドレスが利用されます。アドレスがない場合は VPN 接続は行えません。

9.6　IPsec 関連情報

9.6.1　template ipsec ike protocol

[機能]

自動鍵交換用 IPsec 情報のセキュリティプロトコルの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ipsec ike protocol <protocol>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<protocol>

自動鍵交換用 IPsec SA のセキュリティプロトコルを指定します。

- none
  セキュリティプロトコル未指定
- esp
  暗号
- ah
  認証

[動作モード]

構成定義モード (管理者クラス)

[説明]

自動鍵交換用 IPsec SA の、セキュリティプロトコルの設定を行います。

[未設定時]

自動鍵交換用 IPsec 情報のセキュリティプロトコルは未指定となります。

```
template <number> ipsec ike protocol none
```

9.6.2 template ipsec ike encrypt

[機能]

自動鍵交換用 IPsec 情報の暗号情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ipsec ike encrypt <enc_algo>[,<enc_algo>...]

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<enc_algo>

暗号アルゴリズムを指定します。
複数のアルゴリズムを指定することができます。複数定義する時は、アルゴリズムを空白なしでカンマ’,’ で区切ります。

- des-cbc
- 3des-cbc
- aes-cbc-128
- aes-cbc-192
- aes-cbc-256
- null
- none

[動作モード]

構成定義モード (管理者クラス)

[説明]

送受信パケットを暗号化/復号化するための、暗号アルゴリズムの設定を行います。
暗号アルゴリズムを複数指定する場合、指定順序にかかわらず以下の優先順位となります。
暗号アルゴリズムの"aes-cbc"に続く数字は鍵長を表しています。
数字が大きいほど強固な鍵になりますが、その分処理時間を要します。

- aes-cbc-256
- aes-cbc-192
- aes-cbc-128
- 3des-cbc
- des-cbc
- null

[未設定時]

IPsec によるパケット暗号は行われません。

```
template <number> ipsec ike encrypt none
```

9.6.3 template ipsec ike auth

[機能]

自動鍵交換用 IPsec 情報の認証情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ipsec ike auth <auth_algo>[,<auth_algo>...]

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<auth_algo>

認証アルゴリズムを指定します。
複数のアルゴリズムを指定することができます。複数定義する時は、アルゴリズムを空白なしでカンマ',' で区切ります。

- hmac-md5
- hmac-sha1
- none

[動作モード]

構成定義モード (管理者クラス)

[説明]

送受信パケットを認証するための、認証アルゴリズムの設定を行います。
認証アルゴリズムを複数指定する場合、指定順序にかかわらず以下の優先順位となります。

- hmac-md5
- hmac-sha1

[未設定時]

IPsec によるパケット認証は行われません。

```
template <number> ipsec ike auth none
```

9.6.4　template ipsec ike pfs

[機能]

自動鍵交換用 IPsec 情報の PFS 使用時の DH(Diffie-Hellman) グループの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ipsec ike pfs <pfs_group>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<pfs_group>

Diffie-Hellman グループについて指定します。

- modp768
  Diffie-Hellman グループの MODP768(グループ 1)
- modp1024
  Diffie-Hellman グループの MODP1024(グループ 2)
- modp1536
  Diffie-Hellman グループの MODP1536(グループ 5)
- off
  Diffie-Hellman グループを使用しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPsec セッションの鍵素材を保護する、PFS 使用時の DH(Diffie-Hellman) グループの設定を行います。

[未設定時]

PFS による鍵交換データ保護は行いません。セキュア通信を行いたい場合は適切な PFS 使用時の DH グループを設定してください。

```
template <number> ipsec ike pfs off
```

9.6.5 template ipsec ike lifetime

[機能]

自動鍵交換用 IPsec 情報の SA 有効時間の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ipsec ike lifetime <lifetime>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<lifetime>

- SA 有効時間
  SA 有効時間を、600 秒 (10 分)〜86400 秒 (1 日) の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPsec セッションの通信データを保護する、IPsec SA の SA 有効時間 (秒) の設定を行います。

[未設定時]

IPsec SA の有効時間として 8h(8 時間) が設定されたものとして扱います。

```
template <number> ipsec ike lifetime 8h
```

9.6.6　template ipsec ike lifebyte

[機能]

自動鍵交換用 IPsec 情報の SA 有効パケット量の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ipsec ike lifebyte <lifebyte>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<lifebyte>

- SA 有効パケット量
  IPsec 用 Security Association(SA) 有効パケット量のバイト数を、0 または 2400k〜108000m の範囲で指定します。
  単位は以下の 3 種類です。1k は 1024 バイトで計算されます。

  k:　キロバイト (例: 2400k → 2400k)

  m:　メガバイト (例: 4m → 4096k)

  g:　ギガバイト (例: 1g → 1048576k)

  0 を指定した場合は、lifebyte による IPsec SA の更新を行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPsec セッションの通信データを保護する、IPsec SA の SA 有効パケット量 (キロバイト) の設定を行います。

[未設定時]

SA 有効パケット量に 0 バイトを指定したものとみなされます。

```
template <number> ipsec ike lifebyte 0
```

9.6.7 template ipsec ike newsa initiator

[機能]

自動鍵交換用 IPsec 情報の New SA Initiator(更新時間/更新データ量) の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ipsec ike newsa initiator <time> [<byte>]

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<time>

- Initiator SA 更新時間
  Initiator SA 更新時間を、30 秒～180 秒 (3 分) の範囲で指定します。
  単位は、m(分)、s(秒) のどれかを指定します。

<byte>

- Initiator SA 更新データ量
  Initiator SA 更新データ量を、0 または 120kbyte～230400kbyte の範囲で指定します。
  単位は、k(キロバイト)、m(メガバイト) のどれかを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

自側が Initiator の場合に、IPsec SA の有効時間または SA 有効データ量が満了になる前に、IPsec SA の更新を行うための時間／データ量の設定を行います。
相手側の New SA Responder と同じ時間／データ量にならないように設定してください。
また、SA 有効データ量の設定を行い、更新データ量設定が 0 指定時には有効データ量満了した時点で SA 更新が行われます。

[未設定時]

Initiator SA 更新時間として 90s(90 秒)、データ量として 0k(0kbyte) が設定されたものとして扱います。

```
template <number> ipsec ike newsa initiator 90s 0
```

9.6.8　template ipsec ike newsa responder

[機能]

自動鍵交換用 IPsec 情報の New SA Responder(更新時間／更新データ量) の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ipsec ike newsa responder <time> [<byte>]

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<time>

- Responder SA 更新時間
  Responder SA 更新時間を、30 秒～180 秒 (3 分) の範囲で指定します。
  単位は、m(分)、s(秒) のどれかを指定します。
- off
  Responder 側からの SA 更新は行いません。

<byte>

- Responder SA 更新データ量
  Responder SA 更新データ量を、0 または 120kbyte～230400kbyte の範囲で指定します。
  単位は、k(キロバイト)、m(メガバイト) のどれかを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

自側が Responder の場合に、IPsec SA の有効時間または SA 有効データ量が満了になる前に、IPsec SA の更新を行うための時間／データ量の設定を行います。
相手側の New SA Initiator と同じ時間／データ量にならないように設定してください。
また、SA 有効データ量の設定を行い、更新データ量設定が 0 指定時には有効データ量満了した時点で SA 更新が行われます。更新時間設定が off 指定時には Responder 側からの SA 更新は行いません。

[未設定時]

Responder SA 更新時間として 30s(30 秒)、データ量として 0k(0kbyte) が設定されたものとして扱います。
RADIUS では、SA 更新時間として off、データ量として 0k(0kbyte) が設定されたものとして扱います。

```
template <number> ipsec ike newsa responder 30s 0
```

9.7 IKE 関連情報

9.7.1 template ike shared key

[機能]

IKE セッション確立時の共有鍵 (Pre-shared key) の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ike shared key <kind> [<shared_key> [encrypted]]

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<kind>

鍵種別を指定します。

- hex
  16 進数鍵を使用します。
- text
  文字列鍵を使用します。
- dynamic
  動的 VPN 機能により配布された共有鍵を使用する場合に指定します。

<shared_key>

共有鍵 (事前共有秘密鍵方式) を指定します。

- 暗号化されていない共有鍵を指定します。
  文字列鍵の場合は、0x22(ダブルクォーテーション) を除く [0x20-0x7e] の範囲のコードで構成される ASCII 文字列で指定します。ただし、文字列鍵で 0x20(空白文字) を使用する場合は、文字列鍵をダブルクォーテーション (") で囲う必要があります。
  以下に、入力範囲を示します。

鍵種別	16進数鍵	文字列鍵
共有鍵	1～256桁	1～128文字

- 暗号化された共有鍵を指定します。
  show コマンドで表示される暗号化された共有鍵を encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化共有鍵指定
  <shared_key>に暗号化された共有鍵を指定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

SA 確立のネゴシエーションのときに接続相手を認証するための、共有鍵の設定を行います。
show コマンドでは、暗号化された共有鍵が encrypted と共に表示されます。
動的 VPN 接続を行う場合に限り、<kind>に dynamic を指定することができます。
dynamic を指定した場合は、共有鍵の指定はできません。

[注意]

dynamic は、テンプレートが利用する機能の設定で dvpn を指定したときだけ有効となります。

[未設定時]

共有鍵が設定されません。
動的 VPN 機能を利用して IKE により鍵交換を行う場合は必ず設定してください。

9.7.2 template ike proposal move

[機能]

IKE セッション用 Proposal 定義優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ike proposal move <proposal_number> <new_number>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<proposal_number>

- 移動元の Proposal 定義優先順序を指定します。

<new_number>

- 移動先の Proposal 定義優先順序を指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IKE セッション用の Proposal 定義優先順序を変更します。IKE セッション用 Proposal 定義とネゴシエーションの関係

	ネゴシエーション情報	Proposal	Proposal	...
a	暗号情報	3des-cbc	des-cbc	...
b	認証(ハッシュ)情報	hmac-md5	0	...
c	DHグループ	modp768	modp1024	...
d	SA有効時間	600s	0	...

※ a を複数指定 (<proposal_number>0,1,2 を定義) した場合、ほかの情報は定義しなければ各情報のデフォルト値を採用します。
IKE セッションのネゴシエーションは、Proposal 単位 (a〜d を一組) として行います。その中で a〜c は相手装置の定義と一致することが条件となります。
自側が Responder の場合は、相手の Proposal が許容できるかを判断するため、自装置の定義は参照されません。
本装置を Aggressive Mode で動作させる時に、IKE セッション用 Proposal 定義を複数設定する場合、DH グループ設定はすべて同じ値を設定してください。
これは、Aggressive Mode が Diffie-Hellman のグループについてネゴシエーションができないためです。
(Initiator が最初の ISAKMP パケットに載せる鍵素材の計算に使用するため、Diffie-Hellman のグループは同じである必要があります)
Aggressive Mode は、相手 (リモート) 情報 tunnel 利用時の自側の tunnel endpoint address を未設定にし、IKE 情報の自装置識別情報を設定します。

9.7.3　template ike proposal encrypt

[機能]

IKE セッション用暗号情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ike proposal [<proposal_number>] encrypt <enc_algo>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<proposal_number>

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。
  省略時は、0 を指定したものとみなされます。

<enc_algo>

暗号アルゴリズムを指定します。

- des-cbc
- 3des-cbc
- aes-cbc-128
- aes-cbc-192
- aes-cbc-256

[動作モード]

構成定義モード (管理者クラス)

[説明]

IKE セッションの送受信パケットを暗号化/復号化するための、暗号アルゴリズムの設定を行います。
コマンドによる定義を行う場合は、必ず設定してください。
IKE セッション用暗号情報設定が未定義ですと IKE が動作しません。

[未設定時]

IKE セッション用暗号情報が設定されません。IKE により鍵交換を行う場合は必ず設定してください。

9.7.4 template ike proposal hash

[機能]

IKE セッション用認証 (ハッシュ) 情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ike proposal [<proposal_number>] hash <hash_algo>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<proposal_number>

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。
  省略時は、0 を指定したものとみなされます。

<hash_algo>

認証 (ハッシュ) アルゴリズムを指定します。

- hmac-md5
- hmac-sha1

[動作モード]

構成定義モード (管理者クラス)

[説明]

IKE セッションのネゴシエーションパケットを認証するための、ハッシュアルゴリズムの設定を行います。

[未設定時]

認証のためのハッシュアルゴリズムに hmac-md5 を指定したものとみなされます。

```
template <number> ike proposal <proposal_number> hash hmac-md5
```

9.7.5　template ike proposal pfs

[機能]

IKE セッション用 DH(Diffie-Hellman) グループの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ike proposal [<proposal_number>] pfs <pfs_group>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<proposal_number>

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。
  省略時は、0 を指定したものとみなされます。

<pfs_group>

Diffie-Hellman グループについて指定します。

- modp768
  MODP768(グループ 1) の Diffie-Hellman グループ
- modp1024
  MODP1024(グループ 2) の Diffie-Hellman グループ
- modp1536
  MODP1536(グループ 5) の Diffie-Hellman グループ

[動作モード]

構成定義モード (管理者クラス)

[説明]

IKE セッションのネゴシエーションパケットを保護するための、DH(Diffie-Hellman) グループの設定を行います。

[未設定時]

DH グループに modp768 を指定したものとみなされます。

```
template <number> ike proposal <proposal_number> pfs modp768
```

9.7.6 template ike proposal lifetime

[機能]

IKE 情報の SA 有効時間の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ike proposal [<proposal_number>] lifetime <lifetime>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<proposal_number>

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。
  省略時は、0 を指定したものとみなされます。

<lifetime>

- SA 有効時間
  SA 有効時間を、600 秒 (10 分)〜86400 秒 (1 日) の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IKE セッションのネゴシエーションパケットを保護するための、SA 有効時間 (秒) の設定を行います。

[未設定時]

IKE SA の有効時間として 24h(24 時間) が設定されたものとして扱われます。

```
template <number> ike proposal <proposal_number> lifetime 24h
```

9.7.7　template ike retry

[機能]

IKE 情報の初回再送時間および再送回数の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ike retry <time> <count>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<time>

- 初回再送時間
  初回再送時間を、1 秒～60 秒 (1 分) の範囲で指定します。
  単位は、m(分)、s(秒) のどちらかを指定します。

<count>

- 再送回数
  再送回数を、1～10 の範囲で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IKE セッションのネゴシエーションパケットに対する初回再送時間および再送回数の設定を行います。

[未設定時]

初回再送時間に 10 秒、再送回数に 3 回を設定したものとみなされます。

```
template <number> ike retry 10s 3
```

9.7.8 template ike idtype

[機能]

IKE 情報の送信 ID タイプの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ike idtype <id_type>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<id_type>

ネゴシエーションの送信 ID タイプを指定します。

- fqdn
  省略なしドメイン名
- user_fqdn
  省略なしユーザ識別名

[動作モード]

構成定義モード (管理者クラス)

[説明]

IKE セッションを確立する、ネゴシエーションの ID タイプの設定を行います。
IKE セッション確立のネゴシエーションパケットの ID payload に使用されます。

[未設定時]

IKE セッション確立のネゴシエーションパケットの ID タイプとして FQDN が設定されたものとして扱われます。

```
template <number> ike idtype fqdn
```

9.7.9　template ike release

[機能]

IPsec/IKE 情報の解放動作の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ike release <mode>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

IPsec/IKE の SA 情報の解放動作設定を指定します。

- on
  回線切断時に解放処理を行います。
- off
  解放処理は行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

自動鍵設定で作成された SA 情報の解放動作設定を行います。
on を指定した場合は、回線切断時に自動鍵設定が使用している SA 情報の解放動作を行います。
off を指定した場合は、回線切断時に自動鍵設定が使用している SA 情報の解放動作を行いません。

[注意]

本コマンド は、以下の回線切断動作時に有効です。
ただし、動的 VPN 接続で使用している回線が常時接続で切断された場合、動的 VPN 機能により追加された経路情報が削除されることにより本コマンド の設定にかかわらず IKE SA 情報および動的 VPN 接続が切断されます。

- ISDN(回線交換) を使用した時の回線切断時 (※ Si-R260B Si-R240 Si-R180 を除く)
- PPPoE を使用した時の切断時
- モデムを使用した時の切断時 (※ Si-R220B のみ)
- データ通信カード を使用した時の切断時 (※ Si-R240 のみ)

[未設定時]

回線切断時に IKE SA 情報の解放を行うものとみなされます。

```
template <number> ike release on
```

9.7.10　template ike mode

[機能]

IKE 情報の交換モードの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ike mode <mode>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

- IKE ネゴシエーションの交換モード
  IKE ネゴシエーションの交換モードを指定します。

  auto： テンプレートが利用する機能として DVPN を選択した場合は、Main Mode と判別します。
  テンプレートが利用する機能として AAA を選択した場合は、Aggressive Mode と判別します。

  aggressive：
  IKE 情報の交換モードとして Aggressive Mode を使用します。

  main： IKE 情報の交換モードとして Main Mode を使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IKE セッションを確立する、IKE ネゴシエーション交換モードの設定を行います。
ISAKMP SA のネゴシエーション交換モードについては、remote ap ike mode を参照してください。

[注意]

テンプレートが利用する機能として DVPN を選択し、<mode>に aggressive を設定した場合は、構成定義エラーとなります。

[未設定時]

IKE 情報の交換モードとして自動判別を行うものとみなされます。

```
template <number> ike mode auto
```

9.7.11 template ike nat-traversal use

[機能]

IKE 情報の NAT トラバーサル利用可否の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

template [<number>] ike nat-traversal use <mode>

[オプション]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mode>

NAT トラバーサルを利用するかどうかを指定します。

- off
  NAT トラバーサルを利用しない場合に指定します。
- on
  NAT トラバーサルを利用する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IKE ネゴシエーションパケットおよび IPsec パケットを NAT トラバーサルするための設定を行います。

[注意]

NAT トラバーサル機能を利用するときは、以下の点に注意してください。

- IKE を行う双方の装置で設定してください。片方の装置での利用や NAT トラバーサルのバージョンが異なると、NAT トラバーサルはできません。
  NAT トラバーサルは、以下の RFC、Internet Draft のバージョンをサポートします。

  “ Negotiation of NAT-Traversal in the IKE ”

  RFC3947
  draft-ietf-ipsec-nat-t-ike-03
  draft-ietf-ipsec-nat-t-ike-02

  “ UDP Encapsulation of IPsec ESP Packets ”

  RFC3948

- IPsec トンネルに存在する NAT 装置の変換テーブルが解放されると、NAT トラバーサルは動作できなくなります。変換テーブルを保持するために、接続先監視機能と併用することを推奨します。

- 自動鍵交換用 IPsec 情報の暗号アルゴリズムを設定し、自動鍵交換用 IPsec 情報のセキュリティプロトコルを暗号 (esp) を指定してください。暗号アルゴリズムおよびセキュリティプロトコルが暗号でない場合は動作しません。
- 自側トンネルエンドポイントアドレスに IPv4 アドレスを設定してください。IPv6 アドレスを設定した場合は動作しません。
- テンプレートが利用する機能に不特定相手着信 (aaa) を指定してください。動的 VPN(dvpn) を設定した場合は動作しません。
- IKE 情報の交換モードに Aggressive Mode(aggressive) を指定してください。Main Mode(main) を指定した場合は動作しません。

[未設定時]

IKE 情報の NAT トラバーサル利用に off を指定したものとみなされます。

```
template <number> ike nat-traversal use off
```

第 10 章　動的 VPN 情報の設定

- 動的 VPN クライアント定義番号の指定範囲

  本章のコマンドの [オプション] に記載されている<number>(動的 VPN クライアント定義番号) に指定する通し番号 (10 進数値) は、機種ごとに以下に示す範囲で指定してください。

範囲	機種
0〜5	Si-R570　Si-R370
0〜2	Si-R220B
0〜1	Si-R260B　Si-R240　Si-R180

10.1　動的 VPN サーバ情報

10.1.1　dvpn server use

[機能]

動的 VPN サーバ利用可否の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

dvpn server use <mode>

[オプション]

<mode>

- off
  利用しません。
- on
  利用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN サーバを利用するかどうかを設定します。

[未設定時]

動的 VPN サーバを利用しないものとみなされます。

```
dvpn server use off
```

10.1.2 dvpn server domain

[機能]

動的 VPN サーバが管理するドメイン名の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

dvpn server domain <domain>

[オプション]

<domain>

- ドメイン名
  使用する SIP ドメイン名を、0x21,0x23〜0x7e の 80 文字以内の ASCII 文字列で指定します。なお、RFC1034 では英数字、"-"(ハイフン)、"."(ピリオド) でドメイン名をつけることを推奨しています。

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN サーバが管理するドメイン名を設定します。

[未設定時]

動的 VPN サーバが管理するドメイン名が設定されていないものとみなされます。

10.1.3　dvpn server auth use

[機能]

動的 VPN サーバの認証の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

dvpn server auth use <mode>

[オプション]

<mode>

- off
  認証を行いません。
- on
  認証を行います。

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN サーバで認証を行うかどうかを設定します。

[未設定時]

動的 VPN サーバ認証を行わないものとみなされます。

```
dvpn server auth use off
```

10.1.4 dvpn server auth aaa

[機能]

動的 VPN サーバが参照する AAA 情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

dvpn server auth aaa [<group_id>]

[オプション]

<group_id>

- AAA のグループ ID
  AAA のグループ ID を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜9	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN サーバが認証を行う場合に参照する AAA のグループ ID を指定します。

[未設定時]

グループ ID に、0 を指定したものとみなされます。

```
dvpn server auth aaa 0
```

10.2　動的 VPN クライアント情報

10.2.1　dvpn client encode

[機能]

交換情報のエンコードタイプの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

dvpn client encode <type>

[オプション]

<type>

交換する情報のエンコードタイプを設定します。

- off
  交換する情報をエンコードしません。
- base64
  交換する情報を base64 エンコードします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

情報を交換する際の、エンコードタイプを設定します。
<type>に off を設定した場合は、情報をエンコードしないで交換します。

[注意]

V30 のソフトウェアと情報を交換する場合は、<type>に off を設定する必要があります。

[未設定時]

情報を base64 でエンコードして交換します。

```
dvpn client encode base64
```

10.2.2 dvpn client server address

[機能]

動的 VPN サーバのアドレス、ポート番号の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

dvpn client [<number>] server <count> address <address> [<port>]
dvpn client [<number>] server <count> address <fqdn> [<port>]

[オプション]

<number>

- 動的 VPN クライアント定義番号
  動的 VPN クライアントの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 動的 VPN サーバ定義番号
  動的 VPN サーバの定義番号を、0 から 1 までの 10 進数値で指定します。

<address>

- 動的 VPN サーバの IP アドレス
  動的 VPN サーバとなる IPv4 アドレスまたは IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  IPv4: 1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  IPv6: ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<fqdn>

- 動的 VPN サーバの FQDN
  動的 VPN サーバの FQDN を、0x21,0x23～0x7e の 80 文字以内の ASCII 文字列で指定します。なお、RFC1034 では英数字、"-"(ハイフン)、"."(ピリオド) でドメイン名をつけることを推奨しています。

<port>

- 動的 VPN サーバのポート番号
  動的 VPN サーバが要求を受信するポート番号を、1～65535 の 10 進数値で指定します。
  省略時は 5070 が指定されたものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN サーバのアドレス、ポート番号を設定します。
アドレスは、IP アドレスまたは、FQDN で指定します。
動的 VPN 機能を利用する場合は、本コマンドを必ず実行してください。

[注意]

動的 VPN サーバの IP アドレスを複数設定したときは一番小さい動的 VPN サーバ定義番号に設定したものをプライマリ動的 VPN サーバとして扱います。

[未設定時]

動的 VPN サーバのアドレス、ポート番号を設定しないものとみなされます。

10.2.3 dvpn client server auth

[機能]

動的 VPN サーバの認証情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

dvpn client [<number>] server <count> auth <id> <password> [encrypted]

[オプション]

<number>

- 動的 VPN クライアント定義番号
  動的 VPN クライアントの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 動的 VPN サーバ定義番号
  動的 VPN サーバの定義番号を、0 から 1 までの 10 進数値で指定します。

<id>

- 認証 ID
  認証 ID を、0x21,0x23～0x7e の文字で構成される 50 文字以内の文字列を指定します。

<password>

- 認証パスワード
  認証パスワードを、0x21,0x23～0x7e の文字で構成される 50 文字以内の文字列を指定します。
  show コマンドで表示される暗号化された認証パスワード文字列を encrypted とともに指定することもできます。その場合、表示された文字列をそのまま正確に入力してください。文字列は 50 文字を超えていてもかまいません。
- 暗号化された認証パスワード
  show コマンドで表示される暗号化された認証パスワードを encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化認証パスワード指定
  <password>に暗号化された認証パスワードを設定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN サーバへ自装置情報を登録する時に使用する認証情報 (認証 ID およびパスワード) を設定します。
show コマンドでは、暗号化された認証パスワードが encrypted と共に表示されます。

[未設定時]

使用する認証情報を設定しないものとみなされます。

10.2.4　dvpn client expire register

[機能]

動的 VPN の情報有効期間の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

dvpn client [<number>] expire register <time>

[オプション]

<number>

- 動的 VPN クライアント定義番号
  動的 VPN クライアントの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<time>

- 情報有効期間
  動的 VPN サーバに登録する自装置の有効期間を 90 秒～86400 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  省略時は 1h が指定されたものとみなします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN サーバに登録する自装置情報の有効期間を設定します。

[未設定時]

情報有効期間に 1h を指定したものとみなされます。

```
dvpn client <number> expire register 1h
```

10.2.5 dvpn client expire session

[機能]

動的 VPN のセッション更新間隔の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

dvpn client [<number>] expire session <time>

[オプション]

<number>

- 動的 VPN クライアント定義番号
  動的 VPN クライアントの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<time>

- セッション更新間隔
  確立した動的 VPN セッションを更新する時間を 90 秒〜3600 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  省略時は 5m が指定されたものとみなします。
- off
  確立した動的 VPN セッションの更新は行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

確立した動的 VPN セッションの更新間隔を設定します。

[未設定時]

セッション更新間隔に 5m を指定したものとみなされます。

```
dvpn client <number> expire session 5m
```

10.2.6　dvpn client ua

[機能]

動的 VPN クライアントのアドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

dvpn client [<number>] ua <address>

[オプション]

<number>

- 動的 VPN クライアント定義番号
  動的 VPN クライアントの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<address>

- 動的 VPN クライアントの IP アドレス
  動的 VPN クライアントとなる IPv4 アドレスまたは IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  IPv4: 1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  IPv6: ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

  IPv6 DHCP クライアントが取得したプレフィックスを使用する場合は上位を"dhcp@インタフェース名"の形式で指定し、下位 80bit 分を IPv6 アドレス形式で指定します。インタフェース名には、rmt インタフェースを以下の範囲で指定します。

範囲	機種
rmt0～rmt999	Si-R570
rmt0～rmt499	Si-R370
rmt0～rmt99	Si-R260B　Si-R240　Si-R220B
rmt0～rmt49	Si-R180

例) rmt0 で動作する IPv6 DHCP クライアントが取得した IPv6 プレフィックスを使用する場合の設定例
dhcp@rmt0::
dhcp@rmt0::1:2:3:4

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN クライアントのアドレスを設定します。
動的 VPN 機能を利用する場合は、本コマンドを必ず実行してください。

[注意]

動的 VPN クライアントのアドレスに IPv6 DHCP クライアントが取得したプレフィックスを使用する場合、プレフィックスが割り当てられるインタフェースと同じ値になるように指定してください。

[未設定時]

動的 VPN クライアントのアドレスを設定しないものとみなされます。

10.2.7　dvpn client domain

[機能]

動的 VPN ドメイン名の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

dvpn client [<number>] domain <domain>

[オプション]

<number>

- 動的 VPN クライアント定義番号
  動的 VPN クライアントの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<domain>

- ドメイン名
  動的 VPN サーバに登録する動的 VPN ドメイン名を、0x21,0x23〜0x7e の 80 文字以内の ASCII 文字列で指定します。なお、RFC1034 では英数字、"-"(ハイフン)、"." (ピリオド) でドメイン名をつけることを推奨しています。

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN ドメイン名を指定します。動的 VPN ドメイン名は、動的 VPN サーバに登録する自側ユーザ ID の一部として使用されます。
動的 VPN 機能を利用する場合は、本コマンドを必ず実行してください。

[未設定時]

動的 VPN サーバに登録する動的 VPN ドメイン名を設定しないものとみなされます。

10.2.8 dvpn client localnet

[機能]

動的 VPN で接続する自側ネットワークの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

dvpn client [<number>] localnet <count> <address>/<mask> [<register>]

[オプション]

<number>

- 動的 VPN クライアント定義番号
  動的 VPN クライアントの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- プレフィックス定義番号
  プレフィックスの定義番号を、0 から 19 までの 10 進数値で指定します。
  指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つプレフィックス定義がすでに存在する場合は、既存の定義を変更します。

<address>/<mask>

- 自側ネットワーク
  自側ネットワークを IPv4 アドレス/マスクビット数 (またはマスク値) または IPv6 アドレスとプレフィックス長で指定します。

  IPv4: IPv4 アドレスとマスクビット数の組み合わせで指定します。
  マスク値は、最上位ビットから 1 で連続した値にしてください。
  デフォルトルートを設定する場合は、0.0.0.0/0(0.0.0.0/0.0.0.0) を指定します。

  IPv6: IPv6 アドレスとプレフィックスの組み合わせで指定します。
  リンクローカルアドレスは指定できません。
  デフォルトルートを設定する場合は、::/0 を指定します。
  IPv6 DHCP クライアントが取得したプレフィックスを使用する場合は上位を"dhcp@インタフェース名"の形式で指定し、下位 80bit 分を IPv6 アドレス形式で指定します。インタフェース名には、rmt インタフェースを以下の範囲で指定します。

範囲	機種
rmt0～rmt999	Si-R570
rmt0～rmt499	Si-R370
rmt0～rmt99	Si-R260B Si-R240 Si-R220B
rmt0～rmt49	Si-R180

rmt0 で動作する IPv6 DHCP クライアントが取得した IPv6 プレフィックスを使用する場合の設定例
dhcp@rmt0::/64
dhcp@rmt0::1:2:3:4/64
プレフィックス長には 64 を指定してください。

<register>

- on
  自側ユーザ ID を生成して動的 VPN サーバに登録します。
- off
  自側ユーザ ID を生成しないで動的 VPN サーバに登録しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN で接続する自側ネットワークを IPv4 アドレス/マスクビット数 (またはマスク値) または IPv6 アドレスとプレフィックス長と自側ユーザ ID を生成して動的 VPN サーバに登録するかどうかを指定します。
自側ユーザ ID を生成して動的 VPN サーバに登録すると指定した場合、通信パケット契機で動的 VPN 接続をすることができます。通常は、動的 VPN サーバに登録するにしてください。
自側ユーザ ID は、自側ネットワークとドメイン名を結合して以下のように生成されます。

例) 自側ネットワークに 192.168.1.0/24(2001:db8:1111:1::/64)、ドメイン名に example.com を指定した場合

IPsecIKE)c0a80100/24@example.com

IPsecIKE)20010db81111000100000000000000000/64@example.com

動的 VPN 機能を利用する場合は、本コマンドを必ず実行してください。

[注意]

自側ネットワーク設定の 0 番目の定義は、IKE ネゴシエーションに使用します。よって、相手装置の自側ネットワーク設定の 0 番目定義のアドレスファミリと一致するように設定してください。
動的 VPN で接続する自側ネットワークを異るアドレスファミリで設定した場合、拡張 IPsec 対象範囲として 1 定義分使用されます。
拡張 IPsec 対象範囲機能未対応版数 (V30) の装置と動的 VPN 接続を行う場合、動的 VPN で接続する自側ネットワークに異るアドレスファミリの設定を行わないでください。
自側ネットワークに IPv6 DHCP クライアントが取得したプレフィックスを使用する場合、プレフィックスが割り当てられるインタフェースと同じ値になるように指定してください。
自側ネットワークは、本コマンドおよび template dvpn localnet コマンドで重複しないように指定してください。

[未設定時]

動的 VPN で接続する自側ネットワークを設定しないものとみなされます。

10.2.9 dvpn client localid

[機能]

動的 VPN サーバに登録する自側ユーザ ID の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

dvpn client [<number>] localid <id>

[オプション]

<number>

- 動的 VPN クライアント定義番号
  動的 VPN クライアントの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<id>

- 自側ユーザ ID
  自側ユーザ ID となる ID を、50 文字以内の ASCII 文字列で指定します。
  指定可能な範囲は以下のとおりです。

文字	範囲
半角アルファベット	a〜z, A〜Z
半角数値	0〜9
半角記号	'-', '_', '.'

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN サーバに登録する自側ユーザ ID を指定します。
本コマンドで指定した自側ユーザ ID は、ドメイン名と結合して以下のように生成されて動的 VPN サーバに登録されます。

例) dvpn client localid shisya、dvpn client domain example.com と指定した場合
shisya@example.com
オペレータの指示で動的 VPN 接続を行いたい場合に指定してください。

[未設定時]

動的 VPN サーバに登録する自側ユーザ ID を設定しないものとみなされます。

10.2.10　dvpn client interface

[機能]

VPN 通信で利用するインタフェースの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

dvpn client [<number>] interface <kind> <conf_number> [<nexthop>]

[オプション]

<number>

- 動的 VPN クライアント定義番号
  動的 VPN クライアントの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<kind>

- lan
  lan 定義によって指定される回線を利用する場合に指定します。
- rmt
  rmt 定義によって指定される回線を利用する場合に指定します。

<conf_number>

lan 定義または rmt 定義の定義番号を指定します。

- lan 定義の定義番号
  利用する lan の定義番号を、10 進数値で指定します。

範囲	機種
0〜19	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
0〜9	Si-R180

- rmt 定義の定義番号
  利用する rmt の定義番号を、10 進数値で指定します。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B　Si-R240　Si-R220B
0〜49	Si-R180

<nexthop>

<kind>に lan を指定した場合で、相手 IPsec トンネル IP アドレスに対する経路を設定する場合に利用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN として接続される IPsec トンネルが通信に利用するインタフェースを設定します。
動的 VPN 機能を利用する場合は、本コマンド を必ず実行してください。

[未設定時]

VPN 通信で利用するインタフェースを設定しないものとみなされます。

10.2.11　dvpn client global

[機能]

VPN 通信の終端グローバルアドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

dvpn client [<number>] global <address>

[オプション]

<number>

- 動的 VPN クライアント定義番号
  動的 VPN クライアントの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<address>

相手装置に通知する VPN 終端グローバルアドレスを以下の範囲で指定します。
1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手装置に通知する VPN 終端グローバルアドレスを指定します。
この設定は、dvpn client interface コマンドで指定されたインタフェースで NAT 機能を使用している場合にのみ参照されます。

[未設定時]

dvpn client interface コマンドで lan を指定した場合は、指定された lan インタフェースに設定されたアドレスが利用されます。
dvpn client interface コマンドで remote を指定した場合は、指定された rmt インタフェースに設定されたアドレス、または PPP により割り当てられたアドレスが利用されます。アドレスがない場合は VPN 接続は行えません。

10.2.12 dvpn client priority

[機能]

動的 VPN クライアントの優先度の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

dvpn client [<number>] priority <priority>

[オプション]

<number>

- 動的 VPN クライアント定義番号
  動的 VPN クライアントの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<priority>

- 優先度
  動的 VPN サーバへ異なる装置で同一の自装置情報を登録する時に優先度を 1〜10 の範囲で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

複数の動的 VPN クライアント装置が、同じ「動的 VPN で接続する自側ネットワークの設定」を動的 VPN サーバへ登録する時に優先度を指定します。
同じ優先度で動的 VPN サーバへ登録すると最後に登録した動的 VPN クライアント装置の情報のみ有効となります。

[未設定時]

動的 VPN クライアントの優先度に 10 を指定したものとみなされます。

```
dvpn client <number> priority 10
```

10.2.13　dvpn client ip route distance

[機能]

動的 VPN IPv4 経路情報の優先度の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

dvpn client [<number>] ip route distance <distance>

[オプション]

<number>

- 動的 VPN クライアント定義番号
  動的 VPN クライアントの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<distance>

- 優先度
  動的 VPN 情報交換で相手から配布された IPv4 の経路情報の優先度を、1～254 の 10 進数値で指定します。
  優先度は、同じあて先への経路情報が複数ある場合、優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN 情報交換で相手から配布された IPv4 経路情報に対する優先度を指定します。

[未設定時]

優先度に 1 を指定したものとみなされます。

```
dvpn client <number> ip route distance 1
```

10.2.14 dvpn client ip6 route distance

[機能]

動的 VPN IPv6 経路情報の優先度の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

dvpn client [<number>] ip6 route distance <distance>

[オプション]

<number>

- 動的 VPN クライアント定義番号
  動的 VPN クライアントの通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<distance>

- 優先度
  動的 VPN 情報交換で相手から配布された IPv6 の経路情報の優先度を、1〜254 の 10 進数値で指定します。
  優先度は、同じあて先への経路情報が複数ある場合、優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

動的 VPN 情報交換で相手から配布された IPv6 経路情報に対する優先度を指定します。

[未設定時]

優先度に 1 を指定したものとみなされます。

```
dvpn client <number> ip6 route distance 1
```

第 11 章　ルーティングプロトコル情報の設定

11.1 ルーティングマネージャ情報

11.1.1 routemanage ip distance

[機能]

IPv4 ルーティングプロトコル優先度の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

routemanage ip distance rip <rip_distance>
routemanage ip distance bgp <external_distance> [<internal_distance>]
routemanage ip distance ospf <ospf_distance>
routemanage ip distance dns <dns_distance>

[オプション]

<rip_distance>

- RIP 優先度
  RIP の優先度を、1〜254 の 10 進数値で指定します。

<external_distance>

- EBGP 優先度
  EBGP の優先度を、1〜254 の 10 進数値で指定します。

<internal_distance>

- IBGP 優先度
  IBGP の優先度を、1〜254 の 10 進数値で指定します。
  省略時は 200 が指定されたものとみなされます。

<ospf_distance>

- OSPF 優先度
  OSPF の優先度を、1〜254 の 10 進数値で指定します。

<dns_distance>

- DNS 優先度
  DNS の優先度を、1〜254 の 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv4 ルーティングプロトコルの優先度を設定します。
優先度は、同じあて先への経路情報が複数ある場合、優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。

[注意]

優先度は、ほかのルーティングプロトコルやスタティック経路情報に設定されている値と同じ値を指定しないでください。
優先度を動的定義反映した場合、動的定義反映後に登録する経路情報に対しては、反映後の優先度値を設定しますが、すでに登録している経路情報の優先度値は変更しません。登録済の優先度値を変更する場合は、clear ip route コマンドを実行してください。

[未設定時]

RIP の優先度を 120、EBGP の優先度を 20、IBGP の優先度を 200、OSPF の優先度を 110、DNS の優先度を 15 として優先経路選択を行うものとみなされます。

```
routemanage ip distance rip 120
routemanage ip distance bgp 20 200
routemanage ip distance ospf 110
routemanage ip distance dns 15
```

11.1.2 routemanage ip redist rip

[機能]

RIP 再配布経路の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

routemanage ip redist rip <redist_info> <mode> [<metric>]

[オプション]

<redist_info>

経路種別を指定します。

- static
  スタティック経路情報を示します。
- connected
  インタフェース経路情報を示します。
- bgp
  BGP 経路情報を示します。
- ospf
  OSPF 経路情報を示します。
- dns
  DNS 経路情報を示します。

<mode>

RIP に再配布するかどうかを指定します。

- off
  再配布しません。
- on
  再配布します。

<metric>

- RIP に再配布するメトリック値
  RIP に再配布する際のメトリック値を、0～16 の 10 進数値で指定します。
  BGP、OSPF、または DNS で受信した経路情報を RIP に再配布する場合に指定できます。
  RIP 広報メトリック値は、以下の計算値で決定されます。
  - RIP 広報値=インタフェースの加算メトリック値+1+<metric>

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP に再配布する経路情報を設定します。
なお、IKE 経路は再配布できません。

[注意]

RIP を使用しているインタフェースの経路は、インタフェース経路情報の再配布設定にかかわらず再配布されます。

[未設定時]

スタティック経路情報とインタフェース経路情報だけを RIP に再配布するものとみなされます。

```
routemanage ip redist rip static on
routemanage ip redist rip connected on
routemanage ip redist rip bgp off 0
routemanage ip redist rip ospf off 0
routemanage ip redist rip dns off 0
```

11.1.3 routemanage ip redist bgp

[機能]

BGP 再配布経路の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

routemanage ip redist bgp <redist_info> <mode>
routemanage ip redist bgp vrf [<vrf_number>] <redist_info> <mode>

[オプション]

<redist_info>

経路種別を指定します。

- static
  スタティック経路情報を示します。
- connected
  インタフェース経路情報を示します。
- rip
  RIP 経路情報を示します。
  routemanage ip redist bgp vrf では指定できません。
- ospf
  OSPF 経路情報を示します。
  routemanage ip redist bgp vrf では指定できません。
- dns
  DNS 経路情報を示します。
  routemanage ip redist bgp vrf では指定できません。

<vrf_number>

- VRF 定義番号
  VRF の定義番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0～3	Si-R570 Si-R370
0～1	Si-R260B Si-R240 Si-R220B Si-R180

<mode>

BGP に再配布するかどうかを指定します。

- off
  再配布しません。
- on
  再配布します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

BGP に再配布する経路情報を設定します。
なお、IKE 経路は再配布できません。

[未設定時]

すべての経路種別を BGP に再配布しないものとみなされます。

```
routemanage ip redist bgp static off
routemanage ip redist bgp connected off
routemanage ip redist bgp rip off
routemanage ip redist bgp ospf off
routemanage ip redist bgp dns off
```

11.1.4 routemanage ip redist ospf

[機能]

OSPF 再配布経路の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

routemanage ip redist ospf <redist_info> <mode> [<metric> [<metric_type>]]

[オプション]

<redist_info>

経路種別を指定します。

- static
  スタティック経路情報を示します。
- connected
  インタフェース経路情報を示します。
- rip
  RIP 経路情報を示します。
- bgp
  BGP 経路情報を示します。
- dns
  DNS 経路情報を示します。

<mode>

OSPF に再配布するかどうかを指定します。

- off
  再配布しません。
- on
  再配布します。

<metric>

- メトリック値
  OSPF に再配布する際のメトリック値を、0～16777214 の 10 進数で指定します。
  省略時は、20 を指定したものとみなされます。

<metric_type>

外部経路のメトリックタイプを指定します。
省略時は、type2 を指定したものとみなされます。

- type1
  メトリックタイプを type1 とします。
- type2
  メトリックタイプを type2 とします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

OSPF に再配布する経路情報を設定します。
なお、IKE 経路は再配布できません。

[未設定時]

すべての経路種別を OSPF に再配布しないものとみなされます。

```
routemanage ip redist ospf static off 20 type2
routemanage ip redist ospf connected off 20 type2
routemanage ip redist ospf rip off 20 type2
routemanage ip redist ospf bgp off 20 type2
routemanage ip redist ospf dns off 20 type2
```

11.1.5 routemanage ip ecmp mode

[機能]

IPv4 ルーティングの ECMP の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

routemanage ip ecmp mode <mode>

[オプション]

<mode>

- off
  ECMP を使用しません。
- roundrobin
  ECMP を使用し、送出パス選択方式としてラウンド ロビン方式を利用します。
- hash
  ECMP を使用し、送出パス選択方式としてハッシュ方式を使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv4 ルーティング機能の ECMP の使用の有無を設定します。なお、ECMP を使用する場合、以下の 2 種類の送出パス選択方式を選択します。

- ラウンド ロビン方式
  パケット ごとに送出パスを順次切り替える方式です。すべてのトラフィックがほぼ均等に分散される利点がある一方、通信の連続性 (個々の通信セッションが同じパスを利用するか) とパケット の到達順は送信時から保証されないという欠点があります。
- ハッシュ方式
  送信元 IP アド レス、あて先 IP アド レスを基にハッシュ値を計算し、その値に従って送出パスを決定する方式です。通信の連続性および到達順はほぼ保証されますが、トラフィックが一部の通信パスにかたよる可能性があります。

[未設定時]

ECMP を利用しないものとみなされます。

```
routemanage ip ecmp mode off
```

11.1.6　routemanage ip ecmp ospf

[機能]

OSPF ルーティングプロトコルの最大 ECMP 数の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

routemanage ip ecmp ospf <max-multipath>

[オプション]

<max-multipath>

- 最大 ECMP 数
  最大 ECMP 数を、1～4 までの 10 進数値で指定します。
  1 を指定した場合、OSPF では ECMP 経路を扱いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

OSPF が生成した経路情報での、設定可能な ECMP 数を指定します。

[未設定時]

<max-multipath>に 1 を設定するものとみなされます。

```
routemanage ip ecmp ospf 1
```

11.1.7 routemanage ip redist ldp

[機能]

LDP ラベル広報経路情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

routemanage ip redist ldp <redist_info> <mode>

[オプション]

<redist_info>

- static
  本装置に設定されているスタティックルーティングの経路情報を示します。
- connected
  インタフェースが接続されているネットワークの経路情報を示します。
- rip
  RIP で受信した経路情報を示します。
- ospf
  OSPF で受信した経路情報を示します。
- bgp
  BGP で受信した経路情報を示します。

<mode>

- off
  <redist_info>で指定した経路情報をラベル広報しません。
- on
  <redist_info>で指定した経路情報をラベル広報します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

LDP でラベル広報する経路情報の種別を選択します。

[未設定時]

以下の設定とみなされます。

- LDP で static を広報された経路をラベル広報しない
- LDP で connected の経路をラベル広報する
- LDP で rip で広報された経路をラベル広報する
- LDP で ospf で広報された経路をラベル広報する
- LDP で bgp で広報された経路をラベル広報しない

```
routemanage ip redist ldp static off
routemanage ip redist ldp connected on
routemanage ip redist ldp rip on
routemanage ip redist ldp ospf on
routemanage ip redist ldp bgp off
```

11.1.8 routemanage interface floating

[機能]

インタフェース経路のフローティング設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

routemanage interface floating <mode>

[オプション]

<mode>

- off
  フローティング機能を使用しません。
- on
  フローティング機能を使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

インタフェース経路のフローティング機能を設定します。
<mode>が on の場合、インタフェースが通信可能 (リンクアップなど) 状態ならば、インタフェース経路をルーティングテーブルに追加します。通信不可能 (リンクダウンなど) 状態ならば、インタフェース経路をルーティングテーブルから削除します。
<mode>が off の場合、インタフェースの通信状態に関係なく、インタフェース経路をルーティングテーブルに追加します。
本設定は、IPv4 機能、IPv6 機能で共通となります。

[注意]

ルーティングプロトコル優先度<distance>が 0 のスタティックルーティングも、<mode>が on の場合、インタフェースの状態変動によって、ルーティングテーブルへの追加・削除を制御します。
<mode>が on の場合、インタフェースが利用不可能な状態の場合はインタフェース経路がルーティングテーブルから削除されるとともに、インタフェースに設定された IP アドレスが通信に利用できなくなります。常に利用可能な IP アドレスが必要な場合は、loopback インタフェースに追加 IP アドレスを設定してください。
なお、以下のコマンドでは自装置の IP アドレスを指定します。これらのコマンドで常に利用可能な IP アドレスが必要な場合は、loopback インタフェースの追加 IP アドレスを使用してください。

- snmp agent address
- remote ap sessionwatch
- remote ap tunnel local

<mode>が on で自 IP アドレスを指定していない remote インタフェースから送信される場合、送信元 IP アドレスは以下の順番で選ばれます。

1. loopback インタフェース追加アドレス
2. 利用可能な lan の IP アドレス (定義番号の小さいものが優先)

3. 利用可能な remote の IP アドレス (定義番号の小さいものが優先)

常に同じアドレスが選択されるようにするためには、loopback インタフェースに追加 IP アドレスを設定してください。この設定がない場合、インタフェースの状態によって送信元 IP アドレスが変化する場合があります。
<mode>が on でマルチキャストで自装置が RP として動作している場合、RP として動作しているインタフェースの状態の変化により以下の動作になります。

- RP を自動選択にしている場合

  RP として動作しているインタフェースがダウンした場合、利用可能なインタフェースを自動検索し更新します。この場合、ネットワーク上にて RP が更新されるため、その RP を利用している通信は RP が更新されるまで一定時間停止します。また、インタフェース回線がふたたびアップすることで、RP が切り戻るため、やはりその RP を利用している通信は切り戻るまでの一定時間停止します。

  利用可能なインタフェースが検索できなかった場合は、RP としての動作を停止しますが、インタフェースがふたたびアップすることで復旧します。

- RP を手動選択にしている場合

  選択されているインタフェースがダウンした場合、RP としての動作を停止します。この場合、ネットワーク上にて RP が更新されるため、その RP を利用している通信が RP が更新されるまで一定時間停止します。

  また、インタフェースがふたたびアップすることで、RP は切り戻りますが、やはりその RP を利用している通信が切り戻るまでの一定時間停止します。

<mode>が on でマルチキャストで自装置が BSR として動作している場合、BSR として動作しているインタフェースの状態の変化により以下の動作になります。

- BSR を自動選択にしている場合

  RP として動作しているインタフェースがダウンした場合、利用可能なインタフェースを自動検索し更新します。この場合、ネットワーク上にて BSR が更新されるため、その BSR を利用している通信は BSR が更新されるまでの一定時間停止します。また、インタフェースがふたたび UP することで、BSR が切り戻るため、やはりその BSR を利用している通信は BSR が切り戻るまでの一定時間停止します。

  なお検索できなかった場合は、BSR としての動作を停止しますが、インタフェース回線がふたたびアップすることで復旧します。

- BSR を手動選択にしている場合

  選択されているインタフェースがダウンした場合は、BSR としての動作を停止します。この場合、ネットワーク上にて BSR が更新されるため、その BSR を利用している通信は BSR が更新されるまでの一定時間停止します。

  また、インタフェースがふたたびアップすることで BSR は切り戻りますが、やはりその BSR を利用している通信は切り戻るまでの一定時間停止します。

[未設定時]

インタフェースの通信状態に関係なく、常にインタフェース経路をルーティングテーブルに追加するものとみなされます。

```
routemanage interface floating off
```

11.1.9 routemanage ip6 distance

[機能]

IPv6 ルーティングプロトコル優先度の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

routemanage ip6 distance rip <rip_distance>
routemanage ip6 distance dns <dns_distance>
routemanage ip6 distance dhcp <dhcp_distance>

[オプション]

<rip_distance>

- RIP 優先度
  RIP の優先度を、1〜254 の 10 進数値で指定します。

<dns_distance>

- DNS 優先度
  DNS の優先度を、1〜254 の 10 進数値で指定します。

<dhcp_distance>

- DHCP 優先度
  DHCP の優先度を、1〜254 の 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv6 ルーティングプロトコルの優先度を設定します。
優先度は、同じあて先への経路情報が複数ある場合、優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。
DHCP 経路情報の blackhole 経路、reject 経路の優先度は、DHCP 優先度の値となります。

[注意]

優先度は、ほかのルーティングプロトコルやスタティック経路情報に設定されている値と同じ値を指定しないでください。
優先度を動的定義反映した場合、動的定義反映後に登録する経路情報に対しては、反映後の優先度値を設定しますが、すでに登録している経路情報の優先度値は変更しません。登録済の優先度値を変更する場合は、clear ipv6 route コマンドを実行してください。

[未設定時]

RIP の優先度を 120、DNS の優先度を 15、DHCP の優先度を 10 として優先経路選択を行うものとみなされます。

```
routemanage ip6 distance rip 120
routemanage ip6 distance dns 15
routemanage ip6 distance dhcp 10
```

11.1.10 routemanage ip6 redist rip

[機能]

IPv6 RIP 再配布経路の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

routemanage ip6 redist rip <redist_info> <mode> [<metric>]

[オプション]

<redist_info>

経路種別を指定します。

- static
  スタティック経路情報を示します。
- connected
  インタフェース経路情報を示します。
- dns
  DNS 経路情報を示します。
- dhcp
  DHCP 経路情報を示します。

<mode>

RIP に再配布するかどうかを指定します。

- off
  再配布しません。
- on
  再配布します。

<metric>

- RIP に再配布するメトリック値
  RIP に再配布する際のメトリック値を、0～16 の 10 進数値で指定します。
  DNS、または DHCP で受信した経路情報を RIP に再配布する場合に指定できます。
  RIP 広報メトリック値は、以下の計算値で決定されます。
  - RIP 広報値=インタフェースの加算メトリック値+1+<metric>

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP に再配布する経路情報を設定します。
DHCP 経路情報を再配布すると設定しても、DHCP 経路情報の blackhole 経路、reject 経路は、再配布できません。
また、IKE 経路は再配布できません。

[注意]

RIP を使用しているインタフェースの経路は、インタフェース経路情報の再配布設定にかかわらず再配布されます。

[未設定時]

スタティック経路情報とインタフェース経路情報を RIP に再配布するものとみなされます。

```
routemanage ip6 redist rip static on
routemanage ip6 redist rip connected on
routemanage ip6 redist rip dns off 0
routemanage ip6 redist rip dhcp off 0
```

11.2 RIP 情報

11.2.1 rip ip timers basic

[機能]

RIP タイマの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

rip ip timers basic <update> <timeout> <garbage>

[オプション]

<update>

- 定期広報タイマ値
  定期広報タイマ値を、10 秒～3600 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、10s～3600s、1m～60m、1h です。

<timeout>

- 有効期限タイマ値
  有効期限タイマ値を、10 秒～3600 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、10s～3600s、1m～60m、1h です。

<garbage>

- ガーベージタイマ値
  ガーベージタイマ値を、10 秒～3600 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、10s～3600s、1m～60m、1h です。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP の基準となる定期広報タイマ値、有効期限タイマ値、ガーベージタイマ値を指定します。
<update>は、定期広報の送信間隔を設定します。なお、次に定期広報を行うまでの時間は、送信間隔に送信間隔の最大± 50%のゆらぎ幅の範囲で乱数により求められる値を加算した値が使用されます。ゆらぎ幅は、rip ip timers jitter コマンド で変更することができます。
<timeout>は、隣接ルータから一定時間通知がない場合、その隣接ルータから受信していた経路を無効とするまでの時間を設定します。
<garbage>では、無効となった経路情報を削除するまでの時間を設定します。無効となった経路は削除されるまでの間、定期広報でメトリック 16 として広報されます。

[未設定時]

定期広報タイマ値に 30 秒、有効期限タイマ値に 3 分、ガーベージタイマ値に 2 分が設定されているものとみなされます。

```
rip ip timers basic 30s 3m 2m
```

11.2.2 rip ip timers jitter

[機能]

RIP 定期広報ゆらぎ幅の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

rip ip timers jitter <jitter>

[オプション]

<jitter>

- ゆらぎ幅

  ゆらぎ幅 (%) を、0〜50 の 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP 定期広報のゆらぎ幅を設定します。
次に定期広報を行うまでの時間は、定期広報の送信間隔にゆらぎ時間を加算した値が使用されます。
ゆらぎ幅は、定期広報の送信間隔に対するゆらぎ時間の割合の±の最大値を設定します。
ゆらぎ時間は、ゆらぎ幅の範囲で乱数により求められます。
<jitter>に 0 が設定された場合、ゆらぎ時間は 0 秒となります。

[注意]

ゆらぎ幅に 0 が設定されている場合、隣接ルータとの間で RIP パケットの衝突が繰り返し発生し、RIP ルーティングは収束遅延する可能性があります。

[未設定時]

RIP 定期広報のゆらぎ幅に、50(%) が設定されているものとみなされます。

```
rip ip timers jitter 50
```

11.2.3　rip ip multipath

[機能]

RIP マルチパスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

rip ip multipath <path_num>

[オプション]

<path_num>

- 同一パス数
  同一パス数を、1〜2 までの 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP テーブルに、同一パスの追加を有効とするかどうかを設定します。
<path_num>に 2 を指定した場合、同一パスの追加は有効となり、受信した RIP 経路や再配布経路が、RIP テーブルに追加可能となります。
同一パスの追加を有効とした場合、経路情報が無効状態となった時点で次の経路情報を瞬時に追加し、経路切り替りの待ち時間を削減することができます。
同一パスを保持した場合、定期広報対象となる経路情報は、メトリックの小さい経路情報とします。
ただし、再配布経路と RIP 経路が混在した場合は、ルーティングプロトコル優先度の高い経路情報とします。
RIP 経路の同一パスをルーティングテーブルに追加する場合、メトリックの小さい経路を使用します。
同一メトリックの場合は、先に受信した RIP 経路を使用します。ただし、再配布経路と RIP 経路が混在した場合は、ルーティングプロトコル優先度の高い経路情報とします。
<path_num>に 1 を指定した場合、同一パスの追加はできません。

[注意]

<path_num>を超えた同一パスを RIP で受信した場合、追加済の RIP 経路情報とメトリックの比較を行い、メトリックの大きい RIP 経路情報は破棄されます。

[未設定時]

RIP テーブルに同一パスは、追加できないものとみなされます。

```
rip ip multipath 1
```

11.2.4 rip ip redist

[機能]

RIP 再配布フィルタの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

rip ip redist <number> <action> <address>/<mask> [<prefix_match>]

[オプション]

<number>

- フィルタリング定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜499	Si-R570
0〜249	Si-R370
0〜49	上記以外

<action>

フィルタリング条件に一致した場合の動作を指定します。

- pass
  該当する経路情報を透過します。
- reject
  該当する経路情報を遮断します。

<address>/<mask>

フィルタリング対象とする経路情報を指定します。

- IPv4 アドレス/マスクビット数 (またはマスク値)
  フィルタリング対象とする経路情報を、IPv4 アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
  - IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
  - IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)
- any
  すべての経路情報をフィルタリング対象とする場合に指定します。
- default
  デフォルトルートをフィルタリング対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<prefix_match>

経路情報 (IPv4 アドレス/マスク) の検索条件を指定します。
省略時は、exact を指定したものとみなされます。
<address>/<mask>に"any"または"default"を指定した場合は、<prefix_match>は指定できません。

- exact
  指定した<address>/<mask>と経路情報の IPv4 アドレス/マスクを比較し、一致した場合に、フィルタリング対象とします。
- inexact
  指定した<address>と経路情報の IPv4 アドレスを比較し、<mask>まで一致した場合、フィルタリング対象とします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP に再配布する経路情報に対するフィルタリング条件と動作を設定します。
フィルタリング条件は優先順位で検索され、条件に一致した場合にフィルタリングの動作が行われ、それ以降の条件は参照されません。
すべてのフィルタリング条件に一致しない経路情報は RIP に再配布されません。
<number>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。
RIP 再配布フィルタは、本装置全体で以下の数まで定義できます。

範囲	機種
500	Si-R570
250	Si-R370
50	上記以外

[未設定時]

RIP 再配布フィルタが設定されていないものとみなされます。

11.2.5 rip ip redist move

[機能]

RIP 再配布フィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

rip ip redist move <number> <new_number>

[オプション]

<number>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義番号を指定します。

<new_number>

- 移動先フィルタリング定義番号
  <number>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0〜499	Si-R570
0〜249	Si-R370
0〜49	上記以外

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP 再配布フィルタの優先順序を変更します。
<new_number>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、<new_number>は順番にソートされてリナンバリングされます。

11.2.6　rip ip neighbor

[機能]

RIP ユニキャスト送信の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

rip ip neighbor [<count>] <neighbor_address> <version>

[オプション]

<count>

- ユニキャスト送信相手の定義番号
  ユニキャスト送信相手の定義番号を、0〜29 の 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<neighbor_address>

RIP 経路をユニキャストで送信する相手ルータの IP アドレスを指定します。
指定可能な範囲は以下のとおりです。

1.0.0.1 〜 126.255.255.254
128.0.0.1 〜 191.255.255.254
192.0.0.1 〜 223.255.255.254

<version>

送信バージョンを指定します。

- v1
  RIPv1 で送信します。
- v2
  RIPv2 で送信します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

特定の相手ルータに対して、RIP 経路をユニキャストで広報する場合に設定します。
<neighbor_address>には、LAN 側ネットワークに存在する RIP ルータを指定してください。
RIP 経路を広報する相手ルータは、本装置全体で 30 個まで定義できます。

[注意]

<neighbor_address>が属する LAN インタフェースで設定されている lan ip rip コマンドの<send>パラメタとは無関係に、ユニキャスト送信を行います。ただし、加算メトリックと認証機能については、lan ip rip で設定されている値を使用します。
自ネットワーク以外の相手ルータは指定できません。

[未設定時]

RIP ユニキャスト送信を設定しないものとみなします。

11.2.7 rip ip gwfilter

[機能]

RIP 相手フィルタの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

rip ip gwfilter <number> <action> <gateway_address>

[オプション]

<number>

- 相手フィルタリングの定義番号
  フィルタリングの優先度を表す定義番号を、0〜29 の 10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

<action>

フィルタリング条件に一致した場合の動作を指定します。

- pass
  該当する相手ルータの RIP パケットを受信します。
- reject
  該当する相手ルータの RIP パケットを破棄します。

<gateway_address>

フィルタリング対象とする相手ルータ情報を指定します。

- IPv4 アドレス
  対象とする相手ルータの IPv4 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  1.0.0.1 〜 126.255.255.254
  128.0.0.1 〜 191.255.255.254
  192.0.0.1 〜 223.255.255.254

- any
  すべての相手ルータを対象とする場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

特定の相手ルータから RIP 経路を受信する場合、フィルタリング条件に一致した相手ルータの RIP パケットを受信 (pass) させるか破棄 (reject) させるかを設定します。
フィルタリング条件は優先順位で検索し、条件に一致した相手ルータ情報があった時点でフィルタリングが行われ、それ以降の条件は参照されません。
すべてのフィルタリング条件に一致しない相手ルータ情報からの RIP パケットは破棄されます。
<number>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。
RIP 相手フィルタは、本装置全体で 30 個まで定義できます。

[未設定時]

RIP 相手フィルタを設定しないものとみなします。

11.2.8 rip ip gwfilter move

[機能]

RIP 相手フィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

rip ip gwfilter move <number> <new_number>

[オプション]

<number>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義番号を指定します。

<new_number>

- 移動先フィルタリング定義番号
  <number>に対する新しい順序を、0〜29 の 10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP 相手フィルタの優先順序を変更します。
<new_number>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、<new_number>は順番にソートされてリナンバリングされます。

11.2.9　rip ip6 timers basic

[機能]

IPv6 RIP タイマの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

rip ip6 timers basic <update> <timeout> <garbage>

[オプション]

<update>

- 定期広報タイマ値
  定期広報タイマ値を、10 秒～3600 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、10s～3600s、1m～60m、1h です。

<timeout>

- 有効期限タイマ値
  有効期限タイマ値を、10 秒～3600 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、10s～3600s、1m～60m、1h です。

<garbage>

- ガーベージタイマ値
  ガーベージタイマ値を、10 秒～3600 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、10s～3600s、1m～60m、1h です。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP(IPv6) の基準となる定期広報タイマ値、有効期限タイマ値、ガーベージタイマ値を指定します。
<update>は、定期広報の送信間隔を設定します。なお、次に定期広報を行うまでの時間は、送信間隔に送信間隔の最大± 50%のゆらぎ幅の範囲で乱数により求められる値を加算した値が使用されます。
<timeout>は、隣接ルータから一定時間通知がない場合、その隣接ルータから受信していた経路を無効とするまでの時間を設定します。
<garbage>では、無効となった経路情報を削除するまでの時間を設定します。無効となった経路は削除されるまでの間、定期広報でメトリック 16 として広報されます。

[未設定時]

定期広報タイマ値に 30 秒、有効期限タイマ値に 3 分、ガーベージタイマ値に 2 分が設定されているものとみなされます。

```
rip ip6 timers basic 30s 3m 2m
```

11.2.10 rip ip6 multipath

[機能]

IPv6 RIP マルチパスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

rip ip6 multipath <path_num>

[オプション]

<path_num>

- 同一パス数
  同一パス数を、1〜2 までの 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP テーブルに、同一パスの追加を有効とするかどうかを設定します。
<path_num>に 2 を指定した場合、同一パスの追加は有効となり、受信した RIP 経路や再配布経路が、RIP テーブルに追加可能となります。
同一パスの追加を有効とした場合、経路情報が無効状態となった時点で次の経路情報を瞬時に追加し、経路切り替りの待ち時間を削減することができます。
同一パスを保持した場合、定期広報対象となる経路情報は、メトリックの小さい経路情報とします。
ただし、再配布経路と RIP 経路が混在した場合は、ルーティングプロトコル優先度の高い経路情報とします。
RIP 経路の同一パスをルーティングテーブルに追加する場合、メトリックの小さい経路を使用します。
同一メトリックの場合は、先に受信した RIP 経路を使用します。ただし、再配布経路と RIP 経路が混在した場合は、ルーティングプロトコル優先度の高い経路情報とします。
<path_num>に 1 を指定した場合、同一パスの追加はできません。

[注意]

<path_num>を超えた同一パスを RIP で受信した場合、追加済の RIP 経路情報とメトリックの比較を行い、メトリックの大きい RIP 経路情報は破棄されます。

[未設定時]

RIP テーブルに同一パスは、追加できないものとみなされます。

```
rip ip6 multipath 1
```

11.2.11　rip ip6 redist

[機能]

IPv6 RIP 再配布フィルタの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

rip ip6 redist <number> <action> <address>/<prefixlen> [<prefix_match>]

[オプション]

<number>

- フィルタリング定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜499	Si-R570
0〜249	Si-R370
0〜49	上記以外

<action>

フィルタリング条件に一致した場合の動作を指定します。

- pass
  該当する経路情報を透過します。
- reject
  該当する経路情報を遮断します。

<address>/<prefixlen>

フィルタリング対象とする経路情報を指定します。

- IPv6 アドレス/プレフィックス長
  フィルタリング対象とする経路情報を、IPv6 アドレスとプレフィックス長の組み合わせで指定します。
- any
  すべての経路情報をフィルタリング対象とする場合に指定します。
- default
  デフォルトルートをフィルタリング対象とする場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<prefix_match>

経路情報 (IPv6 アドレス/プレフィックス長) の検索条件を指定します。
省略時は、exact を指定したものとみなされます。
<address>/<prefixlen>に"any"または"default"を指定した場合は、<prefix_match>は指定できません。

- exact
  指定した<address>/<mask>と経路情報の IPv6 アドレス/プレフィックス長を比較し、一致した場合に、フィルタリング対象とします。

- inexact

  指定した<address>と経路情報の IPv6 アドレスを比較し、<prefixlen>まで一致した場合、フィルタリング対象とします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP(IPv6) に再配布する経路情報に対するフィルタリング条件と動作を設定します。
フィルタリング条件は優先順位で検索され、条件に一致した場合にフィルタリングの動作が行われ、それ以降の条件は参照されません。
すべてのフィルタリング条件に一致しない経路情報は RIP(IPv6) に再配布されません。
<number>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。
RIP(IPv6) 再配布フィルタは、本装置全体で以下の数まで定義できます。

範囲	機種
500	Si-R570
250	Si-R370
50	上記以外

[未設定時]

RIP(IPv6) 再配布フィルタが設定されていないものとみなされます。

11.2.12　rip ip6 redist move

[機能]

IPv6 RIP 再配布フィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

rip ip6 redist move <number> <new_number>

[オプション]

<number>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義番号を指定します。

<new_number>

- 移動先フィルタリング定義番号
  <number>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0～499	Si-R570
0～249	Si-R370
0～49	上記以外

[動作モード]

構成定義モード (管理者クラス)

[説明]

RIP(IPv6) 再配布フィルタの優先順序を変更します。
<new_number>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、<new_number>は順番にソートされてリナンバリングされます。

11.3 BGP 情報

11.3.1 bgp as

[機能]

BGP AS 番号の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp as <as_number>

[オプション]

<as_number>

- 自装置の属する AS 番号
  自装置の属する AS 番号を、0〜65535 の 10 進数値で指定します。
  0 を指定した場合、BGP の機能は動作しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

自装置の属する AS 番号を指定します。

[未設定時]

BGP を動作させないものとみなされます。

```
bgp as 0
```

11.3.2　bgp id

[機能]

BGP ID の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp id <identifier>

[オプション]

<identifier>

- BGP の ID
  IPv4 アドレスを 0.0.0.0〜255.255.255.255 のドット形式で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

BGP 接続で自装置を一意に示す ID を設定します。
ID はほかのルータと重複しない値を指定し、一般的には自装置の IPv4 アドレスを使用します。
本コマンドを省略または 0.0.0.0 が設定されている場合は、以下のとおり ID を自動的に選択し使用します。

- loopback インタフェースに追加 IP アドレスが設定されている場合は、その IP アドレスを選択します。
- loopback インタフェースに追加 IP アドレスが設定されていない場合は、lan/remote インタフェースに設定されている IP アドレスの中からインタフェースの Up/Down の状態に関係なく最大のものを選択します。なお、remote インタフェースの相手側 IP アドレスおよび、lan インタフェースのセカンダリ IP アドレスは選択の対象となりません。

[未設定時]

自動的に選択された ID が使用されるものとみなされます。

```
bgp id 0.0.0.0
```

11.3.3 bgp vrf rd

[機能]

BGP/MPLS VPN ルート識別子の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp vrf [<vrf_number>] rd <as_number> <id>

[オプション]

<vrf_number>

- VRF 定義番号
  VRF の定義番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜3	Si-R570 Si-R370
0〜1	Si-R260B Si-R240 Si-R220B Si-R180

<as_number>

- AS 番号
  AS 番号を、1〜65535 の 10 進数値で指定します。

<id>

- ID 番号
  VRF の ID を、0〜4294967295 の 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

BGP/MPLS VPN で使用するルート識別子を AS 番号と ID で設定します。
<as_number>は、自装置の属する AS 番号を設定します。
<id>は、VPN を一意に示す id を設定します。

[未設定時]

ルート識別子が設定されていないものとみなされます。

11.3.4　bgp mpls-resolution

[機能]

BGP MPLS 解決の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp mpls-resolution <mode>

[オプション]

<mode>

MPLS 解決を行うかどうかを指定します。

- on
  MPLS 解決を行います。
- off
  MPLS 解決を行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

BGP で受信した経路を MPLS で解決するかどうかを設定します。
<mode>が on の場合は、BGP で受信した経路を MPLS のラベルパスにマッピングします。off の場合は、マッピングしません。

[注意]

MPLS トンネル接続上で BGP を使用する場合は、本設定を off にしてください。

[未設定時]

MPLS 解決を行わないものとみなされます。

```
bgp mpls-resolution off
```

11.3.5 bgp network route

[機能]

BGP ネットワークの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp network route [<count>] <address>/<mask>

[オプション]

<count>

- BGP ネットワークの定義番号
  BGP ネットワークの定義番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜199	Si-R570
0〜15	上記以外

<address>/<mask>

- BGP ネットワークアドレス/マスクビット数 (またはマスク値)
  BGP ネットワークを IPv4 アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。
  以下に、有効な記述形式を示します。
  - BGP ネットワークアドレス/マスクビット数 (例: 192.168.1.0/24)
  - BGP ネットワークアドレス/マスク値 (例: 192.168.1.0/255.255.255.0)

[動作モード]

構成定義モード (管理者クラス)

[説明]

BGP ネットワークを設定します。
本コマンドは、BGP テーブルにない経路情報を広報する場合に設定します。
bgp network igp コマンドで IGP 経路との同期が設定されている場合、設定された BGP ネットワークが IGP 経路として有効な場合に広報します。なお、IGP 経路の状態変更を認識するまで最大 15 秒かかります。
bgp network igp コマンドで IGP 経路との同期が設定されていない場合、IGP 経路が有効/無効のどちらの場合でも広報します。

[注意]

BGP/MPLS VPN で使用する IBGP では、本コマンドで設定した経路は広報されません。

[未設定時]

BGP ネットワークが設定されていないものとみなされます。

11.3.6　bgp network igp

[機能]

BGP ネットワークの IGP との同期設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp network igp <mode>

[オプション]

<mode>

IGP 経路と同期させるかどうかを指定します。

- on
  IGP 経路と同期させます。
- off
  IGP 経路と同期させません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

BGP ネットワークを、IGP 経路と同期して広報するかどうかを設定します。
<mode>に on を設定した場合、IGP 経路が有効な場合にだけ広報し、無効な場合は広報しません。
<mode>に off を設定した場合、IGP 経路に関係なく広報します。

[未設定時]

BGP ネットワークを、IGP 経路と同期して広報するものとみなされます。

```
bgp network igp on
```

11.3.7 bgp aggregate

[機能]

BGP 集約経路の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp aggregate [<count>] <address>/<mask> [<action>]

[オプション]

<count>

- BGP 集約経路の定義番号
  集約経路の定義番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜49	Si-R570
0〜15	上記以外

<address>/<mask>

- BGP 集約経路アドレス/マスクビット数 (またはマスク値)
  集約経路を IPv4 アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。
  以下に、有効な記述形式を示します。
  - BGP 集約経路アドレス/マスクビット数 (例: 192.168.1.0/24)
  - BGP 集約経路アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)

  0.0.0.0/0, 0.0.0.0/0.0.0.0 は指定できません。

<action>

動作を指定します。

- summary-only
  BGP 集約経路だけを広報し、集約される個々の経路を広報しない場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

BGP 集約経路の設定を行います。
設定された集約経路に含まれる経路情報がある場合、集約経路情報を生成します。
<action>に summary-only が設定されていない場合は、集約経路と集約経路に含まれる個々の経路情報の両方が広報されます。summary-only が設定されている場合、集約経路に含まれる個々の経路情報はサプレス経路となり、集約経路だけを広報します。

[注意]

BGP/MPLS VPN で使用する IBGP では、本コマンドで経路を集約することはできません。

[未設定時]

BGP 集約経路が設定されていないものとみなされます。

11.3.8 bgp full-route

[機能]

BGP フルルートの設定

[適用機種]

Si-R 570

[入力形式]

bgp full-route <mode>

[オプション]

<mode>

フルルートを使用するかどうかを指定します。

- on
  フルルートを使用します。
- off
  フルルートを使用しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

BGP でフルルート (15 万経路) を使用するかどうかを設定します。
フルルートを使用することにより、BGP テーブルエントリ数の最大値が拡張され、15 万経路を扱えるようになります。

フルルートを使用しない場合：

エントリの最大値が 6000 エントリ

フルルートを使用した場合 ：

エントリの最大値が 150000 エントリ

フルルートは、拡張用 512M メモリモジュールが搭載されているときにのみ使用できます。
フルルートを使用するときに設定できる BGP セッションは、BGP 相手情報の定義番号 0 に設定された EBGP(マルチホップを除く) の 1 セッションだけです。
フルルートは、以下の機能と併用して使用することはできません。

- BGP への再配布、および、BGP 経路情報の RIP/OSPF/LDP への再配布機能
- BGP/MPLS VPN 機能
- BGP MPLS 解決機能

[注意]

フルルートの設定は以下のどれかの場合に無効となります。

- 拡張用 512M メモリモジュールが搭載されていない。
- BGP 相手情報に定義番号 0 以外が設定されている。
- IBGP としての設定がされている。

- 以下のどれかの定義を有効とする設定がされている。
  bgp neighbor 0 ebgp-multihop
  bgp neighbor 0 enforce-multihop
  bgp mpls-resolution
  routemanage ip redist bgp connected
  routemanage ip redist bgp static
  routemanage ip redist bgp rip
  routemanage ip redist bgp ospf
  routemanage ip redist bgp dns
  routemanage ip redist rip bgp
  routemanage ip redist ospf bgp
  routemanage ip redist ldp bgp
- 以下の定義が設定がされている。
  bgp neighbor 0 family vpnv4

[未設定時]

フルルートを使用しないものとみなされます。

11.3.9 bgp redist

[機能]

BGP 再配布フィルタの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp redist <number> <action> <address>/<mask> [<prefix_match>]

[オプション]

<number>

- フィルタリング定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜499	Si-R570
0〜249	Si-R370
0〜49	上記以外

<action>

フィルタリング条件に一致した場合の動作を指定します。

- pass
  該当する経路情報を透過します。
- reject
  該当する経路情報を遮断します。

<address>/<mask>

フィルタリング対象とする経路情報を指定します。

- IPv4 アドレス/マスクビット数 (またはマスク値)
  フィルタリング対象とする経路情報を、IPv4 アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
  - IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
  - IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)
- any
  すべての経路情報をフィルタリング対象とする場合に指定します。
- default
  デフォルトルートをフィルタリング対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<prefix_match>

経路情報 (IPv4 アドレス/マスク) の検索条件を指定します。
省略時は、exact を指定したものとみなされます。
<address>/<mask>に"any"または"default"を指定した場合は、<prefix_match>は指定できません。

- exact
  指定した<address>/<mask>と経路情報の IPv4 アドレス/マスクを比較し、一致した場合に、フィルタリング対象とします。
- inexact
  指定した<address>と経路情報情報の IPv4 アドレスを比較し、<mask>まで一致した場合、フィルタリング対象とします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

BGP に再配布する経路情報に対するフィルタリング条件と動作を設定します。
フィルタリング条件は優先順位で検索され、条件に一致した場合にフィルタリングの動作が行われ、それ以降の条件は参照されません。
すべてのフィルタリング条件に一致しない経路情報は BGP に再配布されません。
<number>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。
BGP 再配布フィルタは、本装置全体で以下の数まで定義できます。

範囲	機種
500	Si-R570
250	Si-R370
50	上記以外

[未設定時]

BGP 再配布フィルタが設定されていないものとみなされます。

11.3.10 bgp redist move

[機能]

BGP 再配布フィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp redist move <number> <new_number>

[オプション]

<number>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義番号を指定します。

<new_number>

- 移動先フィルタリング定義番号
  <number>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0〜499	Si-R570
0〜249	Si-R370
0〜49	上記以外

[動作モード]

構成定義モード (管理者クラス)

[説明]

BGP 再配布フィルタの優先順序を変更します。
<new_number>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、<new_number>は順番にソートされてリナンバリングされます。

11.4　BGP 相手側情報

11.4.1　bgp neighbor address

[機能]

BGP 相手側 IP アドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp neighbor [<count>] address <address>

[オプション]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜199	Si-R570
0〜49	Si-R370
0〜3	Si-R260B　Si-R240　Si-R220B　Si-R180

<address>

- 相手装置の IPv4 アドレス
  指定可能な範囲は以下のとおりです。

  1.0.0.1 〜 126.255.255.254
  128.0.0.1 〜 191.255.255.254
  192.0.0.1 〜 223.255.255.254

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手装置の定義番号および IPv4 アドレスを設定します。相手側情報の設定では、まず本コマンドを実行し、定義番号と IPv4 アドレスを設定しなければなりません。

[注意]

BGP/MPLS VPN 運用では、相手装置は 1 つだけ設定できます。

[未設定時]

相手側情報が設定されていないものとみなされます。

11.4.2 bgp neighbor as

[機能]

BGP 相手側 AS 番号の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp neighbor [<count>] as <as_number>

[オプション]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜199	Si-R570
0〜49	Si-R370
0〜3	Si-R260B Si-R240 Si-R220B Si-R180

<as_number>

- 相手側 AS 番号
  BGP 相手側 AS 番号を、1〜65535 の 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手装置の属する AS 番号を設定します。
IP-VPN 接続を行う場合は、自装置の属する AS 番号とは異なる値を設定しなければなりません。
BGP/MPLS VPN を使用する場合は、本装置と同じ AS 番号を設定します。

[注意]

IP-VPN 接続と BGP/MPLS VPN 接続は併用することはできません。

[未設定時]

相手装置の AS 番号が設定されていないものとみなされます。

11.4.3　bgp neighbor timers

[機能]

BGP 無通信監視タイマの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp neighbor [<count>] timers <keepalive> <holdtime>

[オプション]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜199	Si-R570
0〜49	Si-R370
0〜3	Si-R260B　Si-R240　Si-R220B　Si-R180

<keepalive>

- keepalive タイマ値
  keepalive タイマ値を、1 秒〜65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、1s〜65535s、1m〜1092m、1h〜18h です。

<holdtime>

- HoldTime のタイマ値 (秒)
  HoldTime のタイマ値を、3 秒〜65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、3s〜65535s、1m〜1092m、1h〜18h です。

[動作モード]

構成定義モード (管理者クラス)

[説明]

<keepalive>では、無通信状態で、相手装置との通信可否を確認するために送信する KEEPALIVE メッセージのタイマ値を設定します。相手装置の<holdtime>が自装置の<holdtime>よりも小さな値が設定されている場合、相手装置の<holdtime>の 3 分の 1 の値が使用されます。
<holdtime>では無通信状態で通信異常と判断する時間を設定します。本値は相手装置とネゴシエーションし、より小さな値をお互いの装置で使用します。
<keepalive>には<holdtime>よりも小さな値を指定してください。
<holdtime>と<keepalive>の設定値は、上位単位で表示可能な場合、上位単位で表示されます。

[未設定時]

<keepalive>に 30 秒、<holdtime>に 90 秒が設定されているものとみなされます。

```
bgp neighbor <count> timers 30s 90s
```

11.4.4　bgp neighbor medmetric

[機能]

BGP MED メトリックの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp neighbor [<count>] medmetric <medmetric>

[オプション]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜199	Si-R570
0〜49	Si-R370
0〜3	Si-R260B　Si-R240　Si-R220B　Si-R180

<medmetric>

- 相手装置に広報する MED メトリック値
  相手装置に広報する MED メトリック値を、0〜4294967295 の 10 進数値で指定します。
  本パラメタ値は、小さい値がより高い優先度を示します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手装置に EBGP で広報する MED メトリック値を指定します。
<medmetric>に 0 以外を指定した場合、相手装置に広報する経路情報すべてに対して MED メトリック値を広報します。<medmetric>に 0 を指定した場合、MED メトリック値として 0 を広報します。

[注意]

BGP フィルタを設定している場合は、BGP フィルタでの MED メトリック値の設定が使用されます。

[未設定時]

MED メトリック値として 0 を広報するものとみなされます。

```
bgp neighbor <count> medmetric 0
```

11.4.5 bgp neighbor asprepend

[機能]

BGP AS パスプリペンドの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp neighbor [<count>] asprepend <asprepend>

[オプション]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜199	Si-R570
0〜49	Si-R370
0〜3	Si-R260B Si-R240 Si-R220B Si-R180

<asprepend>

- AS 番号の追加数
  AS 番号の追加数を、0〜4 の 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手装置に EBGP で広報する AS 番号の個数を追加します。
<asprepend>で 0 を指定した場合は、広報される AS 番号は、自 AS 番号だけの 1 個として扱われます。

[注意]

BGP フィルタを設定している場合は、BGP フィルタでの AS 番号の追加数の設定が使用されます。

[未設定時]

広報する AS 番号の個数を追加しないとみなされます。

```
bgp neighbor <count> asprepend 0
```

11.4.6　bgp neighbor localpref

[機能]

BGP ローカル優先度の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp neighbor [<count>] localpref <localpref>

[オプション]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜199	Si-R570
0〜49	Si-R370
0〜3	Si-R260B　Si-R240　Si-R220B　Si-R180

<localpref>

- ローカル優先度
  ローカル優先度を、0〜4294967295 の 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

EBGP で受信する経路情報のローカル優先度 (LOCAL_PREF 属性) を設定します。
ローカル優先度は、IBGP で広報され、同じ自律システム内での優先経路選択に使用されます。
ローカル優先度は、大きい値がより高い優先度を示します。

[注意]

BGP フィルタを設定している場合は、BGP フィルタでのローカル優先度の設定が使用されます。

[未設定時]

EBGP で受信する経路情報のローカル優先度として 100 が設定されているものとみなされます。

```
bgp neighbor <count> localpref 100
```

11.4.7 bgp neighbor nexthopself

[機能]

BGP ネクストホップセルフの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp neighbor [<count>] nexthopself <mode>

[オプション]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜199	Si-R570
0〜49	Si-R370
0〜3	Si-R260B Si-R240 Si-R220B Si-R180

<mode>

ネクストホップセルフを行うかどうかを指定します。

- on
  ネクストホップセルフを行います。
- off
  ネクストホップセルフを行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IBGP で広報する経路情報のネクストホップを、自装置の IP アドレスに変更するかどうかを設定します。
<mode>に on を設定した場合は、IBGP で広報する経路情報のネクストホップを自装置の IP アドレスに変更して広報します。
<mode>に off を設定した場合は、IBGP で広報する経路情報のネクストホップを自装置の IP アドレスに変更しないで広報します。

[未設定時]

IBGP で広報する経路情報のネクストホップを自装置の IP アドレスに変更しないものとみなされます。

```
bgp neighbor <count> nexthopself off
```

11.4.8　bgp neighbor ebgp-multihop

[機能]

EBGP マルチホップの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp neighbor [<count>] ebgp-multihop <ttl>

[オプション]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜199	Si-R570
0〜49	Si-R370
0〜3	Si-R260B　Si-R240　Si-R220B　Si-R180

<ttl>

- TTL 値
  TTL 値を、1〜255 の 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

直接接続していない相手装置と EBGP 接続する場合に必要なホップ数 (IP パケットの TTL 値) を設定します。

[未設定時]

<ttl>に 1 が設定されているものとみなされます。

```
bgp neighbor <count> ebgp-multihop 1
```

11.4.9 bgp neighbor enforce-multihop

[機能]

BGP エンフォースマルチホップの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp neighbor [<count>] enforce-multihop <mode>

[オプション]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜199	Si-R570
0〜49	Si-R370
0〜3	Si-R260B Si-R240 Si-R220B Si-R180

<mode>

エンフォースマルチホップとして動作させるかどうかを指定します。

- on
  エンフォースマルチホップとして動作させます。
- off
  エンフォースマルチホップとして動作させません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

エンフォースマルチホップとして動作させるかどうかを設定します。
エンフォースマルチホップは、EBGP のマルチホップ接続で EBGP マルチホップの TTL 値に 1 が設定されていても、受信した経路情報を破棄しないようにする機能です。
MPLS-IX 接続で EBGP を用いて経路交換を行う場合は、通常、LSP 未確立時には EBGP を確立しないようにするために、TTL 値 1 での EBGP が用いられる。LSP 確立時には、TTL 値の減算なしでフォワーディングされるため、TTL 値 1 での BGP マルチホップでの経路交換が可能となります。
通常のマルチホップ接続では、相手装置からの経路を TTL 値 1 で受信した場合は破棄しますが、本設定により受け取ることが可能となります。

[未設定時]

エンフォースマルチホップとして動作しないものとみなされます。

```
bgp neighbor <count> enforce-multihop off
```

11.4.10 bgp neighbor default-originate

[機能]

BGP デフォルトルート広報可否の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp neighbor [<count>] default-originate <mode>

[オプション]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜199	Si-R570
0〜49	Si-R370
0〜3	Si-R260B Si-R240 Si-R220B Si-R180

<mode>

- off
  デフォルトルートを広報しません。
- on
  デフォルトルートを広報します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

デフォルトルートを広報するかどうかを設定します。
<mode>に on を設定した場合、広報する経路情報にデフォルトルートがあるときは広報します。
<mode>に off を設定した場合、広報する経路情報にデフォルトルートがあっても広報しません。

[未設定時]

デフォルトルートを広報しないものとみなされます。

```
bgp neighbor <count> default-originate off
```

11.4.11　bgp neighbor family

[機能]

BGP アドレスファミリの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp neighbor [<count>] family <address_family>

[オプション]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜199	Si-R570
0〜49	Si-R370
0〜3	Si-R260B　Si-R240　Si-R220B　Si-R180

<address_family>

- ipv4
  アドレスファミリとして IPv4 ユニキャストを使用します。
- vpnv4
  アドレスファミリとして VPN IPv4 ユニキャストを使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

BGP で使用するアドレスファミリを設定します。
<address_family>で vpnv4 は、本装置全体で 1 つだけ設定できます。

[未設定時]

アドレスファミリとして IPv4 ユニキャストを使用するものとみなされます。

```
bgp neighbor <count> family ipv4
```

11.4.12 bgp neighbor source

[機能]

BGP 自側 IP アドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp neighbor [<count>] source <address>

[オプション]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜199	Si-R570
0〜49	Si-R370
0〜3	Si-R260B Si-R240 Si-R220B Si-R180

<address>

- 自インタフェースアドレス
  自装置のインタフェースのアドレスをドット形式で指定します。
  指定可能な範囲は以下のとおりです。

  1.0.0.1 〜 126.255.255.254
  128.0.0.1 〜 191.255.255.254
  192.0.0.1 〜 223.255.255.254

[動作モード]

構成定義モード (管理者クラス)

[説明]

BGP セッションで使用する自側 IP アドレスを設定します。
BGP/MPLS VPN を使用する場合は、loopback インタフェースのアドレスを指定します。

[未設定時]

BGP セッションの自側 IP アドレスを自動的に選択するものとみなされます。

11.4.13　bgp neighbor authentication

[機能]

BGP TCP-MD5 認証鍵の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp neighbor [<count>] authentication <key> [encrypted]

[オプション]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜199	Si-R570
0〜49	Si-R370
0〜3	Si-R260B　Si-R240　Si-R220B　Si-R180

<key>

- テキスト認証鍵
  相手装置との MD5 認証で使用する認証鍵を 50 文字以下で指定します。
  0x22(ダブルクォーテーション) を除く [0x20-0x7e] の範囲のコードで構成される ASCII 文字列で指定します。ただし、文字列鍵で 0x20(空白文字) を使用する場合は、テキスト認証鍵を""で囲う必要があります。
- 暗号化されたテキスト認証鍵
  show コマンドで表示される暗号化されたテキスト認証鍵を encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

[encrypted]

- 暗号化テキスト認証鍵指定
  <key>に暗号化されたテキスト認証鍵を指定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

当該相手装置との BGP セッションで使用する TCP-MD5 認証用の認証鍵を設定します。

[未設定時]

当該相手装置との BGP セッションで TCP-MD5 認証を使用しないものとみなされます。

11.4.14 bgp neighbor filter act

[機能]

BGP フィルタの動作設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp neighbor [<count>] filter <number> act <action> [<direction>]

[オプション]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜199	Si-R570
0〜49	Si-R370
0〜3	Si-R260B Si-R240 Si-R220B Si-R180

<number>

- フィルタの定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜799	Si-R570
0〜199	上記以外

<action>

フィルタリング条件に一致した場合の動作を指定します。

- pass
  該当する経路情報を透過します。
- reject
  該当する経路情報を遮断します。

<direction>

フィルタリングを行う方向を指定します。
省略時は out を指定したものとみなされます。

- in
  受信時にフィルタリングを行います。
- out
  送信時にフィルタリングを行います。

[動作モード]

構成定義モード (管理者クラス)

[説明]

BGP での経路情報送受信時に、フィルタリング条件に一致した経路情報を通過 (pass) させるか遮断 (reject) させるかを設定します。フィルタリング条件は優先度順に検索し、条件に一致した経路情報があった時点でフィルタリングが行われ、それ以降の条件は参照されません。全条件に不一致の経路情報は遮断されます。
フィルタリング条件は、bgp neighbor filter as コマンドを使用し AS 番号を、または、
bgp neighbor filter route コマンドを使用し経路情報を設定します。
<number>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。
BGP フィルタは、本装置全体で以下の数まで定義できます。

範囲	機種
800	Si-R570
200	上記以外

[注意]

フィルタリング条件が設定されていない場合、本コマンドの設定は無効となります。
BGP/MPLS VPN 運用では、BGP フィルタを使用できません。

[未設定時]

BGP フィルタを使用しないものとみなされ、すべての BGP の経路情報が透過します。

11.4.15 bgp neighbor filter move

[機能]

BGP フィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp neighbor [<count>] filter move <number> <new_number>

[オプション]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜199	Si-R570
0〜49	Si-R370
0〜3	Si-R260B Si-R240 Si-R220B Si-R180

<number>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義番号を指定します。

<new_number>

- 移動先フィルタリング定義番号
  <number>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0〜799	Si-R570
0〜199	上記以外

[動作モード]

構成定義モード (管理者クラス)

[説明]

BGP フィルタの優先順序を変更します。
<new_number>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、<new_number>は順番にソートされてリナンバリングされます。

11.4.16　bgp neighbor filter as

[機能]

BGP フィルタの AS 番号設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp neighbor [<count>] filter <number> as <as_number>

[オプション]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜199	Si-R570
0〜49	Si-R370
0〜3	Si-R260B　Si-R240　Si-R220B　Si-R180

<number>

- フィルタの定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。

範囲	機種
0〜799	Si-R570
0〜199	上記以外

<as_number>

- AS 番号
  AS 番号を、1〜65535 の 10 進数で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

AS 番号をフィルタ条件として設定します。

[未設定時]

AS 番号をフィルタ条件としないものとみなされます。

11.4.17 bgp neighbor filter route

[機能]

BGP フィルタの経路情報設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp neighbor [<count>] filter <number> route <address>/<mask> [<prefix_match>]

[オプション]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜199	Si-R570
0〜49	Si-R370
0〜3	Si-R260B Si-R240 Si-R220B Si-R180

<number>

- フィルタの定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。

範囲	機種
0〜799	Si-R570
0〜199	上記以外

<address>/<mask>

- IPv4 アドレス/マスクビット数 (またはマスク値)
  フィルタリング対象とするルーティング情報を指定します。
  フィルタリング対象とするルーティング情報を、IPv4 アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
  - IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
  - IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)
- any
  すべてのルーティング情報をフィルタリング対象とする場合に指定します。
- default
  デフォルトルートをフィルタリング対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<prefix_match>

ルーティング情報 (IPv4 アドレス/マスク) の検索条件を指定します。
省略時は、exact を指定したものとみなされます。
<address>/<mask>に"any"または"default"を指定した場合は、<prefix_match>は指定できません。

- exact
  指定した<address>/<mask>とルーティング情報の IPv4 アドレス/マスクを比較し、一致した場合に、フィルタリング対象とします。
- inexact
  指定した<address>とルーティング情報の IPv4 アドレスを比較し、<mask>まで一致した場合、フィルタリング対象とします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

経路情報をフィルタ条件として設定します。

[注意]

同じフィルタ定義番号のフィルタ条件として AS 番号が設定されている場合、AS 番号がフィルタ条件となります。

[未設定時]

経路情報をフィルタ条件としないものとみなされます。

11.4.18 bgp neighbor filter set medmetric

[機能]

BGP フィルタの MED メトリック設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp neighbor [<count>] filter <number> set medmetric <medmetric>

[オプション]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜199	Si-R570
0〜49	Si-R370
0〜3	Si-R260B Si-R240 Si-R220B Si-R180

<number>

- フィルタの定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。

範囲	機種
0〜799	Si-R570
0〜199	上記以外

<medmetric>

- MED メトリック値
  相手装置に広報する MED メトリック値を、0〜4294967295 の範囲で設定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手装置に広報する MED メトリック値を設定します。
送信時のフィルタ条件に一致した場合、MED メトリック値に<medmetric>を設定して広報します。
受信時のフィルタに本設定を行っても、MED メトリック値の設定は行われません。

[注意]

フィルタリング条件が設定されていない場合、本コマンド の設定は無効となります。

[未設定時]

MED メトリック値を 0 として広報します。

11.4.19 bgp neighbor filter set asprepend

[機能]

BGP フィルタの AS パスプリペンド設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp neighbor [<count>] filter <number> set asprepend <asprepend>

[オプション]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜199	Si-R570
0〜49	Si-R370
0〜3	Si-R260B Si-R240 Si-R220B Si-R180

<number>

- フィルタの定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。

範囲	機種
0〜799	Si-R570
0〜199	上記以外

<asprepend>

- AS 番号追加数
  相手装置に広報する AS 番号の追加数を、0〜4 の 10 進数で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手装置に広報する AS 番号の追加数を設定します。
送信時のフィルタ条件に一致した場合、<asprepend>で設定した個数の AS 番号を追加して広報します。
受信時のフィルタに本設定を行っても、AS 番号の追加は行われません。

[注意]

フィルタリング条件が設定されていない場合、本コマンドの設定は無効となります。

[未設定時]

AS 番号の追加を行わないものとみなされます。

11.4.20 bgp neighbor filter set localpref

[機能]

BGP フィルタのローカル優先度設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bgp neighbor [<count>] filter <number> set localpref <localpref>

[オプション]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜199	Si-R570
0〜49	Si-R370
0〜3	Si-R260B Si-R240 Si-R220B Si-R180

<number>

- フィルタの定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。

範囲	機種
0〜799	Si-R570
0〜199	上記以外

<localpref>

- ローカル優先度
  ローカル優先度を、0〜4294967295 の 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

EBGP で受信する経路情報のローカル優先度 (LOCAL_PREF 属性) を設定します。
EBGP 受信時のフィルタ条件に一致した場合、ローカル優先度に<localpref>を設定します。
IBGP 受信時のフィルタおよび、送信時のフィルタに本設定を行っても、ローカル優先度の設定は行われません。

[注意]

フィルタリング条件が設定されていない場合、本コマンド の設定は無効となります。

[未設定時]

EBGP で受信する経路情報のローカル優先度として 100 が設定されたものとみなされます。

11.5 OSPF 情報

11.5.1 ospf ip id

[機能]

OSPF ID の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

ospf ip id <identifier>

[オプション]

<identifier>

- OSPF の ID
  IPv4 アドレスを 0.0.0.0〜255.255.255.255 のドット形式で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

OSPF 接続で自装置を一意に示す ID を設定します。
ID はほかのルータと重複しない値を指定し、一般的には自装置の IPv4 アドレスを使用します。
本コマンドを省略または 0.0.0.0 が設定されている場合は、以下のとおり ID を自動的に選択し使用します。

- loopback インタフェースに追加 IP アドレスが設定されている場合は、その IP アドレスを選択します。
- loopback インタフェースに追加 IP アドレスが設定されていない場合は、lan/remote インタフェースに設定されている IP アドレスの中からインタフェースの Up/Down の状態に関係なく最大のものを選択します。なお、remote インタフェースの相手側 IP アドレスおよび、lan インタフェースのセカンダリ IP アドレスは選択の対象となりません。

[未設定時]

自動的に選択された ID が使用されるものとみなされます。

```
ospf ip id 0.0.0.0
```

11.6　OSPF エリア情報

11.6.1　ospf ip area id

[機能]

OSPF エリア ID の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

ospf ip area [<area_number>] id <area_id>

[オプション]

<area_number>

- エリア定義番号
  エリアの定義番号を指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜9	Si-R570
0〜3	Si-R370
0〜2	Si-R260B　Si-R240　Si-R220B
0〜1	Si-R180

<area_id>

- エリア ID
  エリア ID を IPv4 アドレス表記 (ドット形式) または 10 進数表記で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

エリア ID を設定します。同じエリア ID を複数設定することはできません。

[注意]

OSPF を利用する場合は、エリア ID を必ず設定してください。

[未設定時]

エリア ID が設定されていないものとみなされます。

11.6.2 ospf ip area type

[機能]

OSPF エリアタイプの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

ospf ip area [<area_number>] type <area_type>

[オプション]

<area_number>

- エリア定義番号
  エリアの定義番号を指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜9	Si-R570
0〜3	Si-R370
0〜2	Si-R260B Si-R240 Si-R220B
0〜1	Si-R180

<area_type>

エリアタイプを指定します。

- transit
  通常エリア。
- stub
  スタブエリア。
- nssa
  準スタブエリア。

[動作モード]

構成定義モード (管理者クラス)

[説明]

バックボーンエリア以外のエリアに対し、エリアタイプを設定します。

[注意]

バックボーンエリアに stub または nssa を設定しても通常エリアとして動作します。

[未設定時]

エリアタイプとして通常エリアが設定されているものとみなされます。

```
ospf ip area <area_number> type transit
```

11.6.3 ospf ip area defcost

[機能]

OSPF スタブエリア用デフォルトルートコストの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

ospf ip area [<area_number>] defcost <cost>

[オプション]

<area_number>

- エリア定義番号
  エリアの定義番号を指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜9	Si-R570
0〜3	Si-R370
0〜2	Si-R260B Si-R240 Si-R220B
0〜1	Si-R180

<cost>

- デフォルトルートコスト
  デフォルトルートのコストを、0〜16777215 で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

エリア境界ルータがスタブエリア、準スタブエリアに広報するデフォルトルートのコストを設定します。

[未設定時]

デフォルトルートのコストを 1 として広報するものとみなされます。

```
ospf ip area <area_number> defcost 1
```

11.6.4　ospf ip area range

[機能]

OSPF エリア内部集約経路の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

ospf ip area [<area_number>] range <range_number> <address>/<mask> [<cost>]

[オプション]

<area_number>

- エリア定義番号
  エリアの定義番号を指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0～9	Si-R570
0～3	Si-R370
0～2	Si-R260B　Si-R240　Si-R220B
0～1	Si-R180

<range_number>

- 集約経路定義番号
  集約経路の定義番号を指定します。

範囲	機種
0～49	Si-R570
0～29	Si-R370
0～3	Si-R260B　Si-R240　Si-R220B　Si-R180

<address>/<mask>

- IPv4 ネットワークアドレス/マスクビット数 (またはマスク値)
  集約経路を IPv4 ネットワークアドレスとマスクビット数の組み合わせで指定します。
  有効な記述形式は以下のとおりです。なお、ネットマスク値は最上位ビットから 1 で連続した値でなければなりません。

  - IPv4 ネットワークアドレス/マスクビット数 (例: 192.168.1.0/24)
  - IPv4 ネットワークアドレス/マスク値 (例: 192.168.1.0/255.255.255.0)

  0.0.0.0/0 は指定できません。

<cost>

- 集約経路のコスト
  集約経路のコストを、0～16777215 の 10 進数値で指定します。
  省略、または 0 を指定した場合は、集約される経路の中でもっとも大きいコストの値が指定されたものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

エリア境界ルータでのエリア内部経路の集約を設定します。
ほかのエリアには、集約した経路だけを広報します。集約された経路は広報されません。
集約される経路がない場合は、集約経路を広報しません。
<cost>を設定した場合、集約される経路のコストに関係なく、設定された値をコストとして使用します。省略、または 0 が設定された場合は、集約される経路の中でもっとも大きいコストの値が使用されます。
<range_number>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。

[未設定時]

エリア内部経路を集約しないものとみなされます。

11.6.5　ospf ip area type3-lsa

[機能]

OSPF エリア間でのサマリ LSA 入出力可否の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

ospf ip area [<area_number>] type3-lsa <count> <action> <address>/<mask> <direction> [<prefix_match>]

[オプション]

<area_number>

- エリア定義番号
  エリアの定義番号を指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜9	Si-R570
0〜3	Si-R370
0〜2	Si-R260B　Si-R240　Si-R220B
0〜1	Si-R180

<count>

- サマリ LSA 入出力可否定義番号
  サマリ LSA 入出力可否の優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜49	Si-R570
0〜29	上記以外

<action>

サマリ LSA 入出力可否条件と一致した場合の動作を指定します。

- pass
  該当するサマリ LSA を透過します。
- reject
  該当するサマリ LSA を遮断します。

<address>/<mask>

- IPv4 アドレス/マスクビット数 (またはマスク値)
  サマリ LSA 入出力可否の条件とする経路情報を、IPv4 アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。
  以下に、有効な記述形式を示します。
  - IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
  - IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)
- any
  すべての経路情報をサマリ LSA 入出力可否の条件とする場合に指定します。

<direction>

サマリ LSA 入出力の方向を示します。

- in
  ほかのエリアからのサマリ LSA の入力を示します。
- out
  ほかのエリアへのサマリ LSA の出力を示します。

<prefix_match>

経路情報 (IPv4 アドレス/マスク) の検索条件を指定します。
省略時は、exact を指定したものとみなされます。
<address>/<mask>に"any"を指定した場合は、<prefix_match>は指定できません。

- exact
  指定した<address>/<mask>と経路情報の IPv4 アドレス/マスクを比較し、一致した場合に、サマリ LSA 入出力可否の対象とします。
- inexact
  指定した<address>と経路情報の IPv4 アドレスを比較し、<mask>まで一致した場合に、サマリ LSA 入出力可否の対象とします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

エリア境界ルータで、エリア間で入出力するサマリ LSA を透過 (pass) するか、または遮断 (reject) するかを設定します。
ほかのエリアからサマリ LSA の入力があった場合は、優先度順に<direction>に in が設定されているサマリ LSA 入出力可否条件から一致する条件を検索します。一致する条件がない場合は、遮断されます。一致する条件があった場合は、その条件に設定されている<action>により動作が決定されます。
pass が設定されている場合は、透過され、reject が設定されている場合は、遮断されます。<direction>に in が設定されている条件がない場合は、透過されます。
ほかのエリアへサマリ LSA を出力する場合は、優先度順に<direction>に out が設定されているサマリ LSA 入出力可否条件から一致する条件を検索します。一致する条件がない場合は、遮断されます。
一致する条件があった場合は、その条件に設定されている<action>により動作が決定されます。
pass が設定されている場合は、透過され、reject が設定されている場合は、遮断されます。
<direction>に out が設定されている条件がない場合は、透過されます。
LSA 入出力可否条件に一致する条件があった場合、それ以降の条件は参照されません。
<count>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。

サマリ LSA 入出力可否は、本装置全体で以下の数まで定義できます。

範囲	機種
50	Si-R570
30	上記以外

[注意]

ospf ip area range コマンドを使用し集約経路を設定しているエリアで、集約経路はサマリ LSA 入出力可否の対象となります。集約される経路は対象にならないことに注意してください。
また、以下の経路情報は、サマリ LSA 入出力可否の対象となりません。

- 各エリアの AS 境界ルータから注入された AS 外部経路
- スタブエリアおよび準スタブエリアのエリア境界ルータが注入するデフォルト経路

[未設定時]

エリア間でのサマリ LSA すべて透過するものとみなされます。

11.6.6 ospf ip area type3-lsa move

[機能]

OSPF エリア間でのサマリ LSA 入出力可否の優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

ospf ip area [<area_number>] type3-lsa move <count> <new_count>

[オプション]

<area_number>

- エリア定義番号
  エリアの定義番号を指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜9	Si-R570
0〜3	Si-R370
0〜2	Si-R260B Si-R240 Si-R220B
0〜1	Si-R180

<count>

- サマリ LSA 入出力可否定義番号
  優先順序を変更するサマリ LSA 入出力可否定義番号を指定します。

<new_count>

- 移動先サマリ LSA 入出力可否定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0〜49	Si-R570
0〜29	上記以外

[動作モード]

構成定義モード (管理者クラス)

[説明]

サマリ LSA 入出力可否定義の優先順序を変更します。
<count>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、<new_count>は順番にソートされてリナンバリングされます。

11.7　OSPF バーチャルリンク情報

11.7.1　ospf ip area vlink id

[機能]

OSPF バーチャルリンク接続先の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

ospf ip area [<area_number>] vlink [<vlink_number>] id <router_id>

[オプション]

<area_number>

- エリア定義番号
  エリアの定義番号を指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜9	Si-R570
0〜3	Si-R370
0〜2	Si-R260B　Si-R240　Si-R220B
0〜1	Si-R180

<vlink_number>

- バーチャルリンク定義番号
  バーチャルリンクの定義番号を、0〜1 で指定します。
  省略時は、0 を指定したものとみなされます。

<router_id>

- 接続先 OSPF ルータ ID
  接続先ルータの OSPF ルータ ID を指定します。
  IPv4 アドレスをドット形式で指定します。0.0.0.0 は指定できません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

バーチャルリンクの接続先を OSPF ルータ ID で設定します。
バーチャルリンクは、Si-R570 では、本装置全体で 8 個まで定義できます。

[注意]

バーチャルリンクは、スタブエリア、準スタブエリアでは使用できません。

[未設定時]

バーチャルリンクを使用しないものとみなされます。

11.7.2 ospf ip area vlink hello

[機能]

OSPF バーチャルリンク用 Hello パケット送信間隔の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

ospf ip area [<area_number>] vlink [<vlink_number>] hello <hello_interval>

[オプション]

<area_number>

- エリア定義番号
  エリアの定義番号を指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜9	Si-R570
0〜3	Si-R370
0〜2	Si-R260B Si-R240 Si-R220B
0〜1	Si-R180

<vlink_number>

- バーチャルリンク定義番号
  バーチャルリンクの定義番号を、0〜1 で指定します。
  省略時は、0 を指定したものとみなされます。

<hello_interval>

- Hello パケット送信間隔
  Hello パケットの送信間隔を、1 秒〜65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、1s〜65535s、1m〜1092m、1h〜18h です。

[動作モード]

構成定義モード (管理者クラス)

[説明]

バーチャルリンク接続先との OSPF 隣接関係の維持に用いられる Hello パケットの送信間隔を設定します。
hello_interval の値はバーチャルリンク接続先と同じ値を設定します。

[注意]

バーチャルリンク接続先と異なる Hello パケット送信間隔を設定した場合、ルーティングが行えません。

[未設定時]

バーチャルリンク用 Hello パケット送信間隔に 10 秒が設定されているものとみなされます。

```
ospf ip area <area_number> vlink <vlink_number> hello 10s
```

11.7.3 ospf ip area vlink dead

[機能]

OSPF バーチャルリンク用隣接ルータ停止確認間隔の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

ospf ip area [<area_number>] vlink [<vlink_number>] dead <dead_interval>

[オプション]

<area_number>

- エリア定義番号
  エリアの定義番号を指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜9	Si-R570
0〜3	Si-R370
0〜2	Si-R260B Si-R240 Si-R220B
0〜1	Si-R180

<vlink_number>

- バーチャルリンク定義番号
  バーチャルリンクの定義番号を、0〜1 で指定します。
  省略時は、0 を指定したものとみなされます。

<dead_interval>

- 隣接ルータ停止確認間隔
  隣接ルータ停止確認の間隔を、1 秒〜65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、1s〜65535s、1m〜1092m、1h〜18h です。

[動作モード]

構成定義モード (管理者クラス)

[説明]

バーチャルリンクでの OSPF 隣接関係の維持に用いられる隣接ルータ停止確認間隔を設定します。
隣接ルータ停止確認間隔の間に Hello パケットを受信しなかった場合は、バーチャルリンク接続先との隣接関係は解除されます。
dead_interval の値はバーチャルリンク接続先と同じ値を設定します。
dead_interval の値は Hello パケット送信間隔よりも大きな値を設定する必要があります。
Hello パケット送信間隔の 4 倍を設定することを推奨します。

[注意]

バーチャルリンク接続先と異なる隣接ルータ停止確認間隔を設定した場合、ルーティングが行えません。

[未設定時]

バーチャルリンク用隣接ルータ停止確認間隔に 40 秒が設定されているものとみなされます。

```
ospf ip area <area_number> vlink <vlink_number> dead 40s
```

11.7.4 ospf ip area vlink retrans

[機能]

OSPF バーチャルリンク用パケット再送間隔の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

ospf ip area [<area_number>] vlink [<vlink_number>] retrans <retransmit_interval>

[オプション]

<area_number>

- エリア定義番号
  エリアの定義番号を指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜9	Si-R570
0〜3	Si-R370
0〜2	Si-R260B Si-R240 Si-R220B
0〜1	Si-R180

<vlink_number>

- バーチャルリンク定義番号
  バーチャルリンクの定義番号を、0〜1 で指定します。
  省略時は、0 を指定したものとみなされます。

<retransmit_interval>

- パケット再送間隔
  パケットの再送間隔を、1 秒〜65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、1s〜65535s、1m〜1092m、1h〜18h です。

[動作モード]

構成定義モード (管理者クラス)

[説明]

バーチャルリンクで OSPF パケットを再送する間隔を設定します。

[未設定時]

バーチャルリンク用パケット再送間隔に 5 秒が設定されているものとみなされます。

```
ospf ip area <area_number> vlink <vlink_number> retrans 5s
```

11.7.5　ospf ip area vlink delay

[機能]

OSPF バーチャルリンク用 LSU パケット送信遅延時間の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

ospf ip area [<area_number>] vlink [<vlink_number>] delay <transmit_delay>

[オプション]

<area_number>

- エリア定義番号
  エリアの定義番号を指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜9	Si-R570
0〜3	Si-R370
0〜2	Si-R260B　Si-R240　Si-R220B
0〜1	Si-R180

<vlink_number>

- バーチャルリンク定義番号
  バーチャルリンクの定義番号を、0〜1 で指定します。
  省略時は、0 を指定したものとみなされます。

<transmit_delay>

- LSU パケット送信遅延時間
  LSU パケットを送信する場合の遅延時間を、1 秒〜65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、1s〜65535s、1m〜1092m、1h〜18h です。

[動作モード]

構成定義モード (管理者クラス)

[説明]

LSU(Link State Update) パケットの送信遅延時間を設定します。
LSU パケットでは、LSA(Link State Advertisement) を作成してからの経過時間に<transmit_delay>の値を加算して広報します。

[注意]

一般的な装置では、作成してからの経過時間が 1 時間となった LSA を破棄します。このため、LSU 送信遅延時間に 1 時間以上を設定した場合は、正しくルーティングできない場合があります。

[未設定時]

バーチャルリンク用 LSU パケット送信遅延時間に 1 秒が設定されているものとみなされます。

```
ospf ip area <area_number> vlink <vlink_number> delay 1s
```

11.7.6　ospf ip area vlink auth type

[機能]

OSPF バーチャルリンク用パケット認証方式の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

ospf ip area [<area_number>] vlink [<vlink_number>] auth type <authtype>

[オプション]

<area_number>

- エリア定義番号
  エリアの定義番号を指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜9	Si-R570
0〜3	Si-R370
0〜2	Si-R260B　Si-R240　Si-R220B
0〜1	Si-R180

<vlink_number>

- バーチャルリンク定義番号
  バーチャルリンクの定義番号を、0〜1 で指定します。
  省略時は、0 を指定したものとみなされます。

<authtype>

パケット認証方式を指定します。

- off
  認証を行いません。
- text
  テキスト認証を使用します。
- md5
  MD5 認証を使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

バーチャルリンクで OSPF パケットに対する認証方式を設定します。

[注意]

authtype で text を設定した場合は、テキスト認証鍵の設定が必要です。md5 を設定した場合は、MD5 認証鍵情報の設定が必要です。

[未設定時]

バーチャルリンクで OSPF パケット認証を使用しないものとみなされます。

```
ospf ip area <area_number> vlink <vlink_number> auth type off
```

11.7.7　ospf ip area vlink auth textkey

[機能]

OSPF バーチャルリンク用テキスト認証鍵の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

ospf ip area [<area_number>] vlink [<vlink_number>] auth textkey <kind> <key> [encrypted]

[オプション]

<area_number>

- エリア定義番号
  エリアの定義番号を指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜9	Si-R570
0〜3	Si-R370
0〜2	Si-R260B　Si-R240　Si-R220B
0〜1	Si-R180

<vlink_number>

- バーチャルリンク定義番号
  バーチャルリンクの定義番号を、0〜1 で指定します。
  省略時は、0 を指定したものとみなされます。

<kind>

鍵種別を指定します。

- text
  文字列鍵を使用します。
- hex
  16 進数鍵を使用します。

<key>

- テキスト認証鍵
  文字列鍵の場合は、0x21,0x23〜0x7e のコードで構成される 8 文字以内の ASCII 文字列で指定します。
  16 進数鍵の場合は、16 桁以内の 16 進数値で指定します。16 桁未満の値を指定したときは左詰めで設定され、残りは 16 桁になるまで 0x0 でパディングされます。
- 暗号化されたテキスト認証鍵
  show コマンドで表示される暗号化されたテキスト認証鍵を encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化テキスト認証鍵指定
  <key>に暗号化されたテキスト認証鍵を指定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

バーチャルリンクのテキスト認証で使用する鍵を設定します。
show コマンドでは、暗号化されたテキスト認証鍵が encrypted と共に表示されます。

[未設定時]

バーチャルリンク用テキスト認証鍵が設定されていないものとみなされます。

11.7.8　ospf ip area vlink auth md5key

[機能]

OSPF バーチャルリンク用 MD5 認証鍵情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

ospf ip area [<area_number>] vlink [<vlink_number>] auth md5key <key_id> <key> [encrypted]

[オプション]

<area_number>

- エリア定義番号
  エリアの定義番号を指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0～9	Si-R570
0～3	Si-R370
0～2	Si-R260B　Si-R240　Si-R220B
0～1	Si-R180

<vlink_number>

- バーチャルリンク定義番号
  バーチャルリンクの定義番号を、0～1 で指定します。
  省略時は、0 を指定したものとみなされます。

<key_id>

- MD5 認証鍵 ID
  MD5 認証鍵 ID を、1～255 で指定します。
- 暗号化された MD5 認証鍵 ID
  show コマンドで表示される暗号化された MD5 認証鍵 ID を encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

<key>

- MD5 認証鍵
  MD5 認証鍵を、0x21,0x23～0x7e のコードで構成される 16 文字以内の ASCII 文字列で指定します。
- 暗号化された MD5 認証鍵
  show コマンドで表示される暗号化された MD5 認証鍵を encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化 MD5 認証鍵情報指定
  <key_id>と<key>に暗号化された MD5 認証鍵 ID と MD5 認証鍵を指定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

バーチャルリンクの MD5 認証で使用する鍵情報 (MD5 認証鍵 ID、MD5 認証鍵) を設定します。show コマンドでは、暗号化された MD5 認証鍵 ID と MD5 認証鍵が encrypted と共に表示されます。

[未設定時]

バーチャルリンク用 MD5 認証鍵情報が設定されていないものとみなされます。

11.8　ASBR 情報

11.8.1　ospf ip definfo

[機能]

OSPF AS 境界ルータのデフォルトルート広報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

ospf ip definfo <mode> [<metric> [<metric_type>]]

[オプション]

<mode>

- off
  デフォルトルートを広報しません。
- always
  デフォルトルートを広報します。
- exist
  AS 外部経路にデフォルトルートが存在した場合だけ広報します。

<metric>

- メトリック値
  デフォルトルートのメトリック値を、0〜16777214 で指定します。
  省略時は、10 を指定したものとみなされます。

<metric_type>

- type1
  外部メトリックタイプ 1 を指定します。
- type2
  外部メトリックタイプ 2 を指定します。
  省略時は、type2 を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

AS 境界ルータのデフォルトルートの広報を設定します。

[注意]

本設定は、AS 境界ルータとして動作している場合にだけ有効となります。

[未設定時]

AS 境界ルータでデフォルトルートを広報しないものとみなされます。

```
ospf ip definfo off
```

11.8.2　ospf ip summary

[機能]

OSPF AS 外部経路集約の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

ospf ip summary <summary_number> <address>/<mask>

[オプション]

<summary_number>

- 集約経路定義番号
  集約経路の定義番号を指定します。

範囲	機種
0〜49	Si-R570
0〜29	Si-R370
0〜3	Si-R260B　Si-R240　Si-R220B　Si-R180

<address>/<mask>

- IPv4 ネットワークアドレス/マスクビット数 (またはマスク値)
  集約経路の IPv4 ネットワークアドレスとマスクビット数の組み合わせを指定します。
  有効な記述形式は以下のとおりです。なお、ネットマスク値は最上位ビットから 1 で連続した値でなければなりません。
  - IPv4 ネットワークアドレス/マスクビット数 (例: 10.10.0.0/16)
  - IPv4 ネットワークアドレス/マスク値 (例: 10.10.0.0/255.255.0.0)

  0.0.0.0/0 は指定できません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

AS 境界ルータの AS 外部経路の集約を設定します。
AS 外部の経路を広報する場合は、集約した経路を広報します。
<summary_number>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。

[注意]

本設定は、AS 境界ルータとして動作している場合にだけ有効となります。

[未設定時]

AS 外部経路の集約を行わないものとみなされます。

11.8.3 ospf ip redist

[機能]

OSPF 再配布フィルタの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

ospf ip redist <number> <action> <address>/<mask> [<prefix_match> [<metric> <metric_type>]]

[オプション]

<number>

- フィルタリング定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜499	Si-R570
0〜249	Si-R370
0〜49	上記以外

<action>

フィルタリング条件に一致した場合の動作を指定します。

- pass
  該当する経路情報を透過します。
- reject
  該当する経路情報を遮断します。

<address>/<mask>

フィルタリング対象とする経路情報を指定します。

- IPv4 アドレス/マスクビット数 (またはマスク値)
  フィルタリング対象とする経路情報を、IPv4 アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
  - IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
  - IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)
- any
  すべての経路情報をフィルタリング対象とする場合に指定します。
- default
  デフォルトルートをフィルタリング対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<prefix_match>

経路情報 (IPv4 アドレス/マスク) の検索条件を指定します。
省略時は、exact を指定したものとみなされます。
<address>/<mask>に"any"または"default"を指定した場合は、<prefix_match>は指定できません。

- exact
  指定した<address>/<mask>と経路情報の IPv4 アドレス/マスクを比較し、一致した場合に、フィルタリング対象とします。
- inexact
  指定した<address>と経路情報の IPv4 アドレスを比較し、<mask>まで一致した場合、フィルタリング対象とします。

<metric>

再配布する経路情報のメトリック値を指定します。
省略時は、IPv4 ルーティングプロトコル再配布の設定で指定した値となります。
<action>に"reject"を指定した場合は、<metric>は指定できません。

- 再配布するメトリック値
  設定可能範囲は、0〜16777214 です。

<metric_type>

再配布する経路情報のメトリックタイプを指定します。
省略時は、IPv4 ルーティングプロトコル再配布の設定で指定した値となります。
<action>に"reject"を指定した場合は、<metric_type>は指定できません。

- type1
  外部経路のメトリックタイプが type1
- type2
  外部経路のメトリックタイプが type2

[動作モード]

構成定義モード (管理者クラス)

[説明]

OSPF に再配布する経路に対するフィルタリング条件と動作を設定します。
フィルタリング条件は優先順位で検索され、条件に一致した場合にフィルタリングの動作が行われそれ以降の条件は参照されません。
すべてのフィルタリング条件に一致しない経路情報は再配布されません。
再配布する経路情報にメトリック値、およびメトリックタイプを指定できます。
<address>/<mask>に"any"を指定した場合、メトリック値、およびメトリックタイプは、IPv4 ルーティングプロトコル再配布の設定で指定した値となります。また、"default"を指定した場合は、ospf ip definfo コマンドで指定した値となります。
<number>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。
OSPF 再配布フィルタは、本装置全体で以下の数まで定義できます。

範囲	機種
500	Si-R570
250	Si-R370
50	上記以外

[注意]

デフォルトルートを再配布する場合は、ospf definfo コマンドの設定も必要です。

[未設定時]

OSPF 再配布フィルタが設定されていないものとみなされます。

11.8.4　ospf ip redist move

[機能]

OSPF 再配布フィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

ospf ip redist move <number> <new_number>

[オプション]

<number>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義番号を指定します。

<new_number>

- 移動先フィルタリング定義番号
  <number>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0～499	Si-R570
0～249	Si-R370
0～49	上記以外

[動作モード]

構成定義モード (管理者クラス)

[説明]

OSPF 再配布フィルタの優先順序を変更します。
<new_number>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、<new_number>は順番にソートされてリナンバリングされます。

第 12 章　ブリッジ情報の設定

12.1　ブリッジ情報

12.1.1　bridge age

[機能]

ブリッジ学習テーブルの生存時間の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bridge [<group_id>] age <age_time>

[オプション]

<group_id>

- ブリッジグループ識別子
  ブリッジグループ識別子を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜19	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
0〜7	Si-R180

<age_time>

- 生存時間
  MAC アドレス学習によって学習した情報の生存時間を、10 秒〜1000000 秒の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本コマンドは、ブリッジ機能を使用する場合にだけ有効です。
アドレス学習テーブルの生存時間を設定します。
アドレス学習機能によって学習された MAC アドレステーブルを最後に使用してから削除されるまでの時間を設定します。

[注意]

ブリッジグループ 0 に設定された値がすべてのブリッジグループで使用され、ブリッジグループ 0 以外に設定された値は使用されません。

[未設定時]

アドレス学習テーブルの生存時間として 5 分を定義するものとみなされます。

```
bridge <group_id> age 5m
```

12.1.2　bridge stp priority

[機能]

ブリッジ優先度の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bridge [<group_id>] stp priority <priority>

[オプション]

<group_id>

- ブリッジグループ識別子
  ブリッジグループ識別子を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜19	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
0〜7	Si-R180

<priority>

- 優先度
  ブリッジネットワーク内での本装置の優先度を、0〜65535 の 10 進数値で指定します。値が小さいほど、優先度が高くなります。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本コマンドは、STP を使用する場合にだけ有効です。
ルートブリッジ決定アルゴリズムで使用するブリッジの優先度を指定します。一般的なブリッジネットワークではルートブリッジにトラフィックが集中するため、バックボーンに近いブリッジが優先となるように設定してください。ルートブリッジにするブリッジには、最小の値を指定してください。

[注意]

ブリッジグループ 0 以外のブリッジグループでは STP は動作しません。

[未設定時]

優先度として 32768 を定義するものとみなされます。

```
bridge <group_id> stp priority 32768
```

12.1.3 bridge stp age

[機能]

Hello メッセージ待ち時間の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bridge [<group_id>] stp age <max_age>

[オプション]

<group_id>

- ブリッジグループ識別子
  ブリッジグループ識別子を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜19	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B
0〜7	Si-R180

<max_age>

- 待ち時間
  ルートブリッジから送出される構成情報 BPDU の待ち時間を、6 秒〜40 秒の範囲で指定します。
  単位は、s(秒) を指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本コマンドは、STP を使用する場合にだけ有効です。
ルートブリッジまたは代表ブリッジから送出される構成情報 BPDU の待ち時間を指定します。

[注意]

ブリッジグループ 0 以外のブリッジグループでは STP は動作しません。

[未設定時]

待ち時間に 20 秒を設定したものとみなされます。

```
bridge <group_id> stp age 20s
```

12.1.4　bridge stp hello

[機能]

Hello メッセージ送出間隔の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bridge [<group_id>] stp hello <time>

[オプション]

<group_id>

- ブリッジグループ識別子
  ブリッジグループ識別子を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜19	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
0〜7	Si-R180

<time>

- 送出間隔
  ルートブリッジになったときに定期的に送出する構成情報 BPDU の送出間隔の時間を、1 秒〜10 秒の範囲で指定します。
  単位は、s(秒) を指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本コマンドは、STP を使用する場合にだけ有効です。
本装置がルートブリッジとなったときに送出する構成情報 BPDU の送出間隔を指定します。
STP を使用する場合でも、本装置がルートブリッジとならなかった場合は、設定が無効となります。

[注意]

ブリッジグループ 0 以外のブリッジグループでは STP は動作しません。

[未設定時]

送出間隔に 2 秒を設定したものとみなされます。

```
bridge <group_id> stp hello 2s
```

12.1.5 bridge stp delay

[機能]

最大中継遅延時間の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bridge [<group_id>] stp delay <delay_time>

[オプション]

<group_id>

- ブリッジグループ識別子
  ブリッジグループ識別子を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜19	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B
0〜7	Si-R180

<delay_time>

- 最大中継遅延時間
  最大中継遅延時間を、4 秒〜30 秒の範囲で指定します。
  単位は、s(秒) を指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本コマンドは、STP を使用する場合にだけ有効です。
最大中継遅延時間を設定します。
STP を使用する場合でも、本装置がルートブリッジとならなかった場合は、設定が無効となります。
STP で Listening 状態から Learning 状態に変化する場合、または Learning 状態から Forwarding 状態に変化するまでの時間 (ルートブリッジから広報される時間) を指定します。

[注意]

ブリッジグループ 0 以外のブリッジグループでは STP は動作しません。

[未設定時]

最大中継遅延時間に 15 秒を設定したものとみなされます。

```
bridge <group_id> stp delay 15s
```

12.1.6　bridge ip routing

[機能]

IPv4 ルーティングの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bridge [<group_id>] ip routing <mode>

[オプション]

<group_id>

- ブリッジグループ識別子
  ブリッジグループ識別子を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜19	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
0〜7	Si-R180

<mode>

- on
  IPv4 ルーティングを有効にします。
- off
  IPv4 ルーティングを無効にし、IPv4 フレームをブリッジにより制御します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv4 ルーティングの設定します。
IPv4 ルーティングを無効とした場合、IPv4 フレームはブリッジにより制御されます。

[未設定時]

IPv4 をルーティングにより制御するものとみなされます。

```
bridge <group_id> ip routing on
```

12.1.7 bridge ip policy

[機能]

IPv4 転送ポリシの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bridge [<group_id>] ip policy <mode>

[オプション]

<group_id>

- ブリッジグループ識別子
  ブリッジグループ識別子を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜19	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B
0〜7	Si-R180

<mode>

- strict
  IPv4 ブリッジを行う場合に、グループ外からグループ内およびグループ内からグループ外へのルーティングによる転送を行いません。
- loose
  IPv4 ブリッジを行う場合に、グループ外からグループ内およびグループ内からグループ外へのルーティングによる転送を行います。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本コマンドは、IPv4 をブリッジ対象とした場合にだけ有効です。
IPv4 ブリッジを行う場合に、グループ外からグループ内、およびグループ内からグループ外へのルーティングによる転送を行うかどうかを設定します。
IPv4 ブリッジ動作時にグループ内からグループ外へのルーティングによる転送が行われるのは以下の場合です。

- 受信フレームのあて先 MAC アドレスが受信インタフェースあてであるが、あて先 IP アドレスが受信インタフェースあてでない場合。

IPv4 ブリッジ動作時にグループ外からグループ内へのルーティングによる転送が行われるのは以下の場合です。

- IPv4 をルーティングするインタフェースで受信したパケットがルーティングにより IPv4 をブリッジするインタフェースへ出力される場合。

<mode>が strict の場合、これらの転送をブロックすることで、ブリッジ転送対象外のパケットに対してもグループ内に閉じた通信を行うことができます。

[未設定時]

グループ外からグループ内、およびグループ内からグループ外へのルーティングによる転送を行わないものとして動作します。

```
bridge <group_id> ip policy strict
```

12.1.8 bridge ip6 routing

[機能]

IPv6 ルーティングの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bridge [<group_id>] ip6 routing <mode>

[オプション]

<group_id>

- ブリッジグループ識別子
  ブリッジグループ識別子を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜19	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B
0〜7	Si-R180

<mode>

- on
  IPv6 ルーティングを有効にします。
- off
  IPv6 ルーティングを無効にし、IPv6 フレームをブリッジにより制御します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv6 ルーティングの設定します。
IPv6 ルーティングを無効とした場合、IPv6 フレームはブリッジにより制御されます。

[未設定時]

IPv6 をルーティングにより制御するものとみなされます。

```
bridge <group_id> ip6 routing
```

12.1.9　bridge ip6 policy

[機能]

IPv6 転送ポリシの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bridge [<group_id>] ip6 policy <mode>

[オプション]

<group_id>

- ブリッジグループ識別子
  ブリッジグループ識別子を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜19	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
0〜7	Si-R180

<mode>

- strict
  IPv6 ブリッジを行う場合に、グループ外からグループ内およびグループ内からグループ外へのルーティングによる転送を行いません。
- loose
  IPv6 ブリッジを行う場合に、グループ外からグループ内およびグループ内からグループ外へのルーティングによる転送を行います。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本コマンドは、IPv6 をブリッジ対象とした場合にだけ有効です。
IPv6 ブリッジを行う場合に、グループ外からグループ内、およびグループ内からグループ外へのルーティングによる転送を行うかどうかを設定します。
IPv6 ブリッジ動作時にグループ内からグループ外へのルーティングによる転送が行われるのは以下の場合です。

- 受信フレームのあて先 MAC アドレスが受信インタフェースあてであるが、あて先 IP アドレスが受信インタフェースあてでない場合。

IPv6 ブリッジ動作時にグループ外からグループ内へのルーティングによる転送が行われるのは以下の場合です。

- IPv6 をルーティングするインタフェースで受信したパケットがルーティングにより IPv6 をブリッジするインタフェースへ出力される場合。

<mode>が strict の場合、これらの転送をブロックすることで、ブリッジ転送対象外のパケットに対してもグループ内に閉じた通信を行うことができます。

[未設定時]

グループ外からグループ内、およびグループ外からグループ内へのルーティングによる転送を行わないものとして動作します。

```
bridge <group_id> ip6 policy strict
```

12.1.10　bridge vlan tag transmit

[機能]

VLAN タグの転送方式の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bridge [<group_id>] vlan tag transmit <mode>

[オプション]

<group_id>

- ブリッジグループ識別子
  ブリッジグループ識別子を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜19	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
0〜7	Si-R180

<mode>

- on
  VLAN タグをつけたまま透過ブリッジします。
- off
  VLAN タグを挿抜してブリッジします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

VLAN インタフェースで受信した VLAN タグ付きフレームのタグを透過転送するかどうかを設定します。VLAN タグを挿抜する設定の場合、VLAN インタフェースで受信してリモートインタフェースへ出力する際には VLAN タグを除去して転送し、リモートインタフェースで受信して VLAN インタフェースへ出力する際には VLAN タグを挿入して転送します。

[未設定時]

VLAN タグを挿抜してブリッジします。

```
bridge <group_id> vlan tag transmit off
```

12.1.11 bridge inter-remote

[機能]

リモートインタフェース間のブリッジ転送の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bridge [<group_id>] inter-remote <mode>

[オプション]

<group_id>

- ブリッジグループ識別子
  ブリッジグループ識別子を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜19	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B
0〜7	Si-R180

<mode>

- on
  リモートインタフェース間のブリッジ転送を行います。
- off
  リモートインタフェース間のブリッジ転送を行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

リモートインタフェース間でブリッジ転送を行うか行わないかを設定します。
リモートインタフェースと LAN インタフェースの間のブリッジだけを許し、あるリモートインタフェースから別のリモートインタフェースへのブリッジ転送をブロックしたい場合に<mode> に off を設定します。

[未設定時]

リモートインタフェース間でブリッジ転送を行います。

```
bridge <group_id> inter-remote on
```

12.1.12　bridge control

[機能]

MAC コントロールフレーム転送設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

bridge [<group_id>] control <protocol>

[オプション]

<group_id>

- ブリッジグループ識別子
  ブリッジグループ識別子を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜19	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
0〜7	Si-R180

<protocol>

ブリッジ転送する MAC コントロールフレームを、以下の中から指定します。複数指定する場合は、","(カンマ) で区切ります。

- stp
  STP のフレーム (BPDU) をブリッジ転送します。
- lacp
  LACP のフレームをブリッジ転送します。
- eapol
  IEEE 802.1X のフレーム (EAPOL) をブリッジ転送します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

MAC コントロールフレームのブリッジ転送を有効にするかどうかを設定します。
ここで転送を行うと定義されたプロトコルは、本装置では受信しません。そのため、STP を転送すると定義した場合、STP でのループ検出はできなくなります。

[注意]

本コマンドで定義可能なフレームは IEEE 802.1D でブリッジ転送を禁止しているフレームです。
Si-R180 ではスイッチポートを使用しないまたはスイッチポートの VLAN tag 透過転送の設定が有効となっている場合のみ利用が可能です。

[未設定時]

定義なしとして、MAC コントロールフレームの転送をしません。

第 13 章　MPLS 情報の設定

13.1　LDP 情報

13.1.1　mpls ldp router-id

[機能]

LDP ROUTER-ID の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

mpls ldp router-id <identifier>

[オプション]

<identifier>

- LDP を使用するルータを特定するための ID
  IPv4 アドレスで指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

自装置を一意に示す ID を設定します。設定する ID はほかのルータと重複しない ID を指定します。通信可能な自装置の IP アドレス (IPv4) を設定します。
0.0.0.0 を指定した場合、自動的にどれかの自装置の IP アドレス (IPv4) を使用します。

[未設定時]

0.0.0.0 が設定されているものとみなされ、router-id は自動的に設定されます。

```
mpls ldp router-id 0.0.0.0
```

13.1.2 mpls ldp control

[機能]

LDP 制御方式の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

mpls ldp control <mode>

[オプション]

<mode>

- ordered
  Ordered Label Distribution Control を使用します。
- independent
  Independent Label Distribution Control を使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

LDP の制御方式を指定します。

[未設定時]

independent が選択されたものとして動作します。

```
mpls ldp control independent
```

13.1.3　mpls ldp ip transport

[機能]

IPv4 Transport Address の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

mpls ldp ip transport <address>

[オプション]

<address>

- LDP セッションの送信元 IPv4 アドレス
  IPv4 アドレスを指定します。以下の範囲で指定してください。

  0.0.0.0
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[動作モード]

構成定義モード (管理者クラス)

[説明]

LDP がピアとの通信に用いる送信元 IPv4 アドレスを設定します。本装置に設定された IPv4 アドレスを指定します。
インタフェースの設定で IPv4 Transport Address を指定しない場合に、本設定が使用されます。本定義に 0.0.0.0 を指定した場合は、LDP が動作するインタフェースの IPv4 アドレスを IPv4 Transport Address として使用します。

[未設定時]

IPv4 Transport Address の設定を行わず、LDP が動作するインタフェースの IPv4 アドレスを送信元として使用します。

```
mpls ldp ip transport 0.0.0.0
```

[注意]

IPv4 Transport Address を指定する場合は、必ず本装置に存在するにアドレスを指定する必要があります。本装置に存在しないアドレスを指定した場合は、LDP を使用できません。

13.1.4 mpls ip propagate-ttl

[機能]

MPLS TTL 伝達の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

mpls ip propagate-ttl <mode>

[オプション]

<mode>

- on
  MPLS から IP または IP から MPLS にパケットを交換する際に、TTL の情報を伝達します。
- off
  MPLS から IP または IP から MPLS にパケットを交換する際に、TTL の情報を伝達しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

MPLS と IP の間での TTL の伝達方法を指定します。
mode が on の場合は。MPLS ラベル PUSH 時に IP パケットの TTL が伝達され、MPLS ラベル POP 時に IP パケットの TTL に書き戻されるため、MPLS ドメインを転送される IP パケットはドメインの hop 数分だけ TTL が減少します。
mode が off の場合は。MPLS ラベル PUSH 時に IP パケットの TTL が伝達されず、MPLS パケットの TTL は無条件で 255 となり、また MPLS ラベル POP 時にも IP パケットの TTL は書き戻されないため、MPLS ドメインを転送される IP パケットはドメインの hop 数を意識することがなく、ドメインを 1 つの仮想的なルータとして見るようになります。

[注意]

本設定は MPLS ドメイン中のすべてのルータで一致させる必要があります。

[未設定時]

on が選択されたものとして動作します。

```
mpls ip propagate-ttl on
```

第 14 章　マルチキャスト 情報の設定

14.1 マルチキャスト情報

14.1.1 multicast ip pimsm candrp mode

[機能]

PIM-SM(IPv4) の RP の動作の指定。

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

multicast ip pimsm candrp mode <mode>

[オプション]

<mode>

PIM-SM の RP としての動作モードを以下で指定します。

- off
  RP として動作しない
- on
  RP として動作する

[動作モード]

構成定義モード (管理者クラス)

[説明]

PIM-SM(IPv4) の RP としての動作モードを指定します。

[未設定時]

RP として動作しません。

```
multicast ip pimsm candrp mode off
```

14.1.2　multicast ip pimsm candrp address

[機能]

PIM-SM(IPv4) の RP のアドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

multicast ip pimsm candrp address <address>

[オプション]

<address>

- RP アドレス
  PIM-SM(IPv4) の RP として動作するインタフェースのアドレスを指定します。
  0.0.0.0 を指定すると利用できるアドレスを自動で検索します。
  指定可能な範囲は以下のとおりです。

  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[動作モード]

構成定義モード (管理者クラス)

[説明]

RP として動作するインタフェースのアドレスを指定します。

[未設定時]

利用できるアドレスを自動で検索します。

```
multicast ip pimsm candrp address 0.0.0.0
```

14.1.3 multicast ip pimsm candrp priority

[機能]

PIM-SM(IPv4) の RP としての動作時のプライオリティ

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

multicast ip pimsm candrp priority <priority>

[オプション]

<priority>

- プライオリティ
  PIM-SM(IPv4) の RP としての動作時のプライオリティを 0〜255 の 10 進数値で設定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RP としての動作時のプライオリティを設定します。

[注意]

指定した値が小さいほど、優先順位が高くなります。

[未設定時]

0(最高) が指定されたものとみなされます。

```
multicast ip pimsm candrp priority 0
```

14.1.4　multicast ip pimsm candbsr mode

[機能]

PIM-SM(IPv4) の BSR の動作の指定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

multicast ip pimsm candbsr mode <mode>

[オプション]

<mode>

PIM-SM(IPv4) の BSR としての動作モードを以下で指定します。

- off
  BSR として動作しない
- on
  BSR として動作する

[動作モード]

構成定義モード (管理者クラス)

[説明]

PIM-SM の BSR としての動作モードを指定します。

[未設定時]

BSR として動作しません。

```
multicast ip pimsm candbsr mode off
```

14.1.5 multicast ip pimsm candbsr address

[機能]

PIM-SM(IPv4) の BSR のアドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

multicast ip pimsm candbsr address <address>

[オプション]

<address>

- BSR アドレス
  PIM-SM(IPv4) の BSR として動作するインタフェースのアドレスを指定します。
  0.0.0.0 を指定すると利用できるアドレスを自動で検索します。
  指定可能な範囲は以下のとおりです。

  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[動作モード]

構成定義モード (管理者クラス)

[説明]

BSR として動作するインタフェースのアドレスを指定します。

[未設定時]

利用できるアドレスを自動で検索します。

```
multicast ip pimsm candbsr address 0.0.0.0
```

14.1.6　multicast ip pimsm candbsr priority

[機能]

PIM-SM(IPv4) の BSR のプライオリティの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

multicast ip pimsm candbsr priority <priority>

[オプション]

<priority>

- プライオリティ

  PIM-SM(IPv4) の BSR としての動作時のプライオリティを 0〜255 の 10 進数値で設定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

BSR としての動作時のプライオリティを設定します。

[注意]

指定した値が大きいほど、優先順位が高くなります。

[未設定時]

0(最低) が設定されたものとみなされます。

```
multicast ip pimsm candbsr priority 0
```

14.1.7 multicast ip pimsm spt mode

[機能]

PIM-SM(IPv4) の SPT への経路変更の動作の指定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

multicast ip pimsm spt mode <mode>

[オプション]

<mode>

PIM-SM(IPv4) の SPT への経路変更の動作モードを以下で指定します。

- on
  経路変更を行う
- off
  経路変更を行わない

[動作モード]

構成定義モード (管理者クラス)

[説明]

PIM-SM(IPv4) の SPT への経路変更の動作モードを指定します。

[注意]

SPT への切り替えは、マルチキャスト・パケットの受信者の直前のルータ (lasthop router) が行います。SPT の設定は、lasthop router 上で行います。

[未設定時]

経路変更を行います。

```
multicast ip pimsm spt mode on
```

14.1.8　multicast ip pimsm spt rate

[機能]

PIM-SM(IPv4) の SPT への経路変更のしきい値

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

multicast ip pimsm spt rate <rate>

[オプション]

<rate>

- データ転送速度

  PIM-SM(IPv4) の SPT への経路変更のしきい値となるデータ転送速度を、10 進数値と単位文字で指定します。

  10 進数値の末尾に k または m の単位文字を付与することで単位を指定できます。

  単位文字を付与しない場合、単位は Kbps となります。

  単位文字 k を付与した場合、単位は Kbps となります。

  単位文字 m を付与した場合、単位は Mbps となります。

  1Kbps は 1000bps、1Mbps は 1000Kbps です。

  0 の場合、経路変更を即座に行います。

範囲	機種
1〜1000000 1k〜1000000k 1m〜1000m	Si-R570
1〜100000 1k〜100000k 1m〜100m	上記以外

[動作モード]

構成定義モード (管理者クラス)

[説明]

SPT への経路変更のしきい値をデータ転送速度で設定します。

[注意]

経路変更が行われるまで、最大で 5 秒のタイムラグが発生する場合があります。

[未設定時]

即座に SPT への経路変更を行います。

```
multicast ip pimsm spt rate 0
```

14.1.9 multicast ip pimsm register checksum

[機能]

PIM-SM(IPv4) の Register パケットの送信時のチェックサムの計算方法

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

multicast ip pimsm register checksum <checksum>

[オプション]

<checksum>

PIM-SM(IPv4) の Register パケットの送信時のチェックサムの計算方法を以下で指定します。

- header
  ヘッダ部だけで計算する
- full
  パケット全体で計算する

[動作モード]

構成定義モード (管理者クラス)

[説明]

PIM-SM(IPv4) の Register パケットの送信時のチェックサムの計算方法を設定します。

[注意]

PIM Register パケットは、RFC2362 ではヘッダ部だけで計算するように定義されていますが、一部のルータはパケット全体で計算します。このようなルータが RP を行う場合は、PIM Register パケットが受信されない可能性があるため、チェックサムの計算範囲を「パケット全体」に変更する必要があります。
本装置は PIM Register パケットの受信時には、ヘッダ部 (RC2362 準拠) とパケット全体の 2 通りの方法で計算するため、本装置が RP を行う場合は、どちらの計算方法のパケットを受信しても問題はありません。

[未設定時]

ヘッダ部だけで計算します。

```
multicast ip pimsm register checksum header
```

14.1.10　multicast ip route

[機能]

IPv4 マルチキャスト・スタティックルーティング情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

multicast ip route <count> <src_address> <group_address> <incoming> <outgoing> [<igmp_mode>]

[オプション]

<count>

- スタティックルーティング定義番号スタティックルーティング定義番号を、0〜19 の 10 進数値で指定します。

<src_address>

- 配送元ホストアドレス
  配送元ホストを IPv4 アドレスで指定します。
  指定可能な範囲は以下のとおりです。

  1.0.0.1 〜 126.255.255.254
  128.0.0.1 〜 191.255.255.254
  192.0.0.1 〜 223.255.255.254

<group_address>

- マルチキャスト・グループアドレス
  マルチキャスト・グループアドレスを以下の範囲の IPv4 アドレスで指定します。

  224.0.1.0 〜 239.255.255.255

<incoming>

- 入力インタフェース
  入力インタフェースとして lan または、rmt インタフェースを指定します。

<outgoing>

- 出力インタフェース
  出力インタフェースとして lan または、rmt インタフェースを指定します。
  複数指定する場合は、","(カンマ) で区切ります。また、範囲指定する場合は、「rmt1-rmt4」のように"-"(ハイフン) を使用して指定します。

最大出力インタフェース数	機種
20	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
5	Si-R180

<igmp_mode>

- IGMP グループ参加
  入力インタフェースでの IGMP グループ参加を指定します。

  off　　グループ参加を行わない
  on　　グループ参加を行う

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv4 マルチキャスト・スタティックルーティング情報を設定します。
入力インタフェースおよび出力インタフェースの指定は以下の範囲で指定します。

範囲	機種
lan0〜lan19 rmt0〜rmt999	Si-R570
lan0〜lan19 rmt0〜rmt499	Si-R370
lan0〜lan19 rmt0〜rmt99	Si-R260B Si-R240 Si-R220B
lan0〜lan9 rmt0〜rmt49	Si-R180

[未設定時]

IPv4 マルチキャスト・スタティックルーティング情報を設定しないものとみなされます。

第 15 章　UPnP 情報の設定

15.1 UPnP 情報

15.1.1 upnp use

[機能]

VoIP NAT トラバーサル機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

upnp use <mode>

[オプション]

<mode>

- off
  VoIP NAT トラバーサル機能を使用しません。
- on
  VoIP NAT トラバーサル機能を使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

VoIP NAT トラバーサル機能を使用するかどうかを設定します。
VoIP NAT トラバーサル機能は、NAT 機能を使用すると通信できない VoIP アダプタを通信できるようにします。ただし、VoIP アダプタが UPnP(Universal Plug and Play) に対応していなければ通信できません。
同様に、UPnP に対応したアプリケーションプログラム (UPnP クライアント) も通信できるようになることがあります。
VoIP アダプタ (UPnP クライアント) および通信相手は、以下に示すインタフェースに接続してください。

- VoIP アダプタ (UPnP クライアント)
  NAT 機能を使用しない lan インタフェースに接続してください。
  ない場合、VoIP NAT トラバーサル機能は動作しません。
- 通信相手
  NAT を使用する定義番号が一番小さい lan インタフェースに接続してください。
  ない場合、NAT を使用する定義番号が一番小さい remote インタフェースに接続してください。
  どれもない場合、VoIP アダプタ (UPnP クライアント) は通信できません。

[注意]

VoIP アダプタ (UPnP クライアント) との通信に、以下のポート番号を使用します。
そのため、これらのポートを IP フィルタリングで遮断しないでください。

プロトコル	ポート番号
UDP TCP	1900 5432

UPnP クライアントは通常の NAT 変換も併用することがあります。NAT の割当時間が短いと通信が切断されることがありますので、NAT の定義で必要十分な割当時間を設定してください。
NAT の定義でグローバル IP アドレスの個数には 1 を指定してください。2 以上を指定すると UPnP が正しく動作しないことがあります。

[未設定時]

VoIP NAT トラバーサル機能を使用しないものとみなされます。

```
upnp use off
```

15.1.2 upnp portmapping lease

[機能]

ポートマッピング有効期限の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

upnp portmapping lease <time>

[オプション]

<time>

- ポートマッピング有効期限

  UPnP クライアントがポートマッピングを無期限で設定しようとしたときに、強制的に設定する有効期限を指定します。

  有効期限は、60 秒 (1 分)〜86400 秒 (1 日) の範囲で、数字と単位をつなげて指定します。

  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

UPnP クライアントがポートマッピングを無期限で設定しようとしたときに、強制的に設定する有効期限を設定します。設定したポートマッピングが使用されなくなってから有効期限を過ぎたとき、そのポートマッピングを強制的に削除します。
本設定がなく、UPnP クライアントがポートマッピングを無期限で登録した場合、UPnP クライアントがポートマッピングを削除するまでポートマッピングが設定されたままになります。

[注意]

本設定によってポートマッピングが強制的に削除された場合、そのポートマッピングを設定した UPnP クライアントが通信できなくなります。その場合、その UPnP クライアントを再起動してください。

[未設定時]

ポートマッピング有効期限を設定しないものとみなされ、ポートマッピングを強制的に削除しません。

第 16 章　ACL 情報の設定

- ACL 定義番号の指定範囲本章のコマンド の [オプション] に記載されている<acl_count>(ACL 定義番号) に指定する ACL 定義の通し番号 (10 進数値) は、機種ごとに以下に示す範囲で指定してください。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B　Si-R240　Si-R220B
0〜149	Si-R180

16.1 ACL 情報

16.1.1 acl mac

[機能]

ACL MAC 定義

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

acl <acl_count> mac <src_mac> <dst_mac> llc <value> [<vlan_analyze>]
acl <acl_count> mac <src_mac> <dst_mac> snap <value> [<vlan_analyze>]
acl <acl_count> mac <src_mac> <dst_mac> ether <value> [<vlan_analyze>]
acl <acl_count> mac <src_mac> <dst_mac> any

[オプション]

<acl_count>

- ACL 定義番号
  ACL 定義の通し番号を、10 進数値で指定します。

<src_mac>

ACL 対象とする送信元 MAC アドレスを指定します。

- any
  すべての MAC アドレスを対象とする場合に指定します。
- bcast
  ブロードキャスト MAC アドレスを対象とする場合に指定します。
- mcast
  マルチキャスト MAC アドレスを対象とする場合に指定します。
- 上記以外
  対象とする MAC アドレスを指定します。ACL 対象とする送信元 MAC アドレスを、xx:xx:xx:xx:xx:xx(xx は 2 桁の 16 進数値) の形式で指定します。

<dst_mac>

ACL 対象とするあて先 MAC アドレスを指定します。

- any
  すべての MAC アドレスを対象とする場合に指定します。
- bcast
  ブロードキャスト MAC アドレスを対象とする場合に指定します。
- mcast
  マルチキャスト MAC アドレスを対象とする場合に指定します。
- 上記以外
  対象とする MAC アドレスを指定します。ACL 対象とする送信元 MAC アドレスを、xx:xx:xx:xx:xx:xx(xx は 2 桁の 16 進数値) の形式で指定します。

llc <value>

<value>の値と LSAP が一致する LLC 形式フレームを対象とする場合に指定します。<value>には、0～ffff の 16 進数値を指定します。
すべての LLC 形式フレームを対象とする場合は<value>に any を指定します。

snap <value>

<value>の値とタイプフィールドが一致する SNAP 形式フレームを対象とする場合に指定します。<value>には、0～ffff の 16 進数値を指定します。
すべての SNAP 形式フレームを対象とする場合は<value>に any を指定します。

ether <value>

<value>の値とタイプフィールドが一致する Ethernet 形式フレームを対象とする場合に指定します。<value>には、5dd～ffff の 16 進数値を指定します。
すべての Ethernet 形式フレームを対象とする場合は<value>に any を指定します。

any

すべてのフレームを対象とする場合に指定します。

<vlan_analyze>

VLAN タグ付きフレームに対してタグの解析を行うかどうかを指定します。
省略時は、off を指定したものとみなされます。

- on

  VLAN タグ付きフレームの場合に VLAN タグを解析してフィルタリング処理を行います。VLAN タグ付きフレームの場合は、タグの長さ分ずれた位置にある LLC 形式フレームの LSAP や Ethernet 形式フレームのタイプに対してフィルタリング処理を行います。

- off

  VLAN タグ付きフレームの場合に VLAN タグを解析しないでフィルタリング処理を行います。VLAN タグ付きフレームの場合でもタグの長さ分ずらさずにそのままフィルタリング処理を行うため、VLAN タグの TPID が、<value>との比較対象になります。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ACL 定義で etherframe パターンを指定します。

[未設定時]

ACL 定義でどのような etherframe パターンでも対象とします。

16.1.2 acl ip

[機能]

ACL IPv4 定義

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

acl <acl_count> ip <src_addr>/<mask> <dst_addr>/<mask> [<protocol> [any]]
acl <acl_count> ip <src_addr>/<mask> <dst_addr>/<mask> [<protocol> [tos <value>]]
acl <acl_count> ip <src_addr>/<mask> <dst_addr>/<mask> [<protocol> [dscp <value>]]

[オプション]

<acl_count>

- ACL 定義番号
  ACL 定義の通し番号を、10 進数値で指定します。

<src_addr>/<mask>

ACL 対象とする送信元 IP アドレスとマスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  ACL 対象とする送信元 IP アドレスとマスクビット数の組み合わせを指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。
  以下に、有効な記述形式を示します。
  - IP アドレス/マスクビット数 (例: 192.168.1.1/24)
- any
  すべての送信元 IP アドレスを ACL 対象とする場合に指定します。
  0.0.0.0/0 を指定するのと同じ意味になります。

<dst_addr>/<mask>

ACL 対象とするあて先 IP アドレスとマスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  ACL 対象とするあて先 IP アドレスとマスクビット数の組み合わせを指定します。
  記述形式は、<src_addr>/<mask>と同様です。
- any
  すべてのあて先 IP アドレスを ACL 対象とする場合に指定します。
  0.0.0.0/0 を指定するのと同じ意味になります。

<protocol>

ACL 対象とするプロトコル番号を指定します。

- プロトコル番号
  ACL 対象とするプロトコル番号を、1～255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号を ACL 対象とする場合に指定します。

省略時は、any を指定したものとみなされます。

<type>

ACL 対象とする QoS の判断する方法を指定します。

- tos
  TOS 値で ACL 対象を判断する場合に指定します。
- dscp
  DSCP 値で ACL 対象を判断する場合に指定します。
- any
  すべての TOS 値、すべての DSCP 値を ACL 対象とする場合に指定します。

省略時は、any を指定したものとみなされます。

<value>

ACL 対象とする TOS 値、または DSCP 値を指定します。

- TOS 値
  ACL 対象とする TOS 値を、0〜ff の 16 進数値で指定します。
  複数の TOS 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。
  TOS 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 00〜ff の 16 進数値 (例: ff = ff の TOS 値)
  - TOS 値-TOS 値 (例: 32-64 = 32 から 64 までの TOS 値)
  - TOS 値- (例: 80- = 80 から ff までの TOS 値)
  - -TOS 値 (例: -7f = 0 から 7f までの TOS 値)
  - TOS 値,TOS 値,… (例: 10,20,30- = 10 と 20 と 30 以降の TOS 値)
- DSCP 値
  ACL 対象とする DSCP 値を、0〜63 の 10 進数値で指定します。
  複数の DSCP 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-63」のように"-"(ハイフン) を使用して指定します。
  DSCP 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 0〜63 の 10 進数値 (例: 63 = 63 の DSCP 値)
  - DSCP 値-DSCP 値 (例: 32-47 = 32 から 47 までの DSCP 値)
  - DSCP 値- (例: 32- = 32 から 63 までの DSCP 値)
  - -DSCP 値 (例: -31 = 0 から 31 までの DSCP 値)
  - DSCP 値,DSCP 値,… (例: 10,20,30- = 10 と 20 と 30 以降の DSCP 値)

[動作モード]

構成定義モード (管理者クラス)

[説明]

ACL 定義で IPv4 パケットのパターンを指定します。

[注意]

TCP,UDP,ICMP などの L3 プロトコル利用時には必ず acl ip を定義してください。

[未設定時]

ACL 定義でどのような IPv4 パケットのパターンでも対象とします。
(all any 設定時、未定義では acl 定義は存在しません)

16.1.3　acl ip6

[機能]

ACL IPv6 定義

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

acl <acl_count> ip6 <src_addr>/<prefixlen> <dst_addr>/<prefixlen> [<protocol> [any]]
acl <acl_count> ip6 <src_addr>/<prefixlen> <dst_addr>/<prefixlen> [<protocol> [tc <value>]]
acl <acl_count> ip6 <src_addr>/<prefixlen> <dst_addr>/<prefixlen> [<protocol> [dscp <value>]]

[オプション]

<acl_count>

- ACL 定義番号
  ACL 定義の通し番号を、10 進数値で指定します。

<src_addr>/<prefixlen>

フィルタリング対象とする送信元 IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長
  フィルタリング対象とする送信元 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- any
  すべての送信元 IPv6 アドレスをフィルタリング対象とする場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<dst_addr>/<prefixlen>

フィルタリング対象とするあて先 IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長
  フィルタリング対象とするあて先 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- any
  すべてのあて先 IPv6 アドレスをフィルタリング対象とする場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<protocol>

ACL 対象とするプロトコル番号を指定します。

- プロトコル番号
  ACL 対象とするプロトコル番号を、1〜255 の 10 進数値で指定します (例: ICMPv6:58、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号を ACL 対象とする場合に指定します。

省略時は、any を指定したものとみなされます。

<type>

ACL 対象とする QoS の判断する方法を指定します。

- tc

  Traffic Class 値で ACL 対象を判断する場合に指定します。

- dscp

  DSCP 値で ACL 対象を判断する場合に指定します。

- any

  すべての TOS 値、すべての DSCP 値を ACL 対象とする場合に指定します。

省略時は、any を指定したものとみなされます。

<value>

ACL 対象とする Traffic Class 値、または DSCP 値を指定します。

- ACL 対象 Traffic Class 値

  ACL 対象となる Traffic Class フィールドの値を 0-ff までの 16 進数値、または、"-"を使用して表現される 16 進数値の範囲を指定します。

  Traffic Class 値の指定は、"," を区切として 10 個まで設定可能です。

  複数の Traffic Class 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。

  Traffic Class 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。

  以下に、有効な記述形式を示します。

  - 00～ff の 16 進数値 (例: ff = ff の Traffic Class 値)
  - Traffic Class 値-Traffic Class 値 (例: 32-64 = 32 から 64 までの Traffic Class 値)
  - Traffic Class 値- (例: 80- = 80 から ff までの Traffic Class 値)
  - -Traffic Class 値 (例: -7f = 0 から 7f までの Traffic Class 値)
  - Traffic Class 値,Traffic Class 値,… (例: 10,20,30- = 10 と 20 と 30 以降の Traffic Class 値)

- DSCP 値

  ACL 対象とする DSCP 値を、0～63 の 10 進数値で指定します。

  複数の DSCP 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-63」のように"-"(ハイフン) を使用して指定します。

  DSCP 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。

  以下に、有効な記述形式を示します。

  - 0～63 の 10 進数値 (例: 63 = 63 の DSCP 値)
  - DSCP 値-DSCP 値 (例: 32-47 = 32 から 47 までの DSCP 値)
  - DSCP 値- (例: 32- = 32 から 63 までの DSCP 値)
  - -DSCP 値 (例: -31 = 0 から 31 までの DSCP 値)
  - DSCP 値,DSCP 値,… (例: 10,20,30- = 10 と 20 と 30 以降の DSCP 値)

[動作モード]

構成定義モード (管理者クラス)

[説明]

ACL 定義で IPv6 パケットのパターンを指定します。

[注意]

TCP,UDP,ICMP などの L3 プロトコル利用時には必ず acl ip6 を定義してください。

[未設定時]

ACL 定義でどのような IPv6 パケットのパターンでも対象とします。
(all any 設定時、未定義では acl 定義は存在しません)

16.1.4 acl tcp

[機能]

ACL TCP 定義

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

acl <acl_count> tcp <src_port> <dst_port> <tcpconnect>

[オプション]

<acl_count>

- ACL 定義番号
  ACL 定義の通し番号を、10 進数値で指定します。

<src_port>

ACL 対象とする送信元ポート番号を指定します。

- ポート番号
  ACL 対象とする送信元ポート番号を、1～65535 の 10 進数値で指定します。
  複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。
  ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 1～65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)
- any
  すべての送信元ポート番号を ACL 対象とする場合に指定します。

<dst_port>

ACL 対象とするあて先ポート番号を指定します。

- ポート番号
  ACL 対象とするあて先ポート番号を、1～65535 の 10 進数値で指定します。
  記述形式は、<src_port>と同様です。
- any
  すべてのあて先ポート番号を ACL 対象とする場合に指定します。

<tcpconnect>

- yes
  TCP プロトコルでコネクション接続要求を ACL 対象に含めます。
- no
  TCP プロトコルでコネクション接続要求を ACL 対象に含めません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ACL 定義で TCP パケットのパターンを指定します。

[注意]

利用時には必ず acl ip/ip6 にて protocol(tcp 6) を指定してください。

[未設定時]

ACL 定義でどのような TCP パケットのパターンでも対象とします。

16.1.5 acl udp

[機能]

ACL UDP 定義

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

acl <acl_count> udp <src_port> <dst_port>

[オプション]

<acl_count>

- ACL 定義番号
  ACL 定義の通し番号を、10 進数値で指定します。

<src_port>

ACL 対象とする送信元ポート番号を指定します。

- ポート番号
  ACL 対象とする送信元ポート番号を、1〜65535 の 10 進数値で指定します。
  複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、
  <dst_port>合わせて 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)
- any
  すべての送信元ポート番号を ACL 対象とする場合に指定します。

<dst_port>

ACL 対象とするあて先ポート番号を指定します。

- ポート番号
  ACL 対象とするあて先ポート番号を、1〜65535 の 10 進数値で指定します。
  記述形式は、<src_port>と同様です。
- any
  すべてのあて先ポート番号を ACL 対象とする場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ACL 定義で UDP パケットのパターンを指定します。

[注意]

利用時には必ず acl ip/ip6 にて protocol(udp 17) を指定してください。

[未設定時]

ACL 定義でどのような UDP パケットのパターンでも対象とします。

16.1.6 acl icmp

[機能]

ACL ICMP 定義

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

acl <acl_count> icmp <icmptype> <icmpcode>

[オプション]

<acl_count>

- ACL 定義番号
  ACL 定義の通し番号を、10 進数値で指定します。

<icmptype>

ACL 対象とする ICMP TYPE を指定します。

- ICMP TYPE
  ACL 対象とする送信元 ICMP TYPE を、0～255 の 10 進数値で指定します。
  複数の ICMP TYPE を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「8-30」のように"-"(ハイフン) を使用して指定します。ICMP TYPE は、","(カンマ) および"-"(ハイフン) を使用して、10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 0～255 の 10 進数値 (例: 8 = ICMP TYPE 8)
  - ICMP TYPE-ICMP TYPE (例: 2-8 = 2 から 8 までの ICMP TYPE)
  - ICMP TYPE- (例: 8- = 8 から 255 までの ICMP TYPE)
  - -ICMP TYPE (例: -200 = 0 から 200 までの ICMP TYPE)
  - ICMP TYPE,ICMP TYPE,… (例: 0,8,30- = 0 と 8 と 30 以降の ICMP TYPE)
- any
  すべての ICMP TYPE を ACL 対象とする場合に指定します。

<icmpcode>

ACL 対象とする ICMP CODE を指定します。

- ICMP CODE
  ACL 対象とする送信元 ICMP CODE を、0～255 の 10 進数値で指定します。
  複数の ICMP CODE を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「8-30」のように"-"(ハイフン) を使用して指定します。
  ICMP CODE は、","(カンマ) および"-"(ハイフン) を使用して、10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 0～255 の 10 進数値 (例: 8 = ICMP CODE 8)
  - ICMP CODE-ICMP CODE (例: 2-8 = 2 から 8 までの ICMP CODE)
  - ICMP CODE- (例: 8- = 8 から 255 までの ICMP CODE)
  - -ICMP CODE (例: -200 = 0 から 200 までの ICMP CODE)
  - ICMP CODE,ICMP CODE,… (例: 0,8,30- = 0 と 8 と 30 以降の ICMP CODE)
- any
  すべての ICMP CODE を ACL 対象とする場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ACL 定義で ICMP パケットのパターンを指定します。

[注意]

利用時には必ず acl ip/ip6 にて<protocol>(icmp 1) を指定してください。

[未設定時]

ACL 定義でどのような ICMP パケットのパターンでも対象とします。

16.1.7 acl description

[機能]

ACL description 定義

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

acl <acl_count> description <description>

[オプション]

<acl_count>

- ACL 定義番号
  ACL 定義の通し番号を、10 進数値で指定します。

<description>

- 設定の説明
  この ACL 定義番号で設定の説明を、0x20, 0x21,0x23～0x7e の 50 文字以内の ASCII 文字列で記入します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

この ACL 定義番号で設定の説明を記入します。

[未設定時]

設定の説明を記入しないものとみなされます。

第 17 章　ポリシーグループ定義情報の設定

- policy-group 定義番号の指定範囲

  本章のコマンド の [オプション] に記載されている<policy-group_number>(policy-group 定義番号) に指定する policy-group 定義の通し番号 (10 進数値) は、機種ごとに以下に示す範囲で指定してください。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B　Si-R220B
0〜49	Si-R180

17.1 ポリシーグループ定義情報

17.1.1 policy-group pattern

[機能]

ポリシールール一致パターンの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

policy-group <policy-group_number> pattern <pattern_number> <action> acl <acl_number>

[オプション]

<policy-group_number>

- ポリシーグループ番号
  ポリシーグループの通し番号を、10 進数値で指定します。

<pattern_number>

- パターン番号
  同一グループ内のポリシーパターンの通し番号を、10 進数値で指定します。
  ほかの ACL 参照定義 (IP フィルタ、帯域制御 (WFQ) など) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B Si-R240 Si-R220B
450	Si-R180

<action>

動作
acl 定義に一致した場合の動作を指定します。

- match
  acl 定義に一致した場合、このポリシーグループのポリシーに従います。
- unmatch
  acl 定義に一致した場合、このポリシーグループのポリシーに従いません。
- backup
  以降の policy-group 定義に一致しなかった場合に、このポリシーグループのポリシーに従います。

<acl_number>

- 参照 ACL 番号
  ポリシーとして参照する ACL 定義の定義番号を指定します。
  指定した<acl_count>の ACL が定義されていない場合、その定義は無効となり、無視されます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B　Si-R240　Si-R220B
0〜149	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

ポリシーグループのルールを ACL を利用して指定します。

[注意]

参照すべき ACL 定義が未定義の場合、該当するポリシー定義は無効となりますが、定義あり状態となります。

[未設定時]

ポリシーグループ定義は無効とみなされます。

17.1.2 policy-group pattern move

[機能]

ポリシールール一致パターン優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

policy-group <policy-group_number> pattern move <count> <new_count>

[オプション]

<policy-group_number>

- ポリシーグループ番号
  ポリシーグループの通し番号を、10 進数値で指定します。

<count>

- 対象ポリシーグループパターン定義番号
  優先順序を変更するポリシーグループパターン定義の番号を指定します。

<new_count>

- 移動先ポリシーグループパターン定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

Ingress ポリシールーティングの優先順序を変更します。

17.1.3　policy-group interface

[機能]

送出先インタフェースの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

policy-group <policy-group_number> interface <interface_name>

[オプション]

<policy-group_number>

- ポリシーグループ番号
  ポリシーグループの通し番号を、10 進数値で指定します。

<interface_name>

- 送出先インタフェース名
  送出先インタフェースを以下のように指定します。
  - rmt<remote_number>
    相手定義番号
  - lan<lan_number>
    LAN 定義番号

[動作モード]

構成定義モード (管理者クラス)

[説明]

通常経路によらないポリシーグループ送出先を設定します。

[注意]

送出先インタフェースに lan を指定した場合、nexthop/nexthop6 の指定を行わないとそのアドレスファミリでの定義が無効となり、無視されます。

[未設定時]

ポリシーグループ定義は無効とみなされます。

17.1.4 policy-group nexthop

[機能]

送出先 IPv4 ルータの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

policy-group <policy-group_number> nexthop <address>

[オプション]

<policy-group_number>

- ポリシーグループ番号
  ポリシーグループの通し番号を、10 進数値で指定します。

<address>

- 送出先となる IPv4 ルータの IP アドレスを指定します。
  以下の範囲で指定してください。
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[動作モード]

構成定義モード (管理者クラス)

[説明]

通常経路によらないポリシーグループ送出先の IPv4 ルータの IP アドレスを設定します。
送出先インタフェースに lan を指定した場合、IPv4 でポリシールーティングを行う場合は必ず指定する必要があります。

[注意]

送出先インタフェースに rmt を設定した場合は無視されます。

[未設定時]

送出先インタフェースに lan を指定した場合、IPv4 ルータを設定しないものとみなされ、IPv4 定義が無効となります。

17.1.5　policy-group nexthop6

[機能]

送出先 IPv6 ルータの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

policy-group <policy-group_number> nexthop6 <address>

[オプション]

<policy-group_number>

- ポリシーグループ番号
  ポリシーグループの通し番号を、10 進数値で指定します。

<address>

- 転送先となる IPv6 ルータの IPv6 アドレスを指定します。
  以下の範囲で指定してください。
  ::2 ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

[動作モード]

構成定義モード (管理者クラス)

[説明]

通常経路によらないポリシーグループ送出先 IPv6 ルータの IPv6 アドレスを設定します。
送出先インタフェースに lan を指定した場合、IPv6 でポリシールーティングを行う場合は必ず指定する必要があります。

[注意]

送出先インタフェースに rmt を設定した場合は無視されます。

[未設定時]

送出先インタフェースに lan を指定した場合、IPv6 ルータを設定しないものとみなされ、IPv6 定義が無効となります。

17.1.6 policy-group sessionwatch address

[機能]

接続先監視のアドレス設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

policy-group <policy-group_number> sessionwatch address <source> <destination>

[オプション]

<policy-group_number>

- ポリシーグループ番号
  ポリシーグループの通し番号を、10 進数値で指定します。

<source>

- ICMP ECHO パケットの送信元 IP アドレス
  ICMP ECHO パケットの送信元 IP アドレスを指定します。装置に設定されている自側 IPv4/IPv6 アドレスのどれかを指定してください。
  指定可能な範囲は以下のとおりです。

  IPv4: 1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  IPv6: ::2 ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<destination>

- ICMP ECHO パケットのあて先 IP アドレス
  監視対象となる IPv4/IPv6 アドレスを指定します。
  <source>と同じプロトコルアドレスで指定してください。
  指定可能な範囲は以下のとおりです。

  IPv4: 1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  IPv6: ::2 ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

[動作モード]

構成定義モード (管理者クラス)

[説明]

接続先の生存確認を行うための動作情報を設定します。
指定したあて先 IP アドレスに対して ICMP ECHO パケットの送受信で生存確認を行います。

[注意]

以下の場合は、監視を行いません。

- policy-group pattern 定義がない場合。
- policy-group interface 定義がない場合。
- policy-group sessionwatch address 定義がない場合。
- policy-group interface 定義に lan を指定し、policy-group sessionwatch address 定義に IPv4 アドレスを指定した時、policy-group nexthop 定義がない場合。
- policy-group interface 定義に lan を指定し、policy-group sessionwatch address 定義に IPv6 アドレスを指定した時、policy-group nexthop6 定義がない場合。
- ISDN 回線を利用する接続先で、常時接続機能を利用していない場合。
- PPPoE 回線を利用する接続先で、常時接続機能を利用していない場合。

[未設定時]

接続先監視機能を利用しないものとみなされます。

17.1.7 policy-group sessionwatch interval

[機能]

接続先監視の各種インターバル設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

policy-group <policy-group_number> sessionwatch interval <normal> <error> <timeout> [<retry>]

[オプション]

<policy-group_number>

- ポリシーグループ番号
  ポリシーグループの通し番号を、10 進数値で指定します。

<normal>

- ICMP ECHO パケットの正常時送信間隔
  ICMP ECHO パケットの正常時送信間隔を、1 秒～60 秒 (1 分) の範囲で指定します。
  単位は、m(分)、s(秒) のどちらかを指定します。

<error>

- ICMP ECHO パケットの異常時送信間隔
  ICMP ECHO パケットの異常時送信間隔を、60 秒～600 秒 (10 分) の範囲で指定します。
  単位は、m(分)、s(秒) のどちらかを指定します。

<timeout>

- 監視タイムアウト
  監視失敗とみなすまでのタイムアウト時間を、5 秒～180 秒 (3 分) の範囲で指定します。
  単位は、m(分)、s(秒) のどちらかを指定します。

<retry>

- ICMP ECHO パケットの再送間隔
  ICMP ECHO パケットの正常時送信に対して応答がない時の ICMP ECHO パケットの再送間隔を、1 秒～<timeout>-1 秒の範囲で指定します。
  単位は、m(分)、s(秒) のどちらかを指定します。
  省略時は、1s が指定されたものとして動作します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

接続先の生存確認を行うための動作情報を設定します。
指定したあて先 IP アドレスに対して ICMP ECHO パケットの送受信で生存確認を行います。
ICMP ECHO パケットの応答が正常に受信できている間は正常時送信間隔で監視を行いますが、ICMP ECHO パケットの応答が受信できなくなると、障害発生とみなし、異常時送信間隔で監視を行います。
ICMP ECHO パケットの応答が受信できた時を復旧とみなし、正常送信間隔での監視に戻ります。

[注意]

以下の場合は、監視を行いません。

- policy-group pattern 定義がない場合。
- policy-group interface 定義がない場合。
- policy-group sessionwatch address 定義がない場合。
- policy-group interface 定義に lan を指定し、policy-group sessionwatch address 定義に IPv4 アドレスを指定した時、policy-group nexthop 定義がない場合。
- policy-group interface 定義に lan を指定し、policy-group sessionwatch address 定義に IPv6 アドレスを指定した時、policy-group nexthop6 定義がない場合。
- ISDN 回線を利用する接続先で、常時接続機能を利用していない場合。
- PPPoE 回線を利用する接続先で、常時接続機能を利用していない場合。

[未設定時]

```
policy-group <policy-group_number> sessionwatch interval 10s 1m 5s 1s
```

17.1.8 policy-group sessionwatch ttl

[機能]

接続先監視の TTL/HopLimit 値設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

policy-group <policy-group_number> sessionwatch ttl <send_ttl>

[オプション]

<policy-group_number>

- ポリシーグループ番号
  ポリシーグループの通し番号を、10 進数値で指定します。

<send_ttl>

- 送信 TTL / HopLimit 値
  ICMP ECHO パケットを送信する時の IPv4 TTL/IPv6 HopLimit 値を、1〜255 の範囲で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

接続先の生存確認を行うための動作情報を設定します。
ICMP ECHO パケットの TTL/HopLimit 値を指定された値で送信します。

[注意]

以下の場合は、監視を行いません。

- policy-group pattern 定義がない場合。
- policy-group interface 定義がない場合。
- policy-group sessionwatch address 定義がない場合。
- policy-group interface 定義に lan を指定し、policy-group sessionwatch address 定義に IPv4 アドレスを指定した時、policy-group nexthop 定義がない場合。
- policy-group interface 定義に lan を指定し、policy-group sessionwatch address 定義に IPv6 アドレスを指定した時、policy-group nexthop6 定義がない場合。
- ISDN 回線を利用する接続先で、常時接続機能を利用していない場合。
- PPPoE 回線を利用する接続先で、常時接続機能を利用していない場合。

[未設定時]

```
policy-group <policy-group_number> sessionwatch ttl 255
```

17.1.9　policy-group sessionwatch recovery

[機能]

接続先監視の復旧タイミング設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

policy-group <policy-group_number> sessionwatch recovery <count>

[オプション]

<policy-group_number>

- ポリシーグループ番号
  ポリシーグループの通し番号を、10 進数値で指定します。

<count>

- 応答受信回数
  異常状態から正常状態へ復旧するまでの連続応答受信回数を 1～100 の範囲で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

接続先の生存確認を行うための動作情報を設定します。
異常状態から正常状態へ復旧するために必要な連続応答受信回数を設定します。これにより、回線状態が不安定な場合のダウン／アップのばたつきを防ぎます。
連続応答待ち状態での ICMP ECHO パケット送信間隔は、正常時送信間隔を使用します。
本装置起動後を含め、回線接続直後に通信可能な状態であっても、必要な回数の応答を受信するまで通信可能とはなりませんので、ご注意ください。

[注意]

以下の場合は、監視を行いません。

- policy-group pattern 定義がない場合。
- policy-group interface 定義がない場合。
- policy-group sessionwatch address 定義がない場合。
- policy-group interface 定義に lan を指定し、policy-group sessionwatch address 定義に IPv4 アドレスを指定した時、policy-group nexthop 定義がない場合。
- policy-group interface 定義に lan を指定し、policy-group sessionwatch address 定義に IPv6 アドレスを指定した時、policy-group nexthop6 定義がない場合。
- ISDN 回線を利用する接続先で、常時接続機能を利用していない場合。
- PPPoE 回線を利用する接続先で、常時接続機能を利用していない場合。

[未設定時]

```
policy-group <policy-group_number> sessionwatch recovery 1
```

17.1.10　policy-group sessionwatch error-wait

[機能]

接続先監視の異常時送信開始待ち時間設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

policy-group <policy-group_number> sessionwatch error-wait <time>

[オプション]

<policy-group_number>

- ポリシーグループ番号
  ポリシーグループの通し番号を、10 進数値で指定します。

<time>

- 異常時送信開始待ち時間
  異常時 ICMP ECHO パケットの送信開始待ち時間を、0 秒〜86400 秒 (1 日) の範囲で指定します。0 秒が指定された場合は待ち合わせをしません。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

接続先の生存確認を行うための動作情報を設定します。
正常状態から異常状態に遷移した場合に、最初の ICMP ECHO パケットを送信するまでの待ち時間を設定します。

[注意]

以下の場合は、監視を行いません。

- policy-group pattern 定義がない場合。
- policy-group interface 定義がない場合。
- policy-group sessionwatch address 定義がない場合。
- policy-group interface 定義に lan を指定し、policy-group sessionwatch address 定義に IPv4 アドレスを指定した時、policy-group nexthop 定義がない場合。
- policy-group interface 定義に lan を指定し、policy-group sessionwatch address 定義に IPv6 アドレスを指定した時、policy-group nexthop6 定義がない場合。
- ISDN 回線を利用する接続先で、常時接続機能を利用していない場合。
- PPPoE 回線を利用する接続先で、常時接続機能を利用していない場合。

[未設定時]

```
policy-group sessionwatch error-wait 0s
```

第 18 章　AAA 情報の設定

- グループ ID の指定範囲

  各コマンドの [オプション] に記載されている [<group_id>](グループ ID) に指定するグループの通し番号 (10 進数値) は、機種ごとに以下に示す範囲で指定してください。

範囲	機種
0〜9	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B　Si-R180

- AAA ユーザ情報定義番号の指定範囲

  各コマンドの [オプション] に記載されている [<number>](AAA ユーザ情報定義番号) に指定するグループ内の通し番号 (10 進数値) は、機種ごとに以下に示す範囲で指定してください。

範囲	機種
0〜1999	Si-R570　Si-R370
0〜999	Si-R260B　Si-R240　Si-R220B
0〜199	Si-R180

18.1　グループ ID 情報

18.1.1　aaa name

[機能]

グループ名称の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] name <group_name>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略時は、0 を指定したものとみなされます。

<group_name>

- グループ名
  グループ名を、0x21,0x23～0x7e の 32 文字以内の ASCII 文字列で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

グループ名を設定します。

[注意]

すでに同一名称のグループが登録されている場合は、異常終了します。

[未設定時]

グループ名を設定しないものとみなされます。

18.2 AAA ユーザ情報

18.2.1 aaa user id

[機能]

認証情報の設定 (ユーザ ID)

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] user [<number>] id <id>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略時は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
  グループ内での通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<id>

- ユーザ ID
  ユーザ ID を、0x21,0x23〜0x7e の文字で構成される 64 文字以内の文字列を指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

認証プロトコルに使用する、認証情報 (ユーザ ID) を設定します。
IPsec で利用する場合は、着信相手を識別するために以下のように指定します。

- ユーザ ID とユーザ認証パスワードを同じに設定してください。
- ユーザ ID とユーザ認証パスワードは、テンプレート情報の IKE 情報の交換モードにより以下のように設定します。

  Main Mode の場合：
  相手側 IPsec トンネルアドレス

  Aggressive Mode の場合：
  相手側の装置識別情報

MAC アドレス認証で利用する場合は、アクセスを許可する端末の MAC アドレスをユーザ ID と認証パスワードに 16 進数 12 桁 (コロンで区切らない) で指定してください。

[未設定時]

認証情報 (ユーザ ID) を設定しないものとみなされます。

18.2.2　aaa user password

[機能]

認証情報の設定 (パスワード)

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] user [<number>] password <password> [encrypted]

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略時は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
  グループ内での通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<password>

- 認証パスワード
  認証パスワードを、0x21,0x23〜0x7e の文字で構成される 64 文字以内の文字列を指定します。
  show コマンドで表示される暗号化された認証パスワードを encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化認証パスワード指定
  <password>に暗号化された認証パスワードを設定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

認証プロトコルに使用する、認証情報 (認証パスワード) を設定します。
IPsec で利用する場合は、着信相手を識別するために以下のように指定します。

- ユーザ ID とユーザ認証パスワードを同じに設定してください。
- ユーザ ID とユーザ認証パスワードは、テンプレート情報の IKE 情報の交換モードにより以下のように設定します。

  Main Mode の場合：
  相手側 IPsec トンネルアドレス

  Aggressive Mode の場合：
  相手側の装置識別情報

MAC アドレス認証で利用する場合は、アクセスを許可する端末の MAC アドレスをユーザ ID と認証パスワードに 16 進数 12 桁 (コロンで区切らない) で指定してください。

[注意]

show コマンドでは、暗号化された認証パスワードが encrypted と共に表示されます。

[未設定時]

認証情報 (パスワード) を設定しないものとみなされます。

18.2.3　aaa user called number

[機能]

CLID の設定

[適用機種]

Si-R 570	Si-R 370		Si-R 240	Si-R 220B	

[入力形式]

aaa [<group_id>] user [<number>] called number <called_number> [<subaddress>]

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略時は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
  グループ内での通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<called_number>

- 相手電話番号
  相手の電話番号を、0～9 の数字と、*、#、-、(、)、\ の文字で構成される 32 桁以内の ASCII 文字列で指定します。

<subaddress>

- 相手サブアドレス
  相手のサブアドレスを、0x21,0x23～0x7e の文字で構成される 19 桁以内の ASCII 文字列で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

CLID 相手判定で、チェックする番号を設定します。

[注意]

Si-R370 Si-R220B は PIAFS 接続に対応しています。PIAFS(64Kbps) 着信時には、<subaddress> で設定した相手サブアドレスは無視されますので、設定しないでください。

[未設定時]

CLID 相手判定を行わないものとみなします。

18.2.4 aaa user ip address local

[機能]

自側 IP アドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] user [<number>] ip address local <address>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略時は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
  グループ内での通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<address>

- 自側 IP アドレス
  自側 IP アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  0.0.0.0
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.25

  0.0.0.0 を指定した場合は、設定を削除します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手ネットワークでの自側 IP アドレスを設定します。

[未設定時]

IP アドレスなし (unnumbered) として動作します。

18.2.5　aaa user ip address remote

[機能]

相手側 IP アドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] user [<number>] ip address remote <address>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略時は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
  グループ内での通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<address>

- 相手側 IP アドレス
  相手側 IP アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  0.0.0.0
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  0.0.0.0 を指定した場合は、設定を IP アドレスなし (unnumbered) として動作します。
- depend-template
  テンプレート定義による設定を適用する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

相手ネットワークでの相手側 IP アドレスを設定します。

[未設定時]

テンプレート定義による設定を適用します。

18.2.6 aaa user ip route

[機能]

IPv4 スタティック経路情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] user [<number>] ip route <count> <address>/<mask> <metric> <distance>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略時は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
  グループ内での通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- スタティック経路情報定義番号
  スタティック経路情報定義番号を、10 進数値で指定します。

範囲	機種
0〜1999	Si-R570
0〜1249	Si-R370
0〜255	Si-R260B Si-R240 Si-R220B
0〜127	Si-R180

<address>/<mask>

- IPv4 アドレス/マスクビット数 (またはマスク値)
  あて先ネットワークを IPv4 アドレスとマスクビット数の組み合わせで指定します。
  マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
  - IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
  - IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)
- default
  あて先ネットワークとしてデフォルトルートを設定する場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<metric>

- RIP メトリック値
  このスタティック経路情報を RIP に再配布するときのメトリック値を、1〜15 の 10 進数値で指定します。

<distance>

- 優先度
  このスタティック経路情報の優先度を、1〜254 の 10 進数値で指定します。
  優先度は値が小さい方が高い優先度を示します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv4 スタティック経路 (静的経路) 情報を設定します。
RIP メトリック値は、スタティック経路情報を RIP に再配布するときのメトリック値を設定します。RIP に再配布したときは、設定した RIP メトリック値+1 のメトリック値で RIP テーブルに登録されます。
優先度は、同じあて先への経路情報が複数ある場合、優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。各ダイナミックルーティングプロトコルの優先度については、routemanage ip distance コマンドを参照してください。
優先度の設定値にかかわらず、常にフローティング動作します。
remote インタフェースが通信可能な状態 (リンクアップなど) であれば、スタティック経路情報をルーティングテーブルに追加します。通信不可能な状態 (リンクダウンなど) であれば、ルーティングテーブルから削除します。
複数のスタティック経路情報で ECMP 機能を使用するときは、あて先、RIP メトリック値、優先度がそれぞれ同じとなるようにスタティック経路情報を設定します。また、ECMP 機能を使用する場合は、routemanage ip ecmp mode コマンドで ECMP を使用するように設定します。
ECMP となるスタティック経路情報は、同じあて先への経路情報ごとに装置全体で 4 個まで定義できます。
IPv4 スタティック経路情報は、本装置全体で次の数まで定義できます。

最大定義数	機種
2000	Si-R570
1250	Si-R370
256	Si-R260B　Si-R240　Si-R220B
128	Si-R180

[注意]

同じあて先へのスタティック経路情報を複数設定する場合、以下の点に注意してください。

- 優先度が同じで、RIP メトリック値が違うスタティック経路情報は同時に設定できません。

[未設定時]

IPv4 スタティック経路情報を設定しないものとみなされます。

18.2.7 aaa user ip6 ifid

[機能]

IPv6 インタフェース ID の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] user [<number>] ip6 ifid <interfaceID>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略時は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
  グループ内での通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<interfaceID>

このインタフェースで利用する ID を指定します。

- auto
  本装置が持つ MAC アドレスから、EUI-64 形式の ID を自動生成する場合に指定します。
- インタフェース ID
  このインタフェースで利用する ID を、16 進数値で指定します。4 桁ずつ":"(コロン) で区切ってください。なお、各フィールドの先頭の 0 は省略できます (例: 2a0:c9ff:fe84:759)。
- depend-template
  テンプレート定義による設定を適用する場合に指定します。

通常は auto を指定してください。特定のインタフェース ID を指定する場合は、同一の link 上でホストと衝突しない値を指定してください。

[動作モード]

構成定義モード (管理者クラス)

[説明]

インタフェース ID を設定します。

[未設定時]

テンプレート定義による設定が適用されます。

18.2.8　aaa user ip6 route

[機能]

IPv6 スタティック経路情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] user [<number>] ip6 route <count> <address>/<prefixlen> <metric> <distance>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略時は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
  グループ内での通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- スタティック経路情報定義番号
  スタティック経路情報定義番号を、10 進数値で指定します。

範囲	機種
0〜1999	Si-R570
0〜1249	Si-R370
0〜255	Si-R260B　Si-R240　Si-R220B
0〜127	Si-R180

<address>/<prefixlen>

- IPv6 アドレス/プレフィックス
  あて先ネットワークを IPv6 アドレスとプレフィックスの組み合わせを指定します。
- default
  あて先ネットワークとしてデフォルトルートを設定する場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<metric>

- メトリック値
  このスタティック経路情報を RIPng で広報する場合のメトリック値を、 1〜15 の 10 進数値で指定します。
  RIPng 広報メトリック値は、以下の計算式で決定されます。
  - RIPng 広報メトリック値=出力インタフェースの設定メトリック値+1+<metric>

<distance>

- 優先度
  このスタティック経路情報の優先度を、1〜254 の 10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPv6 スタティック経路 (静的経路) 情報を設定します。
RIP メトリック値は、スタティック経路情報を RIP に再配布するときのメトリック値を設定します。RIP に再配布したときは、設定した RIP メトリック値+1 のメトリック値で RIP テーブルに登録されます。
優先度は、同じあて先への経路情報が複数ある場合、優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。各ダイナミックルーティングプロトコルの優先度については、routemanage ip6 distance コマンドを参照してください。
優先度の設定値にかかわらず、常にフローティング動作します。
remote インタフェースが通信可能な状態 (リンクアップなど) であれば、スタティック経路情報をルーティングテーブルに追加します。通信不可能な状態 (リンクダウンなど) であれば、ルーティングテーブルから削除します。
IPv6 スタティック経路情報は、本装置全体で次の数まで定義できます。

最大定義数	機種
2000	Si-R570
1250	Si-R370
256	Si-R260B Si-R240 Si-R220B
128	Si-R180

[注意]

同じあて先へのスタティック経路情報を複数設定する場合、以下の点に注意してください。

- 優先度が同じスタティック経路情報は同時に設定できません。

[未設定時]

IPv6 スタティック経路情報を設定しないものとみなされます。

18.2.9　aaa user sessionwatch

[機能]

接続先監視アドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] user [<number>] sessionwatch <destination>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略時は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
  グループ内での通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<destination>

- ICMP ECHO パケットのあて先 IP アドレス
  監視対象となる IPv4/IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  IPv4:　1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  IPv6:　::2 ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

[動作モード]

構成定義モード (管理者クラス)

[説明]

接続先の生存確認を行うための接続先監視アドレスを設定します。
指定したあて先 IP アドレスに対して ICMP ECHO パケットの送受信で生存確認を行います。
ICMP ECHO パケットの送信元 IP アドレスについては以下のアドレスを使用します。

テンプレート情報に設定された接続先監視アドレス

接続先監視のパラメタ、および接続先監視と無通信監視タイマの動作については、template sessionwatch を参照してください。

[注意]

テンプレート情報に接続先監視アドレスの設定がない場合は、監視を行いません。

[未設定時]

接続先監視アドレスを設定しないものとみなされます。

18.2.10 aaa user ipsec ike range

[機能]

自動鍵交換用 IPsec 情報の対象範囲の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] user [<number>] ipsec ike range <src_addr>/<mask> <dst_addr>/<mask>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略時は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
  グループ内での通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<src_addr>/<mask>

IPsec 対象となる送信元 IP アドレス、マスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  IPsec 対象となる送信元 IP アドレスとマスクビット数の組み合わせを指定します。
- any4
  すべての IPv4 アドレスを IPsec 対象に含めます。
  0.0.0.0/0(0.0.0.0/0.0.0.0) と同意。
- any6
  すべての IPv6 アドレスを IPsec 対象に含めます。
  ::/0 と同意。

<dst_addr>/<mask>

IPsec 対象となるあて先 IP アドレス、マスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  IPsec 対象となるあて先 IP アドレスとマスクビット数の組み合わせを指定します。
- any4
  すべての IPv4 アドレスを IPsec 対象に含めます。
  0.0.0.0/0(0.0.0.0/0.0.0.0) と同意。
- any6
  すべての IPv6 アドレスを IPsec 対象に含めます。
  ::/0 と同意。

[動作モード]

構成定義モード (管理者クラス)

[説明]

IPsec を適用するセッションの範囲を設定します。(Security Policy Database の情報)

[未設定時]

<src_addr>,<dst_addr>共に any4 が設定されたものとして扱います。

```
aaa <group_id> user <number> ipsec ike range any4 any4
```

18.2.11 aaa user ipsec extension-range

[機能]

拡張 IPsec 対象範囲の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] user [<number>] ipsec extension-range <count> <src_addr>/<mask> <dst_addr>/<mask>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略時は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
  グループ内での通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<count>

- 拡張 IPsec 対象範囲定義番号
  拡張 IPsec 対象範囲の通し番号を、10 進数値で指定します。
  指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つ拡張 IPsec 対象範囲定義がすでに存在する場合は、既存の定義を変更します。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B Si-R240 Si-R220B
0〜49	Si-R180

<src_addr>/<mask>

IPsec 対象となる送信元 IP アドレス、マスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  IPsec 対象となる送信元 IP アドレスとマスクビット数の組み合わせを指定します。
- any4
  すべての IPv4 アドレスを IPsec 対象に含めます。
  0.0.0.0/0(0.0.0.0/0.0.0.0) と同意。
- any6
  すべての IPv6 アドレスを IPsec 対象に含めます。
  ::/0 と同意。

<dst_addr>/<mask>

IPsec 対象となるあて先 IP アドレス、マスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  IPsec 対象となるあて先 IP アドレスとマスクビット数の組み合わせを指定します。
- any4
  すべての IPv4 アドレスを IPsec 対象に含めます。
  0.0.0.0/0(0.0.0.0/0.0.0.0) と同意。
- any6
  すべての IPv6 アドレスを IPsec 対象に含めます。
  ::/0 と同意。

[動作モード]

構成定義モード (管理者クラス)

[説明]

拡張 IPsec 対象範囲を設定します。
拡張 IPsec 対象範囲定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
1000	Si-R570
500	Si-R370
100	Si-R260B　Si-R240　Si-R220B
50	Si-R180

[注意]

拡張 IPsec 対象範囲設定を行わない場合でも「IPsec 情報の対象範囲の設定」を設定することにより IPsec 通信は可能です。「IPsec 情報の対象範囲の設定」以外の IPsec 対象範囲を指定してください。
拡張 IPsec 対象範囲設定は、IKE ネゴシエーション開始契機になりますが、IKE ネゴシエーション情報としては使用しません。IKE ネゴシエーション情報としての IPsec 対象範囲は「自動鍵交換用 IPsec 情報の対象範囲の設定」をご利用ください。
IPsec の相手となる装置が復号化後に IPsec 対象範囲をチェックする場合は、IPsec 通信が遮断される場合があります。
拡張 IPsec 対象範囲を使用して双方向通信を行う場合は、相手装置側にも同様の設定が必要です。相手装置側に、自側装置と同様の設定が存在しない場合は、片側通信のみ暗号化し折り返しの通信は暗号化されない場合があります。

[未設定時]

拡張 IPsec 対象範囲を設定しないものとみなされます。

18.2.12 aaa user ike shared key

[機能]

IKE セッション確立時の共有鍵 (Pre-shared key) の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] user [<number>] ike shared key <kind> <shared_key> [encrypted]

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略時は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
  グループ内での通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<kind>

鍵種別を指定します。

- hex
  16 進数鍵を使用します。
- text
  文字列鍵を使用します。

<shared_key>

共有鍵 (事前共有秘密鍵方式) を指定します。

- 暗号化されていない共有鍵を指定します。
  文字列鍵の場合は、0x22(ダブルクォーテーション) を除く [0x20-0x7e] の範囲のコードで構成される ASCII 文字列で指定します。ただし、文字列鍵で 0x20(空白文字) を使用する場合は、文字列鍵をダブルクォーテーション (") で囲う必要があります。
  以下に、入力範囲を示します。

鍵種別	16進数鍵	文字列鍵
共有鍵	1～256桁	1～128文字

- 暗号化された共有鍵を指定します。
  show コマンドで表示される暗号化された共有鍵を encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化共有鍵指定
  <shared_key>に暗号化された共有鍵を指定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

SA 確立のネゴシエーションのときに接続相手を認証するための、共有鍵の設定を行います。
show コマンドでは、暗号化された共有鍵が encrypted と共に表示されます。

[未設定時]

共有鍵が設定されません。IKE により鍵交換を行う場合は必ず設定してください。

18.2.13 aaa user supplicant vid

[機能]

ユーザに割り当てる VLAN ID の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] user [<number>] supplicant vid <vid>

[パラメタ]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略時は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
  グループ内での通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<vid>

Supplicant に割り当てる VLAN ID を指定します。
指定可能な範囲は、1〜4094 です。

[動作モード]

構成定義モード (管理者クラス)

[説明]

Supplicant(ユーザ端末) に割り当てる VLAN ID を指定します。

[注意]

本設定で指定した VLAN ID は、RADIUS サーバから送出される Access-Accept 中の
Tunnel-Private-Group-Id アトリビュートで送信されます。また本設定を行った場合は、
Tunnel-Private-Group-Id アトリビュートに加えて、Tunnel-Type アトリビュートが値 13 (VLAN) で、
Tunnel-Medium-Type アトリビュートが値 6 (IEEE802) が同時に送信されます。
未設定の場合は、これらのアトリビュートは送信されません。

[未設定時]

割り当てる VLAN ID が存在しないものとして扱われます。

18.2.14　aaa user supplicant mac

[機能]

Supplicant MAC アドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] user [<number>] supplicant mac <mac>

[パラメタ]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略時は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
  グループ内での通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<mac>

- Supplicant の MAC アドレス
  Supplicant(ユーザ端末) の MAC アドレスを xx:xx:xx:xx:xx:xx(xx は 2 桁の 16 進数値) の形式で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

認証プロトコルで使用する、認証情報 (MAC アドレス) を設定します。

[注意]

本設定を行うと、RADIUS の Calling-Station-Id アトリビュートで送信されたサプリカントの MAC アドレスと本設定が一致しているかをチェックし、AAA ユーザ情報定義で定義したユーザ名とパスワードに加えて、本設定の MAC アドレスが一致している場合にのみ認証が成功するようになります。
Calling-Station-Id アトリビュートを送信しない RADIUS クライアント装置を使用する場合は本設定は行わないでください。常に認証が失敗します。
サプリカントが複数の MAC アドレスを使用する場合は、同じユーザ名とパスワードで別の AAA ユーザ情報定義を定義し、本設定の MAC アドレスを異なる値で設定することで、複数の MAC アドレスで認証することができます。ただし、本設定のない AAA ユーザ情報定義を作成した場合は、Calling-Station-Id アトリビュートの有無や内容によらず認証が成功してしまうため、MAC アドレスを併用した認証を行うことはできません。

[未設定時]

認証情報 (MAC アドレス) を設定しないものとみなされます。

18.3 RADIUS 情報

- RADIUS クライアント定義番号の指定範囲

  各コマンドの [オプション] に記載されている [<number>](RADIUS クライアント定義番号) に指定するグループの通し番号 (10 進数値) は、機種ごとに以下に示す範囲で指定してください。

範囲	機種
0〜3	Si-R570 Si-R370
0	Si-R260B Si-R240 Si-R220B Si-R180

- RADIUS サーバ定義番号の指定範囲

  各コマンドの [オプション] に記載されている [<number>](RADIUS サーバ定義番号) に指定するグループ内の通し番号 (10 進数値) は、機種ごとに以下に示す範囲で指定してください。

範囲	機種
0〜3	Si-R570 Si-R370
0〜1	Si-R260B Si-R240 Si-R220B Si-R180

18.3.1　aaa radius service

[機能]

RADIUS サービスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] radius service <service> [<type>]

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略時は、0 を指定したものとみなされます。

<service>

- server
  RADIUS サーバ機能として使用します。
- client
  RADIUS クライント機能として使用します。
- off
  RADIUS 機能を使用しません。

<type>

<service>に server または client を指定した場合に有効なパラメタです。

- auth
  RADIUS 認証機能を有効にします。
- accounting
  RADIUS アカウンティング機能を有効にします。
- both
  RADIUS 認証機能と RADIUS アカウンティング機能を有効にします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

自装置で使用する RADIUS 機能の設定を行います。

[注意]

同一装置上で RADIUS サーバ機能と RADIUS クライント機能の併用はできません。
また、RADIUS サーバ機能を複数の AAA グループで同時に動作させせることはできません。

[未設定時]

RADIUS 認証機能を使用しないものとみなされます。

```
aaa [<group_id>] radius service off
```

18.3.2　aaa radius auth source

[機能]

RADIUS 認証装置の自側 IP アドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] radius auth source <address>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。

<address>

- 自側 IP アドレス
  自側 RADIUS 認証サーバの IPv4 アドレスまたは IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  IPv4:　1.0.0.1 ～ 126.255.255.2544
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  IPv6:　::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

[動作モード]

構成定義モード (管理者クラス)

[説明]

自側 RADIUS 認証装置の IP アドレスを設定します。
本装置を RADIUS 認証サーバとして使用する場合は、RADIUS 認証クライアントとの通信に使用する自側 IP アドレスを設定します。
本装置を RADIUS 認証クライアントとして使用する場合は、RADIUS 認証サーバとの通信に使用する自側 IP アドレスを設定します。

[未設定時]

相手側の RADIUS 認証装置と通信を行う自側 IP アドレスを自動的に選択するものとみなされます。

18.3.3 aaa radius auth message-authenticator

[機能]

Message-Authenticator の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] radius auth message-authenticator <mode>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。

<mode>

- off
  Message-Authenticator による認証を行いません。
- on
  Message-Authenticator による認証を行います。

[動作モード]

構成定義モード (管理者クラス)

[説明]

Message-Authenticator による認証を行うかどうかを設定します。
本装置では、認証要求メッセージにのみ使用できます。

[未設定時]

Message-Authenticator による認証を行いません。

```
aaa [<group_id>] radius auth message-authenticator off
```

18.3.4　aaa radius accounting source

[機能]

RADIUS アカウンティング装置の自側 IP アドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] radius accounting source <address>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。

<address>

- 自側 IP アドレス
  自側 RADIUS アカウンティング装置の IPv4 アドレスまたは IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  IPv4:　1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  IPv6:　::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

[動作モード]

構成定義モード (管理者クラス)

[説明]

自側 RADIUS アカウンティング装置の IP アドレスを設定します。
本装置を RADIUS アカウンティングサーバとして使用する場合は、RADIUS アカウンティングクライアントとの通信に使用する自側 IP アドレスを設定します。
本装置を RADIUS アカウンティングクライアントとして使用する場合は、RADIUS アカウンティングサーバとの通信に使用する自側 IP アドレスを設定します。

[未設定時]

相手側の RADIUS アカウンティング装置と通信を行う自側 IP アドレスを自動的に選択するものとみなされます。

18.3.5 aaa radius server client-info secret

[機能]

RADIUS クライアント用共有鍵 (RADIUS シークレット) の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] radius server client-info [<number>] secret <secret> [encrypted]

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略時は、0 を指定したものとみなされます。

<number>

- RADIUS クライアント定義番号
  RADIUS サーバが管理する RADIUS クライアントのグループ内での通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<secret>

- 共有鍵 (RADIUS シークレット)
  本装置と RADIUS 認証クライアントとの間で取り決めた共有鍵 (RADIUS シークレット) を、0x21,0x23〜0x7e の 64 文字以内の ASCII 文字で指定します。
- 暗号化された RADIUS シークレット文字列 show コマンドで表示される暗号化された共有鍵 (RADIUS シークレット) を encrypted と共に指定します。

encrypted

- 暗号化共有鍵 (RADIUS シークレット) 指定
  <secret>に暗号化された共有鍵 (RADIUS シークレット) を指定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本装置と RADIUS クライアントで共有する共有鍵 (RADIUS シークレット) を設定します。
show コマンドでは、暗号化された共有鍵 (RADIUS シークレット) が encrypted と共に表示されます。

[未設定時]

共有鍵 (RADIUS シークレット) を設定しないものとみなします。

18.3.6　aaa radius server client-info address

[機能]

相手側 RADIUS クライアントの IP アドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] radius server client-info [<number>] address <address>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。

<number>

- RADIUS クライアント定義番号
  RADIUS サーバが管理する RADIUS クライアントのグループ内での通し番号を、10 進数値で指定します。
  省略時は、0 を指定したものとみなされます。

<address>

- 相手側 IP アドレス
  相手側となる RADIUS クライアントの IPv4 アドレスまたは IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  IPv4:　1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  IPv6:　::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

  any:　相手側となる RADIUS クライアントを特定しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本装置が通信する RADIUS クライアントの IP アドレスを設定します。

[未設定時]

通信相手となる RADIUS クライアントの IP アドレスを設定しないものとみなされます。

18.3.7 aaa radius client server-info auth secret

[機能]

RADIUS 認証サーバ用共有鍵 (RADIUS シークレット) の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] radius client server-info auth [<number>] secret <secret> [encrypted]

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略時は、0 を指定したものとみなされます。

<number>

- サーバ定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます

<secret>

- 共有鍵 (RADIUS シークレット)
  本装置と RADIUS 認証サーバとの間で取り決めた共有鍵 (RADIUS シークレット) を、0x21,0x23〜0x7e の 64 文字以内の ASCII 文字で指定します。
- 暗号化された共有鍵 (RADIUS シークレット)
  show コマンド で表示される暗号化された共有鍵 (RADIUS シークレット) を encrypted と共に指定します。

encrypted

- 暗号化共有鍵 (RADIUS シークレット) 指定
  <secret>に暗号化された共有鍵 (RADIUS シークレット) を指定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本装置と RADIUS 認証サーバとの間で共有する共有鍵 (RADIUS シークレット) を設定します。
show コマンド では、暗号化された共有鍵 (RADIUS シークレット) が encrypted と共に表示されます。

[未設定時]

共有鍵 (RADIUS シークレット) を設定しないものとみなします。

18.3.8　aaa radius client server-info auth address

[機能]

相手側 RADIUS 認証サーバの IP アドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] radius client server-info auth [<number>] address <address>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。

<number>

- サーバ定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます

<address>

- 相手側 IP アドレス
  相手側となる RADIUS 認証装置の IPv4 アドレスまたは IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

IPv4:　1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

IPv6:　::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

[動作モード]

構成定義モード (管理者クラス)

[説明]

本装置と通信する RADIUS 認証サーバの IP アドレスを設定します。

[未設定時]

相手側 RADIUS 認証装置の IP アドレスが設定がされません。RADIUS 認証機能を使用する場合は必ず設定してください。

18.3.9 aaa radius client server-info auth port

[機能]

認証サーバ UDP ポートの指定 (旧 RFC 仕様対応)

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] radius client server-info auth [<number>] port <port>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。

<number>

- サーバ定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます

<port>

- 1812
  最新 RFC 仕様の RADIUS 認証サーバに割り当てられた UDP ポート番号
- 1645
  旧 RFC 仕様の RADIUS 認証サーバに割り当てられた UDP ポート番号

[動作モード]

構成定義モード (管理者クラス)

[説明]

RADIUS 認証クライアントが認証要求する RADIUS 認証サーバの UDP ポート番号を設定します。認証要求する RADIUS 認証サーバが旧 RFC 仕様の UDP ポートで実装されている場合はポート番号に 1645 を設定してください。

[未設定時]

RADIUS 認証サーバの UDP ポート番号に 1812 を使用するものとみなします。

```
aaa radius client server-info auth port 1812
```

18.3.10　aaa radius client server-info auth deadtime

[機能]

復旧待機時間の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] radius client server-info auth [<number>] deadtime <deadtime>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。

<number>

- サーバ定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます

<deadtime>

- 復旧待機時間
  RADIUS サーバが dead 状態になってから、自動的に再び alive 状態に復旧するまでの時間を指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。
  指定可能な範囲は以下のとおりです。

  0〜86400(秒)

  0s を指定した場合は、自動的に alive 状態に復旧しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RADIUS サーバから aaa radius client retry コマンドで設定した応答待ち受け時間を経過しても応答が得られなかった場合、その RADIUS サーバは dead 状態となり、優先度は最非優先となります。dead 状態となった RADIUS サーバは、alive 状態のサーバが存在する限り使わなくなります。本設定は、dead 状態になってから、設定した優先度となる alive 状態へ自動的に復旧するための待ち時間を設定します。
dead 状態から alive 状態に復旧するためには、以下のどれかの条件を満たす必要があります。

- 本設定の時間が経過した場合
- 利用可能なすべてのサーバが dead 状態となった後、dead 状態の RADIUS サーバにパケットを送信し、応答が得られた場合
- 運用コマンドで、手動で復旧させた場合

[未設定時]

自動的に復旧しないものとみなします。

```
aaa radius client server-info auth deadtime 0s
```

18.3.11　aaa radius client server-info auth priority

[機能]

優先度の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] radius client server-info auth [<number>] priority <priority>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。

<number>

- サーバ定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます

<priority>

- 優先度
  同一グループ内での RADIUS サーバを使用する優先度を指定します。
  0 を最優先、255 を最非優先とし、数字が小さい程、高い優先度となります。

  0〜255　255 を指定した場合はその RADIUS サーバは常に dead 状態となります。

[動作モード]

構成定義モード (管理者クラス)

[説明]

同一グループ内の複数の RADIUS サーバから、認証の際に使用する RADIUS サーバを決める際に使用する優先度を指定します。同一グループの中で、dead 状態になっていないもっとも高い優先度の RADIUS サーバが使われます。もっとも高い優先度の RADIUS サーバが複数存在する場合は、使用する RADIUS サーバはランダムに決定されます。

[未設定時]

最優先が指定されたものとみなします。

```
aaa radius client server-info auth priority 0
```

18.3.12 aaa radius client server-info auth source

[機能]

自側 IP アドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] radius client server-info auth [<number>] source <address>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。

<number>

- サーバ定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます

<address>

- 自側 IP アドレス
  自側 RADIUS 認証サーバの IPv4 アドレスまたは IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  IPv4: 1.0.0.1 〜 126.255.255.254
  128.0.0.1 〜 191.255.255.254
  192.0.0.1 〜 223.255.255.254

  IPv6: ::2 〜 fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: 〜 feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

[動作モード]

構成定義モード (管理者クラス)

[説明]

自側 RADIUS 認証装置の IP アドレスを設定します。本定義の内容は、aaa radius client source による、自側 RADIUS 認証装置の IP アドレスの設定より優先されます。

[未設定時]

aaa radius client source による自側 RADIUS 認証装置の IP アドレスの設定に従うものとみなされます。

18.3.13　aaa radius client server-info accounting secret

[機能]

RADIUS アカウンティングサーバ用共有鍵 (RADIUS シークレット) の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] radius client server-info accounting [<number>] secret <secret> [encrypted]

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略時は、0 を指定したものとみなされます。

<number>

- サーバ定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます

<secret>

- 共有鍵 (RADIUS シークレット)
  本装置と RADIUS アカウンティングサーバとの間で取り決めた共有鍵 (RADIUS シークレット) を、0x21,0x23～ 0x7e の 64 文字以内の ASCII 文字で指定します。
- 暗号化された RADIUS シークレット文字列
  show コマンドで表示される暗号化された共有鍵 (RADIUS シークレット) を encrypted と共に指定します。

encrypted

- 暗号化共有鍵 (RADIUS シークレット) 指定
  <secret>に暗号化された共有鍵 (RADIUS シークレット) を設定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本装置と RADIUS アカウンティングサーバとの間で共有する共有鍵 (RADIUS シークレット) を設定します。
show コマンドでは、暗号化された共有鍵 (RADIUS シークレット) が encrypted と共に表示されます。

[未設定時]

共有鍵 (RADIUS シークレット) を設定しないものとみなします。

18.3.14 aaa radius client server-info accounting address

[機能]

相手側 RADIUS アカウンティングサーバの IP アドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] radius client server-info accounting [<number>] address <address>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。

<number>

- サーバ定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます

<address>

- 相手側 IP アドレス
  相手側となる RADIUS アカウンティング装置の IPv4 アドレスまたは IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  IPv4: 1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  IPv6: ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

[動作モード]

構成定義モード (管理者クラス)

[説明]

本装置と通信する RADIUS アカウンティングサーバの IP アドレスを設定します。

18.3.15　aaa radius client server-info accounting port

[機能]

アカウンティングサーバ UDP ポートの指定 (旧 RFC 仕様対応)

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] radius client server-info accounting [<number>] port <port>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。

<number>

- サーバ定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます

<port>

- 1813
  最新 RFC 仕様の RADIUS アカウンティングサーバに割り当てられた UDP ポート番号
- 1646
  旧 RFC 仕様の RADIUS アカウンティングサーバに割り当てられた UDP ポート番号

[動作モード]

構成定義モード (管理者クラス)

[説明]

RADIUS アカウンティングクライアントがアカウンティング要求する RADIUS アカウンティングサーバの UDP ポート番号を設定します。
アカウンティング要求する RADIUS アカウンティングサーバが旧 RFC 仕様の UDP ポートで実装されている場合はポート番号に 1646 を設定してください。

[未設定時]

RADIUS アカウンティングサーバの UDP ポート番号に 1813 を使用するものとみなします。

```
aaa radius client server-info accounting port 1813
```

18.3.16 aaa radius client server-info accounting deadtime

[機能]

復旧待機時間の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] radius client server-info accounting [<number>] deadtime <deadtime>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。

<number>

- サーバ定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます

<deadtime>

- 復旧待機時間
  RADIUS サーバが dead 状態になってから、自動的に再び alive 状態に復旧するまでの時間を指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。
  指定可能な範囲は以下のとおりです。

  0〜86400(秒)

  0s を指定した場合は、自動的に alive 状態に復旧しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RADIUS サーバから aaa radius client retry コマンドで設定した応答待ち受け時間を経過しても応答が得られなかった場合、その RADIUS サーバは dead 状態となり、優先度は最非優先となります。dead 状態となった RADIUS サーバは、alive 状態のサーバが存在する限り使わなくなります。本設定は、dead 状態になってから、設定した優先度となる alive 状態へ自動的に復旧するための待ち時間を設定します。
dead 状態から alive 状態に復旧するためには、以下のどれかの条件を満たす必要があります。

- 本設定の時間が経過した場合
- 利用可能なすべてのサーバが dead 状態となった後、dead 状態の RADIUS サーバにパケットを送信し、応答が得られた場合
- 運用コマンドで、手動で復旧させた場合

[未設定時]

自動的に復旧しないものとみなします。

```
aaa radius client server-info accounting deadtime 0s
```

18.3.17 aaa radius client server-info accounting priority

[機能]

優先度の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] radius client server-info accounting [<number>] priority <priority>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。

<number>

- サーバ定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます

<priority>

- 優先度
  同一グループ内での RADIUS サーバを使用する優先度を指定します。
  0 を最優先、255 を最非優先とし、数字が小さい程、高い優先度となります。

  0〜255　255 を指定した場合はその RADIUS サーバは常に dead 状態となります。

[動作モード]

構成定義モード (管理者クラス)

[説明]

同一グループ内の複数の RADIUS サーバから、アカウンティングの際に使用する RADIUS サーバを決める際に使用する優先度を指定します。同一グループの中で、dead 状態になっていないもっとも高い優先度の RADIUS サーバが使われます。もっとも高い優先度の RADIUS サーバが複数存在する場合は、使用する RADIUS サーバはランダムに決定されます。

[未設定時]

最優先が指定されたものとみなします。

```
aaa radius client server-info accounting priority 0
```

18.3.18　aaa radius client server-info accounting source

[機能]

自側 IP アドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] radius client server-info accounting [<number>] source <address>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。

<number>

- サーバ定義番号
  相手装置の定義番号を 10 進数値で指定します。
  省略時は、0 を指定したものとみなされます

<address>

- 自側 IP アドレス
  自側 RADIUS アカウンティングサーバの IPv4 アドレスまたは IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  IPv4:　1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  IPv6:　::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

[動作モード]

構成定義モード (管理者クラス)

[説明]

自側 RADIUS アカウンティング装置の IP アドレスを設定します。本定義の内容は、aaa radius client source による、自側 RADIUS アカウンティング装置の IP アドレスの設定より優先されます。

[未設定時]

aaa radius client source による自側 RADIUS アカウンティング装置の IP アドレスの設定に従うものとみなされます。

18.3.19 aaa radius client retry

[機能]

RADIUS パケット再送回数・送信間隔の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] radius client retry <interval> <retry>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。

<interval>

- 送信間隔
  RADIUS サーバ未応答時のパケットの送信間隔を設定します。
  指定可能な範囲は以下のとおりです。

  1〜10(秒)

<retry>

- 再送回数
  RADIUS サーバ未応答時のパケット再送回数を設定します。
  指定可能な範囲は以下のとおりです。

  1〜10(回)

[動作モード]

構成定義モード (管理者クラス)

[説明]

RADIUS サーバ未応答時のパケットの再送回数・送信間隔を設定します。
サーバからの応答待ち受け時間は、送信間隔× (再送回数+1) 秒となります。

[未設定時]

送信間隔を 1 秒、再送回数を 2 回として動作します。
この場合は、サーバからの応答待ち受け時間はパケットの初回送信後、3 秒となります。

```
aaa 0 client radius retry 1 2
```

18.3.20　aaa radius client nas-identifier

[機能]

NAS 識別子の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 260 | Si-R 220B | Si-R 180

[入力形式]

aaa [<group_id>] radius client nas-identifier <nas_id>

[オプション]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略時は、0 を指定したものとみなされます。

<nas_id>

- NAS 識別子
  RADIUS 認証クライアントおよびアカウンティングクライアントが RADIUS サーバに送出する Nas-Identifier アトリビュートの値を、0x21,0x23〜0x7e の 64 文字以内の ASCII 文字列で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

Nas-Identifier アトリビュートで指定する NAS 識別子を設定します。認証およびアカウンティングで有効です。未設定時は、Nas-Identifier アトリビュートを送信しません。

[未設定時]

Nas-Identifier アトリビュートを送信しません。

第 19 章　装置情報の設定

19.1　SNMP 情報

19.1.1　snmp service

[機能]

SNMP エージェント機能および SNMP トラップ機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

snmp service <mode>

[オプション]

<mode>

- on
  SNMP エージェント機能および SNMP トラップ機能を有効にします。
- off
  SNMP エージェント機能および SNMP トラップ機能を停止します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

SNMP エージェント機能および SNMP トラップ機能を有効にするかどうかを設定します。

[未設定時]

SNMP エージェント機能を停止するとみなされます。

```
snmp service off
```

19.1.2 snmp agent contact

[機能]

SNMP エージェント機能での管理者名の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

snmp agent contact <syscontact>

[オプション]

<syscontact>

- 管理者名 (sysContact 値)
  本装置の管理者名を表す MIB 変数 sysContact を、40 文字以内で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

SNMP エージェント機能での管理者名を設定します。

[未設定時]

管理者名を設定しないものとみなされます。

19.1.3　snmp agent sysname

[機能]

SNMP エージェント機能での機器名称の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

snmp agent sysname <sysname>

[オプション]

<sysname>

- 機器名称 (sysName 値)
  本装置の機器名称を表す MIB 変数 sysName を、32 文字以内で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

SNMP エージェント機能での機器名称を設定します。

[未設定時]

機器名称を設定しないものとみなされます。

19.1.4 snmp agent location

[機能]

SNMP エージェント機能での機器設置場所の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

snmp agent location <syslocation>

[オプション]

<syslocation>

- 機器設置場所 (sysLocation 値)
  本装置の設置場所を表す MIB 変数 sysLocation を、72 文字以内で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

SNMP エージェント機能での機器設置場所を設定します。

[未設定時]

機器設置場所を設定しないものとみなされます。

19.1.5　snmp agent address

[機能]

SNMP エージェントアドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

snmp agent address <address>

[オプション]

<address>

- エージェントアドレス
  本装置のエージェントアドレスを設定します。
  0.0.0.0 を指定した場合は、SNMP エージェントアドレスを削除します。
  指定可能な範囲は以下のとおりです。

  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[動作モード]

構成定義モード (管理者クラス)

[説明]

SNMP エージェントのアドレスを設定します。本設定は TRAP 送信時の自局アドレスにも使用されます。
SNMP エージェント機能を使用する場合は必ず設定してください。

[未設定時]

エージェントアドレスを設定しないものとみなされます。その場合、TRAP パケットの自局 IP アドレスは不定となります。

19.1.6 snmp manager

[機能]

SNMP ホスト情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

snmp manager <manager_number> <address> <community> <trap> [<write>]

[オプション]

<manager_number>

- SNMP ホスト定義番号
  SNMP ホスト定義の通し番号を、0〜7 の 10 進数値で指定します。

<address>

- アクセス許可/トラップ送信アドレス
  アクセス許可およびトラップを送信するあて先 IP アドレスを、XXX.XXX.XXX.XXX(XXX は 3 桁の 10 進数値) の形式で指定します。
  0.0.0.0 を指定すると、すべてのホストからのアクセスを許可し、trap 送信は行いません。
  指定可能な範囲は以下のとおりです。

  1.0.0.1 〜 126.255.255.254
  128.0.0.1 〜 191.255.255.254
  192.0.0.1 〜 223.255.255.254

<community>

コミュニティ名を指定します。

- コミュニティ名
  トラップを送信するときのコミュニティ名を、1〜32 文字で指定します。
- public
  任意の SNMP マネージャと通信する場合に指定します。

<trap>

トラップ送信するかどうかを指定します。

- on
  トラップ送信する場合に指定します。
- off
  トラップ送信しない場合に指定します。

<write>

SNMP マネージャからの書き込みを許可するかどうか指定します。

- enable
  SNMP マネージャからの書き込みを許可する場合に指定します。
- disable
  SNMP マネージャからの書き込みを許可しない場合に指定します。

省略時は、disable を指定したものとみなされます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

SNMP ホストの情報を設定します。

[未設定時]

SNMP ホストの情報を設定しないものとみなされます。

19.1.7 snmp trap coldstart

[機能]

coldStart トラップの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

snmp trap coldstart <mode>

[オプション]

<mode>

トラップの動作を指定します。

- enable
  トラップを有効にします。
- disable
  トラップを無効にします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

coldStart トラップを有効または無効にするかを設定します。

[未設定時]

coldStart トラップが有効とみなされます。

```
snmp trap coldstart enable
```

19.1.8　snmp trap linkdown

[機能]

linkDown トラップの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

snmp trap linkdown <mode>

[オプション]

<mode>

トラップの動作を指定します。

- enable
  トラップを有効にします。
- disable
  トラップを無効にします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

linkDown トラップを有効または無効にするかを設定します。

[未設定時]

linkDown トラップが有効とみなされます。

```
snmp trap linkdown enable
```

19.1.9 snmp trap linkup

[機能]

linkUp トラップの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

snmp trap linkup <mode>

[オプション]

<mode>

トラップの動作を指定します。

- enable
  トラップを有効にします。
- disable
  トラップを無効にします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

linkUp トラップを有効または無効にするかを設定します。

[未設定時]

linkUp トラップが有効とみなされます。

```
snmp trap linkup enable
```

19.1.10　snmp trap authfail

[機能]

authenticationFailure トラップの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

snmp trap authfail <mode>

[オプション]

<mode>

トラップの動作を指定します。

- enable
  トラップを有効にします。
- disable
  トラップを無効にします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

authenticationFailure トラップを有効または無効にするかを設定します。

[未設定時]

authenticationFailure トラップが有効とみなされます。

```
snmp trap authfail enable
```

19.1.11 snmp trap newroot

[機能]

newRoot トラップの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

snmp trap newroot <mode>

[オプション]

<mode>

トラップの動作を指定します。

- enable
  トラップを有効にします。
- disable
  トラップを無効にします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

newRoot トラップを有効または無効にするかを設定します。

[未設定時]

newRoot トラップが有効とみなされます。

```
snmp trap newroot enable
```

19.1.12　snmp trap topologychange

[機能]

topologyChange トラップの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

snmp trap topologychange <mode>

[オプション]

<mode>

トラップの動作を指定します。

- enable
  トラップを有効にします。
- disable
  トラップを無効にします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

topologyChange トラップを有効または無効にするかを設定します。

[未設定時]

topologyChange トラップが有効とみなされます。

```
snmp trap topologychange enable
```

19.1.13 snmp trap vrrpnewmaster

[機能]

vrrpTrapNewMaster トラップの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

snmp trap vrrpnewmaster <mode>

[オプション]

<mode>

トラップの動作を指定します。

- enable
  トラップを有効にします。
- disable
  トラップを無効にします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

vrrpTrapNewMaster トラップを有効または無効にするかを設定します。

[未設定時]

vrrpTrapNewMaster トラップが有効とみなされます。

```
snmp trap vrrpnewmaster enable
```

19.1.14　snmp trap vrrpauthfail

[機能]

vrrpTrapAuthFailure トラップの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

snmp trap vrrpauthfail <mode>

[オプション]

<mode>

トラップの動作を指定します。

- enable
  トラップを有効にします。
- disable
  トラップを無効にします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

vrrpTrapAuthFailure トラップを有効または無効にするかを設定します。

[未設定時]

vrrpTrapAuthFailure トラップが有効とみなされます。

```
snmp trap vrrpauthfail enable
```

19.1.15 snmp trap noserror

[機能]

nosError トラップの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

snmp trap noserror <mode>

[オプション]

<mode>

トラップの動作を指定します。

- enable
  トラップを有効にします。
- disable
  トラップを無効にします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

nosError トラップを有効または無効にするかを設定します。

[未設定時]

nosError トラップが有効とみなされます。

```
snmp trap noserror enable
```

19.2　システムログ情報

19.2.1　syslog server

[機能]

システムログ情報の受信サーバの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

syslog server <address>

[オプション]

<address>

- IP アドレス
  システムログ情報 (メッセージ) を受信するサーバの IP アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[動作モード]

構成定義モード (管理者クラス)

[説明]

システムログ情報 (メッセージ) を受信するサーバを設定します。
以下に、システムログ情報の出力方法を示します。

1) syslog server <address>
   で設定した IP アドレスのホストに送信します。
2) show logging syslog コマンドで表示します。

[未設定時]

システムログ情報を受信するサーバを指定しないものとみなされます。

19.2.2 syslog pri

[機能]

システムログ情報の出力対象プライオリティの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

syslog pri <mode>

[オプション]

<mode>

- プライオリティ

  システムログ情報を出力する対象となるプライオリティを、以下の中から指定します。複数指定する場合は、","(カンマ) で区切ります。

  error プライオリティLOG_ERROR を対象とする場合に指定します。

  warn プライオリティLOG_WARNING を対象とする場合に指定します。

  notice プライオリティLOG_NOTICE を対象とする場合に指定します。

  info プライオリティLOG_INFO を対象とする場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

システムログ情報を出力する対象となるプライオリティを指定します。

[未設定時]

何も指定しないものとみなされ、システムログ情報は収集されません。

19.2.3　syslog facility

[機能]

システムログ情報のファシリティの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

syslog facility <num>

[オプション]

<num>

- ファシリティ
  システムログ情報のファシリティを、0〜23 の 10 進数値で設定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

システムログ情報のファシリティを指定します。

[未設定時]

0 を指定したものとみなされます。

```
syslog facility 0
```

19.2.4 syslog security

[機能]

システムログ情報の出力対象セキュリティの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

syslog security <securetype>

[オプション]

<securetype>

- セキュリティ対象セキュリティログ情報の出力対象を、以下の中から指定します。複数指定する場合は、","(カンマ) で区切ります。

ipfilter	IP filter モジュールを対象とする場合に指定します。
nat	NAT モジュールを対象とする場合に指定します。
ids	IDS モジュールを対象とする場合に指定します。
ppp	PPP モジュールを対象とする場合に指定します。
dhcp	DHCP モジュールを対象とする場合に指定します。
proxydns	ProxyDNS モジュールを対象とする場合に指定します。
macauth	MAC アドレス認証モジュールを対象とする場合に指定します。
none	すべてのモジュールを対象外とする場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

システムログ情報を出力する対象となるセキュリティを指定します。

[未設定時]

すべてを指定したものとみなされます。

```
syslog security ipfilter,nat,ids,ppp,dhcp,proxydns,macauth
```

19.2.5　syslog dupcut

[機能]

システムログ情報の重複メッセージ出力の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

syslog dupcut <cut>

[オプション]

<cut>

- yes
  直前に出力されたメッセージが重複した場合、出力しません。
- no
  重複チェックを行わず、すべてのメッセージを出力します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

システムログにメッセージを出力する際、直前に出力したメッセージと重複した場合に出力するかどうかを指定します。

[未設定時]

重複チェックを行わないものとみなされます。

```
syslog dupcut no
```

19.3 自動時刻設定情報

19.3.1 time auto server

[機能]

時刻情報の提供サーバの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

time auto server <address> <protocol>

[オプション]

<address>

- IPv4 アドレス
  時刻情報を提供しているサーバの IPv4 アドレスを指定します。
  DHCP サーバが広報する時刻提供サーバに従う場合は、0.0.0.0 を指定します。
  指定可能な範囲は以下のとおりです。

  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

- IPv6 アドレス
  時刻情報を提供しているサーバの IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<protocol>

使用するプロトコルを指定します。

- time
  TIME プロトコル (TCP) を使用する場合に指定します。
- sntp
  簡易 NTP プロトコル (UDP) を使用する場合に指定します。
- dhcp
  DHCP サーバから広報される TIME プロトコルまたは簡易 NTP に従います。

[動作モード]

構成定義モード (管理者クラス)

[説明]

時刻提供サーバの情報を設定します。
time auto server の<address>で指定した時刻提供サーバから、<protocol>で指定したプロトコルを使用して、自動的に時刻を設定します。
本装置のインタフェースが DHCP クライアントとして動作している場合に限り、<protocol>で dhcp を指定することができます。この場合、DHCP サーバが広報する時刻提供サーバから指定されたプロトコルを使用して設定します。また、TIME プロトコルと SNTP が同時に広報された場合は、SNTP を優先します。

[未設定時]

自動時刻設定を行わないものとみなされます。

19.3.2 time auto interval

[機能]

時刻情報の自動設定間隔の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

time auto interval <time>

[オプション]

<time>

時刻情報を設定する間隔を指定します。

- start
  電源投入時またはリセット時に一度だけ、時刻情報を設定する場合に指定します。
- 間隔
  時刻情報を設定する間隔を、0 秒～最大 10 日の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

自動時刻を設定する間隔を設定します。

[未設定時]

時刻提供サーバを使用する場合だけ、電源投入時またはリセット時に一度だけ時刻情報設定するものとみなされます。

```
time auto interval start
```

19.3.3　time zone

[機能]

時刻情報のタイムゾーンの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

time zone <offset>

[オプション]

<offset>

- 差分
  本装置が使用するタイムゾーンを指定します。
  GMT(グリニッジ標準時間) からの時差を指定します。日本で使用する場合は、0900 を指定してください。

[動作モード]

構成定義モード (管理者クラス)

[説明]

タイムゾーンを設定します。

[未設定時]

```
time zone 0
```

19.4 ProxyDNS 情報

19.4.1 proxydns domain

[機能]

プロキシ DNS の順引き動作条件の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

proxydns domain <count> <qtype> <qname> <address>/<mask> reject
(転送要求の破棄)
proxydns domain <count> <qtype> <qname> <address>/<mask> static <ipaddress>
(固定 DNS サーバ指定)
proxydns domain <count> <qtype> <qname> <address>/<mask> to <remote_number>
(相手ネットワークの DNS サーバ指定)
proxydns domain <count> <qtype> <qname> <address>/<mask> on <remote_number> [<route>]
(相手ネットワーク指定)
proxydns domain <count> <qtype> <qname> <address>/<mask> dhcp <interface>
(DHCP 指定)

[オプション]

<count>

- 転送先定義番号

  転送先定義番号として、0〜31 の 10 進数値を指定します。

  指定した値は、設定完了時に順方向にソートされてリナンバリングされます。

  また、指定した定義番号と同じ値を持つ転送先定義番号が存在する場合は、既存定義の前に挿入されます。

<qtype>

- 問い合わせタイプ番号

  1〜11、または 13〜65535 の 10 進数値を指定します。

  以下に、問い合わせタイプの一部分を示します。

名称	番号	説　明
A	1	ホスト・アドレス
NS	2	ドメインに対して認証されたネーム・サーバ
CNAME	5	別名(Alias名、ドメイン名)
SOA	6	ゾーン管理開始
PTR	12	ドメイン名空間のほかの部分へのポインタ
HINFO	13	ホストが使用するCPUとOS
MX	15	ドメインに対するメール交換
SRV	33	サービス

- any

  PTR(12) を除くすべてのタイプを対象する場合に指定します。

<qname>

- ホスト名
  条件となるホスト名を、80 文字以内で指定します。
  ホスト名には、以下のワイルドカードを使用できます。
  - *(アスタリスク)
    0 文字以上の任意の文字列とみなされます。
  - ?(クェスチョンマーク)
    任意の一文字とみなされます。

  以下に、ワイルドカードを使用したホスト名の記述例および一致例を示します。

  www.*.com
  以下のどの文字列とも一致するとみなされます。
  ・www.testa.com
  ・www.test1.test.com

  test　以下のどの文字列とも一致するとみなされます。
  ・www.test.com
  ・test.com
  ・test.co.jp

  www.test?.com
  以下のどの文字列とも一致するとみなされます。
  ・www.test1.com
  ・www.test2.com
  ・www.testA.com

  なお、ホスト名をチェックするときに、大文字と小文字の区別はされません。

<address>/<mask>

対象となる送信元 IPv4 アドレス/マスクビット数または送信元 IPv6 アドレス/プレフィックス長を指定します。

- 送信元 IPv4 アドレス/マスクビット数 (またはマスク値)
  対象となる送信元 IPv4 アドレスとマスクビット数の組み合わせを指定します。
  マスク値は、最上位ビットから 1 で連続した値にしてください。
- 送信元 IPv6 アドレス/プレフィックス長
  対象となる送信元 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- any
  すべてのアドレスを対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) または 0:0:0:0:0:0:0:0/0 を指定するのと同じ意味になります。

<ipaddress>

- DNS サーバ IP アドレス
  要求を転送する DNS サーバの IPv4 アドレスまたは IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  IPv4:　1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  IPv6:　::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<remote_number>

- 転送先相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B Si-R240 Si-R220B
0〜49	Si-R180

<route>

DNS 問い合わせにより経路を設定するかどうかを設定します。

- on
  経路を設定します。
- off
  経路を設定しません。

省略時は、off を指定したものとみなされます。

<interface>

DHCP クライアントが動作しているインタフェースを以下の範囲で指定します。

範囲	機種
lan0〜lan19 rmt0〜rmt999	Si-R570
lan0〜lan19 rmt0〜rmt499	Si-R370
lan0〜lan19 rmt0〜rmt99	Si-R260B Si-R240 Si-R220B
lan0〜lan9 rmt0〜rmt49	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

プロキシ DNS の順引き動作条件を設定します。
各コマンドについて説明します。

転送要求の破棄

proxydns domain <count> <qtype> <qname> <address>/<mask> reject
指定した DNS 要求の転送を無効にするフィルタを設定します。
<qname>で指定するホスト名は、DNS データベースに登録されていても、そのホスト (群) へのアクセスを制限する場合に使用します。条件と一致した場合は破棄されます。

固定 DNS サーバの指定

proxydns domain <count> <qtype> <qname> <address>/<mask> static <ipaddress>
指定した DNS 要求の転送先 IP アドレスを指定します。
以下の場合に有効です。

- 専用線に接続する場合
- LAN 側に DNS サーバが存在する場合
- リモート側の DNS サーバを固定にする場合

相手ネットワークの DNS サーバ指定

proxydns domain <count> <qtype> <qname> <address>/<mask> to <remote_number>
回線から通知された DNS サーバを使用します。
相手情報でマルチルーティングを定義している場合は、その設定に従います。回線切断中は、接続先情報の接続優先順位に従います。

相手ネットワークの指定

proxydns domain <count> <qtype> <qname> <address>/<mask> on <remote_number> [<route>]
回線から通知された DNS サーバへ指定のネットワークを使用して DNS 要求を転送します。
回線切断中は、接続先情報の接続優先順位に従います。
<route>に on を指定すると DNS 要求を転送した相手ネットワークへの経路を動的に設定します。

DHCP 指定

proxydns domain <count> <qtype> <qname> <address>/<mask> dhcp <interface> 指定のインタフェースで動作している DHCP クライアントが取得した DNS サーバへ DNS 要求を転送します。

[未設定時]

プロキシ DNS の順引き動作条件を設定しないものとみなされます。

19.4.2 proxydns domain move

[機能]

プロキシ DNS の順引き動作条件の順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

proxydns domain move <count> <new_count>

[オプション]

<count>

- 変更前転送先定義番号
  順序を変更する転送先定義番号を指定します。

<new_count>

- 新しい転送先定義番号
  <count>に対して、新しい順序を指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

プロキシ DNS の順引き動作条件の順序を変更します。
すでに存在する転送先定義番号と同じ番号を指定した場合は、指定した定義の前に挿入されます。

19.4.3　proxydns address

[機能]

プロキシ DNS の逆引き動作条件の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

proxydns address <count> <address>/<mask> reject
(転送要求の破棄)
proxydns address <count> <address>/<mask> static <ipaddress>
(固定 DNS サーバ指定)
proxydns address <count> <address>/<mask> to <remote_number>
(相手ネットワークの DNS サーバ指定)
proxydns address <count> <address>/<mask> on <remote_number> [<route>]
(相手ネットワーク指定)
proxydns address <count<> <address>/<mask> dhcp <interface>
(DHCP 指定)

[オプション]

<count>

- 転送先定義番号
  転送先定義番号として、0～31 の 10 進数値を指定します。
  指定した値は、設定完了時に順方向にソートされてリナンバリングされます。
  また、指定した定義番号と同じ値を持つ転送先定義番号が存在する場合は、既存定義の前に挿入されます。

<address>/<mask>

逆引き対象 IPv4 アドレス/マスクビット数または IPv6 アドレス/プレフィックス長を指定します。

- 逆引き対象 IPv4 アドレス/マスクビット数 (またはマスク値)
  逆引き対象 IPv4 アドレスとマスクビット数の組み合わせを指定します。
  マスク値は、最上位ビットから 1 で連続した値にしてください。
- 逆引き対象 IPv6 アドレス/プレフィックス長
  逆引き対象 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- any4
  IPv4 アドレスの逆引きのすべてを対象とする場合に指定します。
- any6
  IPv6 アドレスの逆引きのすべてを対象とする場合に指定します。
- any
  すべてのアドレスの逆引きを対象とする場合に指定します。

<ipaddress>

- DNS サーバ IP アドレス
  要求を転送する DNS サーバの IPv4 アドレスまたは IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  IPv4: 1.0.0.1 〜 126.255.255.254
  128.0.0.1 〜 191.255.255.254
  192.0.0.1 〜 223.255.255.254

  IPv6: ::2 〜 fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: 〜 feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<remote_number>

- 転送先相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B Si-R240 Si-R220B
0〜49	Si-R180

<route>

DNS 問い合わせにより経路を設定するかどうかを設定します。

- on
  経路を設定します。
- off
  経路を設定しません。

省略時は、off を指定したものとみなされます。

<interface>

DHCP クライアントが動作しているインタフェースを以下の範囲で指定します。

範囲	機種
lan0〜lan19 rmt0〜rmt999	Si-R570
lan0〜lan19 rmt0〜rmt499	Si-R370
lan0〜lan19 rmt0〜rmt99	Si-R260B Si-R240 Si-R220B
lan0〜lan9 rmt0〜rmt49	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

プロキシ DNS の逆引き動作条件を設定します。
各コマンドについて説明します。

転送要求の破棄

proxydns address <count> <address>/<mask> reject
指定した DNS 要求の転送を無効にするフィルタを設定します。
<qname>で指定するホスト名は、DNS データベースに登録されていても、そのホスト (群) へのアクセスを制限する場合に使用します。条件と一致した場合は破棄されます。

固定 DNS サーバの指定

proxydns address <count> <address>/<mask> static <ipaddress>
指定した DNS 要求の転送先 IP アドレスを指定します。
転送先への経路は、IP ルーティングに従って決められます。
以下の場合に有効です。

- 専用線に接続する場合
- LAN 側に DNS サーバが存在する場合
- リモート側の DNS サーバを固定にする場合

相手ネットワークの DNS サーバ指定

proxydns address <count> <address>/<mask> to <remote_number>
回線から通知された DNS サーバを使用します。
相手情報でマルチルーティングを定義している場合は、その設定に従います。回線切断中は、接続先情報の接続優先順位に従います。

相手ネットワークの指定

proxydns address <count> <address>/<mask> on <remote_number> [<route>]
回線から通知された DNS サーバへ指定のネットワークを使用して DNS 要求を転送します。
回線切断中は、接続先情報の接続優先順位に従います。
<route>に on を指定すると DNS 要求を転送した相手ネットワークへの経路を動的に設定します。

DHCP 指定

proxydns address <count> <address>/<mask> dhcp <interface> 指定のインタフェースで動作している DHCP クライアントが取得した DNS サーバへ DNS 要求を転送します。

[未設定時]

プロキシ DNS の逆引き動作条件を設定しないものとみなされます。

19.4.4 proxydns address move

[機能]

プロキシ DNS の逆引き動作条件の順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

proxydns address move <count> <new_count>

[オプション]

<count>

- 変更前転送先定義番号
  順序を変更する転送先定義番号を指定します。

<new_count>

- 新しい転送先定義番号
  <count>に対して、新しい順序を指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

プロキシ DNS の逆引き動作条件の順序を変更します。
すでに存在する転送先定義番号と同じ番号を指定した場合は、指定した定義の前に挿入されます。

19.4.5　proxydns unicode

[機能]

プロキシ DNS の問い合わせパケットの透過の可否の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

proxydns unicode <action>

[オプション]

<action>

パケットを透過するかどうかを指定します。

- pass
  該当するパケットを透過する場合に指定します。
- reject
  該当するパケットを破棄する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

プロキシ DNS の問い合わせ名 (QNAME) に非表示文字が含まれる場合に、その問い合わせのパケットを透過するかどうかを設定します。

[未設定時]

該当パケットを破棄するものとみなされます。

```
proxydns unicode reject
```

19.5 ホストデータベース情報

19.5.1 host name

[機能]

ホストデータベース情報のホスト名の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

host <number> name <name>

[オプション]

<number>

- 定義番号

  ホストデータベース情報の定義番号を、0〜63 の 10 進数値で指定します。

<name>

- ホスト名

  ホスト名を、英数字、"-"(ハイフン)、"."(ピリオド) で構成される 80 文字以内の ASCII 文字列で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本装置配下に接続されたホストのホスト名をホストデータベースに設定します。
本コマンドは、簡易 DNS サーバ機能、DHCP スタティック機能、リモートパワーオン機能から利用されます。
以下に、各機能とパラメタの関係を示します。

パラメタ 機能	name	ip_address	ip6_address	mac_address	rpon
簡易DNSサーバ	○	○	○	―	―
DHCPスタティック	―	○	―	○	―
リモートパワーオン (手動/schedule)	―	―	―	○	○

○:有効、―:無効

[未設定時]

ホストデータベースを設定しないものとみなされます。

19.5.2　host ip address

[機能]

ホストデータベース情報の IP アドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

host <number> ip address <ip_address>

[オプション]

<number>

- 定義番号
  ホストデータベース情報の定義番号を、0〜63 の 10 進数値で指定します。

<ip_address>

- IP アドレス
  ホストの IP アドレスを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本装置配下に接続されたホストの IP アドレスをホストデータベースに設定します。
本コマンドは、簡易 DNS サーバ機能、DHCP スタティック機能、リモートパワーオン機能から利用されます。
以下に、各機能とパラメタの関係を示します。

パラメタ 機能	name	ip_address	ip6_address	mac_address	rpon
簡易DNSサーバ	○	○	○	―	―
DHCPスタティック	―	○	―	○	―
リモートパワーオン (手動/schedule)	―	―	―	○	○

○:有効、―:無効

[未設定時]

ホストデータベースを設定しないものとみなされます。

19.5.3 host ip6 address

[機能]

ホストデータベース情報の IPv6 アドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

host <number> ip6 address <ip6_address>

[オプション]

<number>

- 定義番号
  ホストデータベース情報の定義番号を、0〜63 の 10 進数値で指定します。

<ip6_address>

- IPv6 アドレス
  ホストの IPv6 アドレスを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本装置配下に接続されたホストの IPv6 アドレスをホストデータベースに設定します。
本コマンドは、簡易 DNS サーバ機能から利用されます。
以下に、各機能とパラメタの関係を示します。

パラメタ 機能	name	ip_address	ip6_address	mac_address	rpon
簡易DNSサーバ	○	○	○	―	―
DHCPスタティック	―	○	―	○	―
リモートパワーオン (手動/schedule)	―	―	―	○	○

○:有効、―:無効

[未設定時]

ホストデータベースを設定しないものとみなされます。

19.5.4　host mac

[機能]

ホストデータベース情報の MAC アドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

host <number> mac <mac_address>

[オプション]

<number>

- 定義番号

  ホストデータベース情報の定義番号を、0〜63 の 10 進数値で指定します。

<mac_address>

- MAC アドレス

  ホストの MAC アドレスを、xx:xx:xx:xx:xx:xx(xx は 2 桁の 16 進数値) の形式で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本装置配下に接続されたホストの MAC アドレスをホストデータベースに設定します。
本コマンドは、簡易 DNS サーバ機能、DHCP スタティック機能、リモートパワーオン機能から利用されます。
以下に、各機能とパラメタの関係を示します。

パラメタ 機能	name	ip_address	ip6_address	mac_address	rpon
簡易DNSサーバ	○	○	○	―	―
DHCPスタティック	―	○	―	○	―
リモートパワーオン (手動/schedule)	―	―	―	○	○

○:有効、―:無効

[未設定時]

ホストデータベースを設定しないものとみなされます。

19.5.5 host rpon

[機能]

ホストデータベース情報のリモートパワーオン対象の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

host <number> rpon <rpon>

[オプション]

<number>

- 定義番号
  ホストデータベース情報の定義番号を、0〜63 の 10 進数値で指定します。

<rpon>

リモートパワーオンの対象にするかどうかを設定します。

- off
  リモートパワーオンの対象にしません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本装置配下に接続されたホストのリモートパワーオン情報をホストデータベースに設定します。
本コマンドは、簡易 DNS サーバ機能、DHCP スタティック機能、リモートパワーオン機能から利用されます。
以下に、各機能とパラメタの関係を示します。

パラメタ 機能	name	ip_address	ip6_address	mac_address	rpon
簡易DNSサーバ	○	○	○	―	―
DHCPスタティック	―	○	―	○	―
リモートパワーオン (手動/schedule)	―	―	―	○	○

○:有効、―:無効

[未設定時]

リモートパワーオンの対象にするものとみなされます。

19.6　スケジュール情報

19.6.1　schedule at

[機能]

システムスケジュールの日時指定コマンド の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

schedule <number> at <day> <time> <command>

[オプション]

<number>

スケジュール定義を指定します。

- スケジュール定義番号
  スケジュール定義番号を、0〜15 の 10 進数値で指定します。
- any
  スケジュール定義番号を省略する場合に指定します。

<day>

- 日
  スケジュールの実行日または開始日を、1〜31 の 10 進数値で指定します。
- 曜日
  スケジュールの実行曜日または開始曜日を、以下の中から指定します。

sun	日曜日
mon	月曜日
tue	火曜日
wed	水曜日
thu	木曜日
fri	金曜日
sat	土曜日

  複数の曜日を指定する場合は、","(カンマ) で区切って指定します。
- any
  スケジュールの実行日または開始日を毎日とする場合に指定します。
  電源投入時または再起動時は、本パラメタを指定してください。

<time>

- 実行時間
  実行する時、分を、0〜9 の 4 桁の 10 進数値で指定します (例: 0635 = 午前 6 時 35 分、2330 = 午後 11 時 30 分)。
- pwon
  電源投入時に実行する場合に指定します。
- rset
  システム再起動時、または電源投入時に実行する場合に指定します。

<command>

実行するコマンド文字列を指定します。

- clear isdn account
  ISDN 課金情報をクリアする場合に指定します。(※ Si-R260B Si-R240 Si-R180 では無効です)
- clear modem account
  モデム課金情報をクリアする場合に指定します。(※ Si-R240 Si-R220B だけ有効です)
- offline remote
  強制切断する場合に指定します。(※ Si-R260B Si-R180 では無効です)
- rpon all
  リモートパワーオンを実行する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

システムスケジュールを設定します。
このスケジュールに従って、指定した時刻にコマンドを実行します。

[未設定時]

スケジュール情報を設定しないものとみなされます。

19.6.2　schedule in

[機能]

システムスケジュールの期間指定動作の設定

[適用機種]

Si-R 570	Si-R 370		Si-R 240	Si-R 220B	

[入力形式]

schedule <number> in <day> <time> <action>

[オプション]

<number>

スケジュール定義を指定します。

- スケジュール定義番号
  スケジュール定義番号を、0～15 の 10 進数値で指定します。
- any
  スケジュール定義番号を省略する場合に指定します。

<day>

- 日
  スケジュールの実行日または開始日を、1～31 の 10 進数値で指定します。
- 曜日
  スケジュールの実行曜日または開始曜日を、以下の中から指定します。

sun	日曜日
mon	月曜日
tue	火曜日
wed	水曜日
thu	木曜日
fri	金曜日
sat	土曜日

  複数の曜日を指定する場合は、","(カンマ) で区切って指定します。
- any
  スケジュールの実行日または開始日を毎日とする場合に指定します。
  電源投入時または再起動時は、本パラメタを指定してください。

<time>

- 開始時刻～終了時刻
  開始時刻～終了時刻を、0～9 の 4 桁の 10 進数値で指定します。開始時刻と終了時刻の間は、"-"(ハイフン) でつなぎます (例: 0900-1700 = 午前 9 時から午後 5 時まで、2300-0800 = 午後 11 時から翌午前 8 時まで)。

<action>

動作を指定します。

- diallock
  <time>で指定した時刻の間、自動発信を抑止します。
- dialreject
  <time>で指定した時刻の間、自動着信を抑止します。(※ Si-R240 では無効です)

[動作モード]

構成定義モード (管理者クラス)

[説明]

システムスケジュールを設定します。
このスケジュールに従って、指定した時刻の間、ある状態を維持することができます。

[未設定時]

スケジュール情報を設定しないものとみなされます。

19.6.3　schedule syslog

[機能]

システムスケジュールのシステムログ出力可否の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

schedule <number> syslog <syslog>

[オプション]

<number>

スケジュール定義を指定します。

- スケジュール定義番号
  スケジュール定義番号を、0〜15 の 10 進数値で指定します。
- any
  スケジュール定義番号を省略する場合に指定します。

<syslog>

- yes
  コマンド 実行時の出力をシステムログで行う場合に指定します。
- no
  コマンド 実行時の出力をシステムログで行わない場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

スケジュールによって起動されたコマンド が出力するメッセージを、システムログに出力するかどうかを指定します。
スケジュールで起動するコマンド が指定されている場合にだけ有効です。

[未設定時]

コマンド 実行時の出力をシステムログに出力しないものとみなされます。

```
schedule <number> syslog no
```

19.7　電話番号変更予約情報

19.7.1　dnconvinfo date

[機能]

電話番号変更予約の日時の設定

[適用機種]

Si-R 570	Si-R 370		Si-R 240	Si-R 220B	

[入力形式]

dnconvinfo <index> date <date>

[オプション]

<index>

- 登録番号
  電話番号変更予約情報の登録番号を、0〜3 の 10 進数値で指定します。

<date>

- 変更日時
  変更日時を、yymmddHHMM の形式で指定します。

yy	西暦の下 2 桁を指定します。西暦 2036 年まで指定できます。
mm	月を、1〜12 の 10 進数値で指定します。
dd	日付を、1〜31 の 10 進数値で指定します。
HH	時間を、0〜23 の 10 進数値で指定します。
MM	分を、0〜59 の 10 進数値で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

すべての構成定義情報の電話番号を一括変更する場合に必要となる、電話番号変更日時を設定します。
変更処理は、以下の 2 つの方法によって行われます。

- 時刻指定によって、スケジュール機能から自動的に実施します。
  なお、スケジュール機能によって実施した場合は、定義情報が保存され、システムがリセットされます。
- 時刻指定によらずに、コマンドで実施します。

[注意]

以下に、スケジュール機能によって電話番号変更を実施する場合の注意事項を示します。

- 装置の時刻を正しく設定してください。
- 実施時刻に、装置の電源を投入しておいてください。

[実行例]

以下に、構成定義情報に定義されている電話番号 123456789 を、1999 年 1 月 1 日午前 2 時にすべて 999999999 へ変更する場合の設定例を示します。

```
# dnconvinfo 0 date 9901010200
# dnconvinfo 0 dial 0 123456789 99999999
# show dnconvinfo
0 date 9901010200
0 dial 0 123456789 99999999
#
```

[未設定時]

電話番号変更予約情報を設定しないものとみなされます。

19.7.2 dnconvinfo dial

[機能]

電話番号変更予約の電話番号の設定

[適用機種]

Si-R 570	Si-R 370		Si-R 240	Si-R 220B	

[入力形式]

dnconvinfo <index> dial <count> <src_number> <dst_number>

[オプション]

<index>

- 登録番号

  電話番号変更予約情報の登録番号を、0〜3 の 10 進数値で指定します。

<count>

- 電話番号情報定義番号

  電話番号情報の定義番号を、0〜3 の 10 進数値で指定します。

<src_number>

- 変更前電話番号

  変更対象の電話番号を、0〜9 の数字と、*、#、-、(、)、\ の文字で構成される 32 桁以内の ASCII 文字列で指定します。

<dst_number>

- 変更後電話番号

  変更後の電話番号を、0〜9 の数字と、*、#、-、(、)、\ の文字で構成される 32 桁以内の ASCII 文字列で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

すべての構成定義情報の電話番号を一括変更する場合に必要となる、変更電話番号を設定します。
変更処理は、以下の 2 つの方法によって行われます。

- 時刻指定によって、スケジュール機能から自動的に実施します。

  なお、スケジュール機能によって実施した場合は、定義情報が保存され、システムがリセットされます。

- 時刻指定によらずに、コマンドで実施します。

[注意]

以下に、スケジュール機能によって電話番号変更を実施する場合の注意事項を示します。

- 装置の時刻を正しく設定してください。
- 実施時刻に、装置の電源を投入しておいてください。

[実行例]

以下に、構成定義情報に定義されている電話番号 123456789 を、1999 年 1 月 1 日午前 2 時にすべて 999999999 へ変更する場合の設定例を示します。

```
# dnconvinfo 0 date 9901010200
# dnconvinfo 0 dial 0 123456789 to 99999999
# show dnconvinfo
0 date 9901010200
0 dial 0 123456789 to 99999999
#
```

[未設定時]

電話番号変更予約情報を設定しないものとみなされます。

19.8 ファームウェア更新情報

19.8.1 updateinfo

[機能]

ファームウェア更新情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

updateinfo <host> <user> <password> <pathname>

[オプション]

<host>

更新するファームウェアの転送元ホスト (ftp サーバ) を、以下の形式で指定します。
ホスト名を指定する場合は、ホストデータベース情報に該当するホスト名が登録されているか、または本装置が DNS サーバを使用できる状態でなければなりません。

- ホスト名
  ホスト名を、0x21,0x23〜0x7e の 128 文字以内の ASCII 文字列で指定します。
- IPv4 アドレス
  指定可能な範囲は以下のとおりです。

  1.0.0.1 〜 126.255.255.254
  128.0.0.1 〜 191.255.255.254
  192.0.0.1 〜 223.255.255.254

- IPv6 アドレス
  指定可能な範囲は以下のとおりです。

  ::2 〜 fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: 〜 feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

  リンクローカルアドレスを指定する場合、アドレスに続けて"%<interface>" を指定して、どのインタフェースを使用するのか指定してください。たとえば、"fe80::1%lan0"のように指定します。

<user>

- ユーザ名
  ftp ユーザ名を、0x21,0x23〜0x7e の 16 文字以内の ASCII 文字列で指定します。

<password>

- パスワード
  ftp パスワードを、0x21,0x23〜0x7e の 32 文字以内の ASCII 文字列で指定します。
  anonymous FTP サーバの場合は、管理者のメールアドレスを指定します。

<pathname>

- パス名
  更新するファームウェアの ftp サーバ上のパス名を、0x21,0x23〜0x7e の 80 文字以内の ASCII 文字列で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ファームウェアを更新するための情報を設定します。
update コマンドで ftp サーバ上のファームウェアを取得する場合は、必ず本コマンドを実行してください。

[未設定時]

ファームウェア更新情報を設定しないものとみなされます。

19.9 MAC アドレス認証情報

19.9.1 macauth password

[機能]

MAC アドレス認証情報 (パスワード) の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

macauth password <password> [encrypted]

[オプション]

<password>

- 認証パスワード
  認証パスワードを、0x21,0x23〜0x7e の文字で構成される 128 文字以内の文字列を指定します。
  show コマンドで表示される暗号化された認証パスワードを encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化認証パスワード指定
  <password>に暗号化された認証パスワードを設定する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

MAC アドレス認証にて使用する、認証情報 (認証パスワード) を設定します。
本コマンドが未設定の場合は、認証端末の MAC アドレスが認証情報として使用されます。

[注意]

- show コマンドでは、暗号化された認証パスワードが encrypted と共に表示されます。

[未設定時]

MAC アドレス認証情報を認証端末の MAC アドレスを使用するものとみなされます。

19.10　その他

19.10.1　addact

[機能]

コマンド実行予約の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

addact <index> <date> <command>

[オプション]

<index>

- 登録番号
  コマンド実行予約情報の登録番号を指定します。
  必ず 0 を指定してください。

<date>

- 実行日時
  コマンド実行日時を、yymmddHHMM の形式で指定します。

yy	西暦の下 2 桁を指定します。西暦 2036 年まで指定できます。
mm	月を、1〜12 の 10 進数値で指定します。
dd	日付を、1〜31 の 10 進数値で指定します。
HH	時間を、0〜23 の 10 進数値で指定します。
MM	分を、0〜59 の 10 進数値で指定します。

<command>

実行するコマンド文字列を指定します。

- reset config1
  構成定義 1 に切り替えて再起動する場合に指定します。
- reset config2
  構成定義 2 に切り替えて再起動する場合に指定します。

上記以外のコマンドを指定した場合の動作は保証されません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

コマンド実行予約を設定します。

[注意]

以下に、スケジュール機能によってコマンドを実行する場合の注意事項を示します。

- 装置の時刻を正しく設定してください。
- 実施時刻に、装置の電源を投入しておいてください。

[実行例]

以下に、1999 年 1 月 1 日 午前 2 時 に構成定義 2 に切り替えて再起動する場合の設定例を示します。

```
# addact 0 9901010200 reset config2
# show addact
0 9901010200 reset config2
#
```

[未設定時]

コマンド の実行予約を行わないものとみなされます。

19.10.2　watchdog service

[機能]

ウォッチドッグリセットの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

watchdog service <mode>

[オプション]

<mode>

- on
  ウォッチドッグリセット機能を起動する場合に指定します。
- off
  ウォッチドッグリセット機能を停止する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ウォッチドッグリセット機能の起動または停止を設定します。
<mode>に"on"を指定した場合、本装置がハングアップすると 16～48 秒以内にリセットがかかり再起動します。
<mode>に"off"を指定した場合、本装置がハングアップしてもリセットがかかりません。
本設定は構成定義を保存したあと、本装置のリセットまたは電源の再投入を行うことによって反映されます。

[未設定時]

ウォッチドッグリセット機能は起動とみなされます。

```
watchdog service on
```

19.10.3 consoleinfo

[機能]

シリアルコンソール接続サービスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

consoleinfo autologout <time>

[オプション]

<time>

- 強制ログアウト時間

  シリアルコンソールでログインしたままコマンド実行が行われない状態が続いたときに強制ログアウトさせる時間を、0 秒〜86400 秒 (1 日) の範囲で指定します。

  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。

  0 秒を指定した場合は、強制ログアウトしません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

シリアルコンソールでログインしたまま<time>で指定した時間内にコマンド実行されなかった場合、強制的にログアウトさせるように設定します。

[未設定時]

強制ログアウトさせないものとみなされます。

```
consoleinfo autologout 0s
```

19.10.4　telnetinfo

[機能]

TELNET 接続サービスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

telnetinfo autologout <time>

[オプション]

<time>

- 自動切断時間

  telnet 接続したクライアントからコマンド入出力が行われない状態で自動切断するまでの時間を、0 秒～86400 秒 (1 日) の範囲で指定します。

  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

TELNET コネクションの入出力がない場合にコネクションを切断するまでの時間を設定します。

[未設定時]

TELNET コネクションの入出力の監視を行わないものとみなされます。

```
telnetinfo autologout 0s
```

19.10.5 sysdown harderr fan

[機能]

冷却ファン異常時の動作の設定

[適用機種]

Si-R 570 | Si-R 370

[入力形式]

sysdown harderr fan <mode>

[オプション]

<mode>

- yes
  システムダウンさせる場合に指定します。
- no
  運用を継続する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

冷却ファン異常 (複数ある場合はすべての冷却ファン異常) 発生時の動作を設定します。
また、Si-R570 では以下のコマンド を使用して、システムダウン時に本装置の電源を切断するかどうかを設定することができます。

- sysdown power <mode>

[未設定時]

冷却ファン異常時に運用を継続するものとみなされます。

```
sysdown harderr fan no
```

19.10.6　sysdown harderr thermal

[機能]

温度異常時の動作の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B

[入力形式]

sysdown harderr thermal <mode>

[オプション]

<mode>

- yes
  システムダウンさせる場合に指定します。
- no
  運用を継続する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

温度異常時の動作を設定します。
また、Si-R570 では以下のコマンド を使用して、システムダウン時に本装置の電源を切断するかどうかを設定することができます。

- sysdown power <mode>

[未設定時]

温度異常時に運用を継続するものとみなされます。

```
sysdown harderr thermal no
```

19.10.7 sysdown power

[機能]

冷却ファン／温度異常時の電源制御の設定

[適用機種]

Si-R 570

[入力形式]

sysdown power <mode>

[オプション]

<mode>

冷却ファン異常 (複数ある場合はすべての冷却ファン異常)、または温度異常を検出した場合に、電源を切断するかどうかを指定します。

- off
  本装置の電源を切断します。
- on
  本装置の電源を切断しません。このとき、本装置はコンソールポートだけ使用可、その他の通信はすべて不可となります。

[動作モード]

構成定義モード (管理者クラス)

[説明]

冷却ファン異常 (複数ある場合はすべての冷却ファン異常)、または温度異常を検出した場合に、本装置の電源を切断するかどうかを設定します。
本設定は、以下のコマンドを使用し、冷却ファン／温度異常時にシステムダウンさせる設定を行った場合に有効です。

- sysdown harderr fan yes
- sysdown harderr thermal yes

電源を切断しない設定の場合、本装置はコンソールポートだけ使用可、その他の通信はすべて不可となります。

[未設定時]

冷却ファン異常 (複数ある場合はすべての冷却ファン異常)、または温度異常を検出した場合に、本装置の電源を切断するものとみなされます。

```
sysdown power off
```

19.10.8　mflag

[機能]

CE 保守ログインの可否の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

mflag <mode>

[オプション]

<mode>

- on
  CE 専用パスワードによるログインを許可する場合に指定します。
- off
  CE 専用パスワードによるログインを拒否する場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

CE 保守ログインを許可するかどうかを設定します。

[未設定時]

CE 専用パスワードによるログインを拒否するものとみなされます。

```
mflag off
```

19.10.9 sysname

[機能]

本装置の名称の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

sysname <name>

[オプション]

<name>

- 名称
  本装置の名称を、0x21,0x23～0x7e の 32 文字以内の ASCII 文字列で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本装置の名称を設定します。
ここで設定した名称は、DHCP クライアント機能で DHCP サーバに対して広報されます。
本コマンドで設定する名称は、SNMP で使用する MIB 変数 sysName としても使用することができます。その場合、snmp agent sysname コマンドで設定している sysName を削除しておくことで本コマンドで設定したホスト名が sysName として使用されます。
本コマンドと snmp agent sysname コマンドとはネットワーク動作として直接の関連性はありませんが、ネットワークの管理上、同じ名称に統一するべきです。

[未設定時]

本装置の名称を設定しないものとみなされます。

19.10.10　loopback ip address

[機能]

loopback インタフェース追加 IP アドレスの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

loopback ip address [<number>] <address>

[オプション]

<number>

- 追加 IP アドレス定義番号

  追加 IP アドレス定義番号として 0 を指定します。

  省略時は、0 とを指定したものとみなされます。

<address>

- IP アドレス

  loopback インタフェースに割り当てる IP アドレスを指定します。IP アドレスに 0.0.0.0 を指定するとその定義番号を持った IP アドレスを無効にします。

  loopback インタフェースに割り当てた IP アドレスを通信に使う場合は、以下の範囲で通信可能なアドレスを設定してください。

  1.0.0.1 ～ 126.255.255.254

  128.0.0.1 ～ 191.255.255.254

  192.0.0.1 ～ 223.255.255.254

[動作モード]

構成定義モード (管理者クラス)

[説明]

loopback インタフェースに追加 IP アドレスを設定します。
なお、loopback インタフェースの IP アドレスとしてはすでに 127.0.0.1 が設定されています。

[注意]

loopback インタフェースにはホストアドレスだけ設定可能であり、ネットマスク長は 32 固定です。
ほかのインタフェースと違うネットワークの IP アドレスを設定する必要があります。

[未設定時]

追加 IP アドレスなしとしてみなします。

```
loopback ip address <number> 0.0.0.0
```

19.10.11 loopback ip ospf use

[機能]

OSPF 利用可否の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

loopback ip ospf use <mode> [<area_number>]

[オプション]

<mode>

- off
  OSPF を利用しません。
- on
  OSPF を利用します。

<area_number>

- エリア定義番号
  OSPF を利用する場合は、エリアの定義番号を指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0〜9	Si-R570
0〜3	Si-R370
0〜2	Si-R260B Si-R240 Si-R220B
0〜1	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

loopback インタフェースで OSPF を利用するかどうかと、属するエリアの定義番号を設定します。
<mode>で on を設定した場合でも、127.0.0.1 の IP アドレスは OSPF の対象外となります。
OSPF は、本装置全体で以下の数まで定義できます。

最大定義数	機種
100	Si-R570 Si-R370 Si-R260B Si-R240 Si-R220B
50	Si-R180

[注意]

OSPF の利用は、"ospf ip area id"を設定した場合にだけ有効です。

[未設定時]

OSPF を使用しないものとみなされます。

```
loopback ip ospf use off
```

19.10.12 loopback mpls ldp interface-label

[機能]

PHP の無効化

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

loopback mpls ldp interface-label <mode>

[オプション]

<mode>

- off
  インタフェースの IP アドレスにラベルを割り当てません。
- on
  インタフェースの IP アドレスにラベルを割り当てます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

インタフェースの IP アドレスに対してラベルを割り当てるかどうかを指定します。
割り当てた場合は、インタフェースあての LSP の PHP を無効にすることができます。

[注意]

MPLS トンネル接続機能を使用する場合、自側エンドポイントと IP アドレスが同一のとき、本設定に依らず、PHP 機能は無効となります。

[未設定時]

off が選択されたものとして動作します。

```
loopback mpls ldp interface-label off
```

19.10.13　serverinfo ftp

[機能]

FTP サーバ機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo ftp ip <mode>

[オプション]

<mode>

- on
  FTP サーバ機能を有効にします。
- off
  FTP サーバ機能を停止します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

FTP サーバ機能を有効にするかどうかを設定します。

[未設定時]

FTP サーバ機能を有効にするとみなされます。

```
serverinfo ftp ip on
```

19.10.14 serverinfo ftp ip6

[機能]

FTP サーバ機能の IPv6 の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo ftp ip6 <mode>

[オプション]

<mode>

- on
  FTP サーバ機能の IPv6 を有効にします。
- off
  FTP サーバ機能の IPv6 を停止します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

FTP サーバ機能の IPv6 を有効にするかどうかを設定します。

[未設定時]

FTP サーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo ftp ip6 on
```

19.10.15　serverinfo ftp filter

[機能]

FTP サーバ機能に対するアプリケーションフィルタ設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo ftp filter <count> <action> acl <acl_count>

[オプション]

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0～9	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B　Si-R180

<action>

フィルタリング条件に一致した場合の動作を指定します。

- accept
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、そのフィルタ定義は無効となり、無視されます。
  アプリケーションフィルタでは、ACL の以下の定義を使用します。
  - ip
    送信元 IP アドレスとマスクビット数のみを使用します。
    ip 値が設定されていない場合、IPv4 に対するフィルタ定義は無効となり、無視されます。
  - ip6
    送信元 IPv6 アドレスとプレフィックス長のみを使用します。
    ip6 値が設定されていない場合、IPv6 に対するフィルタ定義は無効となり、無視されます。

範囲	機種
0～2999	Si-R570
0～1499	Si-R370
0～299	Si-R260B　Si-R240　Si-R220B
0～149	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

FTP サーバ機能に対するアプリケーションフィルタを設定します。

[未設定時]

FTP サーバ機能に対するアプリケーションフィルタを設定しないものとみなされます。

19.10.16　serverinfo ftp filter move

[機能]

FTP サーバ機能に対するアプリケーションフィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo ftp filter move <count> <new_count>

[オプション]

<count>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0～9	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B　Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

FTP サーバ機能に対するアプリケーションフィルタの優先順序を変更します。

19.10.17 serverinfo ftp filter default

[機能]

FTP サーバ機能に対するアプリケーションフィルタのデフォルト動作設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo ftp filter default <action>

[オプション]

<action>

FTP サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- accept
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

FTP サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

どのアプリケーションフィルタテーブルにも一致しないパケットは透過します。

```
serverinfo ftp filter default accept
```

19.10.18　serverinfo sftp

[機能]

SSH FTP サーバ機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo sftp ip <mode>

[オプション]

<mode>

- on
  SSH FTP サーバ機能を有効にします。
- off
  SSH FTP サーバ機能を停止します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

SSH FTP サーバ機能を有効にするかどうかを設定します。
本設定が off、かつ、serverinfo ssh ip コマンドの設定が off の場合、sftp クライアントからの IPv4 アドレスでの接続要求は拒否されます。
本設定が off、かつ、serverinfo ssh ip コマンドの設定が on の場合、sftp クライアントからの IPv4 アドレスでの接続要求はパスワード入力したあとに拒否されます。

[注意]

本設定を有効にすると、本装置電源投入時および reset コマンド実行時に SSH ホスト認証鍵を生成するようになり、数十秒～数分の処理時間を要します。
SSH ホスト認証鍵の生成が完了したあとに sftp 接続できるようになります。
ssh および sftp 機能をすべて off の状態で本装置を起動して本機能を有効にした場合にも SSH ホスト認証鍵を生成し、数十秒から数分の処理時間を要します。その場合、セッション監視タイムアウトが発生するなど、ほかの処理に影響することが考えられますので、ご注意ください。

[未設定時]

SSH FTP サーバ機能を有効にするとみなされます。

```
serverinfo sftp ip on
```

19.10.19 serverinfo sftp ip6

[機能]

SSH FTP サーバ機能の IPv6 の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo sftp ip6 <mode>

[オプション]

<mode>

- on
  SSH FTP サーバ機能の IPv6 を有効にします。
- off
  SSH FTP サーバ機能の IPv6 を停止します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

SSH FTP サーバ機能の IPv6 を有効にするかどうかを設定します。
本設定が off、かつ、serverinfo ssh ip6 コマンドの設定が off の場合、sftp クライアントからの IPv6 アドレスでの接続要求は拒否されます。
本設定が off、かつ、serverinfo ssh ip6 コマンドの設定が on の場合、sftp クライアントからの IPv6 アドレスでの接続要求はパスワード入力したあとに拒否されます。

[注意]

本設定を有効にすると、本装置電源投入時および reset コマンド実行時に SSH ホスト認証鍵を生成するようになり、数十秒～数分の処理時間を要します。
SSH ホスト認証鍵の生成が完了したあとに sftp 接続できるようになります。
ssh および sftp 機能をすべて off の状態で本装置を起動して本機能を有効にした場合にも SSH ホスト認証鍵を生成し、数十秒から数分の処理時間を要します。その場合、セッション監視タイムアウトが発生するなど、ほかの処理に影響することが考えられますので、ご注意ください。

[未設定時]

SSH FTP サーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo sftp ip6 on
```

19.10.20　serverinfo telnet

[機能]

TELNET サーバ機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo telnet ip <mode>

[オプション]

<mode>

- on
  TELNET サーバ機能を有効にします。
- off
  TELNET サーバ機能を停止します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

TELNET サーバ機能を有効にするかどうかを設定します。

[未設定時]

TELNET サーバ機能を有効にするとみなされます。

```
serverinfo telnet ip on
```

19.10.21 serverinfo telnet ip6

[機能]

TELNET サーバ機能の IPv6 の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo telnet ip6 <mode>

[オプション]

<mode>

- on
  TELNET サーバ機能を有効にします。
- off
  TELNET サーバ機能を停止します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

TELNET サーバ機能の IPv6 を有効にするかどうかを設定します。

[未設定時]

TELNET サーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo telnet ip6 on
```

19.10.22　serverinfo telnet filter

[機能]

TELNET サーバ機能に対するアプリケーションフィルタ設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo telnet filter <count> <action> acl <acl_count>

[オプション]

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜9	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B　Si-R180

<action>

フィルタリング条件に一致した場合の動作を指定します。

- accept
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、そのフィルタ定義は無効となり、無視されます。
  アプリケーションフィルタでは、ACL の以下の定義を使用します。
  - ip
    送信元 IP アドレスとマスクビット数のみを使用します。
    ip 値が設定されていない場合、IPv4 に対するフィルタ定義は無効となり、無視されます。
  - ip6
    送信元 IPv6 アドレスとプレフィックス長のみを使用します。
    ip6 値が設定されていない場合、IPv6 に対するフィルタ定義は無効となり、無視されます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B　Si-R240　Si-R220B
0〜149	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

TELNET サーバ機能に対するアプリケーションフィルタを設定します。

[未設定時]

TELNET サーバ機能に対するアプリケーションフィルタを設定しないものとみなされます。

19.10.23　serverinfo telnet filter move

[機能]

TELNET サーバ機能に対するアプリケーションフィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo telnet filter move <count> <new_count>

[オプション]

<count>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0～9	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B　Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

TELNET サーバ機能に対するアプリケーションフィルタの優先順序を変更します。

19.10.24 serverinfo telnet filter default

[機能]

TELNET サーバ機能に対するアプリケーションフィルタのデフォルト動作設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo telnet filter default <action>

[オプション]

<action>

TELNET サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- accept
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

TELNET サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

どのアプリケーションフィルタテーブルにも一致しないパケットは透過します。

```
serverinfo telnet filter default accept
```

19.10.25　serverinfo ssh

[機能]

SSH ログインサーバ機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo ssh ip <mode>

[オプション]

<mode>

- on
  SSH ログインサーバ機能を有効にします。
- off
  SSH ログインサーバ機能を停止します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

SSH ログインサーバ機能を有効にするかどうかを設定します。
本設定が off、かつ、serverinfo sftp ip コマンドの設定が off の場合、ssh クライアントからの IPv4 アドレスでの接続要求は拒否されます。
本設定が off、かつ、serverinfo sftp ip コマンドの設定が on の場合、ssh クライアントからの IPv4 アドレスでの接続要求はパスワード入力したあとに拒否されます。

[注意]

本設定を有効にすると、本装置電源投入時および reset コマンド実行時に SSH ホスト認証鍵を生成するようになり、数十秒～数分の処理時間を要します。
SSH ホスト認証鍵の生成が完了したあとに ssh 接続できるようになります。
ssh および sftp 機能をすべて off の状態で本装置を起動して本機能を有効にした場合にも SSH ホスト認証鍵を生成し、数十秒から数分の処理時間を要します。その場合、セッション監視タイムアウトが発生するなど、ほかの処理に影響することが考えられますので、ご注意ください。

[未設定時]

SSH ログインサーバ機能を有効にするとみなされます。

```
serverinfo ssh ip on
```

19.10.26 serverinfo ssh ip6

[機能]

SSH ログインサーバ機能の IPv6 の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo ssh ip6 <mode>

[オプション]

<mode>

- on
  SSH ログインサーバ機能の IPv6 を有効にします。
- off
  SSH ログインサーバ機能の IPv6 を停止します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

SSH ログインサーバ機能の IPv6 を有効にするかどうかを設定します。
本設定が off、かつ、serverinfo sftp ip6 コマンドの設定が off の場合、ssh クライアントからの IPv6 アドレスでの接続要求は拒否されます。
本設定が off、かつ、serverinfo sftp ip6 コマンドの設定が on の場合、ssh クライアントからの IPv6 アドレスでの接続要求はパスワード入力したあとに拒否されます。

[注意]

本設定を有効にすると、本装置電源投入時および reset コマンド実行時に SSH ホスト認証鍵を生成するようになり、数十秒～数分の処理時間を要します。
SSH ホスト認証鍵の生成が完了したあとに ssh 接続できるようになります。
ssh および sftp 機能をすべて off の状態で本装置を起動して本機能を有効にした場合にも SSH ホスト認証鍵を生成し、数十秒から数分の処理時間を要します。その場合、セッション監視タイムアウトが発生するなど、ほかの処理に影響することが考えられますので、ご注意ください。

[未設定時]

SSH ログインサーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo ssh ip6 on
```

19.10.27　serverinfo ssh filter

[機能]

SSH サーバ機能に対するアプリケーションフィルタ設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo ssh filter <count> <action> acl <acl_count>

[オプション]

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0～9	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B　Si-R180

<action>

フィルタリング条件に一致した場合の動作を指定します。

- accept
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、そのフィルタ定義は無効となり、無視されます。
  アプリケーションフィルタでは、ACL の以下の定義を使用します。
  - ip
    送信元 IP アドレスとマスクビット数のみを使用します。
    ip 値が設定されていない場合、IPv4 に対するフィルタ定義は無効となり、無視されます。
  - ip6
    送信元 IPv6 アドレスとプレフィックス長のみを使用します。
    ip6 値が設定されていない場合、IPv6 に対するフィルタ定義は無効となり、無視されます。

範囲	機種
0～2999	Si-R570
0～1499	Si-R370
0～299	Si-R260B　Si-R240　Si-R220B
0～149	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

SSH サーバ機能に対するアプリケーションフィルタを設定します。
本定義は、SSH ログインサーバ機能および SSH FTP サーバ機能の両方に対して有効となります。
SSH ログインサーバ機能、SSH FTP サーバ機能にそれぞれ異なるフィルタ設定をすることはできません。

[未設定時]

SSH サーバ機能に対するアプリケーションフィルタを設定しないものとみなされます。

19.10.28　serverinfo ssh filter move

[機能]

SSH サーバ機能に対するアプリケーションフィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo ssh filter move <count> <new_count>

[オプション]

<count>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0～9	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B　Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

SSH サーバ機能に対するアプリケーションフィルタの優先順序を変更します。

19.10.29 serverinfo ssh filter default

[機能]

SSH サーバ機能に対するアプリケーションフィルタのデフォルト動作設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo ssh filter default <action>

[オプション]

<action>

SSH サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- accept
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

SSH サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

どのアプリケーションフィルタテーブルにも一致しないパケットは透過します。

```
serverinfo ssh filter default accept
```

19.10.30　serverinfo http

[機能]

HTTP サーバ機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo http ip <mode>

[オプション]

<mode>

- on
  HTTP サーバ機能を有効にします。
- off
  HTTP サーバ機能を停止します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

HTTP サーバ機能を有効にするかどうかを設定します。

[未設定時]

HTTP サーバ機能を有効にするとみなされます。

```
serverinfo http ip on
```

19.10.31 serverinfo http ip6

[機能]

HTTP サーバ機能の IPv6 の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo http ip6 <mode>

[オプション]

<mode>

- on
  HTTP サーバ機能を有効にします。
- off
  HTTP サーバ機能を停止します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

HTTP サーバ機能の IPv6 を有効にするかどうかを設定します。

[未設定時]

HTTP サーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo http ip6 on
```

19.10.32　serverinfo http filter

[機能]

HTTP サーバ機能に対するアプリケーションフィルタ設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo http filter <count> <action> acl <acl_count>

[オプション]

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0～9	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B　Si-R180

<action>

フィルタリング条件に一致した場合の動作を指定します。

- accept
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、そのフィルタ定義は無効となり、無視されます。
  アプリケーションフィルタでは、ACL の以下の定義を使用します。
  - ip
    送信元 IP アドレスとマスクビット数のみを使用します。
    ip 値が設定されていない場合、IPv4 に対するフィルタ定義は無効となり、無視されます。
  - ip6
    送信元 IPv6 アドレスとプレフィックス長のみを使用します。
    ip6 値が設定されていない場合、IPv6 に対するフィルタ定義は無効となり、無視されます。

範囲	機種
0～2999	Si-R570
0～1499	Si-R370
0～299	Si-R260B　Si-R240　Si-R220B
0～149	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

HTTP サーバ機能に対するアプリケーションフィルタを設定します。

[未設定時]

HTTP サーバ機能に対するアプリケーションフィルタを設定しないものとみなされます。

19.10.33　serverinfo http filter move

[機能]

HTTP サーバ機能に対するアプリケーションフィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo http filter move <count> <new_count>

[オプション]

<count>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0～9	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B　Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

HTTP サーバ機能に対するアプリケーションフィルタの優先順序を変更します。

19.10.34 serverinfo http filter default

[機能]

HTTP サーバ機能に対するアプリケーションフィルタのデフォルト動作設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo http filter default <action>

[オプション]

<action>

HTTP サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- accept
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

HTTP サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

どのアプリケーションフィルタテーブルにも一致しないパケットは透過します。

```
serverinfo http filter default accept
```

19.10.35　serverinfo dns

[機能]

DNS サーバ機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo dns ip <mode>

[オプション]

<mode>

- on
  DNS サーバ機能を有効にします。
- off
  DNS サーバ機能を停止します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

DNS サーバ (スタティック) 機能および ProxyDNS 機能を有効にするかどうかを設定します。

[未設定時]

DNS サーバ機能を有効にするとみなされます。

```
serverinfo dns ip on
```

19.10.36 serverinfo dns ip6

[機能]

DNS サーバ機能の IPv6 の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo dns ip6 <mode>

[オプション]

<mode>

- on
  DNS サーバ機能を有効にします。
- off
  DNS サーバ機能を停止します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

DNS サーバ (スタティック) 機能および ProxyDNS 機能の IPv6 を有効にするかどうかを設定します。

[未設定時]

DNS サーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo dns ip6 on
```

19.10.37　serverinfo dns filter

[機能]

DNS サーバ機能に対するアプリケーションフィルタ設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo dns filter <count> <action> acl <acl_count>

[オプション]

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜9	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B　Si-R180

<action>

フィルタリング条件に一致した場合の動作を指定します。

- accept
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、そのフィルタ定義は無効となり、無視されます。
  アプリケーションフィルタでは、ACL の以下の定義を使用します。
  - ip
    送信元 IP アドレスとマスクビット数のみを使用します。
    ip 値が設定されていない場合、IPv4 に対するフィルタ定義は無効となり、無視されます。
  - ip6
    送信元 IPv6 アドレスとプレフィックス長のみを使用します。
    ip6 値が設定されていない場合、IPv6 に対するフィルタ定義は無効となり、無視されます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B　Si-R240　Si-R220B
0〜149	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

DNS サーバ機能に対するアプリケーションフィルタを設定します。

[未設定時]

DNS サーバ機能に対するアプリケーションフィルタを設定しないものとみなされます。

19.10.38　serverinfo dns filter move

[機能]

DNS サーバ機能に対するアプリケーションフィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo dns filter move <count> <new_count>

[オプション]

<count>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0～9	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B　Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

DNS サーバ機能に対するアプリケーションフィルタの優先順序を変更します。

19.10.39 serverinfo dns filter default

[機能]

DNS サーバ機能に対するアプリケーションフィルタのデフォルト動作設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo dns filter default <action>

[オプション]

<action>

DNS サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- accept
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

DNS サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

どのアプリケーションフィルタテーブルにも一致しないパケットは透過します。

```
serverinfo dns filter default accept
```

19.10.40　serverinfo sntp

[機能]

SNTP サーバ機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo sntp ip <mode>

[オプション]

<mode>

- on
  SNTP サーバ機能を有効にします。
- off
  SNTP サーバ機能を停止します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

SNTP サーバ機能を有効にするかどうかを設定します。

[未設定時]

SNTP サーバ機能を有効にするとみなされます。

```
serverinfo sntp ip on
```

19.10.41 serverinfo sntp ip6

[機能]

SNTP サーバ機能の IPv6 の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo sntp ip6 <mode>

[オプション]

<mode>

- on
  SNTP サーバ機能を有効にします。
- off
  SNTP サーバ機能を停止します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

SNTP サーバ機能の IPv6 を有効にするかどうかを設定します。

[未設定時]

SNTP サーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo sntp ip6 on
```

19.10.42　serverinfo sntp filter

[機能]

SNTP サーバ機能に対するアプリケーションフィルタ設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo sntp filter <count> <action> acl <acl_count>

[オプション]

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0～9	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B　Si-R180

<action>

フィルタリング条件に一致した場合の動作を指定します。

- accept
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、そのフィルタ定義は無効となり、無視されます。
  アプリケーションフィルタでは、ACL の以下の定義を使用します。
  - ip
    送信元 IP アドレスとマスクビット数のみを使用します。
    ip 値が設定されていない場合、IPv4 に対するフィルタ定義は無効となり、無視されます。
  - ip6
    送信元 IPv6 アドレスとプレフィックス長のみを使用します。
    ip6 値が設定されていない場合、IPv6 に対するフィルタ定義は無効となり、無視されます。

範囲	機種
0～2999	Si-R570
0～1499	Si-R370
0～299	Si-R260B　Si-R240　Si-R220B
0～149	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

SNTP サーバ機能に対するアプリケーションフィルタを設定します。

[未設定時]

SNTP サーバ機能に対するアプリケーションフィルタを設定しないものとみなされます。

19.10.43　serverinfo sntp filter move

[機能]

SNTP サーバ機能に対するアプリケーションフィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo sntp filter move <count> <new_count>

[オプション]

<count>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0～9	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B　Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

SNTP サーバ機能に対するアプリケーションフィルタの優先順序を変更します。

19.10.44 serverinfo sntp filter default

[機能]

SNTP サーバ機能に対するアプリケーションフィルタのデフォルト動作設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo sntp filter default <action>

[オプション]

<action>

SNTP サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- accept
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

SNTP サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

どのアプリケーションフィルタテーブルにも一致しないパケットは透過します。

```
serverinfo sntp filter default accept
```

19.10.45　serverinfo time ip tcp

[機能]

TCP による TIME サーバ機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo time ip tcp <mode>

[オプション]

<mode>

- on
  TCP による TIME サーバ機能を有効にします。
- off
  TCP による TIME サーバ機能を停止します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

TCP による TIME サーバ機能を有効にするかどうかを設定します。

[未設定時]

TCP による TIME サーバ機能を有効にするとみなされます。

```
serverinfo time ip tcp on
```

19.10.46 serverinfo time ip6 tcp

[機能]

TCP による TIME サーバ機能の IPv6 の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo time ip6 tcp <mode>

[オプション]

<mode>

- on
  TCP による TIME サーバ機能を有効にします。
- off
  TCP による TIME サーバ機能を停止します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

TCP による TIME サーバ機能の IPv6 を有効にするかどうかを設定します。

[未設定時]

TCP による TIME サーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo time ip6 tcp on
```

19.10.47　serverinfo time ip udp

[機能]

UDP による TIME サーバ機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo time ip udp <mode>

[オプション]

<mode>

- on
  UDP による TIME サーバ機能を有効にします。
- off
  UDP による TIME サーバ機能を停止します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

UDP による TIME サーバ機能を有効にするかどうかを設定します。

[未設定時]

UDP による TIME サーバ機能を有効にするとみなされます。

```
serverinfo time ip udp on
```

19.10.48 serverinfo time ip6 udp

[機能]

UDP による TIME サーバ機能の IPv6 の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo time ip6 udp <mode>

[オプション]

<mode>

- on
  UDP による TIME サーバ機能を有効にします。
- off
  UDP による TIME サーバ機能を停止します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

UDP による TIME サーバ機能の IPv6 を有効にするかどうかを設定します。

[未設定時]

UDP による TIME サーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo time ip6 udp on
```

19.10.49　serverinfo time filter

[機能]

TIME サーバ機能に対するアプリケーションフィルタ設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo time filter <count> <action> acl <acl_count>

[オプション]

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜9	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B　Si-R180

<action>

フィルタリング条件に一致した場合の動作を指定します。

- accept
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。

<acl_count>

- ACL 定義番号
  使用する ACL 定義の番号を、10 進数値で指定します。
  指定した<acl_count>の ACL が定義されていない場合、そのフィルタ定義は無効となり、無視されます。
  アプリケーションフィルタでは、ACL の以下の定義を使用します。
  - ip
    送信元 IP アドレスとマスクビット数のみを使用します。
    ip 値が設定されていない場合、IPv4 に対するフィルタ定義は無効となり、無視されます。
  - ip6
    送信元 IPv6 アドレスとプレフィックス長のみを使用します。
    ip6 値が設定されていない場合、IPv6 に対するフィルタ定義は無効となり、無視されます。

範囲	機種
0〜2999	Si-R570
0〜1499	Si-R370
0〜299	Si-R260B　Si-R240　Si-R220B
0〜149	Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

TIME サーバ機能に対するアプリケーションフィルタを設定します。

[未設定時]

TIME サーバ機能に対するアプリケーションフィルタを設定しないものとみなされます。

19.10.50　serverinfo time filter move

[機能]

TIME サーバ機能に対するアプリケーションフィルタの優先順序の変更

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo time filter move <count> <new_count>

[オプション]

<count>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0～9	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B　Si-R180

[動作モード]

構成定義モード (管理者クラス)

[説明]

TIME サーバ機能に対するアプリケーションフィルタの優先順序を変更します。

19.10.51 serverinfo time filter default

[機能]

TIME サーバ機能に対するアプリケーションフィルタのデフォルト動作設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

serverinfo time filter default <action>

[オプション]

<action>

TIME サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- accept
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

TIME サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

どのアプリケーションフィルタテーブルにも一致しないパケットは透過します。

```
serverinfo time filter default accept
```

第 20 章　構成定義情報表示、削除、および操作コマンド

20.1 構成定義情報表示

20.1.1 show candidate-config

[機能]

編集中構成定義情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show candidate-config [all] [<config>]

[オプション]

all

未設定時値も含むすべての構成定義情報を表示します。
省略時は、未設定時値から変更されている構成定義情報のみを表示します。

<config>

<config>で始まる構成定義情報を表示します。
表示される構成定義情報には<config>部分は含まれません。
省略時は、すべての構成定義情報を表示します。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

現在編集中の構成定義情報を表示します。

[実行例]

```
# show candidate-config lan 0
mode auto
ip address 192.168.0.1/24 3
ip rip use v1 v1 0 off
#
```

20.1.2　show running-config

[機能]

動作中構成定義情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show running-config [all] [<config>]

[オプション]

all

未設定時値も含むすべての構成定義情報を表示します。
省略時は、未設定時値から変更されている構成定義情報のみを表示します。

<config>

<config>で始まる構成定義情報を表示します。
表示される構成定義情報には<config>部分は含まれません。
省略時は、すべての構成定義情報を表示します。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

現在動作中の構成定義情報を表示します。

[実行例]

```
# show running-config lan 1
mode auto
ip address 192.168.1.1/24 3
ip rip use v1 v1 0 off
```

20.1.3 show startup-config

[機能]

起動用構成定義情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show startup-config [<config>]

[オプション]

<config>

<config>で始まる構成定義情報を表示します。
<config>には show running-config または show candidate-config で表示されるとおりに、省略可能オプションも省略しないで、数字も表示どおりの文字列で指定してください。
表示される構成定義情報には<config>部分は含まれません。
省略時は、すべての構成定義情報を表示します。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

起動時に使用した構成定義情報、または保存してある起動用構成定義情報を表示します。

[実行例]

```
# show startup-config
lan 0 mode auto
lan 0 ip address 192.168.0.1/24 3
lan 0 ip rip use v1 v1 0 off
lan 1 mode auto
lan 1 ip address 192.168.1.1/24 3
lan 1 ip rip use v1 v1 0 off
syslog pri error,warn,info
syslog facility 23
telnetinfo autologout 5m
time zone 0900
```

20.1.4　diff

[機能]

構成定義情報の差分の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

diff <src_filename> <dst_filename>

[オプション]

<src_filename> <dst_filename>

<src_filename>に比較元の構成定義ファイルを、<dst_filename>に比較先の構成定義情報を指定します。

- running-config
  運用中の構成定義ファイル
- candidate-config
  編集中の構成定義ファイル
- startup-config
  起動用の構成定義ファイル
- config1
  第 1 構成定義ファイル
- config2
  第 2 構成定義ファイル

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

指定された構成定義情報の差分を表示します。<src_filename>にのみ定義されている情報には行の先頭に"< "を、<dst_filename>にのみ定義されている情報には行の先頭に"> "を付加して定義順に表示します。

[実行例]

「編集中の構成定義情報」と「運用中の構成定義情報」の差分を表示する場合

```
# diff candidate-config running-config
===
> remote 0 name rmt0
> remote 1 name rmt1
===
< remote 3 name rmt3
< remote 4 name rmt4
< remote 5 name rmt5
< remote 6 name rmt6
---
> remote 3 name inter3
===
< remote 8 name rmt8
< remote 9 name rmt9
< remote 10 name rmt10
< syslog server 192.168.33.63
#
```

20.2 構成定義情報削除

20.2.1 delete

[機能]

編集中構成定義情報の削除

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

delete <config>

[オプション]

<config>

- 構成定義コマンド
  削除する構成定義コマンド名および引数を指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

指定した構成定義情報を削除して未設定状態にします。
<config>で指定したコマンド名と引数で始まるコマンドがすべて削除されます。
コマンド名だけを指定した場合は、そのコマンド名で始まる構成定義情報がすべて削除されます。
構成定義コマンドの引数がいくつまで指定できるかは、各コマンドによって異なりますが、大抵の場合、可変値の手前の引数まで指定できます。

[注意]

ログインパスワード情報は、以下のように set まで指定しないと削除できません。

```
delete password set
delete password user set
```

[実行例]

```
(config)# delete lan 0 ip dhcp          lan 0 の DHCP情報をすべて削除します
(config)# delete remote 1               remote 1 の 相手情報をすべて削除します
```

20.3　構成定義情報操作

20.3.1　load

[機能]

構成定義の読み込み

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

load <filename>

[オプション]

<filename>

読み込むファイル名を指定します。

- running-config
  運用中の構成定義ファイル
- startup-config
  起動用の構成定義ファイル
- config1
  第 1 構成定義ファイル
- config2
  第 2 構成定義ファイル

[動作モード]

構成定義モード (管理者クラス)

[説明]

指定した構成定義情報を読み込み、編集中の構成定義情報 (candidate-config) に上書きします。

[メッセージ]

```
load failed: config read error
```

本装置の通信負荷が高い状態などでは、上記のメッセージを出力し、コマンドが実行されないことがあります。
この場合は通信負荷を停止して再度本コマンドを実行してください。(※ Si-R180 を除く)

[実行例]

第 1 構成定義ファイルを読み込む場合

```
# load config1
#
```

20.3.2 save

[機能]

構成定義情報の保存

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

save [<filename>]

[オプション]

なし

編集中の構成定義情報 (candidate-config) を起動時の構成定義ファイルに保存します。

<filename>

編集中の構成定義情報 (candidate-config) を保存するファイル名を指定します。

- config1
  第 1 構成定義ファイル
- config2
  第 2 構成定義ファイル

[動作モード]

構成定義モード (管理者クラス)

[説明]

編集中の構成定義情報 (candidate-config) を指定したファイルに保存します。
ファイル名を省略時は、起動時の構成定義ファイルに保存します。

[実行例]

```
# save
#
```

20.3.3　commit

[機能]

構成定義情報の動的反映

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

commit

[オプション]

なし

[動作モード]

構成定義モード (管理者クラス)

[説明]

構成定義コマンドで設定または変更した構成定義情報を、装置の再起動を行わずに反映します。

[注意]

構成定義情報の変更内容によっては、装置内部のアドレス情報などを反映するために一度通信インタフェースがダウンして通信が途切れることがありますのでご注意ください。詳細は、「commit コマンド実行時の影響について」を参照してください。

[メッセージ]

```
<ERROR> Need to do reset after execute the save command.
```

反映ができない構成定義情報を追加または変更したため、構成定義情報を反映できません。
save コマンドを実行後に reset コマンドを実行して再起動してください。

```
<WARNING> The candidate-config is not changed.
```

構成定義情報を追加または変更していません。
commit コマンドを実行する必要はありません。

[実行例]

```
# commit
#
```

20.3.4 discard

[機能]

構成定義情報の変更破棄

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

discard

[オプション]

なし

[動作モード]

構成定義モード (管理者クラス)

[説明]

candidate-config の変更内容を破棄し、running-config と同じ内容に戻します。

[実行例]

```
# discard
```

第 21 章　モード 操作コマンド /ターミナル操作コマンド

21.1 モード操作

21.1.1 admin

[機能]

管理者クラスに移行する

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

admin

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス)

[説明]

一般ユーザクラスから管理者クラスに移行します。
su コマンドと同じ機能です。
移行する際にパスワードを尋ねられますので、管理者パスワードを入力してください。
管理者クラスから一般ユーザクラスに戻るには、exit, end, quit, ! コマンドを実行してください。

[注意]

terminal コマンドおよび alias コマンドで設定した内容は、管理者モードに引き継がれません。

[メッセージ]

```
Password:
```

管理者パスワードを入力してください。

```
<ERROR> Authentication failed
```

管理者パスワードが正しくないため、管理者クラスに移行できませんでした。
正しい管理者パスワードを入力してください。

[実行例]

```
> admin
Password:
# exit
>
```

21.1.2　su

[機能]

管理者クラスに移行する

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

su

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス)

[説明]

一般ユーザクラスから管理者クラスに移行します。
admin コマンド と同じ機能です。
移行する際にパスワード を尋ねられますので、管理者パスワード を入力してください。
管理者クラスから一般ユーザクラスに戻るには、exit, end, quit, ! コマンド を使用します。

[注意]

terminal コマンド および alias コマンド で設定した内容は、管理者モード に引き継がれません。

[メッセージ]

```
Password:
```

管理者パスワード を入力してください。

```
<ERROR> Authentication failed
```

管理者パスワード が正しくないため、管理者クラスに移行できませんでした。
正しい管理者パスワード を入力してください。

[実行例]

```
> su
Password:
#
```

21.1.3 exit

[機能]

クラス、モード、構成定義階層を戻る、または、ログアウトする

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

exit

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

運用管理モードでは、admin コマンドを実行して一般ユーザクラスから管理者クラスに移行していた場合は一般ユーザクラスに戻ります。それ以外の場合はログアウトします。
構成定義モードでは、構成定義階層機能が有効で最上位階層以外の場合はひとつ上位階層に移動します。それ以外の場合、構成定義を変更していなければ運用管理モードに戻り、構成定義を変更していればエラーメッセージが表示されて構成定義モードのままです。構成定義階層機能については configure コマンドを参照してください。

[メッセージ]

```
<ERROR> The candidate-config has been changed but not committed.
```

構成定義情報が反映されていません。
構成定義情報を反映してください。構成定義情報を反映しないで運用管理モードに戻る場合は、end コマンドまたは quit コマンドを使用してください。

[注意]

terminal コマンドおよび alias コマンドで設定した内容は、ログアウト時に破棄されます。

[実行例]

```
(config)# exit
<ERROR> The candidate-config has been changed but not committed.
(config)# end
<WARNING> The candidate-config has been changed but not committed.
# exit
Login:
```

21.1.4　configure

[機能]

構成定義モードに移行する

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

configure

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)

[説明]

運用管理モードから構成定義モードに移行します。
構成定義モードに移行してから Ctrl+O キーを入力すると、構成定義階層機能が有効になります。
構成定義階層機能を有効にすると、入力した構成定義コマンドに応じて階層を移動したように振舞い、構成定義階層以降の引数を入力するだけで構成定義コマンドを実行できます。階層移動している状態でもコマンド名から入力することで通常のコマンドも実行できます。
構成定義階層は入力プロンプトに表示されます。
構成定義階層機能を無効にするには、Ctrl+G キーを入力してください。
構成定義階層機能については、コマンドユーザズガイドの「シェルを使う」を参照してください。
構成定義モードから運用管理モードに戻るには、状況に応じて exit, end, quit, ! コマンドを実行してください。

[注意]

構成定義を変更した状態では exit コマンドおよび ! コマンドで運用管理モードに戻ることができません。
end コマンドまたは quit コマンドで強制的に運用管理モードに戻ることができます。
構成定義階層機能が有効なとき、terminal prompt コマンドで入力プロンプト文字列を変更して構成定義階層を含めていない場合は、入力プロンプトに構成定義階層は表示されません。

[実行例]

```
# configure
(config)#               (CTRL+Oキーを入力して構成定義階層機能を有効にする)
<NOTICE> Directory mode is enabled. To disable, type Ctrl+G.
(config)# lan 0 ip
(config-lan-0-ip)# address 192.168.0.1/24 3
(config-lan-0-ip)# show
address 192.168.0.1/24 3
(config-lan-0-ip)# show candidate-config
lan 0 ip address 192.168.0.1/24 3
(config-lan-0-ip)#     (Ctrl+gキーを入力して構成定義階層機能を無効にする)
<NOTICE> Directory mode is disabled.
(config)#
```

21.1.5 end

[機能]

運用管理モードに戻る

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

end

[オプション]

なし

[動作モード]

構成定義モード (管理者クラス)

[説明]

構成定義モードから運用管理モードに戻ります。
構成定義に変更がある場合はメッセージを表示して運用管理モードに戻ります。
quit コマンドと同じ機能です。

[メッセージ]

```
<WARNING> The candidate-config has been changed but not committed.
```

構成定義情報を反映しないで運用管理モードに戻りました。変更および追加した構成定義情報はそのまま残っています。
構成定義情報を反映しなくてよいか確認してください。

[実行例]

```
(config)# end
#
```

21.1.6　quit

[機能]

運用管理モード に戻る

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

quit

[オプション]

なし

[動作モード]

構成定義モード (管理者クラス)

[説明]

構成定義モード から運用管理モード に戻ります。
構成定義に変更がある場合はメッセージを表示して運用管理モード に戻ります。
end コマンド と同じ機能です。

[メッセージ]

```
<WARNING> The candidate-config has been changed but not committed.
```

構成定義情報を反映しないで運用管理モード に戻りました。変更および追加した構成定義情報はそのまま残っています。
構成定義情報を反映しなくてよいか確認してください。

[実行例]

```
(config)# quit
#
```

21.1.7 top

[機能]

構成定義階層を最上位階層に移動する

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

top

[オプション]

なし

[動作モード]

構成定義モード (管理者クラス)

[説明]

構成定義モードで構成定義階層機能が有効であれば、最上位階層に移動します。最上位階層の場合はそのままです。
構成定義階層機能が無効であれば、何もしません。
構成定義階層機能については configure コマンドを参照してください。

[実行例]

```
(config-lan-0-ip)# top                (lan 0 ip 階層で実行)
(config)#
```

21.1.8　up

[機能]

構成定義階層をひとつ上位階層に移動する

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

up

[オプション]

なし

[動作モード]

構成定義モード (管理者クラス)

[説明]

構成定義モード で構成定義階層機能が有効な場合、構成定義階層をひとつ上位階層に移動します。最上位階層の場合はそのままです。構成定義階層機能が無効であれば、何もしません。構成定義階層機能については configure コマンド を参照してください。

[実行例]

```
(config-lan-0-ip)# up                  (lan 0 ip 階層で実行)
(config-lan-0)#
```

21.1.9 !

[機能]

クラス、モード、構成定義階層を戻る

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

!

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

運用管理モードでは、admin コマンドを実行して一般ユーザクラスから管理者クラスに移行していた場合は一般ユーザクラスに戻ります。それ以外の場合は運用管理モードのままでログアウトはしません。
構成定義モードでは、構成定義階層機能が有効で最上位階層以外の場合はひとつ上位階層に移動します。それ以外の場合、構成定義を変更していなければ運用管理モードに戻り、構成定義を変更していればエラーメッセージが表示されて構成定義モードのままです。構成定義階層機能については configure コマンドを参照してください。
exit コマンドとほとんど同じ機能ですが、運用管理モードでログアウトしないことだけが異なります。

[実行例]

```
# configure                 (構成定義モードに移行)
(config)# !                 (運用管理モードに戻る)
# !                         (ログアウトはせずそのまま)
#
```

21.2　ターミナル操作

21.2.1　terminal pager

[機能]

ページャー機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

terminal pager {enable | disable}

[オプション]

enable

ページャ機能を使用します。

disable

ページャ機能を使用しません。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

ページャ機能を使用するかどうかを指定します。
ページャ機能を使用する場合、コマンドを実行したときにコマンドの表示出力が 1 画面分表示されたらキー入力待ちとなり、キー入力で続きを表示したり、表示をさかのぼって再表示することができます。コマンドの表示出力が 1 画面に満たない場合は、キー入力待ちにならずにコマンド実行が終了します。
ただし、一部のコマンドは表示量が多過ぎるため、さかのぼって再表示できなかったり、キー入力待ちすることなく最後まで表示されます。
ページャー機能はコマンド実行に対してのみ有効で、コマンド補完出力 (引数一覧表示、引数説明表示、コマンド形式表示) などに対しては機能しません。
端末の画面サイズは 24 行 80 桁であるものとして動作します。画面サイズが 24 行 80 桁以外の場合は、terminal window コマンドで行数と桁数を設定してください。設定しない場合は表示が乱れます。telnet か ssh でログインした場合は自動的に行数と桁数が設定されますが、もし画面表示が乱れる場合は terminal window コマンドで行数と桁数を設定してください。
キー入力待ちのとき、以下のようなプロンプトが表示されます。

MORE(xx%):

(xx は全体バイト数に対する表示済バイト数の割合)

または

MORE:　(さかのぼって再表示できない場合)

キー入力待ち時の入力キーと動作の一覧を以下に示します。^x は CTRL キーを押しながら x キーを押すことを、M-x は ESC キーを押してから x キーを押すことを表しています。

入力キー	動作
1 2 3 4 5 6 7 8 9 0	行数、行番号、回数指定(以下のキーを入力する前に指定)
c	最後まで表示
f ^F ^V SPACE	一画面または指定行数前進(途中の行は省略)
b ^B M-v BS	一画面または指定行数後退(途中の行は省略) ※1
z	一画面の行数を指定行数に変更し一画面前進
w	一画面の行数を指定行数に変更し一画面後退 ※1
j ^J e ^E ^N ↓ RETURN	一行または指定行数前進(すべての行を表示)
k ^K y ^Y ^P ↑	一行または指定行数後退(すべての行を表示) ※1
d ^D	半画面の行数を指定行数に変更し半画面前進
u ^U	半画面の行数を指定行数に変更し半画面後退 ※1
g <	先頭画面または指定行番号以降表示 ※1
G >	最終画面または指定行番号以降表示
/検索パターン	順検索(指定数回) ※1
?検索パターン	逆検索(指定数回) ※1
n	同方向に再検索 ※1
N	逆方向に再検索 ※1
M-x	x(任意コマンド)を実行し、最後まで表示しても終了しない
r ^R ^L	画面再表示 ※1
^G	情報表示(行数、バイト数、割合)
h H	ヘルプ表示(キーバインド一覧)
q Q ^C	終了

※1 逆戻りできない表示の場合は無効です。

行番号を指定する場合、画面上での行番号を指定します。コマンドが一行分として画面桁数以上出力した場合、画面上では複数の行として扱われます。先頭行番号は 1 です。
検索時にはプロンプトとしてスラッシュ(/) またはクエスチョン (?) が表示され、検索パターンを入力できるようになります。検索パターンは 76 文字まで入力できます。画面桁数が 80 桁未満の場合、画面桁数以上の検索パターンを入力すると画面表示が乱れますので、画面再表示を行ってください。
検索パターンで使用できる特殊文字を以下に示します。それ以外はその文字自身を検索します。

特殊文字	検索対象
.	任意の一文字
^	行頭
$	行末
\<	単語開始
\>	単語終了
\x	x (xは < > 以外の文字)

検索で見つかった場合は、見つかった文字列が反転表示されます。
検索で見つからなかった場合は、以下のプロンプトが表示されるので、RETURN キーを入力してください。
CTRL+C を入力した場合は、コマンド出力表示が中断されます。

```
MORE: pattern not found (press RETURN)
```

情報表示した場合は、以下のようなプロンプトが表示されます。

```
MORE(line 1-22/515 lines, 1428/33473 bytes, 4%):
          - -- ---         ---- -----         -
          a b  c           d    e             f
```

逆戻りできない表示の場合は以下のようなプロンプトが表示されます。

```
MORE(line 1-22 lines):
          - --
          a b
```

意味:

a:	画面最上行番号
b:	画面最下行番号
c:	全体行数
d:	表示バイト数
e:	全体バイト数
f:	表示バイト数に対する全体バイト数の割合 (d ÷ e × 100)

ヘルプ表示時には、ヘルプ表示後、以下のプロンプトが表示されるので、RETURN キーを入力してください。CTRL+C を入力した場合は、コマンド 出力表示が中断されます。

```
MORE: help (press RETURN)
```

[注意]

本コマンド は運用管理コマンド ですが、管理者クラスで設定した内容は save コマンド を実行することで構成定義情報として保存することができます。また、構成定義モード の delete コマンド で設定を削除することができます。
一般ユーザクラスで設定した内容は、ログアウト時や admin コマンド 実行時に破棄され、保存することはできません。

[未設定時]

ページャ機能を使用しないものとみなされます。

```
terminal pager disable
```

21.2.2 terminal window

[機能]

ターミナル画面サイズの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

terminal window [column <column>] [line <line>]

[オプション]

column <column>

ターミナルの画面桁数を 10 進数値で指定します。

line <line>

ターミナルの画面行数を 10 進数値で指定します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

ターミナルの画面サイズを指定します。
telnet 接続や ssh 接続の場合、接続時や画面サイズ変更時に telnet クライアントや ssh クライアントから通知されるターミナルの画面サイズが使用されます。
通知された後に本コマンドにより画面サイズを変更した場合は、本設定値が使用されます。

[注意]

本コマンドは運用管理コマンドですが、管理者クラスで設定した内容は save コマンドを実行することで構成定義情報として保存することができます。また、構成定義モードの delete コマンドで設定を削除することができます。
一般ユーザクラスで設定した内容は、ログアウト時や admin コマンド実行時に破棄され、保存することはできません。
正しい画面サイズを指定しなかった場合、コマンド入力やコマンド実行時の表示が乱れることがあります。

[未設定時]

ターミナル画面サイズを 80 桁、24 行にするものとみなされます。

```
terminal window column 80 line 24
```

21.2.3　terminal charset

[機能]

漢字コードの設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

terminal charset {EUC | SJIS}

[オプション]

EUC

ターミナルで使用する漢字コードを EUC コードに設定します。

SJIS

ターミナルで使用する漢字コードを ShiftJIS コードに設定します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

ターミナルで使用する漢字コードを指定します。

[注意]

本コマンドは運用管理コマンドですが、管理者クラスで設定した内容は save コマンドを実行することで構成定義情報として保存することができます。また、構成定義モードの delete コマンドで設定を削除することができます。
一般ユーザクラスで設定した内容は、ログアウト時や admin コマンド実行時に破棄され、保存することはできません。

[未設定時]

ターミナルで使用する漢字コードに EUC を設定するものとみなされます。

```
terminal charset EUC
```

21.2.4 terminal prompt

[機能]

入力プロンプト文字列の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

terminal prompt login "<prompt>"
terminal prompt user "<prompt>"
terminal prompt admin "<prompt>"

[オプション]

login
ログイン時の入力プロンプトを設定します。

user
一般ユーザクラスでログインしたときのコマンド入力プロンプトを設定します。

admin
管理者クラスでログインしたときのコマンド入力プロンプトを設定します。

<prompt>
入力プロンプト文字列を指定します。最大 80 文字です。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス) (user オプション)
運用管理モード (管理者クラス) (login,admin オプション)
構成定義モード (管理者クラス)

[説明]

ログインプロンプト、および、コマンド入力プロンプト文字列を指定します。
文字列に空白が含まれる場合は、ダブルクォーテーション (") で囲みます。
プロンプト文字列中に以下に示すバックスラッシュで始まる特殊文字を含めると、その部分は展開した文字列に置き換わります。

特殊文字	展開文字列
\c	構成定義ファイル名がconfig2のときだけ「config2」
\C	構成定義ファイル名の番号 (1または2)
\d	日付(月/日 形式)
\h	ホスト名または機種名(.の手前まで)
\H	ホスト名または機種名(すべて)
\m	機種名
\p	クラスに応じたプロンプト文字列(空白文字含む)
\t	時刻(時:分:秒 形式、24時間制)
\T	時刻(時:分:秒 形式、12時間制)
\@	時刻(時:分NN 形式、12時間制、NN:amかpm)
\v	ファームウェアバージョン
\w	構成定義階層
\!	履歴番号
\\	バックスラッシュ(\)1個

"\c"は、本装置が bank0 の構成定義情報で起動している場合は何も表示されず、"\c"の前または後ろの空白 1 つも表示されません。

bank1 の構成定義情報で起動している場合は"bank1"が表示されます。
"\h"および"\H"は、sysname コマンドで設定したホスト名が表示されます。
ホスト名を設定していない場合は、機種名が表示されます。
"\p"および"\$"の標準プロンプトを以下に示します。

状　態	標準プロンプト
ログイン前 一般ユーザログイン時 管理者ログイン時	: ># # #

21.2.5 terminal timestamp

[機能]

コマンド実行日時表示機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

terminal timestamp {enable|disable}

[オプション]

enable

コマンド実行時に日時を表示します。

disable

コマンド実行時に日時を表示しません。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

コマンドを実行する際にコマンド実行日時を表示するかどうかを指定します。

[注意]

本コマンドは運用管理コマンドですが、管理者クラスで設定した内容は save コマンドを実行することで構成定義情報として保存することができます。また、構成定義モードの delete コマンドで設定を削除することができます。
一般ユーザクラスで設定した内容は、ログアウト時や admin コマンド実行時に破棄され、保存することはできません。

[未設定時]

コマンド実行時に日時を表示しないものとみなされます。

```
terminal timestamp disable
```

21.2.6　terminal bell

[機能]

操作エラーベル機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

terminal bell {enable|disable}

[オプション]

enable

操作エラー時に端末ベルを鳴らします。

disable

操作エラー時に端末ベルを鳴らしません。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

以下の操作エラー時に端末ベルを鳴らすかどうかを設定します。

- 最大文字数 (1022 文字) を超えて入力しようとした場合
- 最大文字数 (1022 文字) を超える貼り付けを行った場合
- 補完候補がない場合

[注意]

本コマンドは運用管理コマンドですが、管理者クラスで設定した内容は save コマンドを実行することで構成定義情報として保存することができます。また、構成定義モードの delete コマンドで設定を削除することができます。
一般ユーザクラスで設定した内容は、ログアウト時や admin コマンド実行時に破棄され、保存することはできません。

[未設定時]

端末ベルを鳴らすものとみなされます。

```
terminal bell enable
```

21.2.7 terminal logging

[機能]

コマンド実行履歴機能の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

terminal logging line <line>

[オプション]

line <line>

コマンド実行履歴行数を 0〜100 の 10 進数値で指定します。
0 を指定すると、コマンド履歴を残しません。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

コマンド実行履歴行数を指定します。
行数を変更した場合、履歴番号や履歴内容は引き継がれますが、0 から増やした場合は履歴番号が 1 からになります。

[注意]

本コマンドは運用管理コマンドですが、管理者クラスで設定した内容は save コマンドを実行することで構成定義情報として保存することができます。また、構成定義モードの delete コマンドで設定を削除することができます。
一般ユーザクラスで設定した内容は、ログアウト時や admin コマンド実行時に破棄され、保存することはできません。

[未設定時]

コマンド実行履歴行数に 24 行を指定するものとみなされます。

```
terminal logging line 24
```

21.2.8　show terminal

[機能]

ターミナル情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show terminal

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

ターミナル情報を表示します。

[注意]

本コマンド は運用管理コマンド ですが、構成定義情報として表示することもできます。その場合、candidate-config と running-config は同一の内容が表示されます。
構成定義情報として表示した場合は、未設定時値以外に設定した内容だけが桁そろえされずに表示されます。

[実行例]

```
# show terminal
pager     enable
window    column 80 line 24
charset   EUC
prompt    login "\p"
prompt    user  "\u@\h \c\p"
prompt    admin "\u@\h \c\w\p"
timestamp disable
bell      enable
logging   line 24
#
```

21.3 コマンド実行履歴

21.3.1 show logging command

[機能]

コマンド実行履歴の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show logging command [brief]

[オプション]

なし

コマンド実行履歴を詳細形式で表示します。

brief

コマンド実行履歴を簡易形式で表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

コマンド実行履歴を表示します。
運用管理モードでは、運用管理モードで実行したコマンド実行履歴が表示されます。
構成定義モードでは、構成定義モードで実行したコマンド実行履歴が表示されます。
一般ユーザクラスでは一般ユーザクラスで実行したコマンド実行履歴だけが表示され、履歴番号は不連続になります。
管理者クラスでは一般ユーザクラスと管理者クラスで実行したコマンド実行履歴が表示されます。
履歴を編集中で実行していない行には、履歴番号のあとに"*"が表示されます。"*"が表示されている場合は、以下のどれかの方法で*"を消すことができます。

- Ctrl+P キーまたは↑キーでその行を表示し、改行キーを押してコマンドを実行します。
- Ctrl+P キーまたは↑キーでその行を表示し、Ctrl+C を押して入力内容を破棄します。
- Ctrl+P キーまたは↑キーでその行を表示し、Ctrl+U を押して空行にしてほかの履歴に移動します。

[注意]

履歴番号が 32767 を超えると、適当な小さい履歴番号に戻ります。

[実行例]

```
# show logging command
Dec 01 15:58:55       1  show system information
Dec 01 15:59:04       2  show date
Dec 01 16:00:19       3  show logging command
# show logging command brief
    1  show system information
    2  show date
    3  show logging command
    4  show logging command brief
#
```

21.3.2 clear logging command

[機能]

コマンド実行履歴の消去

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear logging command

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

運用管理モードおよび構成定義モードでのコマンド実行履歴を消去します。
コマンド実行履歴番号は 1 に戻ります。

[実行例]

```
# clear logging command
#
```

21.4　コマンド エイリアス

21.4.1　alias

[機能]

コマンド エイリアス情報の設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

alias <alias> "<command>"

[オプション]

<alias>

付与するコマンド エイリアス名を 80 文字以内で指定します。
先頭文字は英字、2 文字目以降は英字、数字、ハイフン (-) を指定できます。

<command>

コマンド エイリアスを実行したときに置き換えるコマンド 名およびコマンド オプションをダブルクォーテーションで囲んで指定します。"" を指定すると、定義が削除されます。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

コマンド 名といくつかのコマンド オプションをひとまとめにして新たなコマンド として設定します。最大 30 件設定できます。
設定済みのコマンド エイリアス名を指定すると、以前の登録が削除され指定したコマンド が設定されます。
設定したコマンド エイリアスは即時反映され、すぐ に使用できます。
設定したコマンド エイリアスを実行すると、設定してあるコマンド 名およびコマンド オプションに置き換えられてコマンド が実行されます。
コマンド 実行時、コマンド エイリアスに続けて入力したオプションは、コマンド エイリアスを置き換えたコマンド 名およびオプションの後ろに続けて入力したものとみなされます。
コマンド 実行履歴にはコマンド エイリアスを置き換える前の入力行がそのまま残ります。

[注意]

以下に示すコマンド エイリアス名は登録できません。

- exit, end, quit, up, top, delete, show, clear
- commit, discard, save, load, reset, moff

上記以外の通常コマンド 名をコマンド エイリアス名として登録することはできますが、登録した通常コマンド の動作が変わってしまうのでご注意ください。
本コマンド は運用管理コマンド ですが、管理者クラスで設定した内容は save コマンド を実行することで構成定義情報として保存することができます。また、構成定義モード の delete コマンド で設定を削除することができます。
一般ユーザクラスで設定した内容は、ログアウト 時や admin コマンド 実行時に破棄され、保存することはできません。

[実行例]

```
# alias history "show logging command brief"
# history
    1  alias history "show logging command brief"
    2  history
#
```

[未設定時]

何も登録しないものとみなされます。

21.4.2　show alias

[機能]

コマンド エイリアス情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show alias [<name>]

[オプション]

なし

すべてのコマンド エイリアス情報を表示します。

<name>

指定したコマンド エイリアス名の情報を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

コマンド エイリアス情報を表示します。

[注意]

本コマンド は運用管理コマンド ですが、構成定義情報として表示することもできます。その場合、candidate-config と running-config は同一の内容が表示されます。

[実行例]

```
# show alias
history "show logging command brief"
dsplog "show logging system"
# show alias history
"show logging command brief"
#
```

21.4.3 clear alias

[機能]

コマンドエイリアス情報の削除

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear alias [<name>]

[オプション]

なし

すべてのコマンドエイリアス情報を削除します。

<name>

指定したコマンドエイリアス名の情報を削除します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

コマンドエイリアス情報を削除します。

[注意]

本コマンドは運用管理コマンドですが、構成定義モードの delete コマンドで削除することもできます。

[実行例]

```
# clear alias history
# clear alias
#
```

21.5　コマンド 出力操作

21.5.1　more

[機能]

コマンド の出力を画面単位に表示する

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

<command> | more

[オプション]

<command>

実行するコマンド を指定します。

[動作モード]

運用管理モード (一般ユーザ/管理者クラス)
構成定義モード (管理者クラス)

[説明]

コマンド の出力結果を画面単位に表示します。
本コマンド は、terminal pager enable を指定したときと同じ動作になります。
詳しい説明、キー操作、注意事項については、terminal pager コマンド を参照してください。

[実行例]

```
# show running-config | more
lan 0 mode auto
  (中略)
telnetinfo autologout 5m
MORE(86%):      (qを入力して表示終了)
#
```

21.5.2 tail

[機能]

コマンド出力の最後の部分を表示する

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

<command> | tail [<lines>]

[オプション]

<command>

実行するコマンドを指定します。

<lines>

表示する行数を 1〜1000 の 10 進数で指定します。
省略時は 10 を指定したものとして動作します。

[動作モード]

運用管理モード (一般ユーザ/管理者クラス)
構成定義モード (管理者クラス)

[説明]

指定したコマンドを実行し、そのコマンドの出力の最後の部分を指定した行数だけ表示します。
指定したコマンドの出力が指定した行数に満たない場合は、すべての出力が表示されることになります。
ページャ(terminal pager コマンド参照) が有効な場合は、本コマンドの出力 (指定したコマンドの出力の最後の部分) に対してページャが動作します。

[注意事項]

コマンドパイプ文字 ("|") の前後には空白文字を入力してください。コマンドパイプ文字は一度しか指定できず、tail コマンドを複数指定することはできません。
行数は、改行文字までを 1 行として数えます。1 行が長い場合、画面上では複数行で表示され、引数で指定した行数と画面上の行数が一致しない場合があります。
実行に時間のかかるコマンドを指定した場合、表示開始までしばらく待たされることがあります。
本コマンドは show コマンドのような表示コマンドに対して動作します。telnet コマンドのような制御コマンドに対しては、コマンドの出力をそのまますべて出力します。

[実行例]

```
# show logging syslog | tail 3
Jul 10 09:30:27 192.168.0.1 Si-R180: protocol: master port link recover
Jul 10 09:30:30 192.168.0.1 Si-R180: sshd: generated public/private host key pair.
Jul 10 09:30:52 192.168.0.1 Si-R180: logon: login admin on console
#
```

第 22 章　システム操作および表示コマンド

22.1　システム操作および表示

22.1.1　show system information

[機能]

静的なシステム情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show system information

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

装置の静的なシステム状態・情報を表示します。

[実行例]

Si-R370 基本ソフトウェアの場合

```
# show system information
Current time : Mon Jan 30 14:00:45 2006                ---(1)
Startup time : Mon Jan 30 08:40:05 2006                ---(2)
System : Si-R370                                       ---(3)
Serial No. : 00000123                                  ---(4)
ROM Ver. : 1.5                                         ---(5)
Firm Ver. : V32.00 NY0012 Thu Jan 26 00:44:14 JST 2006  ---(6)
Startup-config : Thu Jan 26 13:08:04 2006 config1      ---(7)
Running-config : Mon Jan 30 08:40:05 2006              ---(8)
MAC : 00000ef16014-00000ef16017                        ---(9)
Memory : 128MB                                         ---(10)
SLOT0 : -----                                          ---(11)
SLOT1 : -----
#
```

1) Current time
現在の日付、時刻が表示されます。

2) Startup time
装置を起動した日付、時刻が表示されます。

3) System
装置名が表示されます。

Si-R180 ：

Si-R180 基本ソフトウェア

Si-R220B ：

Si-R220B 基本ソフトウェア

Si-R240 ：

Si-R240 基本ソフトウェア

Si-R260B ：

Si-R260B 基本ソフトウェア

Si-R370 ：

Si-R370 基本ソフトウェア

Si-R570 ：

Si-R570 基本ソフトウェア

4) Serial No.
装置のシリアル番号が表示されます。

5) ROM Ver.
ROM 版数が表示されます。

6) Firm Ver.
ファームウェアの版数、および作成日時が表示されます。

7) Startup-config
起動用の構成定義を保存した日時、および保存された構成定義ファイル名が表示されます。

8) Running-config
現在動作中の構成定義を反映した日時が表示されます。

9) MAC
MAC アドレスが 12 桁の 16 進数値で表示されます。
Si-R180 の MAC アドレスは 1 つです。

10) Memory
装置に実装されているメモリサイズが表示されます。

11) SLOT
拡張スロットに実装された拡張モジュールが表示されます。
Si-R240 の場合は、SLOT0 と SLOT1 に挿入された PC カードの名称が表示されます。
Si-R370 の場合は、SLOT0 と SLOT1 が表示されます。
Si-R570 の場合は、SLOT0 から SLOT3 が表示されます。
Si-R260B Si-R220B Si-R180 には拡張スロットはないので、表示されません。

BRI-module

: BRI 拡張モジュール L2

PRI-module

: PRI 拡張モジュール L2

100TX-module <MAC アドレス>

: 100BASE-TX 拡張モジュール L2

100FX-module <MAC アドレス>

: 100BASE-FX 拡張モジュール L2

ATM25-module

: ATM25M 拡張モジュール L2

ATM155-module

: ATM155M 拡張モジュール L2

ATM25-module H1

：ATM25M 拡張モジュール H1

ATM155-module H1

：ATM155M 拡張モジュール H1

4Port BRI-module

：BRI4 ポート拡張モジュール H1

Dual 100TX-module <MAC アド レス>

：10/100BASE-TX2 ポート拡張モジュール H1

22.1.2　show system status

[機能]

動的なシステム情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show system status

[オプション]

なし

動的なシステム情報を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

装置の動的なシステム情報を表示します。

[実行例]

以下に、実行例を示します。

実行例 (Si-R180 の場合)

```
# show system status
Current-time         : Mon Nov 17 14:00:45 2003                  ---(1)
Startup-time         : Mon Nov 17 08:40:05 2003                  ---(2)
restart_cause        : power on                                  ---(3)
machine_state        : RUNNING                                   ---(4)
```

1) Current time
   現在の日時
2) Startup time
   システムの起動日時
3) restart_cause
   システム起動要因
   以下のシステム起動要因が表示されます。

   - **power on**
     電源投入
   - **reset**　reset コマンド 発行
   - **reset switch**
     リセットスイッチ押下
   - **system down**
     システムダウン発生

4) machine_state

装置状態

RUNNING

: 動作中

実行例 (Si-R220B Si-R260B の場合)

```
# show system status
Current-time         : Mon Nov 17 14:00:45 2003                  ---(1)
Startup-time         : Mon Nov 17 08:40:05 2003                  ---(2)
restart_cause        : power on                                  ---(3)
machine_state        : RUNNING                                   ---(4)
inspiration_state    : NORMAL                                    ---(5)
inspiration_temp     : 35 C                                      ---(6)
```

1) Current time

現在の日時

2) Startup time

システムの起動日時

3) restart_cause

システム起動要因

以下のシステム起動要因が表示されます。

- **power on**

  電源投入

- **reset** reset コマンド 発行

- **reset switch**

  リセットスイッチ押下

- **system down**

  システムダウン発生

4) machine_state

装置状態

RUNNING

: 動作中

5) inspiration_state

吸気温度状態

NORMAL

: 正常 (温度異常)

HIGHWARNING

: 高温警告

HIGHALARM

: 高温異常

6) inspiration_temp

吸気温度

実行例 (Si-R240 の場合)

```
Si-R240# show system status
Current-time         : Fri Jan 27 19:08:14 2006                  ---(1)
Startup-time         : Fri Jan 27 19:07:55 2006                  ---(2)
restart_cause        : power on                                  ---(3)
machine_state        : RUNNING                                   ---(4)
fan0_state           : UNKNOWN                                   ---(5)
inspiration_state    : UNKNOWN                                   ---(6)
cpu0_state           : NORMAL
fan0_speed           : 0 rpm                                     ---(7)
inspiration_temp     : 25 C                                      ---(8)
cpu0_temp            : 24 C
CONNECTOR              STATUS     SUBSTATUS     ERROR             ---(9)
 slot0   Vodafone VC701SI
 slot1
```

1) Current time

   現在の日時

2) Startup time

   システムの起動日時

3) restart_cause

   システム起動要因

   以下のシステム起動要因が表示されます。

   - **power on**

     電源投入

   - **reset**　reset コマンド発行

   - **reset switch**

     リセットスイッチ押下

   - **system down**

     システムダウン発生

4) machine_state

   装置状態

   RUNNING

   : 動作中

5) fan0_state

   冷却ファンの状態

   NORMAL

   : 冷却ファン正常

   ABNORMAL

   : 冷却ファン異常 (故障／未装着)

   UNKNOWN

   : 冷却ファン停止状態、または、状態不明

6) inspiration_state

   吸気温度状態

   cpu0_state

   CPU0 温度状態

NORMAL

: 正常 (温度異常)

HIGHWARNING

: 高温警告

HIGHALARM

: 高温異常

UNKNOWN

: 非監視状態、または、状態不明

7) fan0_speed

冷却ファンの回転速度

8) inspiration_temp

吸気温度

cpu0_temp

CPU の CPU 温度

9) CONNECTOR

PC カード の名称 (PC カード 内の CIS 情報)

STATUS コネクタの状態 (現在、未使用)

SUBSTATUS

コネクタのサブ状態 (現在、未使用)

ERROR エラー情報 (現在、未使用)

実行例 (Si-R370 の場合)

```
# show system status
Current-time         : Mon Nov 17 14:00:45 2003                  ---(1)
Startup-time         : Mon Nov 17 08:40:05 2003                  ---(2)
restart_cause        : power on                                  ---(3)
machine_state        : RUNNING                                   ---(4)
fan0_state           : NORMAL                                    ---(5)
inspiration_state    : NORMAL                                    ---(6)
cpu0_state           : NORMAL
fan0_speed           : 6700 rpm                                  ---(7)
inspiration_temp     : 35 C                                      ---(8)
cpu0_temp            : 32 C
CONNECTOR            STATUS     SUBSTATUS     ERROR              ---(9)
 slot0   RM-TX100    Online
 slot1   RM-BRI 1    Online
```

1) Current time

現在の日時

2) Startup time

システムの起動日時

3) restart_cause

システム起動要因

以下のシステム起動要因が表示されます。

- **power on**

  電源投入

- **reset** reset コマンド 発行

・**reset switch**

リセットスイッチ押下

・**system down**

システムダウン発生

4) machine_state

装置状態

RUNNING

: 動作中

5) fan0_state

冷却ファンの状態

NORMAL

: 冷却ファン正常

ABNORMAL

: 冷却ファン異常 (故障／未装着)

UNKNOWN

: 状態不明

6) inspiration_state

吸気温度状態

cpu0_state

CPU0 温度状態

NORMAL

: 正常 (温度異常)

HIGHWARNING

: 高温警告

HIGHALARM

: 高温異常

7) fan0_speed

冷却ファンの回転速度

8) inspiration_temp

吸気温度

cpu0_temp

CPU の CPU 温度

9) CONNECTOR

コネクタの名称

なし　: コネクタ未実装

RM-BRI 1

: BRI 拡張モジュール L2

RM-PRI 1

: PRI 拡張モジュール L2

RM-FX100SS

: 100BASE-FX 拡張モジュール L2

RM-TX100

: 100BASE-TX 拡張モジュール L2

RM-ATM25

: ATM25M 拡張モジュール L2

RM-ATM155SS

: ATM155M 拡張モジュール L2

STATUS

コネクタの状態

Online :運用可能

Admindown

:コネクタ DOWN 中

SUBSTATUS

コネクタのサブ状態 (現在、未使用)

ERROR

エラー情報 (現在、未使用)

実行例 (Si-R570 の場合)

```
# show system status
Current-time         : Mon Nov 17 14:00:45 2003                  ---(1)
Startup-time         : Mon Nov 17 08:40:05 2003                  ---(2)
restart_cause        : power on                                  ---(3)
machine_state        : RUNNING                                   ---(4)
power0_state         : NORMAL                                    ---(5)
power1_state         : NORMAL
fan0_state           : NORMAL                                    ---(6)
fan1_state           : NORMAL
inspiration_state    : NORMAL                                    ---(7)
cpu0_state           : NORMAL
fan0_speed           : 6700 rpm                                  ---(8)
fan1_speed           : 6700 rpm
inspiration_temp     : 35 C                                      ---(9)
cpu0_temp            : 32 C
basic_memory         : 256MB                                     ---(10)
expand_memory        : NO_PRESENT
CONNECTOR            STATUS     SUBSTATUS     ERROR               ---(11)
 slot0   RM-TX100    Online
 slot1   RM-BRI 1    Online
 slot2   RMP-TX100D  Online
 slot3   RMP-ATM25   Online
```

1) Current time

現在の日時

2) Startup time

システムの起動日時

3) restart_cause

システム起動要因

以下のシステム起動要因が表示されます。

- **power on**

電源投入

- **reset**　reset コマンド発行
- **reset switch**
  リセットスイッチ押下
- **system down**
  システムダウン発生

4) machine_state
装置状態

RUNNING
: 動作中

5) power0_state
電源ユニット #0 の電源状態
power1_state
電源ユニット #1 の電源状態

NORMAL
: 正常

NO_PRESENT
: 未装着

FAIL　: 電源断状態

UNKNOWN
: 状態不明

6) fan0_state
冷却ファン #0 の状態
fan1_state
冷却ファン #1 の状態

NORMAL
: 冷却ファン正常

ABNORMAL
: 冷却ファン異常 (故障／未装着)

UNKNOWN
: 冷却ファン内蔵の電源ユニットが正常時以外、または、状態不明

7) inspiration_state
吸気温度状態
cpu0_state
CPU0 温度状態

NORMAL
: 正常 (温度異常)

HIGHWARNING
: 高温警告

HIGHALARM
: 高温異常

8) fan0_speed
冷却ファン#0 の回転速度
fan1_speed
冷却ファン#1 の回転速度

9) inspiration_temp
吸気温度
cpu0_temp
CPU 周辺温度

10) basic_memory
基本メモリ実装状態
expand_memory
拡張メモリ実装状態

256MB ：256MB メモリ実装

512MB ：512MB メモリ実装

NO_PRESENT
：未装着

UNKNOWN
：状態不明

11) CONNECTOR
コネクタの名称

なし ：コネクタ未実装

RM-BRI 1
：BRI 拡張モジュール L2

RM-PRI 1
：PRI 拡張モジュール L2

RM-FX100SS
：100BASE-FX 拡張モジュール L2

RM-TX100
：100BASE-TX 拡張モジュール L2

RM-ATM25
：ATM25M 拡張モジュール L2

RM-ATM155SS
：ATM155M 拡張モジュール L2

RMP-TX100D
：10/100BASE-TX2 ポート拡張モジュール H1

RMP-ATM25
：ATM25M 拡張モジュール H1

RMP-ATM155SS
：ATM155M 拡張モジュール H1

RMP-BRI4
：BRI4 ポート拡張モジュール H1

STATUS

コネクタの状態

Online　:運用可能

Admindown

:コネクタ DOWN 中

SUBSTATUS

コネクタのサブ状態 (現在、未使用)

ERROR

エラー情報 (現在、未使用)

22.1.3 show tech-support

[機能]

解析情報の一括表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show tech-support

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

本装置の設定情報や各種ステータスなど解析に必要な情報が一括で表示されます。
ターミナルソフトウェアの出力キャプチャ機能を使用して、本コマンド実行時の出力内容を保存してください。

22.1.4　show logging error

[機能]

エラーログの表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show logging error

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

ROM または I/O ドライバによるハード診断エラー、およびシステムダウンのエラーログ情報を表示します。

[注意]

"Logging time:"で表示する時刻は、構成定義情報にタイムゾーン (time zone <offset>) が指定されていない状態では GMT(グリニッジ標準時間) での表示となります。

[実行例]

Si-R570 の場合

```
# show logging error
------------------ Error Logs in FLASH ------------------
[0] Error Log:
flag=80,mode=00,unit=10,regsp=00000000
Firm information:
Si-R570 V30.00 PTF:NY0001
Error information:
error code [85020000]
Logging time:
Thu Feb 10 11:51:17 2005
Hardware diagnostic error information:
Detail [00142224 00142228 00000080 0000341f]
       [00000000 00000000 00000000 00000000]
       [00000000 00000000 00000000 00000000]
       [00000000 00000000 00000000 00000000]
       [00000000 00000000 00000000 00000000]
       [00000000 00000000 00000000 00000000]

Extended Error Logs:

[1] Error Log:
flag=80,mode=00,unit=10,regsp=00000000
Firm information:
Si-R570 V30.00 PTF:NY0001
Error information:
error code [85020000]
Logging time:
Thu Feb 10 11:59:37 2005
Hardware diagnostic error information:
Detail [00142224 00142228 00000080 00003520]
       [00000000 00000000 00000000 00000000]
       [00000000 00000000 00000000 00000000]
       [00000000 00000000 00000000 00000000]
       [00000000 00000000 00000000 00000000]
       [00000000 00000000 00000000 00000000]

------------------ Error Logs in DRAM -------------------
[0] Error Log:
flag=80,mode=00,unit=80,regsp=04ae9e60
Firm information:
Si-R570 V30.00 PTF:NY0001
System down information:
down code [00000080:00000002]
Logging time:
Thu Feb 10 13:05:23 2005
Register:
    srr0    [0086dab4] srr1    [0002d000] csrr0   [00000000] csrr1   [00000000]
    mcsrr0  [00000000] mcsrr1  [00000000] mcar    [00000000] mcsr    [00000000]
    lr      [00886d74] dear    [0087a01c] esr     [00000000] tsr     [00000000]
    gpr00   [00000000] gpr01   [04ae9f60] gpr02   [00000005] gpr03   [01124844]
    gpr04   [0087a01c] gpr05   [00000005] gpr06   [010cf924] gpr07   [a2c9bdbc]
    gpr08   [c1bcb0a1] gpr09   [00000005] gpr10   [d8c4eab7] gpr11   [00000000]
    gpr12   [aca5a4a5] gpr13   [00000000] gpr14   [00000000] gpr15   [00000000]
    gpr16   [00000000] gpr17   [00000000] gpr18   [00000000] gpr19   [00000000]
    gpr20   [00000000] gpr21   [00000000] gpr22   [00000000] gpr23   [00000000]
    gpr24   [04aea1e0] gpr25   [04aea1f0] gpr26   [0121ff74] gpr27   [00000000]
    gpr28   [00000000] gpr29   [ffffffff] gpr30   [0121ff7c] gpr31   [04aea174]
```

(続く)

(続き)

```
Peripheral Register:
    err_det [00000000] l2errdet[00000000] eedr    [00000000] ltesr   [00000000]
User Stack:
          +0       +4       +8       +C         +0  +4  +8  +C
04ae9f60  04aea1d0 00886d58 04ae9fb8 04ae9fa0   ......mX........
04ae9f70  00c6fcbb fea4cebb d8c4eab7 c1bcb0a1   ................
04ae9f80  a2c9bdbc a8b7c1bc b0a4f2a5 aca5a4a5   ................
04ae9f90  c9a5e9a5 a4a5f3a4 cba4a2a4 efa4bba4   ................
04ae9fa0  eba1a30a 00000000 00000000 00000000   ................
04ae9fb0  04aea1c0 00000000 00000000 00000000   ................
04ae9fc0  85004100 04aea0b0 0000000a 00000000   ..A.............
04ae9fd0  04ae9ff0 04ae9fb0 04ae9fb0 00000100   ................
04ae9fe0  00000000 85004100 00000100 04aea068   ......A........h
04ae9ff0  04aea020 00000000 00000000 00000000   ... ............
04aea000  00000000 04aea0f0 00000007 00000000   ................
04aea010  00000001 04ae9ff0 04aea000 2066696c   ............ fil
04aea020  73666572 000002bf 5472616e 01e89be0   sfer....Tran....
04aea030  42000082 00000000 00000000 00000000   B...............
04aea040  00000000 00000000 00000000 00000000   ................
04aea050  00000000 00000000 00000000 00000000   ................
04aea060  010b0000 04b22114 0000005d 00000000   ......!....]....
04aea070  04aea148 0124269c ffffffff ffffffff   ...H.$&.........
04aea080  00405cfc 0002d000 ffffffff ffffffff   .@\.............
04aea090  0087b9dc 00000000 00000000 42002088   ............B. .
04aea0a0  00000001 00000000 00000000 42002088   ............B. .
04aea0b0  00000001 0002d000 00000100 00000001   ................
04aea0c0  0087b6d4 00000000 00000000 42000084   ............B...
04aea0d0  00000001 00000100 00000002 035fc300   ............_...
04aea0e0  04aea110 01260af0 00004e43 00000020   .....&....NC...
04aea0f0  04aea100 01260af0 00004e43 00000020   .....&....NC...
04aea100  04aea130 0087b810 01261d28 035fcdc0   ...0.....&.(._..
04aea110  04aea140 01260af0 00004e43 42000082   ...@.&....NCB...
04aea120  04aea140 00000022 00000000 035fcdc0   ...@..."....._..
04aea130  04aea140 0087b8c0 00000000 035fcdc0   ...@........._..
04aea140  04aea170 0087a23c 00000022 01230168   ...p...<...".#.h
04aea150  04aea1d0 04b11152 00769eec 01230168   .......R.v...#.h
04aea160  00000000 00000022 04b22114 0000005d   ......"..!....]
04aea170  00000000 0087a01c 00000000 00000200   ................
04aea180  04b71ee0 04b22114 01230168 00000022   ......!..#.h..."
04aea190  04aea1a0 00869238 00000000 00000000   .......8........
04aea1a0  04aea1c0 00867cd8 00000000 00000000   ......|.........
04aea1b0  010b0000 04b11152 00769eec 01230168   .......R.v...#.h
04aea1c0  04b71ee0 01240000 010ed184 01230168   .....$......#.h
04aea1d0  04aea210 00768d20 00000000 00000000   .....v. ........
04aea1e0  04b71ee0 04aea220 01230168 0121fd30   ....... .#.h.!.0
04aea1f0  04aea210 007697d4 00769eec 01230168   .....v...v...#.h
04aea200  04b71ee0 01240000 01230168 01240000   .....$...#.h.$..
04aea210  04aea330 007685d4 04aea200 fffffffb   ...0.v..........
04aea220  4649524d 57415245 2d494e46 4f000000   FIRMWARE-INFO...
04aea230  53692d52 35373000 00000000 00000000   Si-R570.........
04aea240  00000000 00000000 00000000 00000000   ................
04aea250  4e593030 30312056 33302e30 30000000   NY0001 V30.00...
04aea260  00000000 00000000 00000000 00000000   ................
04aea270  4d6f6e20 46656220 20372031 343a3239   Mon Feb  7 14:29
04aea280  3a353920 4a535420 32303035 00000000   :59 JST 2005....
04aea290  00000000 00000000 00000000 00000000   ................
04aea2a0  00000000 00000000 00000000 00000000   ................
04aea2b0  00000000 00000000 00000000 000001d4   ................
04aea2c0  00000000 00000000 00000000 00000000   ................
04aea2d0  00000000 00000000 00000000 00000000   ................
04aea2e0  00000000 00000000 00000000 00000000   ................
04aea2f0  00000000 00000000 00000000 00000000   ................
04aea300  00000000 00000000 00000000 00000000   ................
04aea310  00000000 00000000 00000000 00000000   ................
04aea320  011395e0 00000004 01240000 01240000   .........$...$..
04aea330  04aea360 00769fe4 00000000 035fcdc0   ...‘.v........_..
04aea340  04aea360 0087a23c 7ffffff0 01230168   ...‘...<.....#.h
04aea350  00000004 04aea370 01240000 04b71ee0   .......p.$......
```

(続く)

(続き)

```
Interrupt Stack:
          +0       +4       +8       +C         +0  +4  +8  +C
04ae9e60  00000000 04aea1f0 0121ff74 00000000   .........!.t....
04ae9e70  00000000 04ae9f60 00000005 01124844   .......‘......HD
04ae9e80  0087a01c 00000005 010cf924 a2c9bdbc   ...........$....
04ae9e90  c1bcb0a1 00000005 d8c4eab7 00000000   ................
04ae9ea0  aca5a4a5 00000000 00000000 00000000   ................
04ae9eb0  00000000 00000000 00000000 00000000   ................
04ae9ec0  00000000 00000000 00000000 00000000   ................
04ae9ed0  04aea1e0 04aea1f0 0121ff74 00000000   .........!.t....
04ae9ee0  00000000 ffffffff 0121ff7c 04aea174   .........!.|...t
04ae9ef0  0086dab4 0002d000 00000000 00000000   ................
04ae9f00  00886d74 00000005 00000000 42000082   ..mt........B...
04ae9f10  00000001 0087a01c 00000000 00000000   ................
04ae9f20  00000000 00000000 00000000 00000000   ................
04ae9f30  00000000 00000000 00000000 00000000   ................
04ae9f40  00000000 00000000 00000000 04aea170   ...............p
04ae9f50  04ae9f60 01260af0 00004e43 00000008   ...‘.&....NC....
# exit
```

22.1.5　clear logging error

[機能]

エラーログのクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear logging error

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

すべてのエラーログを消去し、CHECK ランプを消灯します。

[実行例]

```
# clear logging error
#
```

22.1.6 show logging syslog

[機能]

システムログ情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show logging syslog

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

システムログ情報を表示します。最新の情報からさかのぼって、1024 件以上表示できます。

[注意]

本装置の電源 OFF、または clear logging syslog コマンドを実行すると、システムログ情報はクリアされます。reset コマンドの実行やリセットスイッチの押下により本装置をリセットしてもシステムログ情報はクリアされませんが、例外としてファームウエア更新後にリセットされた場合は、システムログ情報はクリアされます。

[実行例]

```
# show logging syslog
Nov 11 08:31:06 192.168.1.1 Si-R370: init: system startup now.
Nov 11 08:31:06 192.168.1.1 Si-R370: protocol: [mb/0] lan port link down
Nov 11 08:31:06 192.168.1.1 Si-R370: protocol: [mb/0] lan port link up
```

22.1.7　clear logging syslog

[機能]

システムログ情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear logging syslog

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

すべてのシステムログ情報をクリアします。

[実行例]

```
# clear logging syslog
#
```

22.1.8 clear statistics

[機能]

全統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear statistics

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

すべての統計情報をクリアします。

[実行例]

```
# clear statistics
#
```

22.1.9　show date

[機能]

現在の装置の日付、時刻の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show date

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

現在の装置の日付、時刻を表示します。

[実行例]

```
# show date
Thu Dec 16 14:26:00 2004  ---(1)
```

1)　現在の日付、時刻が表示されます。

22.1.10 date

[機能]

現在の装置の日付、時刻の表示/設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

date [<YYYY/MM/DD.hh:mm:ss>]

[オプション]

なし

現在の装置の日付、時刻を表示します。

<YYYY/MM/DD.hh:mm:ss>

指定した日付、時刻を設定します。(管理者クラスのみ有効)

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

現在の装置の日付、時刻を表示したり、設定したりします。

[実行例]

日付、時刻を表示する場合

```
# date
Thu Dec 16 14:26:00 2004
#
```

日付、時刻を設定する場合

```
# date 2004/12/16.14:26:00
#
```

22.1.11　rdate

[機能]

リモートホストの日付、時刻を本装置に設定

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

rdate

[オプション]

なし

リモートホストの日付、時刻を本装置に設定します。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

time auto server で指定したリモートホスト (タイムサーバ) の日付、時刻を取得し、本装置の日付、時刻として設定します。

[実行例]

```
# rdate
Thu Dec 16 14:26:00 2004
#
```

22.1.12 reset

[機能]

装置の再起動

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

reset
reset clear
reset <filename>

[オプション]

なし

装置を再起動します。

clear

設定をご購入時の状態に戻し、装置を再起動します。

<filename>

起動時に読み込む構成定義ファイルを指定します。

- config1
  第 1 構成定義ファイルを読み込みます。
- config2
  第 2 構成定義ファイルを読み込みます。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

装置を再起動します。

[実行例]

```
# reset
```

22.1.13　update

[機能]

ファームウェアの更新

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

update

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

updateinfo で指定したファームウェア更新情報に従ってリモートホスト (ftp サーバ) からファームウェアを取得し、本装置の FLASH メモリに格納されたファームウェアを書き換えます。
更新したファームウェアは本装置の再起動後に有効になります。

[注意]

ファームウェアの更新中は、絶対に電源 OFF/リセットは行わないでください。更新中に電源 OFF/リセットした場合は、装置が起動しなくなります。
ハードエラーを検出し、システムダウンペンディング状態では、以下のメッセージを出力し、異常終了します。(※ Si-R180 を除く)

```
detected HARD ERROR, cannot execute
```

[実行例]

以下に、実行例を示します。

```
# update
update: File transfer now!
220 192.168.1.2 FTP server (Version 6.00LS) ready.
331 Password required for hamster.
230 User hamster logged in.
200 Type set to I.
200 PORT command successful.
150 Opening BINARY mode data connection for '/SIR570SOFT.ftp' (4146148 bytes).
Hash mark printing on (4096 bytes/hash mark).
################
################
        :
################
#####
4146148 bytes received in 4.903 seconds (825.814 Kbytes/sec)
226 Transfer complete.
221 Goodbye.
update: File transfer ok.

update: Transfer file check now!
update: Transfer file check ok.

update: File information check now!
[old] Si-R570 V30.00 PTF:NY0001
[new] Si-R570 V30.00 PTF:NY0001
update: File information check ok.

update: Rom firm write now!
target file type 'firm' (4146148 bytes)
Erase now...
@@@@@@@@@@@@@@@@   ..[ 16 s]
@@@@@@@@@@@@@@@@   ..[ 32 s]
@@                 ..[ 34 s]
Erase end. (34 seconds)
Write now...
@@@@@@@@@@@@@@@@   ..[  1 %]
@@@@@@@@@@@@@@@@   ..[  3 %]
        :
@@@@@@@@@@@@@@@@   ..[ 99 %]
@@@@@              ..[100 %]
4146036 bytes wrote in 48.274 seconds (83.878 Kbytes/sec)
update: Rom firm write ok.

#
```

第 23 章　Ethernet のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

23.1 Ethernet のカウンタ・ログ・統計・状態などの表示

23.1.1 show ether

[機能]

Ethernet 物理ポートの情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ether [slot <slot>] [line <line>]

[オプション]

なし

すべての情報を表示します。

slot <slot>

指定されたスロット上の情報を表示します。
また、該当するスロットが無効の場合は情報は表示されません。

- mb
  表示するポートが、基本ボード上にある場合に指定します。
- switch
  表示するポートが、スイッチポート (SW1〜SW4) である場合に指定します。Si-R180 で指定が可能です。
- スロット番号
  拡張モジュールが挿入されているスロットの番号を指定します。

範囲	機種
0〜1	Si-R370
0〜3	Si-R570

line <line>

指定されたポート上の情報を表示します。
また、該当するポート番号が無効の場合は情報は表示されません。

- <slot>で mb 指定された場合

範囲	機種
0〜1	Si-R180 Si-R240
0〜3	Si-R570 Si-R370 Si-R260B Si-R220B

- <slot>で switch 指定された場合

範囲	機種
1〜4	Si-R180

- <slot>で 0〜1 指定された場合

範囲	機種
0	Si-R570　Si-R370

- <slot>で 2〜3 指定された場合

範囲	機種
0〜1	Si-R570

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

Ethernet ポートの情報を表示します。
slot オプションのみ指定した場合は、対象スロット上に搭載されている全ポートの情報が表示されます。
line オプションのみ指定した場合は、基本ボード上の対象ポートの情報が表示されます。
slot オプション、line オプションともに省略時は、本装置に搭載される全ポートの情報が表示されます。

[実行例]

以下に、実行例を示します。

```
# show ether

[LAN PORT-0]
status                    : auto 100M Full MDI   ---(1)
media                     : Fiber                ---(2)
flow control              : send on, receive on  ---(3)
since                     : Oct  2 17:31:26 2002 ---(4)

[LAN PORT-1]
status                    : 100M Full MDI
media                     : Metal
flow control              : send on, receive on
since                     : Oct  2 17:31:26 2002
backup configuration      : master (active)     --- (5)
backup port               : slot 0 line 0       --- (6)

[LAN SLOT-0 PORT-0]
status                    : down
media                     : Metal
flow control              : send off, receive off
since                     : Oct  2 17:31:26 2002
backup configuration      : backup (standby)
master port               : slot mb line 1      --- (7)

#
```

1)　ポートの状態
接続完了時の速度、状態が表示されます。

disable　定義されていないため使用しない状態であることを示します。

down　リンクダウン状態であることを示します。

down(offline)

コマンドにより offline 状態であることを示します。スイッチポートのみ表示されます。

auto オートネゴシエーション有効であることを示します。

10M/100M/1000M

現在リンクしている回線速度 (10Mbps/100Mbps/1000Mbps) を示します。

Full/Half 現在リンクしている全二重/半二重の状態を示します。

MDI/MDI-X

現在リンクしている MDI の種別を示します。
構成定義による MDI 設定が可能なポートにのみ表示されます。

2) 回線種別
回線種別が表示されます。

Fiber 光ケーブル回線を使用していることを示します。

Metal 金属回線を使用していることを示します。

- ポート未使用のため不定であることを示します。

3) フロー制御状態
フロー制御の送信／受信の順で表示します。

on フロー制御が有効であることを示します。

off フロー制御が無効であることを示します。

- ポート未使用のため不定であることを示します。

4) 状態遷移時刻
ポートの状態が現在の状態に変化した時刻を表示します。
ポート未使用時には '-' が表示されます。

5) LAN バックアップ機能の利用時に、自身の役割と状態を表示します。

master マスタポートとして動作しています

backup バックアップポートとして動作しています

active 稼働状態です

standby 待機状態です

6) LAN バックアップ機能の利用時に、自身がマスタポートの場合は、
バックアップポートを表示します。

7) LAN バックアップ機能の利用時に、自身がバックアップポートの場合は、
マスタポートを表示します。

23.1.2　show ether statistics

[機能]

Ethernet 物理ポートの統計情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ether statistics [slot <slot>] [line <line>]

[オプション]

なし

すべての統計情報を表示します。

<slot>

指定されたスロット上の統計情報を表示します。
また、該当するスロットが無効の場合は統計情報は表示されません。

- mb
  表示するインタフェースが、基本ボード上にある場合に指定します。
- switch
  表示するポートが、スイッチポート (SW1～SW4) である場合に指定します。Si-R180 で指定が可能です。
- スロット番号
  拡張モジュールが挿入されているスロットの番号を指定します。

範囲	機種
0～1	Si-R370
0～3	Si-R570

<line>

指定されたポート上の統計情報を表示します。
また、該当するポート番号が無効の場合は統計情報は表示されません。

- <slot>で mb 指定された場合

範囲	機種
0～1	Si-R240　Si-R180
0～3	Si-R570　Si-R370　Si-R260B　Si-R220B

- <slot>で switch 指定された場合

範囲	機種
1～4	Si-R180

- <slot>で 0〜1 指定された場合

範囲	機種
0	Si-R570 Si-R370

- <slot>で 2〜3 指定された場合

範囲	機種
0〜1	Si-R570

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

Ethernet 物理ポートの統計情報を表示します。
<line>を省略時は、対象<slot>上に搭載される全ポートの統計情報が表示されます。
<line> および <slot>を省略時は、本装置に搭載される全ポートの統計情報が表示されます。

[注意]

統計情報は、本装置を再起動するとクリアされます。

[実行例]

以下に、実行例を示します。

```
# show ether statistics

[LAN PORT-0 STATISTICS]
Input packets            : 7388 --- (1)
Input error packets      : 0    --- (2)
 frames too long         : 0    --- (3)
 alignment errors        : 0    --- (4)
 frames too short        : 0    --- (5)
 FCS errors              : 0    --- (6)
 overrun                 : 0    --- (7)
 late collisions         : 0    --- (8)
Output packets           : 7388 --- (9)
Output error packets     : 0    --- (10)
 late collisions         : 0    --- (11)
 excessive collisions    : 0    --- (12)
 underrun                : 0    --- (13)
 carrier sense errors    : 0    --- (14)

[LAN PORT-1 STATISTICS]
Input packets            : 599
Input error packets      : 0
 frames too long         : 0
 alignment errors        : 0
 frames too short        : 0
 FCS errors              : 0
 overrun                 : 0
 late collisions         : 0
Output packets           : 599
Output error packets     : 0
 late collisions         : 0
 excessive collisions    : 0
 underrun                : 0
 carrier sense errors    : 0
```

1) 受信フレーム数
2) 受信エラーフレーム数
3) 最大フレーム長オーバ検出回数
4) アライメントエラー検出回数
5) ショートフレーム検出回数
6) CRC エラー検出回数
7) オーバーラン検出回数
8) レイトコリジョン検出回数
9) 送信フレーム数
10) 送信エラーフレーム数
11) レイトコリジョン検出回数
12) コリジョン発生による送信リトライアウト検出回数
13) アンダーラン検出回数
14) キャリアセンスロスト検出回数

```
# show ether statistics

[LAN PORT-0 STATISTICS]
Input packets             : 7388 --- (1)
Input error packets       : 0    --- (2)
 frames too long          : 0    --- (3)
 alignment errors         : 0    --- (4)
 frames too short         : 0    --- (5)
 FCS errors               : 0    --- (6)
 overrun                  : 0    --- (7)
 late collisions          : 0    --- (8)
 ifInDiscards             : 0    --- (9)
 rxque full count         : 0    --- (10)
Output packets            : 7388 --- (11)
Output error packets      : 0    --- (12)
 late collisions          : 0    --- (13)
 excessive collisions     : 0    --- (14)
 underrun                 : 0    --- (15)
 carrier sense errors     : 0    --- (16)

[LAN PORT-1 STATISTICS]
Input packets             : 599
Input error packets       : 0
 frames too long          : 0
 alignment errors         : 0
 frames too short         : 0
 FCS errors               : 0
 overrun                  : 0
 late collisions          : 0
 ifInDiscards             : 0
 rxque full count         : 0
Output packets            : 599
Output error packets      : 0
 late collisions          : 0
 excessive collisions     : 0
 underrun                 : 0
 carrier sense errors     : 0
```

1) 受信フレーム数
2) 受信エラーフレーム数
3) 最大フレーム長オーバ検出回数
4) アライメントエラー検出回数

5) ショートフレーム検出回数
6) CRC エラー検出回数
7) オーバーラン検出回数
8) レイトコリジョン検出回数
9) 受信 FIFO フルによる破棄パケット数
10) 受信キュー フル状態回数
11) 送信フレーム数
12) 送信エラーフレーム数
13) レイトコリジョン検出回数
14) コリジョン発生による送信リトライアウト検出回数
15) アンダーラン検出回数
16) キャリアセンスロスト検出回数

```
# show ether statistics

[LAN PORT-0 STATISTICS]
Input packets             : 2931615   ---(1)
Input error packets       : 0         ---(2)
 frames too long          : 0         ---(3)
 alignment errors         : 0         ---(4)
 frames too short         : 0         ---(5)
 FCS errors               : 0         ---(6)
 overrun                  : 0         ---(7)
 late collision           : 0         ---(8)
Output packets            : 2957696   ---(9)
Output error packets      : 5         ---(10)
 late collision           : 0         ---(11)
 excessive collisions     : 0         ---(12)
 underrun                 : 0         ---(13)
 carrier sense errors     : 0         ---(14)

[LAN PORT-1 STATISTICS]
Input packets             : 2989811
Input error packets       : 0
 frames too long          : 0
 alignment errors         : 0
 frames too short         : 0
 FCS errors               : 0
 overrun                  : 0
 late collision           : 0
Output packets            : 2930600
Output error packets      : 1
 late collision           : 0
 excessive collisions     : 0
 underrun                 : 0
 carrier sense errors     : 0

[SW PORT-1 STATISTICS]
[Input Statistics]
 Octets                   : 354965866 ---(15)
 Frames                   : 3480097   ---(16)
 Unicast                  : 3479992   ---(17)
 Multicast                : 0         ---(18)
 Broadcast                : 105       ---(19)
 PauseFrames              : 0         ---(20)

 Discards                 : 0         ---(21)
 Filtered                 : 0         ---(22)
 UndersizePkts            : 0         ---(23)
 OversizePkts             : 0         ---(24)
 FCSErrors                : 0         ---(25)
 AlignmentErrors          : 0         ---(26)
 Fragments                : 0         ---(27)
 Jabbers                  : 0         ---(28)

[Output Statistics]
 Octets                   : 298466992 ---(29)
 Frames                   : 2926152   ---(30)
 Unicast                  : 2926143   ---(31)
 Multicast                : 0         ---(32)
 Broadcast                : 9         ---(33)
 PauseFrames              : 0         ---(34)

 Bad octets               : 0         ---(35)
 Discards                 : 2003      ---(36)
 Collisions               : 0         ---(37)
 ExcessiveCollisions      : 0         ---(38)
 LateCollisions           : 0         ---(39)
 SingleCollisionFrames    : 0         ---(40)
 MultipleCollisionFrames  : 0         ---(41)
 DeferredTransmissions    : 0         ---(42)

[SW PORT-2 STATISTICS]
～                                                                          ～
```

1)　受信パケット数

2)　受信エラーパケット数

3) 最大フレーム長オーバ検出回数
4) アライメントエラー検出回数
5) ショートフレーム検出回数
6) CRC エラー検出回数
7) オーバーラン検出回数
8) レイトコリジョン検出回数
9) 送信パケット数
10) 送信エラーパケット数
11) レイトコリジョン検出回数
12) コリジョン発生による送信リトライアウト検出回数
13) アンダーラン検出回数
14) キャリアセンスロスト検出回数
15) 全受信オクテット数
16) 全受信フレーム数
17) 受信したユニキャストフレーム数
18) 受信したマルチキャストフレーム数
19) 受信したブロードキャストフレーム数
20) PAUSE フレーム (MAC 制御フレーム) 受信数
21) 廃棄した受信フレーム数
22) フィルタされて破棄した受信フレーム数
23) ショートサイズフレーム受信数
24) MAXSIZE(1536 オクテット) 以上のフレーム受信数
25) データサイズが 64～MAXSIZE((1536 オクテット) で、FCS エラーを検出したフレーム受信数
26) アライメントエラーを検出したフレーム受信数
27) ショートサイズフレームで FCS エラーを検出したフレーム受信数
28) MAXSIZE(1536 オクテット) 以上で、FCS エラーを検出したフレーム受信数
29) 全送信オクテット数
30) 送信フレーム数
31) 送信したユニキャストフレーム数
32) 送信したマルチキャストフレーム数
33) 送信したブロードキャストフレーム数
34) PAUSE フレーム (MAC 制御フレーム) 送信数
35) FCS エラーを検出した送信オクテット数
36) 廃棄した送信フレーム数
バッファに空きがないため、破棄されたフレーム数
37) コリジョン発生回数
38) 過度のコリジョンによって、送信が失敗したフレーム数
39) レイトコリジョン発生回数
40) 1 回のコリジョン発生後、送信が成功したフレーム数
41) 複数回のコリジョン発生後、送信が成功したフレーム数
42) 伝送路ビジーにより最初の送信が遅れたフレーム数

23.2　Ethernet のカウンタ・ログ・統計などのクリア

23.2.1　clear ether statistics

[機能]

Ethernet 物理ポートの統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear ether statistics [slot <slot>] [line <line>]

[オプション]

なし

指定されたスロットまたはポート上の統計情報をクリアします。

<slot>

指定されたスロット上の統計情報をクリアします。
また、該当するスロットが無効の場合は統計情報はクリアされません。

- mb
  表示するインタフェースが、基本ボード上にある場合に指定します。
- switch
  表示するポートが、スイッチポート (SW1～SW4) である場合に指定します。Si-R180 で指定が可能です。
- スロット番号
  拡張モジュールが挿入されているスロットの番号を指定します。

範囲	機種
0～1	Si-R370
0～3	Si-R570

<line>

指定されたポート上の統計情報をクリアします。
また、該当するポート番号が無効の場合は統計情報はクリアされません。

- <slot>で mb 指定された場合

範囲	機種
0～1	Si-R180　Si-R240
0～3	Si-R570　Si-R370　Si-R260B　Si-R220B

- <slot>で switch 指定された場合

範囲	機種
1～4	Si-R180

- <slot>で 0〜1 指定された場合

範囲	機種
0	Si-R570 Si-R370

- <slot>で 2〜3 指定された場合

範囲	機種
0〜1	Si-R570

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

Ethernet 物理ポートの統計情報をクリアします。
<line>を省略時は、対象<slot>上に搭載される全ポートの統計情報がクリアされます。
<line> および <slot>を省略時は、本装置に搭載される全ポートの統計情報がクリアされます。

[実行例]

以下に、実行例を示します

```
# clear ether statistics
#
```

第 24 章　ISDN のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

24.1 ISDN のカウンタ・ログ・統計・状態などの表示

24.1.1 show isdn

[機能]

ISDN 回線状態の表示

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

show isdn

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

ISDN 回線の現在の状態を表示します。

[実行例]

以下に、実行例を示します。

```
# show isdn
[slot 0 line 0]                                                --- (1)
dial no 0                 : *                                  --- (2)
dial no 1                 : *                                  --- (3)
    [B1ch]
    channel status        : connected(MP)                      --- (4)
    call status           : call-out                           --- (5)
    remote target         : tokyo.ap1 [remote 0 ap 0]          --- (6)
    remote TEL no         : 4588*                              --- (7)
    line speed            : 64000 bps                          --- (8)
    communicated time     : 0000.00:00:01                      --- (9)
    IPCP                  : opened                             --- (10)
    negotiated IP address : local  192.168.1.1                 --- (11)
                          : remote 255.255.255.255             --- (11)
    DNS server address    : 255.255.255.255                    --- (12)
    IPV6CP                : opened                             --- (13)
    BCP                   : opened                             --- (14)
    MPLSCP                : opened                             --- (15)
    send/receive traffic  : 0%/0%                              --- (16)
    [B2ch]
    channel status        : connected(MP)
    call status           : call-out
    remote target         :  [remote 0 ap 0]
    remote TEL no         : 4588*
    line speed            : 64000 bps
    communicated time     : 0000.00:00:04
    IPCP                  : opened
    negotiated IP address : local  192.168.1.1
                          : remote 255.255.255.255
    DNS server address    : 255.255.255.255
    IPV6CP                : opened
    BCP                   : opened
    MPLSCP                : opened
    send/receive traffic  : 0%/0%
```

1) スロット番号、回線番号
スロット番号、および回線番号が表示されます。Si-R220B では表示されません。

2) 自局番号 0
設定済みの自局番号 0 が表示されます。「*」以降はサブアドレスです。

3) 自局番号 1
設定済みの自局番号 1 が表示されます。「*」以降はサブアドレスです。

4) 回線状態
以下のどれかが表示されます。

enabling　同期確立中

synchronization failed
同期外れ状態

idle　チャネル未使用

disconnecting
切断中

connected
通信中

connected(MP)
MP で通信中

callin　着信処理中

alerting　相手呼出中

以下の情報は、通信中 (「channel status」が connected) の場合だけ表示されます。

5) 接続方向
以下のどれかが表示されます。

call-out　発信によって接続

call-in　着信によって接続

6) 相手ネットワーク名、接続先名 (テンプレート着信の場合はテンプレート番号、ユーザ ID)
接続中の相手ネットワーク名と接続先名が表示されます。
テンプレート着信による接続の場合は、テンプレート番号とユーザ ID が表示されます。

7) 接続先電話番号
接続先の電話番号が表示されます。

8) 回線速度
接続中の回線の回線速度が表示されます。

9) 通信時間
通信時間が以下の形式で表示されます。dddd.hh:mm:ss (日. 時:分:秒)

10) IPCP 状態
以下のどれかが表示されます。

opened　IPv4 利用可能

negotiating
IPCP ネゴシエーション中

closed　IPv4 利用不可能

11) 自側 IP アドレス→相手側 IP アドレス

IPCP のアドレスネゴシエーション結果が表示されます。アドレスネゴシエーションなしで接続した場合は、255.255.255.255 となります。

12) DNS サーバアドレス

IPCP の DNS サーバアドレスネゴシエーション結果が表示されます。DNS サーバアドレスネゴシエーションなしで接続した場合は、255.255.255.255 となります。

13) IPV6CP 状態

以下のどれかが表示されます。

opened IPv6 利用可能

negotiating
IPv6CP ネゴシエーション中

closed IPv6 利用不可能

14) BCP 状態

以下のどれかが表示されます。

opened Bridge 利用可能

negotiating
BCP ネゴシエーション中

closed Bridge 利用不可能

15) MPLS 状態

以下のどれかが表示されます。

opened MPLS 利用可能

negotiating
MPLSCP ネゴシエーション中

closed MPLS 利用不可能

16) 送信回線使用率/受信回線使用率

データ送受信の回線使用率が表示されます。

24.1.2　show isdn account

[機能]

ISDN のアカウントの表示

[適用機種]

Si-R 570 | Si-R 370 | | | Si-R 220B | |

[入力形式]

show isdn account

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

ISDN のアカウントを表示します。

[実行例]

以下に、実行例を示します。

```
# show isdn account
[wan 0]
Call Account:
  call setup count    = 2  --- (1)
  call busy count     = 0  --- (2)
  call error count    = 0  --- (3)
Called Account:
  called accept count = 0  --- (4)
  called reject count = 0  --- (5)

Time/Charge Account:
  total time for callout  = 0000.00:03:04      --- (6)
  total charge            = 10                 --- (7)
  peak time   remote      = internet.ISP-1     --- (8)
              time        = 0000.00:02:57      --- (9)
              charge      = 10                 --- (10)
  peak charge remote      = internet.ISP-1     --- (11)
              time        = 0000.00:02:57      --- (12)
              charge      = 10                 --- (13)
  last        remote      = intranet.OFFICE-I  --- (14)
              time        = 0000.00:00:07      --- (15)
              charge      = 0                  --- (16)

Access-point Time/Charge:
  remote  ap    charge  time
       0   0         0  0000.00:00:00
     199  99         0  0000.00:00:00
 └────────┴──┴─────────┴──────────────┘
   (17)  (18)    (19)     (20)
#
```

1) 発信の回数

2) 着ユーザビジーによって発信失敗した回数

3) 着ユーザビジー以外の網理由で発信失敗した回数

4) 着信の回数
5) 着信を拒否した回数
6) 発信接続の総通信時間
7) 総課金額
8) 最長接続時の相手名
9) 最長接続時の接続時間
10) 最長接続時の課金額
11) 最高課金時の相手名
12) 最高課金時の接続時間
13) 最高課金時の課金額
14) 最終接続時の相手名
15) 最終接続時の接続時間
16) 最終接続時の課金額
17) 相手定義番号
18) 接続先定義番号
19) 課金の合計金額
20) 接続の合計時間

24.1.3　show isdn statistics circuit

[機能]

ISDN 回線の統計情報の表示

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

show isdn statistics circuit

[オプション]

なし

ISDN 回線の統計情報を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

ISDN 回線の統計情報を表示します。

[実行例]

以下に、実行例を示します。

(BRI ISDN)(Si-R220B の場合)

```
# show isdn statistics circuit
[LINE STATUS]
date                      : Oct 14 16:00:40 2002      --- (1)
channel                   : [MB][CNCT0][D]            --- (2)
 speed                    : 16k                       --- (3)
 status                   : wait sync                 --- (4)
 since                    : Oct 14 16:00:24 2002      --- (5)
 func                     : Q921                      --- (6)
[D CHANNEL INFORMATION]
received frame            : 0                         --- (7)
         bytes            : 0                         --- (8)
sent     frame            : 0                         --- (9)
         bytes            : 0                         --- (10)
Input frame dropped
  busy                    : 0                         --- (11)
  CRC error               : 0                         --- (12)
  abort frame             : 0                         --- (13)
  bad length              : 0                         --- (14)
  bad octet               : 0                         --- (15)
Output frame dropped
  underrun                : 0                         --- (16)
Collision count           : 0                         --- (17)
SYNC    count             : 0                         --- (18)
        time              : 0                         --- (19)
OUTSYNC count             : 0                         --- (20)
        time              : 53                        --- (21)

[LINE STATUS]
date                      : Oct 14 16:00:40 2002      --- (1)
channel                   : [MB][CNCT0][B1]           --- (2)
 speed                    : 64k                       --- (3)
 status                   : wait setline              --- (4)
 since                    : Oct 14 16:00:24 2002      --- (5)
 func                     : HDLC                      --- (6)
[LINE LOG INFORMATION]
received frame            : 0                         --- (7)
         bytes            : 0                         --- (8)
sent     frame            : 0                         --- (9)
         bytes            : 0                         --- (10)
Input frame dropped
  busy                    : 0                         --- (11)
  CRC error               : 0                         --- (12)
  abort frame             : 0                         --- (13)
  bad length              : 0                         --- (14)
  bad octet               : 0                         --- (15)
Output frame dropped
  underrun                : 0                         --- (16)
Flow control
  limit                   : 0                         --- (22)
  count                   : 0                         --- (23)
  condition               : XON                       --- (24)
Flag send/monitor mode    : yes/no                    --- (25)
  flag recv               : 0                         --- (26)
  idle recv               : 0                         --- (27)
  flag received count     : 0                         --- (28)
                 time     : 0                         --- (29)
  idle received count     : 0                         --- (30)
                 time     : 0                         --- (31)
```

(BRI ISDN)(Si-R570 Si-R370 の場合)

```
# show isdn statistics circuit
[LINE STATUS]
date                      : Oct 14 16:00:40 2002      --- (1)
channel                   : [SLOT0][CNCT0][D]         --- (2)
 speed                    : 16k                       --- (3)
 status                   : wait sync                 --- (4)
 since                    : Oct 14 16:00:24 2002      --- (5)
 func                     : Q921                      --- (6)
[D CHANNEL INFORMATION]
received frame            : 0                         --- (7)
         bytes            : 0                         --- (8)
sent     frame            : 0                         --- (9)
         bytes            : 0                         --- (10)
Input frame dropped
  busy                    : 0                         --- (11)
  CRC error               : 0                         --- (12)
  abort frame             : 0                         --- (13)
  bad length              : 0                         --- (14)
  bad octet               : 0                         --- (15)
Output frame dropped
  underrun                : 0                         --- (16)
Collision count           : 0                         --- (17)
SYNC    count             : 0                         --- (18)
        time              : 0                         --- (19)
OUTSYNC count             : 0                         --- (20)
        time              : 53                        --- (21)

[LINE STATUS]
date                      : Oct 14 16:00:40 2002      --- (1)
channel                   : [SLOT0][CNCT0][B1]        --- (2)
 speed                    : 64k                       --- (3)
 status                   : wait setline              --- (4)
 since                    : Oct 14 16:00:24 2002      --- (5)
 func                     : HDLC                      --- (6)
[LINE LOG INFORMATION]
received frame            : 0                         --- (7)
         bytes            : 0                         --- (8)
sent     frame            : 0                         --- (9)
         bytes            : 0                         --- (10)
Input frame dropped
  busy                    : 0                         --- (11)
  CRC error               : 0                         --- (12)
  abort frame             : 0                         --- (13)
  bad length              : 0                         --- (14)
  bad octet               : 0                         --- (15)
Output frame dropped
  underrun                : 0                         --- (16)
Flow control
  limit                   : 0                         --- (22)
  count                   : 0                         --- (23)
  condition               : XON                       --- (24)
Flag send/monitor mode    : yes/no                    --- (25)
  flag recv               : 0                         --- (26)
  idle recv               : 0                         --- (27)
  flag received count     : 0                         --- (28)
                 time     : 0                         --- (29)
  idle received count     : 0                         --- (30)
                 time     : 0                         --- (31)
```

(PRI ISDN)(Si-R570 Si-R370 の場合)

```
# show isdn statistics circuit
[LINE STATUS]
date                      : Oct 14 16:00:40 2002      --- (1)
channel                   : [SLOT0][CNCT0][D]         --- (2)
 speed                    : 64k                       --- (3)
 status                   : data                      --- (4)
 since                    : Oct 14 16:00:24 2002      --- (5)
 func                     : Q921                      --- (6)
[D CHANNEL INFORMATION]
received frame            : 0                         --- (7)
         bytes            : 0                         --- (8)
sent     frame            : 0                         --- (9)
         bytes            : 0                         --- (10)
Input frame dropped
  busy                    : 0                         --- (11)
  CRC error               : 0                         --- (12)
  abort frame             : 0                         --- (13)
  bad length              : 0                         --- (14)
  bad octet               : 0                         --- (15)
Output frame dropped
  underrun                : 0                         --- (16)
Received Signal count
  No signal Indication    : 10                        --- (32)
  Alarm Indication signal : 0                         --- (33)
  Loss of Synchronization : 7                         --- (34)
  Receive Remote Alarm    : 0                         --- (35)
SYNC    count             : 4                         --- (18)
        time              : 35099                     --- (19)
OUTSYNC count             : 3                         --- (20)
        time              : 6                         --- (21)

                      B1  ～  B22 の表示

[LINE STATUS]
date                      : Oct 14 16:00:40 2002      --- (1)
channel                   : [SLOT0][CNCT0][B23]       --- (2)
 speed                    : 64k                       --- (3)
 status                   : wait setline              --- (4)
 since                    : Oct 14 16:00:24 2002      --- (5)
 func                     : HDLC                      --- (6)
[LINE LOG INFORMATION]
received frame            : 0                         --- (7)
         bytes            : 0                         --- (8)
sent     frame            : 0                         --- (9)
         bytes            : 0                         --- (10)
Input frame dropped
  busy                    : 0                         --- (11)
  CRC error               : 0                         --- (12)
  abort frame             : 0                         --- (13)
  bad length              : 0                         --- (14)
  bad octet               : 0                         --- (15)
Output frame dropped
  underrun                : 0                         --- (16)
Flow control
  limit                   : 0                         --- (22)
  count                   : 0                         --- (23)
  condition               : XON                       --- (24)
Flag send/monitor mode    : yes/yes                   --- (25)
  flag recv               : 0                         --- (26)
  idle recv               : 0                         --- (27)
  flag received count     : 0                         --- (28)
                 time     : 0                         --- (29)
  idle received count     : 0                         --- (30)
                 time     : 0                         --- (31)
```

表示内容の説明 (D/B チャネル表示)

1) コマンド投入時刻

コマンドが入力された時刻を表示します。

2) チャネル種別

スロット番号、ライン番号、D、B1、B2(PRI の場合 B23 まで) のどれかが表示されます。

3) 通信速度

通信速度が kbps 単位で表示されます。

4) チャネル状態

以下のどれかが表示されます。

Init : 初期化中状態

Wait Setline :
チャネル未使用状態

Wait Enable :
チャネル使用開始待ち状態

Wait Sync :
同期確立待ち状態

Wait Call :
発着信待ち状態 (呼毎起動)

Wait Sync_s :
発信時同期確立待ち状態 (呼毎起動)

Outsync : 同期はずれ検出状態

Wait Enable_con :
チャネル起動中状態

Data : データ送受信可能状態

Wait Disable :
チャネル停止指示待ち状態

Wait Disable_con:
チャネル停止完了待ち状態

Wait Flag :
フラグ受信待ち状態

Recv IDLE :
アイドル受信検出状態

5) 状態遷移時刻

チャネル状態が現在の状態に変化した時刻を表示します。

6) 通信種別

以下のどれかが表示されます。

Q921 D チャネルの場合に表示されます

Q921(per-call)
呼毎起動指定時の D チャネルの場合に表示されます

HDLC HDLC プロトコル使用時に表示されます

PIAFS PIAFS プロトコル使用時に表示されます

TRANSPARENT
トランスペアレント使用時に表示されます

7) 受信フレーム数

8) 受信バイト数

9) 送信フレーム数
10) 送信バイト数
11) 受信バッファビジー検出回数
12) 受信 CRC エラー検出回数
13) 受信アボートエラー検出回数
14) 受信フレーム長違反検出回数
15) 受信非オクテットフレーム検出回数
16) 送信アンダーラン検出回数
17) 衝突検出回数
18) 同期確立通知回数
19) 同期確立時間 (100ms 単位)
20) 同期外れ通知回数
21) 同期外れ時間 (100ms 単位)
22) フロー制御しきい値
23) 総送信要求バイト数
24) フロー制御状態
25) フラグ送信・監視モード状態
26) フラグ受信検出回数
27) フラグ断検出回数
28) フラグ受信通知回数
29) フラグ受信時間 (100ms 単位)
30) フラグ断通知回数
31) フラグ断時間 (100ms 単位)
32) No Signal Indication 検出回数
33) Alarm Indication Signal 検出回数
34) Loss of Synchronization 検出回数
35) Receive Remote Alarm 検出回数

24.1.4　show isdn statistics piafs

[機能]

PIAFS 統計情報の表示

[適用機種]

Si-R 370　Si-R 220B

[入力形式]

show isdn statistics piafs

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

PIAFS の統計情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show isdn statistics piafs
[LINE LOG INFORMATION]
channel                   : [MB][CNCT0][B1] --- (1)
received frame            : 548             --- (2)
received byte             : 41648           --- (3)
 bad CRC                  : 45              --- (4)
 buffer full              : 0               --- (5)
sent frame                : 727             --- (6)
sent byte                 : 55252           --- (7)
 sent idle data           : 1               --- (8)
[PIAFS LOG INFORMATION]
 duplicate frame          : 89  --- (9)
 bad FCS                  : 45  --- (10)
 other error              : 0   --- (11)
 send retry (over RTF)    : 1   --- (12)
 re-synchronization       : 0   --- (13)
 t010 timeout             : 1   --- (14)
 t011 timeout             : 0   --- (15)
 t012 timeout             : 0   --- (16)
 resync by Xbit           : 0   --- (17)
 sync 32k                 : 1   --- (18)
 sync 64k                 : 0   --- (19)
 t001 timeout             : 0   --- (20)
 t002 timeout             : 0   --- (21)
 t003 timeout             : 0   --- (22)
 t101 timeout             : 0   --- (23)
 output NEGO
   request                : 4   --- (24)
   accept                 : 1   --- (25)
   reject                 : 0   --- (26)
   reject cause           : 0   --- (27)
 output PARAM
   request                : 0   --- (28)
```

(続く)

(続き)

```
   accept                 : 8   --- (29)
   reject                 : 0   --- (30)
   reject cause           : 0   --- (31)
 output SYNC
   request                : 0   --- (32)
   accept                 : 0   --- (33)
   reject                 : 0   --- (34)
   reject cause           : 0   --- (35)
 output ARQ
   request                : 0   --- (36)
   accept                 : 0   --- (37)
   reject                 : 0   --- (38)
   reject cause           : 0   --- (39)
 output REL
   request                : 0   --- (40)
   accept                 : 6   --- (41)
   reject                 : 0   --- (42)
   request cause          : 0   --- (43)
   reject cause           : 0   --- (44)
 input NEGO
   request                : 7   --- (45)
   accept                 : 0   --- (46)
   reject                 : 0   --- (47)
   reject cause           : 0   --- (48)
 input PARAM
   request                : 8   --- (49)
   accept                 : 0   --- (50)
   reject                 : 0   --- (51)
   reject cause           : 0   --- (52)
 input SYNC
   request                : 0   --- (53)
   accept                 : 0   --- (54)
   reject                 : 0   --- (55)
   reject cause           : 0   --- (56)
 input ARQ
   request                : 0   --- (57)
   accept                 : 0   --- (58)
   reject                 : 0   --- (59)
   reject cause           : 0   --- (60)
 input REL
   request                : 6   --- (61)
   accept                 : 0   --- (62)
   reject                 : 0   --- (63)
   request cause          : 17  --- (64)
   reject cause           : 0   --- (65)
 input unknown            : 0   --- (66)
 input nop                : 0   --- (67)
 input nop2               : 0   --- (68)

[PIAFS CONTROL INFORMATION]
 protocol                 : 4   --- (69)
 negotiated param
   data protocol          : 1   --- (70)
   control protocol       : 2   --- (71)
   rtf                    : 9   --- (72)
   compress               : 0   --- (73)
   p1                     : 0   --- (74)
   p2                     : 0   --- (75)
   frame length           : 80  --- (76)
   M                      : 63  --- (77)
   fi format              : 1   --- (78)
   sync format            : 1   --- (79)

[LINE LOG INFORMATION]
channel                   : [MB][CNCT0][B2]
                ⋮
                ⋮
```

1) チャネル種別

スロット番号、ライン番号、チェネル種別が表示されます。

2) 受信フレーム数

3) 受信バイト数
4) 受信 CRC エラー検出回数
5) 受信バッファビジー検出回数
6) 送信フレーム数
7) 送信バイト数
8) 空フレーム送出回数

以降の情報は接続時に一度クリアされます。

9) データ二重受信
10) FCS エラー発生回数
11) FCS エラー以外発生回数
12) データフレーム再送回数
13) 再同期発生回数
14) 送受信速度切り替えタイマ A(T010) タイムアウト発生回数
15) 送受信速度切り替えタイマ B(T011) タイムアウト発生回数
16) 送受信速度切り替えタイマ C(T012) タイムアウト発生回数
17) 対応伝送速度切り替え通知による速度切り替え発生回数
18) 32Kbps 同期回数
19) 64Kbps 同期回数
20) 同期受付待ちタイマ (T001) タイムアウト発生回数
21) 同期受付送出後タイマ (T002) タイムアウト発生回数
22) 同期要求待ちタイマ (T003) タイムアウト発生回数
23) 制御送信確認待ちタイマ (T101) タイムアウト発生回数
24) ネゴ同期要求送信回数
25) ネゴ同期受付送信回数
26) ネゴ同期拒否送信回数
27) ネゴ同期拒否理由
28) 通信パラメタ設定要求送信回数
29) 通信パラメタ設定受付送信回数
30) 通信パラメタ設定拒否送信回数
31) 通信パラメタ設定拒否理由
32) 同期要求送信回数
33) 同期受付送信回数
34) 同期拒否送信回数
35) 同期拒否理由
36) ARQ パラメタ設定要求送信回数
37) ARQ パラメタ設定受付送信回数
38) ARQ パラメタ設定拒否送信回数
39) ARQ パラメタ設定拒否理由
40) データリンク解放要求送信回数

41) データリンク解放受付送信回数
42) データリンク解放拒否送信回数
43) データリンク解放要求理由
44) データリンク解放拒否理由
45) ネゴ同期要求受信回数
46) ネゴ同期受付受信回数
47) ネゴ同期拒否受信回数
48) ネゴ同期拒否理由
49) 通信パラメタ設定要求受信回数
50) 通信パラメタ設定受付受信回数
51) 通信パラメタ設定拒否受信回数
52) 通信パラメタ設定拒否理由
53) 同期要求受信回数
54) 同期受付受信回数
55) 同期拒否受信回数
56) 同期拒否理由
57) ARQ パラメタ設定要求受信回数
58) ARQ パラメタ設定受付受信回数
59) ARQ パラメタ設定拒否受信回数
60) ARQ パラメタ設定拒否理由
61) データリンク解放要求受信回数
62) データリンク解放受付受信回数
63) データリンク解放拒否受信回数
64) データリンク解放要求理由
65) データリンク解放拒否理由
66) 未定義フレーム受信回数
67) 受信破棄フレーム数
68) 受信破棄フレーム数 2
69) プロトコル種別
70) ARQ データ伝送プロトコルバージョン
71) ARQ 制御情報伝送プロトコルバージョン
72) 測定 RTF 値
73) データ圧縮方式識別子
74) 符号語総数 (P1)
75) 最大文字列長 (P2)
76) フレーム長
77) 最大フレーム番号 (M)
78) FI 構造識別子
79) 同期フレーム構造識別子

24.2　ISDN のカウンタ・ログ・統計などのクリア

24.2.1　clear isdn statistics circuit

[機能]

ISDN 回線の統計情報のクリア

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

clear isdn statistics circuit

[オプション]

なし

統計情報をクリアします。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

ISDN 回線の統計情報をクリアします。

[実行例]

以下に、実行例を示します。

```
# clear isdn statistics
#
```

24.2.2 clear isdn account

[機能]

ISDN のアカウント情報のクリア

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

clear isdn account

[オプション]

なし

ISDN のアカウント情報をクリアします。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

ISDN のアカウント情報をクリアします。

[実行例]

```
# clear isdn account
#
```

24.2.3　clear isdn statistics piafs

[機能]

PIAFS 統計情報のクリア

[適用機種]

	Si-R 370			Si-R 220B	

[入力形式]

clear isdn statistics piafs

[オプション]

なし

PIAFS 統計情報をクリアします。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

PIAFS の統計情報をクリアします。

[実行例]

```
# clear isdn statistics piafs
#
```

第 25 章　フレームリレーのカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

25.1　フレームリレーのカウンタ・ログ・統計・状態などの表示

25.1.1　show fr

[機能]

フレームリレー回線状態の表示

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

show fr

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

フレームリレー回線の現在の状態を表示します。

[実行例]

以下に、実行例を示します。

```
# show fr
[slot 0 line 0]                                          ---(1)
line speed                : 128Kbps                      ---(2)
line status               : synchronization failed       ---(3)
    [DLCI: 17]
    vc status             : active                       ---(4)
    communicated time     : 0000.00:00:00                ---(5)
    remote target         : rmt0.ap0 [remote 0 ap 0]     ---(6)
    remote DLCI           : 0                            ---(7)
    remote IP address     : 192.168.100.2                ---(8)
    local IP address      : 192.168.100.1                ---(9)
    CIR                   : 0                            ---(10)
    send/receive traffic  : 0%/0%                        ---(11)
#
```

1) スロット番号、回線番号

スロット番号、および回線番号が表示されます。Si-R220B では表示されません。

2) 回線速度

回線速度が表示されます。

3) 回線状態

以下のどれかが表示されます。

enabling　同期確立中

synchronization failed

同期外れ状態

connected

通信中

disconnected

利用者指示による停止中

以下は定義された DLCI 単位に表示されます。

4) VC 状態

以下のどれかが表示されます。

- active

  通信可能状態

- inactive

  VC 復旧待ち状態

5) 通信時間

通信時間が以下の形式で表示されます。

dddd.hh:mm:ss (日. 時:分:秒)

6) 相手ネットワーク名、接続先名

接続中の相手ネットワーク名と接続先名が表示されます。

7) 相手 DLCI

相手 DLCI が表示されます。

8) 相手 IP アドレス

相手 IP アドレスが表示されます。

9) 自 IP アドレス

自 IP アドレスが表示されます。

10) CIR

定義した CIR(認定情報速度) が表示されます。

11) 送信回線使用率/受信回線使用率

データ送受信の回線使用率が表示されます。

25.1.2　show fr statistics circuit

[機能]

フレームリレー回線の統計情報の表示

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

show fr statistics circuit

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

フレームリレー回線または専用線の統計情報を表示します。

[実行例]

以下に、実行例を示します。

(BRI フレームリレー/専用線) (Si-R220B の場合)

```
# show fr statistics circuit
[LINE STATUS]
date                      : Oct 14 16:00:40 2002      --- (1)
channel                   : [MB][CNCT0][-]            --- (2)
 speed                    :                           --- (3)
 status                   : data                      --- (4)
 since                    : Oct 14 16:00:24 2002      --- (5)
 func                     :                           --- (6)
[LAYER1 INFORMATION]
SYNC    count             : 4                         --- (18)
        time              : 35099                     --- (19)
OUTSYNC count             : 3                         --- (20)
        time              : 6                         --- (21)

[LINE STATUS]
date                      : Oct 14 16:00:40 2002      --- (1)
channel                   : [MB][CNCT0][-]            --- (2)
 speed                    : 128k                      --- (3)
 status                   : data                      --- (4)
 since                    : Oct 14 16:00:24 2002      --- (5)
 func                     : HDLC                      --- (6)
[LINE LOG INFORMATION]
received frame            : 0                         --- (7)
         bytes            : 0                         --- (8)
sent     frame            : 0                         --- (9)
         bytes            : 0                         --- (10)
Input frame dropped
  busy                    : 0                         --- (11)
  CRC error               : 0                         --- (12)
  abort frame             : 0                         --- (13)
  bad length              : 0                         --- (14)
  bad octet               : 0                         --- (15)
Output frame dropped
  underrun                : 0                         --- (16)
Flow control
  limit                   : 0                         --- (22)
  count                   : 0                         --- (23)
  condition               : XON                       --- (24)
Flag send/monitor mode    : no/no                     --- (25)
  flag recv               : 0                         --- (26)
  idle recv               : 0                         --- (27)
  flag received count     : 0                         --- (28)
                 time     : 0                         --- (29)
  idle received count     : 0                         --- (30)
                 time     : 0                         --- (31)
```

(BRI フレームリレー/専用線)(Si-R570 Si-R370 の場合)

```
# show fr statistics circuit
[LINE STATUS]
date                      : Oct 14 16:00:40 2002      --- (1)
channel                   : [SLOT0][CNCT0][-]         --- (2)
 speed                    :                           --- (3)
 status                   : data                      --- (4)
 since                    : Oct 14 16:00:24 2002      --- (5)
 func                     :                           --- (6)
[LAYER1 INFORMATION]
SYNC    count             : 4                         --- (18)
        time              : 35099                     --- (19)
OUTSYNC count             : 3                         --- (20)
        time              : 6                         --- (21)

[LINE STATUS]
date                      : Oct 14 16:00:40 2002      --- (1)
channel                   : [SLOT0][CNCT0][-]         --- (2)
 speed                    : 128k                      --- (3)
 status                   : data                      --- (4)
 since                    : Oct 14 16:00:24 2002      --- (5)
 func                     : HDLC                      --- (6)
[LINE LOG INFORMATION]
received frame            : 0                         --- (7)
         bytes            : 0                         --- (8)
sent     frame            : 0                         --- (9)
         bytes            : 0                         --- (10)
Input frame dropped
  busy                    : 0                         --- (11)
  CRC error               : 0                         --- (12)
  abort frame             : 0                         --- (13)
  bad length              : 0                         --- (14)
  bad octet               : 0                         --- (15)
Output frame dropped
  underrun                : 0                         --- (16)
Flow control
  limit                   : 0                         --- (22)
  count                   : 0                         --- (23)
  condition               : XON                       --- (24)
Flag send/monitor mode    : no/no                     --- (25)
  flag recv               : 0                         --- (26)
  idle recv               : 0                         --- (27)
  flag received count     : 0                         --- (28)
                 time     : 0                         --- (29)
  idle received count     : 0                         --- (30)
                 time     : 0                         --- (31)
```

(PRI フレームリレー/専用線)(Si-R570 Si-R370 の場合)

```
# show fr statistics circuit
[LINE STATUS]
date                      : Oct 14 16:00:40 2002      --- (1)
channel                   : [SLOT0][CNCT0][-]         --- (2)
 speed                    :                           --- (3)
 status                   : data                      --- (4)
 since                    : Oct 14 16:00:24 2002      --- (5)
 func                     :                           --- (6)
[LAYER1 INFORMATION]
 Received Signal count
  No signal Indication    : 10                        --- (32)
  Alarm Indication signal : 0                         --- (33)
  Loss of Synchronization : 7                         --- (34)
  Receive Remote Alarm    : 0                         --- (35)
SYNC    count             : 4                         --- (18)
        time              : 35099                     --- (19)
OUTSYNC count             : 3                         --- (20)
        time              : 6                         --- (21)

[LINE STATUS]
date                      : Oct 14 16:00:40 2002      --- (1)
channel                   : [SLOT0][CNCT0][-]         --- (2)
 speed                    : 1536k                     --- (3)
 status                   : data                      --- (4)
 since                    : Oct 14 16:00:24 2002      --- (5)
 func                     : HDLC                      --- (6)
[LINE LOG INFORMATION]
received frame            : 151                       --- (7)
         bytes            : 43286                     --- (8)
sent     frame            : 171                       --- (9)
         bytes            : 52577                     --- (10)
Input frame dropped
  busy                    : 0                         --- (11)
  CRC error               : 2                         --- (12)
  abort frame             : 4                         --- (13)
  bad length              : 0                         --- (14)
  bad octet               : 1                         --- (15)
Output frame dropped
  underrun                : 0                         --- (16)
Flow control
  limit                   : 4096                      --- (22)
  count                   : 0                         --- (23)
  condition               : XON                       --- (24)
Flag send/monitor mode    : yes/yes                   --- (25)
  flag recv               : 31                        --- (26)
  idle recv               : 34                        --- (27)
  flag received count     : 4                         --- (28)
                 time     : 35097                     --- (29)
  idle received count     : 4                         --- (30)
                 time     : 2                         --- (31)
```

表示内容の説明 (D/B チャネル表示)

1) コマンド投入時刻

コマンドが入力された時刻を表示します。

2) チャネル種別

スロット番号、ライン番号が表示されます。

3) 通信速度

通信速度が kbps 単位で表示されます。

4) チャネル状態

以下のどれかが表示されます。

Init : 初期化中状態

Wait Setline :

チャネル未使用状態

Wait Enable :

チャネル使用開始待ち状態

Wait Sync :

同期確立待ち状態

Wait Call :

発着信待ち状態 (呼毎起動)

Wait Sync_s :

発信時同期確立待ち状態 (呼毎起動)

Outsync : 同期はずれ検出状態

Wait Enable_con :

チャネル起動中状態

Data : データ送受信可能状態

Wait Disable :

チャネル停止指示待ち状態

Wait Disable_con:

チャネル停止完了待ち状態

Wait Flag :

フラグ受信待ち状態

Recv IDLE :

アイドル受信検出状態

5) 状態遷移時刻

チャネル状態が現在の状態に変化した時刻を表示します。

6) 通信種別

以下のどれかが表示されます。

Q921 D チャネルの場合に表示されます

Q921(per-call)

呼毎起動指定時の D チャネルの場合に表示されます

HDLC HDLC プロトコル使用時に表示されます

PIAFS PIAFS プロトコル使用時に表示されます

TRANSPARENT

トランスペアレント使用時に表示されます

7) 受信フレーム数

8) 受信バイト数

9) 送信フレーム数

10) 送信バイト数

11) 受信バッファビジー検出回数

12) 受信 CRC エラー検出回数

13) 受信アボートエラー検出回数

14) 受信フレーム長違反検出回数

15) 受信非オクテットフレーム検出回数

16) 送信アンダーラン検出回数
17) 衝突検出回数
18) 同期確立通知回数
19) 同期確立時間 (100ms 単位)
20) 同期外れ通知回数
21) 同期外れ時間 (100ms 単位)
22) フロー制御しきい値
23) 総送信要求バイト数
24) フロー制御状態
25) フラグ送信・監視モード状態
26) フラグ受信検出回数
27) フラグ断検出回数
28) フラグ受信通知回数
29) フラグ受信時間 (100ms 単位)
30) フラグ断通知回数
31) フラグ断時間 (100ms 単位)
32) No Signal Indication 検出回数
33) Alarm Indication Signal 検出回数
34) Loss of Synchronization 検出回数
35) Receive Remote Alarm 検出回数

25.1.3　show fr statistics vc

[機能]

フレームリレー回線の PVC 統計情報の表示

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

show fr statistics vc

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

フレームリレー回線の PVC 統計情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show fr statistics vc

[slot 0 line 0]                        --- (1)

[DLCI: 16]                             --- (2)
  CIR                   : 0            --- (3)
  trans state           : active       --- (4)
  load state            : send(min)    --- (5)
  possible send bytes   : 819          --- (6)
  max send bytes        : 819          --- (7)
  max send bytes(lower) : 819          --- (8)
  max send bytes(upper) : 819          --- (9)
  max send bytes(CIR)   : 819          --- (10)
  sending bytes         : 0            --- (11)
  send throughput       : 0 bytes/s    --- (12)
  waiting send packets  : 0            --- (13)
  fecn received         : 0            --- (14)
  becn received         : 0            --- (15)
  send errors           : 0            --- (16)
  receive errors        : 0            --- (17)
  send bytes            : 37141        --- (18)
  receive bytes         : 1426753      --- (19)

[DLCI: 17]
  CIR                   : 0
  trans state           : active
  load state            : send(min)
  possible send bytes   : 819
  max send bytes        : 819
  max send bytes(lower) : 819
  max send bytes(upper) : 819
  max send bytes(CIR)   : 819
  sending bytes         : 0
  send throughput       : 0 bytes/s
  waiting send packets  : 0
  fecn received         : 0
  becn received         : 0
  send errors           : 0
  receive errors        : 0
  send bytes            : 0
  receive bytes         : 0

#
```

1) スロット番号、回線番号

   スロット番号、および回線番号が表示されます。Si-R220B では必ず [MB] (基本ボード) が表示されます。

2) DLCI 番号

3) CIR 値

4) 伝送制御状態

   - disable

     enable 指示待ち

   - inactive

     enable 状態 (inactive)

   - active

     enable 状態 (active)

5) 輻輳制御状態

   - stop

     停止状態

   - send(min)

     下限値で送信中

- send(min..cir)
  下限から CIR で送信中
- send(cir)
  CIR で送信中
- send(cir..max)
  CIR から上限で送信中
- send(max)
  上限値で送信中

6) 送出可能データ量 (byte)
7) Tc(100ms) 時間内に送出できる最大データ長 (byte)
8) Tc(100ms) 時間内に送出できる最大データ長の下限値 (byte)
9) Tc(100ms) 時間内に送出できる最大データ長の上限値 (byte)
10) Tc(100ms) 時間内に送出できる最大データ長に CIR 値適用 (byte)
11) 送信中バイト数 (残り)
12) 送信スループット (byte/s)
13) 送信待ちパケット数
14) 1 時間ごとの FECN ON フレーム受信回数
15) 1 時間ごとの BECN ON フレーム受信回数
16) 送信フレーム破棄回数 (合計)
17) 受信フレーム破棄回数 (合計)
18) 送信バイト数 (合計)
19) 受信バイト数 (合計)

25.2　フレームリレーのカウンタ・ログ・統計などのクリア

25.2.1　clear fr statistics circuit

[機能]

フレームリレー回線の統計情報のクリア

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

clear fr statistics circuit

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

フレームリレー回線または専用線の統計情報をクリアします。

[実行例]

以下に、実行例を示します。

```
# clear fr statistics circuit
#
```

25.2.2　clear fr statistics vc

[機能]

フレームリレー回線の PVC 統計情報のクリア

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

clear fr statistics vc

[オプション]

なし

すべての PVC の統計情報をクリアします。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

フレームリレー回線の PVC 統計情報をクリアします。

[実行例]

```
# clear fr statistics vc
#
```

第 26 章　専用線のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

26.1　専用線のカウンタ・ログ・統計・状態などの表示

26.1.1　show hsd

[機能]

専用線状態の表示

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

show hsd

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

専用線の現在の状態を表示します。

[実行例]

以下に、実行例を示します。

```
# show hsd
[slot 0 line 0]                                          --- (1)
line speed              : 64Kbps                         --- (2)
line status             : connected                      --- (3)
communicated time       : 0000.00:30:03                  --- (4)
IPCP                    : opened                         --- (5)
negotiated IP address   : local  192.168.1.1             --- (6)
                        : remote 192.168.2.1             --- (6)
IPV6CP                  : opened                         --- (7)
BCP                     : opened                         --- (8)
MPLSCP                  : opened                         --- (9)
send/receive traffic    : 0%/0%                          --- (10)
#
```

1) スロット番号、回線番号

スロット番号、および回線番号が表示されます。Si-R220B では表示されません。

2) 回線速度

回線速度が表示されます。

3) 回線状態

以下のどれかが表示されます。

enabling　同期確立中

synchronization failed

同期外れ状態

connected
通信中

disconnected
利用者指示による停止中

flag pattern lost
フラグ未検出状態

idle 回線未使用

以下の情報は、通信中 (「line status」が connected) の場合だけ表示されます。

4) 通信時間
通信時間が以下の形式で表示されます。
dddd.hh:mm:ss (日. 時:分:秒)

5) IPCP 状態
以下のどれかが表示されます。

opened IPv4 利用可能

negotiating
IPCP ネゴシエーション中

closed IPv4 利用不可能

6) 自側 IP アドレス→相手側 IP アドレス
IPCP のアドレスネゴシエーション結果が表示されます。アドレスネゴシエーションなしで接続した場合は、255.255.255.255 となります。

7) IPV6CP 状態
以下のどれかが表示されます。

opened IPv6 利用可能

negotiating
IPv6CP ネゴシエーション中

closed IPv6 利用不可能

8) BCP 状態
以下のどれかが表示されます。

opened Bridge 利用可能

negotiating
BCP ネゴシエーション中

closed Bridge 利用不可能

9) MPLSCP 状態
以下のどれかが表示されます。

opened MPLS 利用可能

negotiating
MPLSCP ネゴシエーション中

closed MPLS 利用不可能

10) 送信回線使用率/受信回線使用率
データ送受信の回線使用率が表示されます。

26.1.2　show hsd statistics circuit

[機能]

専用線の統計情報の表示

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

show hsd statistics circuit

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

専用線またはフレームリレー回線の統計情報を表示します。

[実行例]

以下に、実行例を示します。

(BRI フレームリレー/専用線) (Si-R220B の場合)

```
# show hsd statistics circuit
[LINE STATUS]
date                      : Oct 14 16:00:40 2002      --- (1)
channel                   : [MB][CNCT0][-]            --- (2)
 speed                    :                           --- (3)
 status                   : data                      --- (4)
 since                    : Oct 14 16:00:24 2002      --- (5)
 func                     :                           --- (6)
[LAYER1 INFORMATION]
SYNC    count             : 4                         --- (18)
        time              : 35099                     --- (19)
OUTSYNC count             : 3                         --- (20)
        time              : 6                         --- (21)

[LINE STATUS]
date                      : Oct 14 16:00:40 2002      --- (1)
channel                   : [MB][CNCT0][-]            --- (2)
 speed                    : 128k                      --- (3)
 status                   : data                      --- (4)
 since                    : Oct 14 16:00:24 2002      --- (5)
 func                     : HDLC                      --- (6)
[LINE LOG INFORMATION]
received frame            : 0                         --- (7)
         bytes            : 0                         --- (8)
sent     frame            : 0                         --- (9)
         bytes            : 0                         --- (10)
Input frame dropped
  busy                    : 0                         --- (11)
  CRC error               : 0                         --- (12)
  abort frame             : 0                         --- (13)
  bad length              : 0                         --- (14)
  bad octet               : 0                         --- (15)
Output frame dropped
  underrun                : 0                         --- (16)
Flow control
  limit                   : 0                         --- (22)
  count                   : 0                         --- (23)
  condition               : XON                       --- (24)
Flag send/monitor mode    : no/no                     --- (25)
  flag recv               : 0                         --- (26)
  idle recv               : 0                         --- (27)
  flag received count     : 0                         --- (28)
                 time     : 0                         --- (29)
  idle received count     : 0                         --- (30)
                 time     : 0                         --- (31)
```

(BRI フレームリレー/専用線)(Si-R570 Si-R370 の場合)

```
# show hsd statistics circuit
[LINE STATUS]
date                      : Oct 14 16:00:40 2002      --- (1)
channel                   : [SLOT0][CNCT0][-]         --- (2)
 speed                    :                           --- (3)
 status                   : data                      --- (4)
 since                    : Oct 14 16:00:24 2002      --- (5)
 func                     :                           --- (6)
[LAYER1 INFORMATION]
SYNC    count             : 4                         --- (18)
        time              : 35099                     --- (19)
OUTSYNC count             : 3                         --- (20)
        time              : 6                         --- (21)

[LINE STATUS]
date                      : Oct 14 16:00:40 2002      --- (1)
channel                   : [SLOT0][CNCT0][-]         --- (2)
 speed                    : 128k                      --- (3)
 status                   : data                      --- (4)
 since                    : Oct 14 16:00:24 2002      --- (5)
 func                     : HDLC                      --- (6)
[LINE LOG INFORMATION]
received frame            : 0                         --- (7)
         bytes            : 0                         --- (8)
sent     frame            : 0                         --- (9)
         bytes            : 0                         --- (10)
Input frame dropped
  busy                    : 0                         --- (11)
  CRC error               : 0                         --- (12)
  abort frame             : 0                         --- (13)
  bad length              : 0                         --- (14)
  bad octet               : 0                         --- (15)
Output frame dropped
  underrun                : 0                         --- (16)
Flow control
  limit                   : 0                         --- (22)
  count                   : 0                         --- (23)
  condition               : XON                       --- (24)
Flag send/monitor mode    : no/no                     --- (25)
  flag recv               : 0                         --- (26)
  idle recv               : 0                         --- (27)
  flag received count     : 0                         --- (28)
                 time     : 0                         --- (29)
  idle received count     : 0                         --- (30)
                 time     : 0                         --- (31)
```

(PRI フレームリレー/専用線)(Si-R570 Si-R370 の場合)

```
# show hsd statistics circuit
[LINE STATUS]
date                      : Oct 14 16:00:40 2002      --- (1)
channel                   : [SLOT0][CNCT0][-]         --- (2)
 speed                    :                           --- (3)
 status                   : data                      --- (4)
 since                    : Oct 14 16:00:24 2002      --- (5)
 func                     :                           --- (6)
[LAYER1 INFORMATION]
 Received Signal count
  No signal Indication    : 10                        --- (32)
  Alarm Indication signal : 0                         --- (33)
  Loss of Synchronization : 7                         --- (34)
  Receive Remote Alarm    : 0                         --- (35)
SYNC    count             : 4                         --- (18)
        time              : 35099                     --- (19)
OUTSYNC count             : 3                         --- (20)
        time              : 6                         --- (21)

[LINE STATUS]
date                      : Oct 14 16:00:40 2002      --- (1)
channel                   : [SLOT0][CNCT0][-]         --- (2)
 speed                    : 1536k                     --- (3)
 status                   : data                      --- (4)
 since                    : Oct 14 16:00:24 2002      --- (5)
 func                     : HDLC                      --- (6)
[LINE LOG INFORMATION]
received frame            : 151                       --- (7)
         bytes            : 43286                     --- (8)
sent     frame            : 171                       --- (9)
         bytes            : 52577                     --- (10)
Input frame dropped
  busy                    : 0                         --- (11)
  CRC error               : 2                         --- (12)
  abort frame             : 4                         --- (13)
  bad length              : 0                         --- (14)
  bad octet               : 1                         --- (15)
Output frame dropped
  underrun                : 0                         --- (16)
Flow control
  limit                   : 4096                      --- (22)
  count                   : 0                         --- (23)
  condition               : XON                       --- (24)
Flag send/monitor mode    : yes/yes                   --- (25)
  flag recv               : 31                        --- (26)
  idle recv               : 34                        --- (27)
  flag received count     : 4                         --- (28)
                 time     : 35097                     --- (29)
  idle received count     : 4                         --- (30)
                 time     : 2                         --- (31)
```

表示内容の説明 (D/B チャネル表示)

1) コマンド 投入時刻

コマンド が入力された時刻を表示します。

2) チャネル種別

スロット 番号、ライン番号が表示されます。

3) 通信速度

通信速度が kbps 単位で表示されます。

4) チャネル状態

以下のどれかが表示されます。

Init : 初期化中状態

Wait Setline :

チャネル未使用状態

Wait Enable :
チャネル使用開始待ち状態

Wait Sync :
同期確立待ち状態

Wait Call :
発着信待ち状態 (呼毎起動)

Wait Sync_s :
発信時同期確立待ち状態 (呼毎起動)

Outsync : 同期はずれ検出状態

Wait Enable_con :
チャネル起動中状態

Data : データ送受信可能状態

Wait Disable :
チャネル停止指示待ち状態

Wait Disable_con:
チャネル停止完了待ち状態

Wait Flag :
フラグ受信待ち状態

Recv IDLE :
アイドル受信検出状態

5) 状態遷移時刻
チャネル状態が現在の状態に変化した時刻を表示します。

6) 通信種別
以下のどれかが表示されます。

Q921 D チャネルの場合に表示されます

Q921(per-call)
呼毎起動指定時の D チャネルの場合に表示されます

HDLC HDLC プロトコル使用時に表示されます

PIAFS PIAFS プロトコル使用時に表示されます

TRANSPARENT
トランスペアレント使用時に表示されます

7) 受信フレーム数
8) 受信バイト数
9) 送信フレーム数
10) 送信バイト数
11) 受信バッファビジー検出回数
12) 受信 CRC エラー検出回数
13) 受信アボートエラー検出回数
14) 受信フレーム長違反検出回数
15) 受信非オクテットフレーム検出回数

16) 送信アンダーラン検出回数
17) 衝突検出回数
18) 同期確立通知回数
19) 同期確立時間 (100ms 単位)
20) 同期外れ通知回数
21) 同期外れ時間 (100ms 単位)
22) フロー制御しきい値
23) 総送信要求バイト数
24) フロー制御状態
25) フラグ送信・監視モード状態
26) フラグ受信検出回数
27) フラグ断検出回数
28) フラグ受信通知回数
29) フラグ受信時間 (100ms 単位)
30) フラグ断通知回数
31) フラグ断時間 (100ms 単位)
32) No Signal Indication 検出回数
33) Alarm Indication Signal 検出回数
34) Loss of Synchronization 検出回数
35) Receive Remote Alarm 検出回数

26.1.3　clear hsd statistics circuit

[機能]

専用線の統計情報のクリア

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

clear hsd statistics circuit

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

専用線またはフレームリレー回線の統計情報をクリアします。

[実行例]

以下に、実行例を示します。

```
# clear hsd statistics circuit
#
```

第 27 章　ATM 回線のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

27.1　ATM 回線のカウンタ・ログ・統計・状態などの表示

27.1.1　show atm

[機能]

ATM 回線状態の表示

[適用機種]

Si-R 570	Si-R 370	Si-R 260B			

[入力形式]

show atm [brief]

[オプション]

なし

ATM 回線の状態を表示します。

brief

ATM 回線の状態を簡易表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

ATM 回線の現在の状態を表示します。

[実行例]

以下に、実行例を示します。

```
# show atm
[slot 0]                                                        ---(1)
line speed                    : 25Mbps                          ---(2)
line status                   : enabling                        ---(3)
    [vpi 0]                                                     ---(4)
    vp status                 : active                          ---(5)
    vp rate                   : 200Kbps                         ---(6)
    oam control/status        : on/normal                       ---(7)

        [vpi 0 vci 32]                                          ---(8)
        vc status             : active                          ---(9)
        communicated time     : 0000.01:23:48                   ---(10)
        remote target         : rmt0.ap0 [remote 0 ap 0]        ---(11)
        service type          : CBR(100Kbps)                    ---(12)
        oam control/status    : on/normal                       ---(13)
            f5 fault receive  : 0                               ---(14)
        efci control/status   : on/flow                         ---(15)
        send/receive traffic  : 1234/3456 [byte/s]              ---(16)

        [vpi 0 vci 33]
        vc status             : inactive
        communicated time     : 0000.00:00:00
        remote target         : rmt1.ap0 [remote 1 ap 0]
        service type          : CBR(100Kbps)
        oam control/status    : vcwatch/loopback-timeout
            f5 fault receive  : 0
        efci control/status   : on/normal
        send/receive traffic  : -/- [byte/s]

        [vpi 0 vci 34]
        vc status             : disconnected
        communicated time     : 0000.00:00:00
        remote target         : rmt2.ap0 [remote 2 ap 0]
        service type          : CBR(100Kbps)
        oam control/status    : on/normal
            f5 fault receive  : 0
        efci control/status   : on/normal
        send/receive traffic  : -/- [byte/s]

[slot 1]
line speed                    : 155Mbps
line status                   : synchronization failed

[slot 2]
line speed                    : 25Mbps
line status                   : enabling
    [vpi 127]
    vp status                 : active
    vp rate                   : 3Mbps
    oam control/status        : on/normal

        [vpi 127 vci 1021]
        vc status             : active
        communicated time     : 0000.00:00:00
        remote target         : rmt20.ap0 [remote 20 ap 0]
        service type          : CBR(1Mbps)
        oam control/status    : off/normal
            f5 fault receive  : 0
        efci control/status   : off/normal
        send/receive traffic  : 0/0 [byte/s]

        [vpi 127 vci 1022]
        vc status             : inactive
        communicated time     : 0000.00:00:00
        remote target         : rmt21.ap0 [remote 21 ap 0]
        service type          : VBR(1Mbps/500Kbps)
        oam control/status    : on/fault
            f5 fault receive  : 12
        efci control/status   : on/normal
        send/receive traffic  : -/- [byte/s]
```

(続く)

(続き)

```
[slot 3]
line speed                    : 155Mbps
line status                   : enabling
    [vpi 12]
    vp status                 : active
    vp rate                   : ----
    oam control/status        : on/normal

        [vpi 12 vci 1021]
        vc status             : active
        communicated time     : 0000.00:00:00
        remote target         : rmt40.ap0 [remote 40 ap 0]
        service type          : CBR(1Mbps)
        oam control/status    : off/normal
        efci control/status   : off/normal
        send/receive traffic  : 0/0 [byte/s]

        [vpi 12 vci 1022]
        vc status             : inactive
        communicated time     : 0000.00:00:00
        remote target         : rmt41.ap0 [remote 41 ap 0]
        service type          : VBR(1Mbps/500Kbps)
        oam control/status    : on/fault
        efci control/status   : on/normal
        send/receive traffic  : -/- [byte/s]
    [vpi 255]
    vp status                 : inactive
    vp shaping                : ----
    oam control/status        : on/fault

        [vpi 255 vci 1021]
        vc status             : inactive
        communicated time     : 0000.00:00:00
        remote target         : rmt30.ap0 [remote 30 ap 0]
        service type          : CBR(1Mbps)
        oam control/status    : on/fault
            f5 fault receive  : 0
        efci control/status   : off/normal
        send/receive traffic  : 0/0 [byte/s]

        [vpi 255 vci 1022]
        vc status             : inactive
        communicated time     : 0000.00:00:00
        remote target         : rmt31.ap0 [remote 31 ap 0]
        service type          : VBR(1Mbps/500Kbps)
        oam control/status    : on/fault
            f5 fault receive  : 0
        efci control/status   : on/normal
        send/receive traffic  : -/- [byte/s]

        [vpi 255 vci 1023]
        vc status             : disconnected
        communicated time     : 0000.00:00:00
        remote target         : rmt32.ap0 [remote 32 ap 0]
        service type          : CBR(100Kbps)
        oam control/status    : on/normal
            f5 fault receive  : 0
        efci control/status   : on/normal
        send/receive traffic  : -/- [byte/s]

#
```

1) スロット番号

拡張モジュールが実装されているスロット番号が表示されます。

基本ボード上の ATM 回線の場合は、"mb"が表示されます。

2) 回線速度

回線速度が表示されます。

3) 回線状態

以下のどれかが表示されます。

- enabling
  同期確立中
- synchronization failed
  同期外れ状態

以下の情報は、同期確立中 (「line status」が enabling) の場合だけ表示されます。

4) VP 情報
   VP の VPI 値が表示されます。
5) VP 状態
   以下のどれかが表示されます。
   - active
     通信可能状態
   - inactive
     VPC 復旧待ち状態
     以下の要因により、該当 VP が復旧待ち状態
     - ◇ OAM(F4)-AIS または OAM(F4)-RDI 受信中
6) VP 速度
   VP の VP 速度が表示されます。VP 速度が設定されていない場合は "—-" が表示されます。
7) OAM(F4) 制御の有効・無効と制御状態
   以下のどれかが表示されます。
   OAM(F4) 制御
   - on
     OAM(F4) 受信有効
   - off
     OAM(F4) 受信無効

   状態
   - normal
     通常状態
   - fault
     OAM(F4)-AIS または OAM(F4)-RDI 受信中
8) VC 情報
   VP 配下 VC の VPI 値と VCI 値が表示されます。
9) VC 状態
   以下のどれかが表示されます。
   - active
     通信可能状態
   - inactive
     VC 復旧待ち状態
     以下の要因により、該当 VC が復旧待ち状態
     - ◇ 回線同期外れ

- ◇ OAM(F4)-AIS または OAM(F4)-RDI 受信中
- ◇ OAM(F5)-AIS または OAM(F5)-RDI 受信中
- ◇ VC 監視タイムアウト (ATM 拡張モジュール H1 のみ)

- disconnected
  利用者指示による停止状態

10) 通信時間
通信時間が以下の形式で表示されます。
dddd.hh:mm:ss (日. 時:分:秒)

11) 相手ネットワーク名、接続先名
接続中の相手ネットワーク名と接続先名が表示されます。

12) サービスタイプと速度
定義したサービスタイプと速度が表示されます。

CBR(PCR)
サービスタイプ CBR

VBR(PCR/SCR)
サービスタイプ VBR

UBR+(PCR/MCR)
サービスタイプ UBR+

GFR+(PCR/GR)
サービスタイプ GFR+

13) OAM(F5) 制御の有効・無効と制御状態
以下のどれかが表示されます。
OAM(F5) 制御

- on
  OAM(F5) 受信有効
- off
  OAM(F5) 受信無効
- vcwatch VC 監視有効

VC 監視と OAM(F5) のどちらも有効の場合は vcwatch が表示されます。
状態

- normal
  通常状態
- fault
  OAM(F5)-AIS または OAM(F5)-RDI 受信中
- loopback-timeout
  VC 監視失敗状態

14) OAM(F5) 故障通知検出数
OAM(F5)-AIS または OAM(F5)-RDI を受信した回数が表示されます。

15) 輻輳制御と状態

以下のどれかが表示されます。

輻輳制御

- on
  輻輳制御が有効
- off
  輻輳制御が無効

状態

- normal
  通常状態
- flow
  輻輳制御中

16) 送受信トラフィック

データ送受信トラフィックが [byte/s] で表示されます。

VC 状態が inactive または disconnected の場合は、- が表示されます。

```
# show atm brief
(1)  (2)                     (3)(4)   (5)         (6)          (7)
slot line-status             vpi vci  vp-status   vc-status    efci-status
----+-----------------------+---+----+-----------+------------+-----------
0    enabling                0   32   active      active       flow
0    enabling                0   33   active      inactive     normal
0    enabling                0   34   active      disconnected normal
1    synchronization failed  1   80   inactive    inactive     normal
1    synchronization failed  1   81   inactive    inactive     normal
2    enabling                127 1021 active      active       normal
2    enabling                127 1022 active      inactive     normal
3    enabling                255 1021 inactive    inactive     normal
3    enabling                255 1022 inactive    inactive     normal
3    enabling                255 1023 inactive    disconnected normal

#
```

1) スロット番号

拡張モジュールが実装されているスロット番号が表示されます。

基本ボード上の ATM 回線の場合は、"mb"が表示されます。

2) 回線状態

以下のどれかが表示されます。

- enabling
  同期確立中
- synchronization failed
  同期外れ状態

3) VP 情報

VP の VPI 値が表示されます。

4) VC 情報

VP 配下 VC の VPI 値と VCI 値が表示されます。

5) VP 状態

以下のどれかが表示されます。

- **active**　通信可能状態
- **inactive**

  VP 復旧待ち状態

  以下の要因により、該当 VP が復旧待ち状態

  ・OAM(F4)-AIS または OAM(F4)-RDI 受信中

6) VC 状態

以下のどれかが表示されます。

- **active**　通信可能状態
- **inactive**

  VC 復旧待ち状態

  以下の要因により、該当 VC が復旧待ち状態

  ・回線同期外れ

  ・OAM(F4)-AIS または OAM(F4)-RDI 受信中

  ・OAM(F5)-AIS または OAM(F5)-RDI 受信中

  ・VC 監視タイムアウト (ATM 拡張モジュール H1 のみ)
- **disconnected**

  利用者指示による停止状態

7) 輻輳制御状態

以下のどれかが表示されます。

- **normal**　通常状態
- **flow**　輻輳制御中

27.1.2 show atm statistics circuit

[機能]

ATM 統計情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B

[入力形式]

show atm statistics circuit [slot <slot>]

[オプション]

なし

すべての統計情報を表示します。

slot <slot>

指定されたスロットに挿入された ATM 拡張モジュール上の統計情報を表示します。
また、該当するスロットが無効の場合は統計情報は表示されません。

- mb
  表示するインタフェースが、基本ボード上にある場合に指定します。
- スロット番号
  ATM 拡張モジュールが挿入されているスロットの番号を指定します。

範囲	機種
0〜3	Si-R570
0〜1	Si-R370

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

ATM 統計情報を表示します。

[注意]

統計情報は、本装置を再起動するとクリアされます。

[実行例]

以下に、実行例を示します。

```
# show atm statistics circuit

[ATM SLOT-0 STATUS]
Interface status          : Link up                    --- (1)
  since                   : Nov 17 08:40:05 2003       --- (2)
  driver stage            : up                         --- (3)

[ATM STATISTICS]
Input packets             : 0                          --- (4)
 CLP 1                    : 0                          --- (5)
 CNG 1                    : 0                          --- (6)
Input error packets       : 0                          --- (7)
 abort                    : 0                          --- (8)
 length error frame       : 0                          --- (9)
 CRC error                : 0                          --- (10)
 short cell               : 0                          --- (11)
Output packets            : 0                          --- (12)
 CLP 1                    : 0                          --- (13)
Output error packets      : 0                          --- (14)

[PHYSICAL LAYER STATISTICS]
 utopia error dropped cell: 0                          --- (15)
 misinserted dropped cell : 0                          --- (16)

[LINE TRAFFIC RATE]
 tx cell rate             :      0[cell/sec]           --- (17)
 rx cell rate             :      0[cell/sec]           --- (18)
```

1) インタフェース状態

ケーブルの接続状態を表示します。

Link up　ケーブル接続状態

No Link　ケーブル未接続状態または非活性状態

2) 状態遷移時刻

インタフェース状態が現在の状態に変化した時刻を表示します。

3) ドライバ状態

ドライバの内部状態状態を表示します。

error lock

ハードウェアエラー状態

down　非活性状態

link off　活性中でケーブル抜け状態

up　活性中で通信可能状態

4) 受信フレーム数

5) CLP フラグ 1 のセル受信数

6) CNG フラグ 1 のセル受信数

7) 受信エラーフレーム数

8) ABORT セル受信数

9) フレーム長エラー受信数

10) CRC エラー受信数

11) ショートセル受信数

12) 送信フレーム数

13) CLP フラグ 1 のセル送信数

14) 送信エラーフレーム数

15) UTOPIA エラー数

16) 受信破棄セル数

17) 送信負荷

18) 受信負荷

27.1.3　show atm statistics vc

[機能]

VC 統計情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B

[入力形式]

show atm statistics vc

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

PVC 統計情報を表示します。

[注意]

PVC 統計情報は、本装置を再起動するとクリアされます。

[実行例]

以下に、実行例を示します。

```
# show atm statistics vc

[ATM CONNECTION [0] INFORMATION]
Vc status                 : active                    --- (1)
  since                   : Nov 17 08:40:05 2003      --- (2)

[ATM DRIVER INFORMATION]
Channel status            : active                    --- (3)
  send stage              : act                       --- (4)
  send flow stage         : idle                      --- (5)
  receive stage           : irq                       --- (6)

[CELL RATE]
  service type            : CBR                       --- (7)
  peak cell rate          :  60377[cell/s]            --- (8)

[ATM HEADER]
  vpi                     : 0                         --- (9)
  vci                     : 32                        --- (10)

[EFCI INFORMATION]
  control                 : no                        --- (11)
  status                  : normal                    --- (12)

[INPUT/OUTPUT STATISTICS]
Input packets             : 0                         --- (13)
Input error packets       : 0                         --- (14)
Output packets            : 0                         --- (15)
Output error packets      : 0                         --- (16)

[OAM STATISTICS]
F5 Input counts
   AIS                    : 0                         --- (17)
   RDI                    : 0                         --- (18)
   LPB                    : 0                         --- (19)
F5 Output counts
   LPB                    : 0                         --- (20)

[REPORT CELL STATISTICS]
Input counts
   BRC                    : 0                         --- (21)
Output counts
   BRC                    : 0                         --- (22)
```

1) VC 状態

active 通信可能状態

inactive by cable-off

ケーブル未接続により通信不可状態

inactive by vp-ais

VP-AIS 受信中により通信不可状態

inactive by vp-rdi

VP-RDI 受信中により通信不可状態

inactive by vp-ais

VC-AIS 受信中により通信不可状態

inactive by vc-rdi

VC-RDI 受信中により通信不可状態

inactive by lpb-timeout

VCWATCH Timeout により通信不可状態

2) 状態遷移時刻

VC 状態が現在の状態に変化した時刻を表示します。

3) チャネル状態

チャネルの状態を表示します。

active　通信可能状態

defined　定義されているが、通信不可の状態

4) ドライバ送信状態

bind　送信未起動状態

act　送信起動状態

irq　送信起動後、送信完了待ち状態

irq no bd　送信起動後、送信完了待ち、送信 BD 満充填状態

5) 送信フロー制御状態

送信フローの状態によって以下のように表示されます。

idle　通常状態

flow　送信フロー中

6) ドライバ受信状態

bind　受信未起動状態

bind nobuf
受信未起動、受信バッファなし状態

irq　受信起動中状態

irq nobuf　受信起動中、新規バッファ獲得不可状態

rcvstop　受信停止状態

7) サービスタイプ

実際に設定されているサービスタイプを表示します。

CBR　サービスタイプ CBR

VBR　サービスタイプ VBR

UBR+　サービスタイプ UBR+

GFR+(CBR)
サービスタイプ GFR+

GFR+(VBR)
サービスタイプ GFR+

GFR+(UBR+)
サービスタイプ GFR+

8) VC 速度

実際に設定されている VC 速度を表示します。

サービスタイプによって以下のように表示されます。

- CBR の場合

```
[CELL RATE]
  service type            : CBR                        --- (7)
  peak cell rate          :  60377[cell/s]             --- (8)
```

(8) VC速度

－ VBR の場合

```
[CELL RATE]
  service type           : VBR                        --- (7)
  peak cell rate         :  60377[cell/s]             --- (8-1)
  sustain cell rate      :  23584[cell/s]             --- (8-2)
  max burst size         :     32[cells]              --- (8-3)
```

(8-1) 最大速度
(8-2) 平均速度
(8-3) 最大バースト長

－ UBR+の場合

```
[CELL RATE]
  service type           : UBR+                       --- (7)
  peak cell rate         :  60377[cell/s]             --- (8-1)
  minimum cell rate      :  23584[cell/s]             --- (8-2)
```

(8-1) 最大速度
(8-2) 最低速度

9) VPI 値

10) VCI 値

11) 輻輳制御定義

輻輳制御が有効か無効かを以下のように表示されます。

yes 有効

no 無効

12) 輻輳制御中の状態

輻輳制御の状態によって以下のように表示されます。

normal 通常状態

tiwait 一次回復タイマ起動待ち

t1 一次回復タイマ起動中

t2wait 二次回復タイマ起動待ち

t2 二次回復タイマ起動中

rwait 輻輳制御解除待ち

13) 受信フレーム数

14) 受信エラーフレーム数

15) 送信フレーム数

16) 送信エラーフレーム数

17) OAM(F5)-AIS 受信数

18) OAM(F5)-RDI 受信数

19) OAM(F5)-LPB 受信数

Loopback 要求受信、VCWATCH が有効の場合は Loopback 応答受信の総和を表示します。

20) OAM(F5)-LPB 送信数

Loopback 応答送信、VCWATCH が有効の場合は Loopback 要求送信の総和を表示します。

21) Backward Report Cell 受信数

Backward Report Cell 受信数を表示します。

22) Backward Report Cell 送信数

Backward Report Cell 送信数を表示します。

27.1.4　show atm statistics llc-snap

[機能]

ATM 回線の LLC/SNAP ごとの統計情報表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B

[入力形式]

show atm statistics llc-snap

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

ATM 回線の LLC/SNAP ごとの統計情報を表示します。

[注意]

以下の操作により本統計情報はクリアされます。

- clear atm statistics 実行
- 装置リセット

[実行例]

以下に、実行例を示します。

```
# show atm statistics llc-snap

[slot 0 vp 1 vci 32]                                                --- (1)
50000 packets receive                                               --- (2)
    20000 ipv4 packets                                              --- (3)
    10000 ipv6 packets                                              --- (4)
    0 mpls packets                                                  --- (5)
    10000 bridge packets                                            --- (6)
    10000 unknown packets                                           --- (7)
        last unknown llc is [0011223344556677]                      --- (8)
40000 packets send                                                  --- (9)
    20000 ipv4 packets                                              --- (10)
    10000 ipv6 packets                                              --- (11)
    0 mpls packets                                                  --- (12)
    10000 bridge packets                                            --- (13)

[slot2 vpi 127 vci 1023]
40000 packets receive
    20000 ipv4 packets
    10000 ipv6 packets
    0 mpls packets
    10000 bridge packets
    0 unknown packets
        last unknown llc is [----------------]
40000 packets send
    20000 ipv4 packets
    10000 ipv6 packets
    0 mpls packets
    10000 bridge packets
```

1) スロット番号/VPI 値/VCI 値

2) 受信総数

3) IPv4 LLC/SNAP ヘッダフレーム受信数

4) IPv6 LLC/SNAP ヘッダフレーム受信数

5) MPLS LLC/SNAP ヘッダフレーム受信数

6) 802.3Bridge LLC/SNAP ヘッダフレーム受信数

7) 未対応 LLC/SNAP ヘッダフレーム受信数

8) 受信した未対応 LLC/SNAP ヘッダ

   未対応或いは装置として無効な LLC/SNAP ヘッダフレームを受信した場合に、最後のフレームの先頭 8 バイトが表示されます。

   未対応 LLC/SNAP ヘッダフレームを受信してない場合は"———"が表示されます。

9) 送信総数

10) IPv4 LLC/SNAP ヘッダフレーム送信数

11) IPv6 LLC/SNAP ヘッダフレーム送信数

12) MPLS LLC/SNAP ヘッダフレーム送信数

13) 802.3Bridge LLC/SNAP ヘッダフレーム送信数

27.2　ATM 回線のカウンタ・ログ・統計などのクリア

27.2.1　clear atm statistics

[機能]

ATM 統計情報のクリア

[適用機種]

Si-R 570	Si-R 370	Si-R 260B			

[入力形式]

clear atm statistics

[オプション]

なし

すべての ATM 統計情報をクリアします。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

すべての ATM 統計情報をクリアします。
ATM 拡張モジュールが複数実装されている場合は、全拡張モジュールが対象になります。

[実行例]

```
# clear atm statistics
#
```

第 28 章　モデム／データ通信カード 接続のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

28.1　モデム／データ通信カード 接続のカウンタ・ログ・統計・状態などの表示

28.1.1　show modem

[機能]

モデム／データ通信カード 接続状態の表示

[適用機種]

			Si-R 240	Si-R 220B	

[入力形式]

show modem

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

モデム／データ通信カード 接続の現在の状態を表示します。

[実行例]

以下に、Si-R220B の実行例を示します。

```
# show modem
line status           : connected                        --- (1)
call status           : call-out                         --- (2)
remote target         : rmt0.ap0 [remote 0 ap 0]         --- (3)
remote TEL no         : 1002*                            --- (4)
line speed            : 28800 bps                        --- (5)
communicated time     : 0000.00:00:41                    --- (6)
IPCP                  : opened                           --- (7)
negotiated IP address : local  192.168.2.1               --- (8)
                      : remote 255.255.255.255           --- (8)
DNS server address    : 255.255.255.255                  --- (9)
IPV6CP                : closed                           --- (10)
BCP                   : closed                           --- (11)
send/receive traffic  : 0%/0%                            --- (12)
```

以下に、Si-R240 の実行例を示します。

```
# show modem
line status           : connected                        --- (1)
call status           : call-out                         --- (2)
remote target         : rmt0.ap0 [remote 0 ap 0]         --- (3)
remote TEL no         : *99#                             --- (4)
line speed            : 64000 bps                        --- (5)
communicated time     : 0000.00:01:18                    --- (6)
IPCP                  : opened                           --- (7)
negotiated IP address : local    192.168.2.10            --- (8)
                      : remote   172.16.1.1              --- (8)
DNS server address    : 172.16.2.2                       --- (9)
IPV6CP                : closed                           --- (10)
BCP                   : closed                           --- (11)
send/receive traffic  : 592 bps/944 bps                  --- (12)
```

1) 回線状態

以下のどれかが表示されます。

enabling 同期確立中

synchronization failed
同期外れ状態

idle 回線未使用

disconnecting
切断中

connected
通信中

callin 着信処理中

alerting 相手呼出中

以下の情報は、通信中 (「line status」が connected) の場合だけ表示されます。

2) 接続方向

以下のどれかが表示されます。

call-out 発信によって接続

call-in 着信によって接続

3) 相手ネットワーク名、接続先名

接続中の相手ネットワーク名と接続先名が表示されます。

4) 接続先電話番号

接続先の電話番号が表示されます。

5) 回線速度

接続中の回線の回線速度が表示されます。

データ通信カードの場合は 64000 bps 固定になります。

6) 通信時間

通信時間が以下の形式で表示されます。

dddd.hh:mm:ss (日. 時:分:秒)

7) IPCP 状態

以下のどれかが表示されます。

opened IPv4 利用可能

negotiating
IPCP ネゴシエーション中

closed IPv4 利用不可能

8) 自側 IP アドレス→相手側 IP アドレス

IPCP のアドレスネゴシエーション結果が表示されます。アドレスネゴシエーションなしで接続した場合は、255.255.255.255 となります。

9) DNS サーバアドレス

IPCP の DNS サーバアドレスネゴシエーション結果が表示されます。DNS サーバアドレスネゴシエーションなしで接続した場合は、255.255.255.255 となります。

10) IPV6CP 状態

以下のどれかが表示されます。

opened　IPv6 利用可能

negotiating

IPv6CP ネゴシエーション中

closed　IPv6 利用不可能

11) BCP 状態

以下のどれかが表示されます。

opened　Bridge 利用可能

negotiating

BCP ネゴシエーション中

closed　Bridge 利用不可能

12) 送信回線使用率/受信回線使用率

モデム接続の場合はデータ送受信の回線使用率をパーセントで表示します。

データ通信カード接続の場合はデータ送受信の回線使用量を bps 単位で表示します。

28.1.2 show modem account

[機能]

モデム／データ通信カード接続のアカウントの表示

[適用機種]

			Si-R 240	Si-R 220B	

[入力形式]

show modem account

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

モデム／データ通信カード接続のアカウントを表示します。

[実行例]

```
# show modem account
Call Account:
  call count          = 2  --- (1)
  call busy count     = 0  --- (2)
  call error count    = 0  --- (3)
Called Account:
  called accept count = 0  --- (4)
  called reject count = 0  --- (5)

Time/Charge Account:
  total time for callout  = 0000.00:03:04      --- (6)
  peak time   remote      = internet.ISP-1     --- (7)
              time        = 0000.00:02:57      --- (8)
  last        remote      = intranet.OFFICE-I  --- (9)
              time        = 0000.00:00:07      --- (10)

Access-point Time/Charge:
  remote  ap      time
       0   0    0000.00:02:57
       1   0    0000.00:00:07
 └───────┴───┴──────────────┘
   (11)   (12)      (13)

Access-point disconnect limit Time/Packet:
  remote  ap      time           packet
       0   0    0000.10:02:57     1000000
       1   0    0000.00:00:07         100
 └───────┴───┴──────────────┴──────────┘
   (14)   (15)      (16)         (17)
#
```

1) 発信の回数

2) 着ユーザビジーによって発信失敗した回数

3) 着ユーザビジー以外の網理由で発信失敗した回数

4) 着信の回数

5) 着信を拒否した回数
6) 発信接続の総通信時間
7) 最長接続時の相手名
8) 最長接続時の接続時間
9) 最終接続時の相手名
10) 最終接続時の接続時間
11) 相手定義番号
12) 接続先定義番号
13) 発信接続の合計時間
14) 相手定義番号 (データ通信カード 接続のみ)
15) 接続先定義番号 (データ通信カード 接続のみ)
16) 発信接続の合計時間 (データ通信カード 接続のみ)
17) 接続の合計パケット数 (データ通信カード 接続のみ)

28.1.3 show modem statistics

[機能]

データ通信カードの統計情報表示

[適用機種]

Si-R 240

[入力形式]

show modem statistics [slot <slot>]

[オプション]

なし

すべてのデータ通信カードの統計情報を表示します。

slot <slot>

指定されたスロットに挿入された、データ通信カードの統計情報を表示します。
また、該当するスロットが無効の場合は統計情報は表示されません。

- スロット番号
  データ通信カードが挿入されているスロットの番号を指定します。

範囲	機種
0〜1	Si-R240

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

データ通信カードの統計情報を表示します。

[注意]

統計情報は、本装置を再起動するとクリアされます。
統計情報は、カードの抜き取り／挿入でもクリアされます。

[実行例]

以下に、実行例を示します。

```
Si-R240# show modem statistics

[MODEM SLOT-0 STATUS]
Interface status     : OPEN                              ---(1)
 since               : Jan 11 13:21:15 2006              ---(2)

[MODEM SLOT-0 STATISTICS]
Input bytes          : 11                                ---(3)
 FIFO error          : 0                                 ---(4)
 overrun             : 0                                 ---(5)
 parity error        : 0                                 ---(6)
 framing error       : 0                                 ---(7)
 break sequence      : 0                                 ---(8)
Output bytes         : 5                                 ---(9)

[MODEM SLOT-0 SIGNAL STATUS]
CTS input signal     : ON                                ---(10)
DSR input signal     : ON                                ---(11)
RI  input signal     : OFF                               ---(12)
DCD input signal     : OFF                               ---(13)
DTR output signal    : OFF                               ---(14)
RTS output signal    : OFF                               ---(15)
```

1) インタフェース状態

ケーブルの接続状態を表示します。

OPEN　カード活性化状態

CLOSE　カード非活性化状態

2) 状態遷移時刻

インタフェース状態が現在の状態に変化した時刻を表示します。

3) 受信バイト数

4) FIFO エラー検出回数

5) オーバーラン検出回数

6) パリティエラー検出回数

7) フレーミングエラー検出回数

8) ブレークシーケンス検出回数

9) 送信バイト数

10) CTS 信号状態

11) DSR 信号状態

12) RI 信号状態

13) DCD 信号状態

14) DTR 信号状態

15) RTS 信号状態

28.2　モデム／データ通信カード 接続のカウンタ・ログ・統計などのクリア

28.2.1　clear modem account

[機能]

モデム／データ通信カード 接続のアカウント情報のクリア

[適用機種]

			Si-R 240	Si-R 220B	

[入力形式]

clear modem account

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

モデム／データ通信カード 接続のアカウント情報をクリアします。

[実行例]

```
# clear modem account
#
```

28.2.2　clear modem statistics

[機能]

データ通信カードの統計情報クリア

[適用機種]

Si-R 240

[入力形式]

clear modem statistics

[オプション]

なし

すべてのデータ通信カードの統計情報をクリアします。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

すべてのデータ通信カードの統計情報をクリアします。
複数実装されている場合は、全データ通信カードが対象になります。

[実行例]

```
# clear modem statistics
#
```

第 29 章　インタフェースのカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

29.1　インタフェースのカウンタ・ログ・統計・状態などの表示

29.1.1　show interface

[機能]

インタフェース情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show interface [interface <interface_name>]

[オプション]

なし

全インタフェースの状態、種別を表示します。

interface <interface_name>

指定したインタフェースの状態、種別を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

インタフェース情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show interface
lan0                MTU 1500    <UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST>
-(1)-                   -(2)-   ------------------(3)-------------------
    Type: ethernet                                                      ┐
    MAC address: 00:00:0e:f1:41:dc                                      │
    Status: up since Dec  9 19:23:45 2004                               │
    IP address/masklen:                                                 │
      192.168.1.1/24       Broadcast 192.168.1.255                      │
      192.168.2.1/24       Broadcast 192.168.2.255                      (4)
    ICMP redirect: enabled                                              │
    Proxy ARP: enabled                                                  │
    IPv6 address/prefixlen:                                             │
      fe80::200:eff:fef1:41dc/64                                        │
      2001:db8:ffff:1000:200:eff:fef1:41dc/64                           ┘
lan1                MTU 1500    <UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST>
    Type: tag vlan                                                      ┐
    VLAN ID is 30 on lan0                                               │
    MAC address: 00:00:0e:f1:41:dc                                      │
    Status: up since Dec  9 19:23:45 2004                               (4)
    IP address/masklen:                                                 │
      192.168.3.1/24       Broadcast 192.168.3.255                      │
    ICMP redirect: disabled                                             ┘
    Proxy ARP: disabled
rmt0                MTU 1500    <UP,POINTOPOINT,RUNNING,MULTICAST>
    Type: pseudo P2P interface                                          ┐
    Status: up since Dec  9 19:23:45 2004                               │
    IP address:                                                         (4)
      192.168.1.1 -> 192.168.5.1                                        │
    IPv6 address/prefixlen:                                             ┘
      fe80::200:eff:fef1:41dc/64
      2001:db8:ffff:1001:200:eff:fef1:41dc/64
rmt100                      MTU 1500     <POINTOPOINT,MULTICAST>
    Type: template P2P interface                                        ┐
    Status: up since Dec  9 19:23:45 2004                               (4)
    IP address:                                                         ┘
      192.168.10.1 -> 192.168.20.1
lo0                 MTU 16384   <UP,LOOPBACK,RUNNING,MULTICAST>
    Type: loopback                                                      ┐
    Status: up since Dec  9 19:23:45 2004                               │
    IP address/masklen:                                                 │
      127.0.0.1/32                                                      (4)
      192.168.1.1/32                                                    │
    IPv6 address/prefixlen:                                             │
      fe80::1/64                                                        │
      ::1/128                                                           ┘
```

(1) インタフェース名

(2) MTU サイズ

(3) インタフェースフラグ

(4) Type

インタフェースタイプが以下の文字列で表示されます。

ethernet Ethernet タイプ

tag vlan Ethernet タイプ上の tagged VLAN

pseudo P2P interface

仮想 P2P インタフェース

template P2P interface

仮想 P2P インタフェース (template で利用されるもの)

loopback ループバックインタフェース

VLAN ID

tagged VLAN で利用する場合に、VLAN ID と動作インタフェースが表示されます。

MAC address

このインタフェースで利用される MAC アドレスが表示されます。

Status

インタフェースの状態と、この状態になった時刻が表示されます。

up　利用可能

down　利用不可

admin down

Ethernet タイプのインタフェースで、手動操作により利用不可になった

IP address/masklen

インタフェースの IPv4 アドレスが表示されます。

ICMP redirect

ICMP redirect の動作モードが表示されます。

enabled :

ICMP redirect を送信します。

disabled :

ICMP redirect を送信しません。

Proxy ARP

Proxy ARP の動作モードが表示されます。

enabled :

Proxy ARP が動作しています。

disabled :

Proxy ARP は動作していません。

IPv6 address/prefixlen

インタフェースの IPv6 アドレスが表示されます。

IPv6 アドレスのあとに、必要に応じて以下が表示されます。

tentative :

DAD 処理が未実施であることを示します。

duplicated :

アドレス衝突検出により、利用不可であることを示します。

29.1.2 show interface brief

[機能]

インタフェース情報の簡易表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show interface brief [interface <interface_name>]

[オプション]

なし

全インタフェースを簡易表示します。

interface <interface_name>

指定したインタフェースを簡易表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

インタフェース情報を簡易表示します。

[実行例]

以下に、実行例を示します。

```
# show interface brief
Interface        Status     Type
 --(1)----------- --(2)----- --(3)-----------------
lan0            up         ethernet
lan1            up         tag vlan
rmt0            down       pseudo P2P interface
rmt100          up         template P2P interface
lo0             up         loopback
#
```

1) Interface

インタフェース名が表示されます。

2) Status

インタフェースの状態が表示されます。

up 利用可能

down 利用不可

admin down

Ethernet タイプのインタフェースで、手動操作により利用不可になった

3) Type

インタフェースタイプが表示されます。

ethernet　Ethernet タイプ

tag vlan　Ethernet タイプ上の tagged VLAN

pseudo P2P interface

仮想 P2P インタフェース

template P2P interface

仮想 P2P インタフェース (template で利用されるもの)

loopback　ループバックインタフェース

29.1.3 show interface summary

[機能]

インタフェースエントリ数の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show interface summary

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

インタフェースのエントリ数を表示します。

[実行例]

以下に、実行例を示します。

```
# show interface summary
There are 4 interfaces (up status 4 interfaces)
    Loopback interface      :    1 (up status    1 interfaces)  ---(1)
    Ethernet interface      :    1 (up status    1 interfaces)  ---(2)
    VLAN interface          :    1 (up status    1 interfaces)  ---(3)
    Pseudo P2P interface    :    1 (up status    1 interfaces)  ---(4)
    Template P2P interface  :    1 (up status    1 interfaces)  ---(5)
#
```

(1) ループバックインタフェース

(2) Ethernet タイプ

(3) Ethernet タイプ上の tagged VLAN

(4) 仮想 P2P インタフェース

(5) 仮想 P2P インタフェース (template で利用されるもの)

29.1.4　show interface detail

[機能]

インタフェース情報の詳細表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show interface detail [interface <interface_name>]

[オプション]

なし

全インタフェースを詳細表示します。

interface <interface_name>

指定したインタフェースを詳細表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

インタフェース情報を詳細表示します。

[実行例]

以下に、実行例を示します。

```
# show interface detail
lan0               MTU 1500    <UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST>
-(1)-                  -(2)-   ------------------(3)-------------------
    Type: ethernet                                                      ┐
    MAC address: 00:00:0e:f1:41:dc                                      │
    Status: up since Dec  9 19:23:45 2004                               │
    IP address/masklen:                                                 │
      192.168.1.1/24       Broadcast 192.168.1.255                      │
      192.168.2.1/24       Broadcast 192.168.2.255                      │
    ICMP redirect: enabled                                              │
    Proxy ARP: enabled                                                  │
    IPv6 address/prefixlen:                                             (4)
      fe80::200:eff:fef1:41dc/64                                        │
      2001:db8:ffff:1000:200:eff:fef1:41dc/64                           │
    statistics:                                                         │
      in packets:               608454094 out packets:               393557788
         bytes:                3238235804     bytes:                2432271618
         unicasts:              596068741     unicasts:              385199554
         multicasts/broadcasts   12385353     multicasts/broadcasts    8358234
         discards:                1570663     discards:                     10
                                              drop:                          0 ┘
lan1               MTU 1500    <UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST>
    Type: tag vlan                                                      ┐
    VLAN ID is 30 on lan0                                               │
    MAC address: 00:00:0e:f1:41:dc                                      │
    Status: up since Dec  9 19:23:45 2004                               │
    IP address/masklen:                                                 │
      192.168.3.1/24       Broadcast 192.168.3.255                      │
    ICMP redirect: disabled                                             │
    Proxy ARP: disabled                                                 (4)
    statistics:                                                         │
      in packets:               396600682 out packets:               443178595
         bytes:                2220023450     bytes:                1366703608
         unicasts:              388343780     unicasts:              434826141
         multicasts/broadcasts    8256902     multicasts/broadcasts    8352454
         discards:                 812137     discards:                   2763
                                              drop:                          0 ┘
rmt0               MTU 1500    <UP,POINTOPOINT,RUNNING,MULTICAST>
    Type: pseudo P2P interface                                          ┐
    Status: up since Dec  9 19:23:45 2004                               │
    IP address:                                                         │
      192.168.1.1 -> 192.168.5.1                                        │
    IPv6 address/prefixlen:                                             │
      fe80::200:eff:fef1:41dc/64                                        │
      2001:db8:ffff:1001:200:eff:fef1:41dc/64                           (4)
    statistics:                                                         │
      in packets:               329858329 out packets:               296016656
         bytes:                1007353457     bytes:                961770175
         unicasts:              329858329     unicasts:              296016656
         multicasts/broadcasts          0     multicasts/broadcasts          0
         discards:                 927816     discards:                  18058
                                              drop:                        125 ┘
rmt100                   MTU 1500      <POINTOPOINT,MULTICAST>
    Type: template P2P interface                                        ┐
    Status: up since Dec  9 19:23:45 2004                               │
    IP address:                                                         │
      192.168.10.1 -> 192.168.20.1                                      │
    statistics:                                                         │
      in packets:                    8329 out packets:                  656 (4)
         bytes:                     53457     bytes:                    4175
         unicasts:                   8329     unicasts:                  656
         multicasts/broadcasts          0     multicasts/broadcasts        0
         discards:                    816     discards:                   58
                                              drop:                      125 ┘
```

(続く)

(続き)

```
lo0                MTU 16384   <UP,LOOPBACK,RUNNING,MULTICAST>
    Type: loopback
    Status: up since Dec  9 19:23:45 2004
    IP address/masklen:
      127.0.0.1/32
      192.168.1.1/32
    IPv6 address/prefixlen:
      fe80::1/64                                                        (4)
      ::1/128
    statistics:
      in packets:                  174974 out packets:                 174974
         bytes:                  12391593     bytes:                 12391593
         unicasts:                 174974     unicasts:                174974
         multicasts/broadcasts          0     multicasts/broadcasts         0
         discards:                      0     discards:                     0
                                              drop:                         0
```

(1)　インタフェース名

(2)　MTU サイズ

(3)　インタフェースフラグ

(4)　Type

インタフェースタイプが以下の文字列で表示されます。

ethernet　Ethernet タイプ

tag vlan　Ethernet タイプ上の tagged VLAN

pseudo P2P interface

仮想 P2P インタフェース

template P2P interface

仮想 P2P インタフェース (template で利用されるもの)

loopback　ループバックインタフェース

VLAN ID

tagged VLAN で利用する場合に、VLAN ID と動作インタフェースが表示されます。

MAC address

このインタフェースで利用される MAC アドレスが表示されます。

Status

インタフェースの状態と、この状態になった時刻が表示されます。

up　利用可能

down　利用不可

admin down

Ethernet タイプのインタフェースで、手動操作により利用不可になった

IP address/masklen

インタフェースの IPv4 アドレスが表示されます。

ICMP redirect

ICMP redirect の動作モードが表示されます。

enabled :

ICMP redirect を送信します。

disabled :

ICMP redirect を送信しません。

Proxy ARP

Proxy ARP の動作モードが表示されます。

enabled :

Proxy ARP が動作しています。

disabled :

Proxy ARP は動作していません。

IPv6 address/prefixlen

インタフェースの IPv6 アドレスが表示されます。

IPv6 アドレスのあとに、必要に応じて以下が表示されます。

tentative :

DAD 処理が未実施であることを示します。

duplicated :

アドレス衝突検出により、利用不可であることを示します。

statistics

インタフェースの統計情報が表示されます。

29.1.5　show interface statistics

[機能]

インタフェース統計情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show interface statistics [interface <interface_name>]

[オプション]

なし

全インタフェースの統計情報を表示します。

interface <interface_name>

指定したインタフェースの統計情報を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

インタフェースの統計情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show interface statistics
lan0            Status: up     Type: ethernet
-(1)-                  -(2)-         ---(3)---
    statistics:
      in packets:               608454094 out packets:               393557788
         bytes:                3238235804     bytes:                2432271618
         unicasts:              596068741     unicasts:              385199554
         multicasts/broadcasts   12385353     multicasts/broadcasts    8358234
         discards:                1570663     discards:                     10
                                              drop:                          0
lan1            Status: up     Type: tag vlan
    statistics:
      in packets:               396600682 out packets:               443178595
         bytes:                2220023450     bytes:                1366703608
         unicasts:              388343780     unicasts:              434826141
         multicasts/broadcasts    8256902     multicasts/broadcasts    8352454
         discards:                 812137     discards:                   2763
                                              drop:                          0
rmt0            Status: up     Type: pseudo P2P interface
    statistics:
      in packets:               329858329 out packets:               296016656
         bytes:                1007353457     bytes:                961770175
         unicasts:              329858329     unicasts:              296016656
         multicasts/broadcasts          0     multicasts/broadcasts          0
         discards:                 927816     discards:                  18058
                                              drop:                        125
rmt100          Status: up     Type: template P2P interface
    statistics:
      in packets:                    8329 out packets:                    656
         bytes:                     53457     bytes:                      4175
         unicasts:                   8329     unicasts:                    656
         multicasts/broadcasts          0     multicasts/broadcasts          0
         discards:                    816     discards:                     58
                                              drop:                        125
lo0             Status: up     Type: loopback
    statistics:
      in packets:                  174974 out packets:                  174974
         bytes:                  12391593     bytes:                  12391593
         unicasts:                 174974     unicasts:                 174974
         multicasts/broadcasts          0     multicasts/broadcasts          0
         discards:                      0     discards:                      0
#
```

1) インタフェース名

2) Status

インタフェースの状態が表示されます。

up 利用可能

down 利 用不可

admin down

Ethernet タイプのインタフェースで、手動操作により利用不可になった

3) Type

インタフェースタイプが表示されます。

ethernet Ethernet タイプ

tag vlan Ethernet タイプ上の tagged VLAN

pseudo P2P interface

仮想 P2P インタフェース

template P2P interface

仮想 P2P インタフェース (template で利用されるもの)

loopback ループバックインタフェース

29.1.6　show access-point

[機能]

接続先情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show access-point
show access-point remote <remote_number> [ap <ap_number>]
show access-point access-point <ap_name>

[オプション]

なし

すべての接続先情報を表示します。

remote <remote_number>

指定した相手情報に関する接続先情報を表示します。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B　Si-R240　Si-R220B
0〜49	Si-R180

remote <remote_number> ap <ap_number>

指定した相手情報の、指定した接続先に関する接続先情報を表示します。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B　Si-R240　Si-R220B
0〜49	Si-R180

access-point <ap_name>

指定した接続先に関する接続先情報を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

指定した相手との通信状態を表示します。

[実行例]

以下に、実行例を示します。

```
# show access-point
remote 0 ap 0         : Internet.isp                          --- (1)
  status              : connected                             --- (2)
    detail            : connected                             --- (3)
    since             : Aug 26 10:52:46 2002                  --- (4)
    communicated time : 0000.00:30:03                         --- (5)
  speed               : 128000 bps                            --- (6)
    send traffic      : 1432 byte/s                           --- (7)
    receive traffic   : 10.4K byte/s                          --- (8)
  type                : ISDN                                  --- (9)
    IPCP              : opened                                --- (10)
      local address   :   192.168.1.1                         --- (11)
      DNS server      :   192.168.2.5                         --- (12)
    IPV6CP            : opened                                --- (13)
    BCP               : opened                                --- (14)
    MPLSCP            : opened                                --- (15)

remote 1 ap 0         : yokohama.fr0
  status              : connected
    since             : Aug 26 10:52:46 2002
  speed               : 64000 bps
    send traffic      : 2245 byte/s
    receive traffic   : 42 byte/s
  type                : FR

remote 2 ap 0         : kawasaki.vpn
  status              : connected
    since             : Aug 26 10:52:46 2002
  speed               : not available
    send traffic      : not available
    receive traffic   : not available
  type                : IPsec/IKE
     exchange type    : aggressive                            --- (16)
     IKE SA           : established                           --- (17)
     IPsec SA         : established                           --- (18)
```

1) 定義内容

構成定義で設定された相手ネットワーク名および接続先名が表示されます。

2) 接続状態

現在の接続状態を表示します。以下のどれかが表示されます。

- not attached

  構成定義矛盾などにより利用不可

- linkoff

  利用する回線がダウン

- connectable

  未接続状態

- connected

  接続状態

- force down

  閉塞状態

- watch failed

  接続先監視による通信障害検出状態

3) 接続詳細状態

接続状態の詳細がある場合に表示されます。

- 通信手段が ISDN の場合
  チャネルの詳細状態が表示されます。
  - disc-to-sync
    接続中に同期外れを検出し、切断処理中
  - disc-to-idle
    切断処理中
  - connected
    接続状態
  - callin
    着信処理中
  - alerting
    相手呼出中
- 通信手段が PPPoE の場合
  PPPoE の詳細状態が表示されます。
  - waitPADO
    PADO 受信待ち
  - waitPADS
    PADS 受信待ち
  - connected
    接続状態
- 通信手段が MODEM の場合
  - disc-to-sync
    接続中に同期外れを検出し、切断処理中
  - disc-to-idle
    切断処理中
  - connected
    接続状態
  - callin
    着信処理中 (モデム接続の場合のみ)
  - alerting
    相手呼出中

4) 状態遷移時刻
   「status」が現在の状態に変化した時刻を表示します。
5) 通信時間
   dddd.hh:mm:ss の形式で通信時間を表示します。dddd=日数、hh=時間、mm=分、ss=秒を示します。
   「Type」が ISDN または PPPoE または MODEM の場合にだけ表示されます。
   ISDN または PPPoE の場合、「status」が connected の場合にだけ表示されます。
   MODEM の場合、「detail」が alerting、connected、disc-to-idle、disc-to-sync の場合だけ表示されます。
6) 伝送速度
   現在の伝送速度を表示します。MP の場合は合計速度が表示されます。

7) 送信レート
最新のデータ送信レートを表示します。

8) 受信レート
最新のデータ受信レートを表示します。

9) 通信手段
相手システムとの通信手段を表示します。以下のどれかが表示されます。

- HSD
  専用線
- ISDN
  ISDN 回線
- FR
  FrameRelay 回線
- IPv4
  IPv4 tunnel
- IPv6
  IPv6 tunnel
- ATM
  ATM 回線
- PPPoE
  PPPoE
- IPsec
  IPsec(手動設定鍵を利用)
- IPsec/IKE
  IPsec(IKE による鍵交換を利用)
- overlap
  overlap ap 機能を利用
- mpls
  MPLS LSP
- MODEM
  モデム／データ通信カード

以下の情報は PPP を利用して通信する場合に限り表示されます。

10) IPCP 状態
IPv4 通信の状態を表示します。以下のどれかが表示されます。

- opened
  通信可能
- negotiating
  ネゴシエーション中
- closed
  通信不可

11) IPv4 アドレス
IPCP ネゴシエーションにより決定された自側 IPv4 アドレスが、表示されます。アドレスネゴシエーションが行えなかった場合は 255.255.255.255 となります。

12) DNS サーバアドレス

IPCP ネゴシエーションにより決定された DNS サーバアドレスを表示します。DNS サーバアドレスネゴシエーションが行えなかった場合は、255.255.255.255 となります。

13) IPV6CP 状態

IPv6 通信の状態を表示します。以下のどれかが表示されます。

- opened
  通信可能
- negotiating
  ネゴシエーション中
- closed
  通信不可

14) BCP 状態

ブリッジ通信の状態を表示します。以下のどれかが表示されます。

- opened
  通信可能
- negotiating
  ネゴシエーション中
- closed
  通信不可

15) MPLSCP 状態

MPLS 通信の状態を表示します。以下のどれかが表示されます。

- opened
  通信可能
- negotiating
  ネゴシエーション中
- closed
  通信不可

以下の情報は IPsec/IKE を利用して通信する場合に限り表示されます。

IPsec 手動鍵設定を利用する場合は表示されません。

16) 鍵交換モード

IKE の鍵交換モードを表示します。以下のどれかが表示されます。

- main
  Main モードを利用
- aggressive
  Aggressive モードを利用

17) IKE SA 状態

IKE SA の状態を表示します。以下のどれかが表示されます。

- established
  確立済み

- negotiating
  確立中
- expired
  削除待ち
- none
  未確立

18) IPsec SA 状態
IPsec SA の状態を表示します。以下のどれかが表示されます。

- established
  確立済み
- negotiating
  確立中
- expired
  削除待ち
- none
  未確立

29.1.7　show template

[機能]

テンプレート着信の通信状態

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show template [interface <interface_name>]

[オプション]

なし

全インタフェースの状態、種別を表示します。

interface <interface_name>

指定したインタフェースの状態、種別を表示します。

[動作モード]

運用管理モード (一般ユーザクラス／管理者クラス)
構成定義モード (管理者クラス)

[説明]

テンプレート着信で接続した相手との通信状態を表示します。

[実行例]

以下に、実行例を示します。

```
# show template
[template 0]
status                : active                                  --- (1)
Number of interfaces  :  Active: 1, Free: 9                     --- (2)

rmt30(user id:kawagoe-1)                                        --- (3)
  status              : connected                               --- (4)
    detail            : connected                               --- (5)
    since             : Aug 26 10:52:46 2004                    --- (6)
    communicated time : 0000.00:30:03                           --- (7)
  speed               : 128000 bps                              --- (8)
    send traffic      : 1432 byte/s                             --- (9)
    receive traffic   : 10.4K byte/s                            --- (10)
  type                : ISDN                                    --- (11)
    IPCP              : opened                                  --- (12)
      local address   :   192.168.1.1                           --- (13)
      DNS server      :   192.168.2.5                           --- (14)
    IPV6CP            : opened                                  --- (15)

[template 1]
status                : active                                  --- (1)
Number of interfaces  :  Active: 1, Free: 7                     --- (2)

rmt40(user id:sayama-1@domainname)                              --- (3)
  status              : connected                               --- (4)
    since             : Aug 26 10:53:42 2004                    --- (6)
  speed               : not available                           --- (8)
    send traffic      : not available                           --- (9)
    receive traffic   : not available                           --- (10)
  type                : IPsec/IKE                               --- (11)
     exchange type    : aggressive                              --- (16)
     IKE SA           : established                             --- (17)
     IPsec SA         : established                             --- (18)
```

1) テンプレート動作状態が表示されます。以下のどちらかが表示されます。

- active
  動作
- inactive
  非動作

2) テンプレートで予約されたインタフェースの使用状況が表示されます。

3) 定義内容
インタフェース名および着信した接続先のユーザ ID が表示されます。
(PPP 接続時に認証しないで着信した場合はユーザ ID に unknown が表示されます。)

4) 接続状態
現在の接続状態を表示します。以下が表示されます。

- connected
  接続状態

5) 接続詳細状態
接続状態の詳細がある場合に表示されます。

・通信手段が ISDN の場合

チャネルの詳細状態が表示されます。

・disc-to-sync

接続中に同期外れを検出し、切断処理中

・disc-to-idle

切断処理中

・connected

接続状態

6) 状態遷移時刻
「status」が現在の状態に変化した時刻を表示します。

7) 通信時間
dddd.hh:mm:ss の形式で通信時間を表示します。dddd=日数、hh=時間、mm=分、ss=秒を示します。
ISDN の場合、「status」が connected の場合にのみ表示されます。

8) 伝送速度
現在の伝送速度を表示します。MP の場合は合計速度が表示されます。

9) 送信レート
最新のデータ送信レートを表示します。

10) 受信レート
最新のデータ受信レートを表示します。

11) 通信手段
相手システムとの通信手段を表示します。以下のどちらかが表示されます。

- ISDN
  ISDN 回線
- IPsec/IKE
  IPsec(IKE による鍵交換を利用)

以下の情報は PPP を利用して通信する場合に限り表示されます。

12) IPCP 状態
IPv4 通信の状態を表示します。以下のどれかが表示されます。

- opened
  通信可能
- negotiating
  ネゴシエーション中
- closed
  通信不可

13) IPv4 アドレス
IPCP ネゴシエーションにより決定された自側 IPv4 アドレスが、表示されます。アドレスネゴシエーションが行えなかった場合は 255.255.255.255 となります。

14) DNS サーバアドレス
IPCP ネゴシエーションにより決定された DNS サーバアドレスを表示します。DNS サーバアドレスネゴシエーションが行えなかった場合は、255.255.255.255 となります。

15) IPV6CP 状態
IPv6 通信の状態を表示します。以下のどれかが表示されます。

- opened
  通信可能
- negotiating
  ネゴシエーション中
- closed
  通信不可

以下の情報は IPsec/IKE を利用して通信する場合に限り表示されます。
IPsec 手動鍵設定を利用する場合は表示されません。

16) 鍵交換モード

IKE の鍵交換モードを表示します。以下のどれかが表示されます。

- main
  Main モードを利用
- aggressive
  Aggressive モードを利用

17) IKE SA 状態

IKE SA の状態を表示します。以下のどれかが表示されます。

- established
  確立済み
- negotiating
  確立中
- expired
  削除待ち
- none
  未確立

18) IPsec SA 状態

IPsec SA の状態を表示します。以下のどれかが表示されます。

- established
  確立済み
- negotiating
  確立中
- expired
  削除待ち
- none
  未確立

29.1.8　show template statistics

[機能]

テンプレート着信の統計情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show template statistics

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス／管理者クラス)
構成定義モード (管理者クラス)

[説明]

テンプレート着信の統計情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show template statistics
[template 0]
pooled interface      = rmt30-rmt39        --- (1)
accept count          = 2                  --- (2)
reject count          = 1                  --- (3)
total time            = 0000.00:13:04      --- (4)
peak time             = 0000.00:12:57      --- (5)
last time             = 0000.00:00:07      --- (6)

[template 1]
pooled interface      = rmt40-rmt37        --- (1)
accept count          = 5                  --- (2)
reject count          = 2                  --- (3)
total time            = 0000.00:19:14      --- (4)
peak time             = 0000.00:10:17      --- (5)
last time             = 0000.00:00:13      --- (6)
```

1) テンプレート着信で使用する予約インタフェース
2) 着信成功回数
3) 着信拒否回数
4) 接続時間の総和
5) 最長接続時の接続時間
6) 最終接続時の接続時間

29.2　インタフェースのカウンタ・ログ・統計などのクリア

29.2.1　clear interface statistics

[機能]

インタフェースの統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear interface statistics [interface <interface_name>]

[オプション]

なし

すべてのインタフェースの統計情報をクリアします。

interface <interface_name>

指定したインタフェースの統計情報をクリアします。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

インタフェースの統計情報をクリアします。

[実行例]

```
# clear interface statistics
#
```

29.2.2　clear template statistics

[機能]

テンプレート着信の統計情報クリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear template statistics

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

テンプレート着信に関する統計情報をクリアします。

[実行例]

```
# clear template statistics
#
```

第 30 章　ARP エントリの表示、削除コマンド

30.1　ARP エントリの表示、削除

30.1.1　show arp

[機能]

ARP エントリの表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show arp [<ip_address>]
show arp summary

[オプション]

なし

すべての ARP エントリを詳細表示します。

<ip_address>

指定した IP アドレスの ARP エントリのみ表示します。

summary

ARP エントリ数を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

ARP テーブルのエントリを表示します。

[実行例]

以下に、実行例を示します。

```
# show arp
IP Address      MAC Address       F  Rest  Interface
--------------- ----------------- -- ----- ---------
(1)             (2)               (3) (4)  (5)
20.0.0.1        00:00:e2:08:57:89    01146 lan0
20.0.0.2        (incomplete)              lan0
20.0.0.255      00:00:02:01:14:00 P  perm  lan0
    Entry:3   --- (6)

# show arp summary
    Entry:3

# show arp 20.0.0.1
IP Address      MAC Address       F  Rest  Interface
--------------- ----------------- -- ----- ---------
20.0.0.1        00:00:e2:08:57:89    01146 lan0
    Entry:1

#
```

1)　IP Address

ARP エントリの IP address が表示されます。

2) MAC Address

ARP エントリの MAC address が表示されます。

未解決の場合は (incomplete) が表示されます。

3) F

エントリ種別が表示されます。詳細を以下に示します。

P	permanent エントリ

4) Rest

ARP エントリの残り生存時間を秒数で示します。Permanent エントリの場合は"perm"と表示されます。

5) Interface

ARP エントリのインタフェースが表示されます。

6) Entry

ARP エントリのエントリ数が表示されます。

30.1.2　clear arp

[機能]

ARP エントリの削除

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear arp [<ip_address>]

[オプション]

なし

すべての ARP エントリを削除します。

<ip_address>

指定した IP アドレスの ARP エントリを削除します。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

ARP テーブルからエントリを削除します。

[実行例]

```
# clear arp
#
```

第 31 章　Neighbor Cache テーブルエントリの表示、削除コマンド

31.1　Neighbor Cache テーブルエントリの表示、削除

31.1.1　show ndp

[機能]

Neighbor Cache テーブルエントリの表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ndp [<ipv6_address>]
show ndp summary

[オプション]

なし

Neighbor Cache テーブルの現在のエントリを表示します。

<ipv6_address>

指定された IPv6 アドレスの Neighbor Cache エントリのみを表示します。
リンクローカルアドレスの場合は、アドレスに続けて % でインタフェース名を指定します。

summary

Neighbor Cache エントリ数を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

Neighbor Cache テーブルのエントリを表示します。

[実行例]

以下に、実行例を示します。

```
# show ndp
IPv6 Address                            MAC Address       S F  Rest  Interface
--------------------------------------- ----------------- - -- ----- ---------
(1)                                     (2)              (3)(4)(5)   (6)
2001:db8:ffff:2000:2a0:c9ff:fed8:904e   00:a0:0e:f8:ff:01 S    01111 lan0
2001:db8:ffff:2000:20c:6eff:fead:54e7   (incomplete)      I          lan0
fe80::2a0:c9ff:fed8:904e%lan0           00:a0:0e:f8:ff:01 R    01111 lan0
    Entry:3   --- (7)

# show ndp summary
    Entry:7

# show ndp 2001:db8:ffff:2000:2a0:c9ff:fed8:904e
IPv6 Address                            MAC Address       S F  Rest  Interface
--------------------------------------- ----------------- - -- ----- ---------
2001:db8:ffff:2000:2a0:c9ff:fed8:904e   00:a0:0e:f8:ff:01 S    01111 lan0
    Entry:1

# show ndp 2001:db8:ffff:2000:2a0:c9ff:fed8:904f
IPv6 Address                            MAC Address       S F  Rest  Interface
--------------------------------------- ----------------- - -- ----- ---------
    Entry:0

#
```

1) IPv6 Address

Neighbor Cache エントリの IPv6 address が表示されます。

2) MAC Address

Neighbor Cache エントリの MAC address が表示されます。

未解決の場合は (incomplete) が表示されます。

3) S

Neighbor Cache エントリの状態が表示されます。詳細を以下に示します。

N	(NoState)
W	(WaitDelete)
I	(Incomplete)
R	(Reachable)
S	(Stale)
D	(Delay)
P	(Probe)

4) F

エントリ種別が表示されます。詳細を以下に示します。

P	Permanent エントリ

5) Rest

Neighbor Cache エントリの残り生存時間を秒数で示します。Permanent エントリの場合は "perm"と表示されます。

6) Interface

Neighbor Cache エントリのインタフェースが表示されます。

7) Entry

Neighbor Cache エントリのエントリ数が表示されます。

31.1.2　clear ndp

[機能]

Neighbor Cache エントリの削除

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear ndp [<ipv6_address>]

[オプション]

なし

すべての動的に学習した Neighbor Cache エントリを削除します。

<ipv6_address>

指定された IPv6 アドレスの、動的に学習した Neighbor Cache エントリを削除します。
リンクローカルアドレスの場合は、アドレスに続けて % でインタフェース名を指定します。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

Neighbor Cache エントリを削除します。

[実行例]

```
# clear ndp
#
```

第 32 章　ルーティングテーブル情報・統計などの表示、クリア操作コマンド

32.1　IPv4 ルーティングテーブル情報・統計などの表示、クリア操作

32.1.1　show ip route

[機能]

ルーティングテーブル情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip route [all]
show ip route connected [all]
show ip route static [all]
show ip route rip [all]
show ip route bgp [all]
show ip route ospf [all]
show ip route dns [all]
show ip route ike [all]
show ip route destination <ip_address>/<mask> [all]
show ip route destination <ip_address>/<mask> longer-prefixes [all]

[オプション]

なし

ルーティングテーブルに登録した経路情報を表示します。

all

ルーティングテーブルに非登録の経路情報を含めてすべての経路情報を表示します。

connected

インタフェース経路情報のみを表示します。

static

スタティック経路情報のみを表示します。

rip

RIP 経路情報のみを表示します。

bgp

BGP 経路情報のみを表示します。

ospf

OSPF 経路情報のみを表示します。

dns

DNS 経路情報のみを表示します。

ike

IKE 経路情報のみを表示します。

destination <ip_address>/<mask>

指定したアドレスとマスクに一致した経路情報のみを表示します。
<mask>は、マスクビット数またはマスク値で指定します。マスク値の場合は、最上位ビットから 1 で連続した値にしてください。

destination <ip_address>/<mask> longer-prefixes

指定した経路情報に含まれる経路情報すべてを表示します。
<mask>は、マスクビット数またはマスク値で指定します。マスク値の場合は、最上位ビットから 1 で連続した値にしてください。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

経路共通管理部に登録している経路情報を表示します。

[注意]

ページャー機能を使用した場合に、さかのぼって再表示するなどの動作が使用できません。
使用できない動作、入力キーについては、terminal pager コマンド (ページャー機能の設定) を参照してください。

[実行例]

以下に、実行例を示します。

・すべての経路情報を表示する場合

```
# show ip route all
FP  Destination/Mask   Gateway         Distance UpTime    Interface
--- ------------------ --------------- -------- --------- ------------------
(1)  (2)                (3)             (4)       (5)      (6)
*C  192.168.10.0/24    192.168.10.50          0 00:00:01  lan0
*O  192.168.11.0/24    192.168.10.20        110 00:00:01  lan0
*C  192.168.16.0/24    192.168.16.50          0 00:00:01  lan1
*C  192.168.17.0/24    192.168.17.50          0 00:00:01  lan2
*O  192.168.20.0/24    192.168.10.70        110 00:00:01  lan0
*O  192.168.30.0/24    192.168.10.70        110 00:00:01  lan0
*E1 192.168.100.0/26   192.168.10.20        110 00:00:01  lan0
*E1 192.168.100.64/26  192.168.10.20        110 00:00:01  lan0
*E2 192.168.100.192/26 192.168.10.20        110 00:00:01  lan0
*A  192.168.200.0.25   192.168.10.70        110 00:00:01  lan0
*A  192.168.201.0/25   192.168.10.70        110 00:00:01  lan0
*A  192.168.201.192/26 192.168.10.70        110 00:00:01  lan0
*O  192.168.253.0/24   192.168.10.70        110 00:00:01  lan0
 R  192.168.253.0/24   192.168.10.80        120 00:00:01  lan0
```

1) FP

カーネルフラグおよびプロトコル種別が表示されます。
以下に、表示されるカーネルフラグを示します。

***** ：カーネルへ登録した経路を示します。

空白 ：カーネルへ登録していない経路を示します。

x ：カーネルへ登録できなかった経路を示します。(経路数上限オーバ)

以下に、表示されるプロトコル種別を示します。

Bi ：BGP(Internal) 経路情報を示します。

Be ：BGP(External) 経路情報を示します。

O ：OSPF(Internal Area) 経路情報を示します。

A ：OSPF(External Area) 経路情報を示します。

E1　：OSPF(External AS Type1) 経路情報を示します。

E2　：OSPF(External AS Type2) 経路情報を示します。

R　：RIP 経路情報を示します。

DN　：DNS 経路情報を示します。

IK　：IKE 経路情報を示します。

S　：スタティック経路情報を示します。

C　：インタフェース (interface route) 経路情報を示します。

L　：インタフェース (PtoP 回線の Local 側) 経路情報を示します。

2) Destination/Mask

あて先アドレス／マスク長が表示されます。

3) Gateway

ゲートウェイアドレスが表示されます。

4) Distance

経路優先度が表示されます。

5) UpTime

経路情報更新時からの経過時間が表示されます。

01:23:45　：1 時間 23 分 45 秒経過 (経過時間が 24 時間以内の場合)

6d23h45m

：6 日と 23 時間 45 分経過 (経過時間が 7 日以内の場合)

3w6d23h　：3 週間と 6 日と 23 時間経過

6) Interface

出力インタフェース名が表示されます。使用不可能状態のインタフェースは、インタフェース名に続いて (inactive) が表示されます。

32.1.2 show ip route summary

[機能]

ルーティングテーブルの経路情報数の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip route summary [all]

[オプション]

なし

ルーティングテーブルに登録した経路情報の数を表示します。

all

ルーティングテーブルに非登録の経路情報を含めてすべての経路情報の数を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

経路共通管理部に登録している経路情報数を表示します。

[注意]

ページャー機能を使用した場合に、さかのぼって再表示するなどの動作が使用できません。
使用できない動作、入力キーについては、terminal pager コマンド (ページャー機能の設定) を参照してください。

[実行例]

以下に、実行例を示します。

```
# show ip route summary
Route Source    Networks
------------    --------
 (1)             (2)
Static                 3
OSPF                   0 (O:0, A:0, E1:0, E2:0)
RIP                    0
BGP                    0 (Be:0, Bi:0)
DNS                    0
IKE                    0
Connected              7
Total                 10
```

1) Route Source

ルーティングプロトコル種別が表示されます。

Static ：スタティック経路情報を示します。

OSPF　：OSPF 経路情報を示します。

Internal Area ／ External Area ／ External AS Type1 ／ External AS Type2 の経路種別ごとの数が表示されます。

RIP　：RIP 経路情報を示します。

BGP　：BGP 経路情報を示します。

External ／ Internal の経路種別ごとの数が表示されます。

DNS　：DNS 経路情報を示します。

IKE　：IKE 経路情報を示します。

Connected

：インタフェース経路情報を示します。

2) Networks

経路数が表示されます。

32.1.3 clear ip route

[機能]

IPv4 ルーティングテーブルの経路情報の再登録

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear ip route
clear ip route rip
clear ip route bgp
clear ip route ospf
clear ip route dns

[オプション]

なし

すべての経路情報を再登録します。

rip

RIP 経路のみ再登録します。

bgp

BGP 経路のみ再登録します。

ospf

OSPF 経路のみ再登録します。

dns

DNS 経路のみ再登録します。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

ルーティングプロトコル部が保持している IPv4 経路情報を、経路共通管理部および IP カーネル部に再登録します。

[注意]

インタフェース経路とスタティック経路、IKE 経路については、再登録しません。
本コマンドは、再登録処理が完了するまで待ち合わせします。なお、CTRL+C を入力した場合、再登録処理を中断します。

[実行例]

以下に、実行例を示します。

```
# clear ip route
```

32.1.4　show ip route kernel

[機能]

IP カーネルのルーティングテーブルの表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip route kernel
show ip route kernel longest-match <ip_address>
show ip route kernel summary

[オプション]

なし

longest-match <ip_address>

IP カーネルのルーティングテーブルのうち、指定されたアドレスに longest match するエントリを表示します。

summary

IP カーネルのルーティングテーブルのエントリ数を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

IP カーネルのルーティングテーブルの、現在の状態を表示します。

[実行例]

以下に、実行例を示します。

```
# show ip route kernel
Routing Tables for Internet

Destination/Masklen Gateway           Flag   Interface             ---(1)
------------------- ----------------- ------ ---------
10.0.0.0/8          192.168.1.5       UGS    lan0
127.0.0.1           127.0.0.1         UH     lo0
192.168.1.0/24      link#1            U      lan0
192.168.1.5         link#1            UH     lan0
192.168.1.11        00:a0:c9:d8:90:4e UH     lan0
224.0.0.0/4         127.0.0.1         UG     lo0
    Entry:6                                                         ---(2)

# show ip route kernel longest-match 10.0.0.1
Routing Tables for Internet

Destination/Masklen Gateway           Flag   Interface
------------------- ----------------- ------ ---------
10.0.0.0/8          192.168.1.5       UGS    lan0
    Entry:1

# show ip route kernel longest-match 20.0.0.1
Routing Tables for Internet

Destination/Masklen Gateway           Flag   Interface
------------------- ----------------- ------ ---------
    Entry:0

# show ip route kernel summary
    Entry:6

#
```

1) Destination/Masklen

あて先ネットワークアドレスとマスク値が表示されます。

ホスト経路の場合はマスク値は表示されません。

Gateway

ゲートウェイアドレスを表示します。

ダイレクト経路はゲートウェイの MAC アドレスを表示します。ゲートウェイのアドレス解決ができていない場合は link#x(x はシステムがインタフェースごとに自動的に付与するインタフェースインデックス番号) で表示します。

Flag

エントリ種別を表示します。詳細を以下に示します。

U (Up) 経路が有効であることを示します。

G (Gateway)
ゲートウェイなどによる中継を必要とする経路を示します。

H (Host) ホストエントリを示します。

S (Static) スタティックルートを示します。

R (Reject)
破棄経路 (ICMP unreach 送信有) であることを示します。

B (Blackhole)
破棄経路 (ICMP unreach 送信無) であることを示します。

Interface

送出先インタフェースを示します。

2) Entry

装置内部で使用する経路を除いたエントリ数が表示されます。

32.1.5　show ip route kernel ecmp statistics

[機能]

ECMP 統計情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip route kernel ecmp statistics

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

ECMP 経路の統計情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show ip route kernel ecmp statistics
ECMP information for Internet

Destination/Masklen  Gateway           Packets    Interface        ---(1)
Since                                                               ---(2)
-------------------- ----------------- ---------- ---------
192.168.10.0/24      192.168.1.2                0 lan0
Jan  1 11:16:01 1970 192.168.2.2                0 lan1
                     192.168.3.2                0 lan2
                     192.168.4.2                0 lan3
#
```

1)　Destination/Masklen

ネットワークまたはホストのあて先 IP アドレス

Gateway　あて先ゲートウェイ IP アドレス

Packets　ECMP 経路が変更されてからの出力パケット数
※ ECMP 経路が変更されたときに 0 になります

Interface　経由インタフェース

2)　Since

ECMP 経路の変更がされた時刻

32.1.6 clear ip route kernel ecmp statistics

[機能]

ECMP 統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear ip route kernel ecmp statistics

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

ECMP 経路の統計情報をクリアします。

[実行例]

```
# clear ip route kernel ecmp statistics
#
```

32.2　IPv6 ルーティングテーブル情報・統計などの表示

32.2.1　show ipv6 route

[機能]

IPv6 ルーティングテーブル情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ipv6 route [all]
show ipv6 route connected [all]
show ipv6 route static [all]
show ipv6 route rip [all]
show ipv6 route dns [all]
show ipv6 route dhcp [all]
show ipv6 route ike [all]
show ipv6 route destination <prefix>/<prefixlen> [all]
show ipv6 route destination <prefix>/<prefixlen> longer-prefixes [all]

[オプション]

なし
IPv6 カーネルのルーティングテーブルに登録した経路情報を表示します。

all
IPv6 カーネルのルーティングテーブルに非登録の経路情報を含めてすべての経路情報を表示します。

connected
インタフェース経路情報のみを表示します。

static
スタティック経路情報のみを表示します。

rip
RIP 経路情報のみを表示します。

dns
DNS 経路情報のみを表示します。

dhcp
DHCP 経路情報のみを表示します。

ike
IKE 経路情報のみを表示します。

destination <prefix>/<prefixlen>
指定したプレフィックス／プレフィックス長に一致した経路情報のみを表示します。

destination <prefix>/<prefixlen> longer-prefixes
指定した経路情報に含まれる経路情報すべてを表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

経路共通管理部に登録している経路情報を表示します。

[注意]

ページャー機能を使用した場合に、さかのぼって再表示するなどの動作が使用できません。
使用できない動作、入力キーについては、terminal pager コマンド (ページャー機能の設定) を参照してください。

[実行例]

以下に、実行例を示します。

・すべての経路情報を表示する場合

```
# show ipv6 route all
FP  Destination/Prefixlen                          UpTime      Distance
(1)  (2)                                            (4)         (5)
        Gateway                                                Interface
         (3)                                                    (6)
--  ------------------------------------------  ---------   ------------------
*C  2001:db8:ffff:1000::/64                     00:00:01           0
        2001:db8:ffff:1000::1                                  lan0
*R  2001:db8:ffff:2000::/64                     00:00:01         110
        fe80::1                                                lan0
 S  2001:db8:ffff:3000::/64                                         1
        fe80::2                                                lan1(inactive)
```

1) FP

カーネルフラグおよびプロトコル種別が表示されます。
以下に、表示されるカーネルフラグを示します。

***** ：IPv6 カーネルに登録した経路を示します。

空白 ：IPv6 カーネルに登録していない経路を示します。

x ：IPv6 カーネルに登録できなかった経路を示します。(経路数上限オーバ)

以下に、表示されるプロトコル種別を示します。

R ：RIP 経路情報を示します。

DN ：DNS 経路情報を示します。

DH ：DHCP 経路情報を示します。

IKE ：IKE 経路情報を示します。

S ：スタティック経路情報を示します。

C ：インタフェース経路情報を示します。

L ：インタフェース経路情報 (PtoP 回線の Local 側) を示します。

2) Destination/Prefixlen

経路情報のあて先がプレフィックス／プレフィックス長で表示されます。
リンクローカルアドレスは表示されません。

3) Gateway

ゲートウェイアドレスが表示されます。

4) UpTime

経路情報更新時からの経過時間が表示されます。

01:23:45　: 1 時間 23 分 45 秒経過 (経過時間が 24 時間以内の場合)

6d23h45m

: 6 日と 23 時間 45 分経過 (経過時間が 7 日以内の場合)

3w6d23h　: 3 週間と 6 日と 23 時間経過

5) Distance

経路情報の優先度が表示されます。

6) Interface

出力インタフェース名が表示されます。使用不可能状態のインタフェースは、インタフェース名に続いて (inactive) が表示されます。

32.2.2 show ipv6 route summary

[機能]

IPv6 ルーティングテーブルの経路数の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ipv6 route summary [all]

[オプション]

なし

IPv6 カーネルのルーティングテーブルに登録した経路情報の数を表示します。

all

IPv6 カーネルのルーティングテーブルに非登録の経路情報を含めてすべての経路情報の数を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

経路共通管理部に登録している経路情報数を表示します。

[注意]

ページャー機能を使用した場合に、さかのぼって再表示するなどの動作が使用できません。
使用できない動作、入力キーについては、terminal pager コマンド (ページャー機能の設定) を参照してください。

[実行例]

以下に、実行例を示します。

```
# show ipv6 route summary
Route Source    Networks
 (1)             (2)
------------    --------
Static                 3
RIP                    0
DHCP                   0
DNS                    0
IKE                    0
Connected              7
Total                 10
```

1) Route Source

ルーティングプロトコル種別が表示されます。

Static ：スタティック経路情報を示します。

RIP ：RIP 経路情報を示します。

DHCP ：DHCP 経路情報を示します。

DNS　：DNS 経路情報を示します。

IKE　：IKE 経路情報を示します。

Connected

：インタフェース経路情報を示します。

2) Networks

経路数が表示されます。

32.2.3 clear ipv6 route

[機能]

IPv6 ルーティングテーブルの経路情報の再登録

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear ipv6 route
clear ipv6 route rip
clear ipv6 route dns
clear ipv6 route dhcp

[オプション]

なし

すべての経路情報を再登録します。

rip

RIP 経路のみ再登録します。

dns

DNS 経路のみ再登録します。

dhcp

DHCP 経路のみ再登録します。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

ルーティングプロトコル部が保持している IPv6 経路情報を、経路共通管理部および IPv6 カーネル部に再登録します。

[注意]

インタフェース経路とスタティック経路、IKE 経路については、再登録しません。
本コマンドは、再登録処理が完了するまで待ち合わせします。なお、CTRL+C を入力した場合、再登録処理を中断します。

[実行例]

以下に、実行例を示します。

```
# clear ipv6 route
```

32.2.4　show ipv6 route kernel

[機能]

IPv6 カーネルのルーティングテーブルの表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ipv6 route kernel
show ipv6 route kernel longest-match <ipv6_address>
show ipv6 route kernel summary

[オプション]

なし

IPv6 カーネルのルーティングテーブルの現在のエントリを表示します。

longest-match <ipv6_address>

IPv6 カーネルのルーティングテーブルのうち、指定されたアドレスに longest match するエントリを表示します。
リンクローカルアドレスの場合は、アドレスに続けて % でインタフェース名を指定します。

summary

IPv6 カーネルのルーティングテーブルのエントリ数を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

IPv6 カーネルのルーティングテーブルの、現在の状態を表示します。

[実行例]

以下に、実行例を示します。

```
# show ipv6 route kernel
Routing Tables for Internet6

Destination/Masklen                        Flag   Interface       ---(1)
    Gateway
------------------------------------------ ------ ---------
::1                                        UH     lo0
    ::1
2001:db8:ffff:1000::/48                    UGS    lan0
    fe80::2a0:c9ff:fed8:904e%lan0
2001:db8:ffff:2000::/64                    U      lan0
    link#1
fe80::2a0:c9ff:fed8:904e%lan0              UH     lan0
    00:a0:c9:d8:90:4e
fe80::%lo0/64                              U      lo0
    fe80::1%lo0
ff01::/32                                  U      lo0
    ::1
ff02::%lan0/32                             UC     lan0
    link#1
ff02::%lo0/32                              UC     lo0
    fe80::1%lo0
    Entry:8                                                          ---(2)

# show ipv6 route kernel longest-match 2001:db8:ffff:1000::1
Routing Tables for Internet6

Destination/Masklen                        Flag   Interface
    Gateway
------------------------------------------ ------ ---------
2001:db8:ffff:1000::/48                    UGS    lan0
    fe80::2a0:c9ff:fed8:904e%lan0
    Entry:1

# show ipv6 route kernel longest-match 2001:db8:ffff:3000::1
Routing Tables for Internet6

Destination/Masklen                        Flag   Interface
    Gateway
------------------------------------------ ------ ---------
    Entry:0

# show ipv6 route kernel summary
    Entry:8

#
```

1) Destination/Masklen

あて先ネットワークアドレスとマスク値が表示されます。

ホスト経路の場合はマスク値は表示されません。

Gateway

ゲートウェイアドレスを表示します。

ダイレクト経路はゲートウェイの MAC アドレスを表示します。ゲートウェイのアドレス解決ができていない場合は link#x(x はシステムがインタフェースごとに自動的に付与するインタフェースインデックス番号) で表示します。

Flag

エントリ種別を表示します。詳細を以下に示します。

U (Up) 経路が有効であることを示します。

G (Gateway)

ゲートウェイなどによる中継を必要とする経路を示します。

H (Host) ホストエントリを示します。

S (Static) スタティックルートを示します。

R (Reject)

破棄経路 (ICMP unreach 送信有) であることを示します。

B (Blackhole)

破棄経路 (ICMP unreach 送信無) であることを示します。

Interface

送出先インタフェースを示します。

2) Entry

装置内部で使用する経路を除いたエントリ数が表示されます。

第 33 章　RIP 情報の表示、クリア操作コマンド

33.1　RIP 情報の表示、クリア操作

33.1.1　show ip rip route

[機能]

RIP 経路情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip rip route

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

RIP の経路情報を表示します。

[注意]

ページャー機能を使用した場合に、さかのぼって再表示するなどの動作が使用できません。
使用できない動作、入力キーについては、terminal pager コマンド (ページャー機能の設定) を参照してください。

[メッセージ]

```
<ERROR> No RIP is configured.
```

原因：　RIP が設定されていません。または、定義が不足しており RIP が動作していません。

対処：　RIP を設定してください。

[実行例]

以下に、実行例を示します。

```
# show ip rip route

FP  Destination/Mask    Gateway          Metric  Time   Interface
(1)  (2)                 (3)             (4)     (5)    (6)
*C  192.168.10.0/24     0.0.0.0               1  none   lan0
*C  192.168.20.0/24     0.0.0.0               1  none   lan1
*S  192.168.30.0/24     192.168.10.11         2  none   lan0
*R  192.168.40.0/24     192.168.10.10         3  02:49  lan0
 R  192.168.40.0/24     192.168.10.12         4  02:31  lan0
*R  192.168.41.0/24     192.168.10.50         3  02:55  lan0
The number of entries : 4   ---(7)
```

1) FP

ベストパスを示すフラグ (F) およびプロトコル種別 (P) が表示されます。

***** ：ベストパスを示します。

空白 ：スペア経路情報を示します。

当該経路のプロトコル種別が表示されます。

R ：RIP 経路情報を示します。

C ：インタフェース経路情報を示します。

S ：スタティック経路情報を示します。

O ：OSPF 経路情報を示します。

B ：BGP 経路情報を示します。

DN ：DNS 経路情報を示します。

2) Destination/Mask

あて先アドレス／マスク長が表示されます。

3) Gateway

ゲートウェイアドレスが表示されます。

4) Metric

ネットワーク上に広報されるメトリック値が表示されます。

5) Time

有効期限タイマの残り時間が表示されます。

00:00 になると、この経路に関しては、メトリック値が 16 で広報されることを意味します。

メトリック値が 16 の場合、ガーベージタイマの残り時間が表示されます。

再配布された経路情報が有効な場合は、none と表示されます。

6) Interface

当該経路を受信したインタフェース名が表示されます。

7) The number of entries : 4

保持している RIP エントリ数が表示されます。インタフェース経路数は含まれません。

33.1.2　show ip rip protocol

[機能]

RIP プロトコル情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip rip protocol

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

RIP のプロトコル情報および統計情報を表示します。

[注意]

ページャー機能を使用した場合に、さかのぼって再表示するなどの動作が使用できません。
使用できない動作、入力キーについては、terminal pager コマンド (ページャー機能の設定) を参照してください。

[メッセージ]

```
<ERROR> No RIP is configured.
```

原因：　RIP が設定されていません。または、定義が不足しており RIP が動作していません。

対処：　RIP を設定してください。

[実行例]

以下に、実行例を示します。

```
# show ip rip protocol
Sending updates every 30 seconds with +/-50%, next due in 24 seconds
 (1)                              (2)          (3)
Timeout after 180 seconds, garbage collect after 120 seconds
 (4)                        (5)
Redistributing: BGP, Connected, Static                                ---(6)
Interface        Send    Recv
 (7)              (8)     (9)
  lan0            2       1 2
  rmt0            2       1 2

Routing Information Sources:
  Gateway           Rcv-Bad-Packets Rcv-Bad-Routes Last-Update
   (10)              (11)            (12)           (13)
  192.168.10.10                   0              0 00:00:07
  192.168.30.10                   0              0 00:00:24
  192.168.10.50                   0              0 00:00:13
Distance: 120                                                         ---(14)
The number of entries : 4                                             ---(15)
```

1) Sending updates every 30 seconds

定期広報タイマ値が表示されます。

2) with +/-50%

ゆらぎ幅が表示されます。50%は、15 秒のゆらぎを示します。

3) next due in 24 seconds

次の定期広報までの時間が表示されます。

4) Timeout after 180 seconds

RIP 有効期限タイマ値が表示されます。

5) garbage collect after 120 seconds

ガーベージ状態タイマ値が表示されます。

6) Redistributing

RIP に再配布したプロトコルに関する情報を表示します。

Connected
: インタフェース経路情報を示します。

Static : スタティック経路情報を示します。

OSPF : OSPF 経路情報を示します。

BGP : BGP 経路情報を示します。

DNS : DNS 経路情報を示します。

7) Interface

RIP で利用するインタフェース名が表示されます。

8) Send

送信モードが表示されます。

OFF : RIP パケットを送信しないことを示します。

1 : RIPv1 で送信することを示します。

2 : RIPv2(ブロードキャスト/マルチキャスト) で送信することを示します。

9) Recv

受信モードが表示されます。

OFF : RIP パケットを受信しないことを示します。

1　　：RIPv1 だけ受信することを示します。

1 2　　：RIPv1,RIPv2(ブロードキャスト/マルチキャスト) で受信することを示します。

10) Gateway
相手ルータの IP アドレスが表示されます。

11) Rcv-Bad-Packets
RIP パケット内の異常パケット数の累積数が表示されます。

12) Rcv-Bad-Routes
RIP パケット内の経路情報に関する異常経路数の累積数が表示されます。

13) Last-Update
相手ルータとの接続時間が表示されます。

14) Distance: 120
本装置の RIP の優先度が表示されます。

15) The number of entries : 4
保持している RIP エントリ数が表示されます。インタフェース経路数は含まれません。

33.1.3 clear ip rip statistics

[機能]

RIP 統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear ip rip statistics

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

RIP 統計情報をクリアします。

[実行例]

```
# clear ip rip statistics
#
```

33.2　IPv6 RIP 情報の表示

33.2.1　show ipv6 rip route

[機能]

IPv6 RIP 経路情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ipv6 rip route

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

IPv6 RIP の経路情報を表示します。

[注意]

ページャー機能を使用した場合に、さかのぼって再表示するなどの動作が使用できません。
使用できない動作、入力キーについては、terminal pager コマンド (ページャー機能の設定) を参照してください。

[メッセージ]

```
<ERROR> No IPv6 RIP is configured.
```

原因：　IPv6 RIP が設定されていません。または、定義が不足しており IPv6 RIP が動作していません。

対処：　IPv6 RIP を設定してください。

[実行例]

以下に、実行例を示します。

```
# show ipv6 rip route

FP  Destination/Prefixlen                          Time        Metric
(1)  (2)                                            (4)         (5)
        Gateway                                                Interface
         (3)                                                    (6)
*C  2001:db8:ffff:1000::/64                        none            1
        ::                                                     lan0
*R  2001:db8:ffff:2000::/64                        02:49           1
        fe80::1                                                lan0
The number of entries : 1  ---(7)
```

1) FP

ベストパスを示すフラグ (F) およびプロトコル種別 (P) が表示されます。

***** ：ベストパスを示します。

空白 ：スペア経路情報を示します。

当該経路のプロトコル種別が表示されます。

R ：IPv6 RIP 経路情報を示します。

C ：インタフェース経路情報を示します。

S ：スタティック経路情報を示します。

DN ：DNS 経路情報を示します。

DH ：DHCP 経路情報を示します。

2) Destination/Prefixlen

あて先アドレス／マスク長が表示されます。

3) Gateway

ゲートウェイアドレスが表示されます。

4) Time

有効期限タイマの残り時間が表示されます。

00:00 になると、この経路に関しては、メトリック値が 16 で広報されることを意味します。

メトリック値が 16 の場合、ガーベージタイマの残り時間が表示されます。

再配布された経路情報が有効な場合は、none と表示されます。

5) Metric

ネットワーク上に広報されるメトリック値が表示されます。

6) Interface

当該経路を受信したインタフェース名が表示されます。

7) The number of entries : 1

保持している RIP エントリ数が表示されます。インタフェース経路数は含まれません。

33.2.2　show ipv6 rip protocol

[機能]

IPv6 RIP プロトコル情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ipv6 rip protocol

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

IPv6 RIP プロトコル情報を表示します。

[注意]

ページャー機能を使用した場合に、さかのぼって再表示するなどの動作が使用できません。
使用できない動作、入力キーについては、terminal pager コマンド (ページャー機能の設定) を参照してください。

[メッセージ]

```
<ERROR> No IPv6 RIP is configured.
```

原因：　IPv6 RIP が設定されていません。または、定義が不足しており IPv6 RIP が動作していません。

対処：　IPv6 RIP を設定してください。

[実行例]

以下に、実行例を示します。

```
# show ipv6 rip protocol
Sending updates every 30 seconds with +/-50%, next due in 24 seconds
 (1)                            (2)          (3)
Timeout after 180 seconds, garbage collect after 120 seconds
 (4)                         (5)
Redistributing: Connected, Static                                    ---(6)
Distance: 120                                                        ---(7)
The number of entries : 1  ---(8)
```

1) Sending updates every 30 seconds
   定期広報タイマ値が表示されます。
2) with +/-50%
   ゆらぎ幅が表示されます。50%は、15 秒のゆらぎを示します。

3) next due in 24 seconds
次の定期広報までの時間が表示されます。

4) Timeout after 180 seconds
RIP 有効期限タイマ値が表示されます。

5) garbage collect after 120 seconds
ガーベージ状態タイマ値が表示されます。

6) Redistributing
RIP に再配布したプロトコルに関する情報を表示します。

Connected
: インタフェース経路情報を示します。

Static : スタティック経路情報を示します。

DNS : DNS 経路情報を示します。

DHCP : DHCP 経路情報を示します。

7) Distance: 120
本装置の RIP の優先度が表示されます。

8) The number of entries : 1
保持している RIP エントリ数が表示されます。インタフェース経路数は含まれません。

第 34 章　BGP 情報の表示、クリア操作コマンド

34.1 BGP 情報の表示、クリア操作

34.1.1 show ip bgp route

[機能]

BGP 経路情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip bgp route
show ip bgp route address <ip_address>/<mask> detail
show ip bgp route address <ip_address>/<mask> longer-prefixes

[オプション]

なし

BGP の経路情報を表示します。

address <ip_address>/<mask> detail

指定されたアドレスとマスクに一致する経路のみ詳細表示します。
<mask>は、マスクビット数またはマスク値で指定します。
マスク値の場合は、最上位ビットから 1 で連続した値にしてください。

address <ip_address>/<mask> longer-prefixes

指定されたアドレスとマスクよりも長いプレフィックスを持つ経路のみすべて表示します。
<mask>は、マスクビット数またはマスク値で指定します。
マスク値の場合は、最上位ビットから 1 で連続した値にしてください。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

BGP の経路情報を表示します。

[注意]

ページャー機能を使用した場合に、さかのぼって再表示するなどの動作が使用できません。
使用できない動作、入力キーについては、terminal pager コマンド (ページャー機能の設定) を参照してください。

[メッセージ]

```
<ERROR> No BGP is configured.
```

原因： BGP が設定されていません。

対処： BGP を設定してください。

```
<ERROR> No such network.
```

原因：　指定したアドレスの経路情報が存在しません。

対処：　正しい経路情報のアドレスを指定してください。

備考：　detail オプションの場合のみ表示されます。

[実行例]

以下に、実行例を示します。

・パラメタなしの場合

```
# show ip bgp route
Local router ID is 192.168.20.1                                          (1)
Status Codes: s suppressed, v valid, * best, i - internal
Origin Codes: i - IGP, e - EGP, ? - incomplete

   Network            Next Hop            Metric  LocalPref Path
    (2)                  (3)               (4)      (5)     (6)
v* 10.10.0.0/16       0.0.0.0                                 i
v* 10.10.20.0/24      192.168.10.2            0        100 65000 65001 65002
    65003 65004 i
v* 11.0.0.0           0.0.0.0                                 i
s* 11.10.0.0/16       10.10.10.100                            ?
v* 20.0.0.0           192.168.10.2            0        100 65000 65001 65002
    65003 65004 i
v*i30.0.0.0/24        192.168.20.3                     100 i
The number of routes is 6                                                (7)

# show ip bgp route address 10.0.0.0/8  longer-prefixes
Local router ID is 192.168.20.1
Status Codes: s suppressed, v valid, * best, i - internal
Origin Codes: i - IGP, e - EGP, ? - incomplete

   Network            Next Hop            Metric  LocalPref Path
v* 10.10.0.0/16       0.0.0.0                                 i
v* 10.10.20.0/24      192.168.10.2            0        100 65000 65001 65002
    65003 65004 i
The number of routes is 2
```

1) Local router ID

本装置の BGP ルータ ID が表示されます。

2) Network

エントリの状態を示す Status Codes とあて先のネットワークアドレスが表示されます。

s　：経路集約によって抑止されていることを示します。

v　：有効であることを示します。

*****　：ベストパスであることを示します。

i　：IBGP で学習したことを示します。

3) Next Hop

ネクストホップの IP アドレスが表示されます。

4) Metric

メトリック (MED 属性) の値が表示されます。

5) LocalPref

ローカル優先度 (LOCAL-PREF 属性) の値が表示されます。

6) Path

経由した AS 番号 (AS-PATH 属性) とオリジン (ORIGIN 属性) が表示されます。
長い AS パスの場合は、改行して表示されます。

i	: AS 内部で生成したエントリを示します。
e	: EGP を通して受信したエントリを示します。
?	: 再配布されたエントリを示します。

7) The number of routes

総エントリ数が表示されます。

・アドレスとマスクに一致する経路の詳細表示の場合

```
# show ip bgp route address 20.0.0.0/8 detail
BGP routing table entry for 20.0.0.0/8                                    (1)
Paths: (1 available, best #1)                                              (2)
  Advertised to non peer-group peers:                                      (3)
  192.168.20.3
  65000 65001 65002 65003 65004                                            (4)
    192.168.10.2 from 192.168.10.2 (192.168.10.2)                          (5)
      Origin IGP, metric 0, localpref 100, valid, external, best           (6)
      Community: no-export                                                 (7)
      Last update: Thu Mar 13 14:39:40 2005                                (8)
```

1) BGP routing table entry for

指定した経路情報が表示されます。

2) Paths: (1 available, best #1)

経路数およびベストパスの有無が表示されます。

available　：有効な経路数が表示されます。

best　：ベストパスが何番目かが表示されます。

no best path

：ベストパスがない場合に表示されます。

not advertised to any peer

：COMMUNITY 属性 (NO_ADVERTISE) により、この経路を BGP で広報しない場合に表示されます。

not advertised to EBGP peer

：COMMUNITY 属性 (NO_EXPORT) により、この経路を EBGP で広報しない場合に表示されます。

Advertisements suppressed by an aggregate.

：AGGREGATOR 属性が設定されている場合に表示されます。

3) Advertised to non peer-group peers:

この経路情報を BGP で広報している場合は、その広報先の IP アドレスとともに表示されます。広報していない場合は、"Not advertised to any peer"と表示されます。

4) 65000 65001 65002 65003 65004

AS パス (AS-PATH 属性) が表示されます。

再配布経路など AS パス (AS-PATH 属性) が存在しない場合は、Local と表示されます。

AGGREGATOR 属性が設定されている場合は、"aggregated by"に続き経路を集約した BGP 装置の AS 番号と BGP のルータ ID が表示されます。

5) 192.168.10.2 from 192.168.10.2 (192.168.10.2)

ネクストホップアドレスと、送信元 IPv4 アドレス (BGP のルータ ID) が表示されます。

インタフェース経路の場合、ネクストホップアドレスと送信元 IPv4 アドレスは 0.0.0.0 と表示されます。

インタフェース経路を除く再配布経路の場合、送信元 IPv4 アドレスは 0.0.0.0 と表示されます。

リカーシブ経路が無効な場合は、"inaccessible"と表示されます。

6) Origin incomplete, metric 0, valid, external, best

Origin　：オリジン (ORIGIN 属性) が表示されます。

"IGP"、"EGP"または、"incomplete"のどれかが表示されます。

metric　：メトリック (MED 属性) が表示されます。

localpref ： ローカル優先度 (LOCAL-PREF 属性) が表示されます。

valid ： 経路情報が有効なことを示します。

external ： EBGP 接続の場合に表示されます。

internal ： IBGP 接続の場合に表示されます。

aggregated, local
： 集約された経路の場合に表示されます。

sourced ： 再配布された経路の場合に表示されます。

sourced, local
： network コマンドで作成した経路の場合に表示されます。

atomic-aggregate
： ATOMIC_AGGREGATE 属性が設定されている場合に表示されます。

best ： ベストパスの場合に表示されます。

7) Community:

COMMUNITY 属性が設定されている場合に表示されます。"no-export" または、"no-advertise"のどちらかが表示されます。

8) Last update:

最後に更新された日時が表示されます。

構成定義情報にタイムゾーンが指定されていない状態では GMT(グリニッジ標準時間) として表示されます。

34.1.2　show ip bgp route summary

[機能]

BGP 経路情報数の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip bgp route summary

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

BGP ルーティングテーブルの経路情報数を表示します。

[注意]

ページャー機能を使用した場合に、さかのぼって再表示するなどの動作が使用できません。
使用できない動作、入力キーについては、terminal pager コマンド (ページャー機能の設定) を参照してください。

[メッセージ]

```
<ERROR> No BGP is configured.
```

原因：　BGP が設定されていません。

対処：　BGP を設定してください。

[実行例]

以下に、実行例を示します。

```
# show ip bgp route summary
Route                                                                   (1)
    Entries                        4                                    (2)
    Total Entries                  6                                    (3)
    Total Prefixes                 6                                    (4)

Attribute                                                               (5)
    AS-PATH                        5                                    (6)
    COMMUNITY                      0                                    (7)
```

1)　Route
経路数に関する情報を示します。

2) Entries

network 経路および aggregate 経路を除く BGP 経路数が表示されます。

3) Total Entries

network 経路および aggregate 経路を含む BGP 経路数が表示されます。

4) Total Prefixes

プレフィックス数が表示されます。

5) Attribute

経路属性に関する情報を示します。

6) AS-PATH

AS-PATH 属性の数が表示されます。同一の属性値は 1 として数えられます。

7) COMMUNITY

COMMUNITY 属性の数が表示されます。同一の属性値は 1 として数えられます。

34.1.3　show ip bgp status

[機能]

BGP セッションの状態表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip bgp status

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

BGP セッションの状態を表示します。

[注意]

ページャー機能を使用した場合に、さかのぼって再表示するなどの動作が使用できません。
使用できない動作、入力キーについては、terminal pager コマンド (ページャー機能の設定) を参照してください。

[メッセージ]

```
<ERROR> No BGP is configured.
```

原因：　BGP が設定されていません。

対処：　BGP を設定してください。

[実行例]

以下に、実行例を示します。

```
# show ip bgp status
Local AS number 65535                                                    (1)
Neighbor            AS    MsgRcvd    MsgSent  Up/Down   State          PfxRcd
   (2)             (3)      (4)        (5)     (6)      (7)             (8)
192.168.10.2     65000         92        103  00:00:06  Active             0
192.168.20.3     65535         93        104  00:45:10  Established        1
```

1) Local AS number
本装置の自律システム番号が表示されます。

2) Neighbor
隣接装置の IP アドレスが表示されます。

3) AS

隣接装置の自律システム番号が表示されます。

4) MsgRcvd

隣接装置から受信した BGP メッセージの累積数が表示されます。

5) MsgSent

隣接装置に送信した BGP メッセージの累積数が表示されます。

6) Up/Down

BGP セッションの継続時間が表示されます。

Established 状態では、Established 状態となってからの時間が表示されます。

Established 以外の状態では、Idle、または Active 状態となってからの時間が表示されます。

01:23:45 : 1 時間 23 分 45 秒経過 (経過時間が 24 時間以内の場合)

6d23h45m
: 6 日と 23 時間 45 分経過 (経過時間が 7 日以内の場合)

3w6d23h : 3 週間と 6 日と 23 時間経過

never ： 隣接装置と一度も BGP のメッセージ交換をしていない状態を示します。

7) State

BGP セッションの現在の状態が表示されます。

BGP 状態は以下のとおりです。

Idle ： アイドル状態

Connect ： 接続中状態

Active ： アクティブ状態

OpenSent
： OPEN メッセージ待ち状態

OpenConfirm
： BGP 接続確立のための KEEPALIVE メッセージ待ち状態

Established
： BGP 接続が確立した状態

8) PfxRcd

隣接装置から受信したプレフィックスの数が表示されます。

34.1.4　show ip bgp neighbors

[機能]

BGP 隣接情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip bgp neighbors [address <ip_address>]

[オプション]

なし

すべての BGP 隣接情報を表示します。

address <ip_address>

指定した隣接アドレスの BGP 隣接情報のみ表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

BGP の隣接情報を表示します。

[注意]

ページャー機能を使用した場合に、さかのぼって再表示するなどの動作が使用できません。
使用できない動作、入力キーについては、terminal pager コマンド (ページャー機能の設定) を参照してください。

[メッセージ]

```
<ERROR> No BGP is configured.
```

原因：　BGP が設定されていません。

対処：　BGP を設定してください。

```
<ERROR> No such neighbor.
```

原因：　指定したアドレスの隣接情報が存在しません。

対処：　正しい隣接情報のアドレスを指定してください。

[実行例]

以下に、実行例を示します。

```
# show ip bgp neighbors
BGP neighbor is 192.168.10.2, remote AS 65000, local AS 65535, external link (1)
  BGP version 4, remote router ID 192.168.10.2                               (2)
  BGP state = Established, up for 00:00:09                                   (3)
  Last read 00:00:08, hold time is 90, keepalive interval is 30 seconds      (4)
  Configured hold time is 90, keepalive interval is 30 seconds               (5)
  Neighbor capabilities:                                                     (6)
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 92 messages, 3 notifications, 0 in queue                          (7)
  Sent 109 messages, 0 notifications, 0 in queue                             (8)
  Route refresh request: received 0, sent 0                                  (9)
  Minimum time between advertisement runs is 30 seconds                     (10)
 Update source is 192.168.10.1                                              (11)

 For address family: IPv4 Unicast                                           (12)
  NEXT_HOP is always this router                                            (13)
  2 accepted prefixes                                                       (14)
  3 announced prefixes                                                      (15)

 Connections established 4; dropped 3                                       (16)
Local host: 192.168.10.1, Local port: 1055                                  (17)
Foreign host: 192.168.10.2, Foreign port: 179                               (18)
Nexthop: 192.168.10.1                                                       (19)
Read thread: on  Write thread: off                                          (20)
```

1) BGP neighbor is 192.168.10.2, remote AS 65000, local AS 65535, external link

   隣接装置の IP アドレス、隣接装置の属する AS 番号, 本装置の属する AS 番号が表示されます。

   "external link"は BGP 接続形態が EBGP であることを示します。

   IBGP の場合は"internal link"と表示されます。

2) BGP version 4, remote router ID 192.168.10.2

   本装置の BGP 版数と隣接装置の BGP ルータ ID が表示されます。

3) BGP state = Established, up for 00:00:09

   BGP 状態と BGP 接続が確立してからの経過時間が表示されます。

   BGP 状態は以下のとおりです。

   Idle ： アイドル状態

   Connect ： 接続中状態

   Active ： アクティブ状態

   OpenSent

   ： OPEN メッセージ待ち状態

   OpenConfirm

   ： BGP 接続確立のための KEEPALIVE メッセージ待ち状態

   Established

   ： BGP 接続が確立した状態

4) Last read 00:00:08, hold time is 90, keepalive interval is 30 seconds

   隣接装置から最後にメッセージ受信してからの経過時間、Holdtime タイマの値、Keepalive タイマの値が表示されます。

5) Configured hold time is 90, keepalive interval is 30 seconds

   本装置での Holdtime タイマの設定値、本装置での Keepalive タイマの設定値が表示されます。

6) Neighbor capabilities:
隣接装置とネゴシエートしたケイパビリティを以下の情報で表示します。

- Route refresh: advertised and received(old and new)
  Route refresh capability(OLD,NEW) を示します。
- Address family IPv4 Unicast: advertised and received
  Multiprotocol extension capability(IPv4 unicast) を示します。
- Address family VPNv4 Unicast: advertised and received
  Multiprotocol extension capability(VPNv4 unicast) を示します。

7) Received 92 messages, 3 notifications, 0 in queue
受信したメッセージ数、受信した NOTIFICATION 数、未処理の受信メッセージ数が表示されます。

8) Sent 109 messages, 0 notifications, 0 in queue
送信したメッセージ数、送信した NOTIFICATION 数、未処理の送信メッセージ数が表示されます。

9) Route refresh request: received 0, sent 0
ROUTE_REFRESH メッセージの送受信メッセージ数が表示されます。

10) Minimum time between advertisement runs is 30 seconds
アドバタイズメントタイマ値が表示されます。EBGP では 30 秒、IBGP では 5 秒が表示されます。

11) Update source is 192.168.10.1
BGP セッションの自側に設定されている IP アドレスが表示されます。

12) For address family: IPv4 Unicast
アドレスファミリが表示されます。
"IPv4 Unicast"または、"VPNv4 unicast"が表示されます。

13) NEXT_HOP is always this router
NEXTHOP 属性を常に本装置のアドレスとして広報することが表示されます。

14) 1 accepted prefixes
隣接装置から受信した経路情報の数が表示されます。

15) 2 announced prefixes
本装置から広報した経路情報の数が表示されます。

16) Connections established 4; dropped 3
Established 状態となった回数、および、Established 状態で BGP 接続を終了した回数が表示されます。
Idle 状態の場合、"Next start timer due in"が表示され、スタートタイマの残り時間を示します。
Idle,Connected 状態以外の場合、Established になるまでの間、"Next connect timer due in"が表示され、コネクトタイマの残り時間を示します。

17) Local host: 192.168.10.1, Local port: 1055
BGP 接続に使用している本装置の IP アドレスとポート番号が表示されます。

18) Foreign host: 192.168.10.2, Foreign port: 179
BGP 接続に使用している隣接装置の IP アドレスとポート番号が表示されます。

19) Nexthop: 192.168.10.1
NEXTHOP として使用する IP アドレスが表示されます。

20) Read thread: on Write thread: off
受信/送信処理状況が表示されます。
受信可能状態の場合は"Read thread: on"が表示され、受信不可状態の場合は"Read thread: off"が表示されます。
送信処理中の場合は"Write thread: on"が表示され、送信処理を行っていない場合は"Write thread: off"が表示されます。

34.1.5 show ip bgp vpnv4 route

[機能]

BGP VPNv4 経路情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip bgp vpnv4 route [vrf <vrf_number>]

[オプション]

なし

すべての VRF の経路情報を表示します。

vrf <vrf_number>

指定した VRF 番号の VRF の経路情報を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

BGP VPNv4 経路情報を表示します。

[注意]

ページャー機能を使用した場合に、さかのぼって再表示するなどの動作が使用できません。
使用できない動作、入力キーについては、terminal pager コマンド (ページャー機能の設定) を参照してください。

[メッセージ]

```
<ERROR> No BGP is configured.
```

原因： BGP が設定されていません。

対処： BGP を設定してください。

```
<ERROR> No VRF is configured.
```

原因： VRF が設定されていません。

対処： VRF を設定してください。

```
<ERROR> No such VRF.
```

原因： 指定した VRF 番号の VRF が存在しません。

対処： 正しい VRF 番号を指定してください。

[実行例]

以下に、実行例を示します。

```
# show ip bgp vpnv4 route
   Network          Next Hop            Metric  LocalPref Path
     (1)               (2)                (3)       (4)    (5)
Route Distinguisher: 100:1 (VRF0)                                          (6)
v*i100.0.0.0        10.1.1.4                         100 ?
v* 192.168.1.0      0.0.0.0                              ?
The number of routes is 2                                                  (7)

Route Distinguisher: 100:2 (VRF1)
v* 192.168.2.0      0.0.0.0                              ?
v*i200.0.0.0        10.1.1.4                         100 ?
The number of routes is 2


# show ip bgp vpnv4 route vrf 0
   Network          Next Hop            Metric  LocalPref Path
Route Distinguisher: 100:1 (VRF0)
v*i100.0.0.0        10.1.1.4                         100 ?
v* 192.168.1.0      0.0.0.0                              ?
The number of routes is 2
```

1) Network

エントリの状態を示す Status Codes とあて先のネットワークアドレスが表示されます。

v　：有効であることを示します。

*****　：ベストパスであることを示します。

i　：IBGP で学習したことを示します。

2) Next Hop

ネクストホップの IP アドレスが表示されます。

3) Metric

メトリック (MED 属性) の値が表示されます。

4) LocalPref

ローカル優先度 (LOCAL-PREF 属性) の値が表示されます。

5) Path

経由した AS 番号 (AS-PATH 属性) とオリジン (ORIGIN 属性) が表示されます。

長い AS パスの場合は、改行して表示されます。

i　：AS 内部で生成したエントリを示します。

e　：EGP を通して受信したエントリを示します。

?　：再配布されたエントリを示します。

6) Route Distinguisher: 100:1 (VRF0)

VRF の RD(Route Distinguisher) および VRF 番号が表示されます。

7) The number of routes

総エントリ数が表示されます。

34.1.6 clear ip bgp statistics

[機能]

BGP 統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear ip bgp statistics

[オプション]

なし

BGP 統計情報をクリアします。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

BGP 統計情報をクリアします。

[実行例]

```
# clear ip bgp statistics
#
```

第 35 章　OSPF 情報の表示、クリア操作コマンド

35.1 OSPF 情報の表示、クリア操作

35.1.1 show ip ospf route

[機能]

OSPF 経路情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip ospf route

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

OSPF の経路情報を表示します。

[注意]

ページャー機能を使用した場合に、さかのぼって再表示するなどの動作が使用できません。
使用できない動作、入力キーについては、terminal pager コマンド (ページャー機能の設定) を参照してください。

[メッセージ]

```
<ERROR> No OSPF is configured.
```

原因： OSPF が設定されていません。または、定義が不足しており OSPF が動作していません。

対処： OSPF を設定してください。

[実行例]

以下に、実行例を示します。

```
# show ip ospf route

Type          Destination/Masklen Nexthop               Cost Area            Interface
 (1)           (2)                 (3)                   (4)  (5)             (6)
Network Intra 10.1.0.0/16         0.0.0.0                  2 0.0.0.2         lan2
Network Intra 10.2.0.0/16         0.0.0.0                  1 0.0.0.2         lan2
Network Intra 10.3.0.0/16         0.0.0.0                  1 0.0.0.2         lan2
Network Intra 192.168.10.0/24     0.0.0.0                  1 0.0.0.0         lan0
Network Intra 192.168.11.0/24     192.168.10.20           11 0.0.0.0         lan0
Network Intra 192.168.13.0/24     192.168.10.20           22 0.0.0.0         lan0
Network Intra 192.168.14.0/24     192.168.10.20           12 0.0.0.0         lan0
Network Type2 192.168.100.0/26    192.168.10.20         1000                 lan0
Network Intra 192.168.100.64/26   192.168.10.20           11 0.0.0.0         lan0
Network Intra 192.168.100.192/26  192.168.10.20           22 0.0.0.0         lan0
Network Intra 192.168.130.0/26    192.168.10.20           21 0.0.0.0         lan0
Network Intra 192.168.200.0/25    192.168.10.70           11 0.0.0.0         lan1
Network Intra 192.168.250.70/32   192.168.10.70           11 0.0.0.0         lan1
Network Intra 192.168.251.70/32   192.168.10.70           11 0.0.0.0         lan1
Router  Intra 192.168.100.65      192.168.10.20            1 0.0.0.0         lan0
Router  Intra 192.168.200.0.70    192.168.10.70            1 0.0.0.0         lan1
Router  Intra 192.168.100.129     192.168.10.20           11 0.0.0.0         lan0
Router  Intra 192.168.100.193     192.168.10.20           12 0.0.0.0         lan0
14 Network entries, and 4 Router entries.   ---(7)
```

1) Type

経路種別が表示されます。

Network　：ネットワーク経路を示します。

Router　：ルータ経路を示します。

Intra　：エリア内経路を示します。

Inter　：エリア外／ AS 内経路を示します。

Type1　：Type1 AS 外部経路を示します。

Type2　：Type2 AS 外部経路を示します。

NSSA1　：NSSA Type1 AS 外部経路を示します。

NSSA2　：NSSA Type2 AS 外部経路を示します。

Discard　：集約経路定義時の破棄経路を示します。

2) Destination/Masklen

ネットワーク経路の場合は、あて先ネットワークとマスク長が表示されます。

ルータ経路の場合は、マスク長は表示されません。

同じコストの経路が複数表示された場合は ECMP 経路を示し、最大 4 経路まで表示されます。

3) Nexthop

OSPF によって学習された経路のうち、もっともコストの小さい経路の次のゲートウェイのアドレスが表示されます。

4) Cost

ネットワーク経路までのコスト値が表示されます。

Type1 の AS 外部経路の場合は、AS 境界ルータまでの AS 内コストに、AS 境界ルータから目的ネットワークまでの Metric 値を加えたコスト値が表示されます。

Type2 の AS 外部経路の場合は、AS 境界ルータから目的ネットワークまでの Metric 値が表示されます。

5) Area

経路がどのエリアに向いているかが表示されます。

6) Interface

出力インタフェース名を表示します。

7) 14 Network entries, and 4 Router entries.

ネットワーク経路とルータ経路の数が表示されます。

35.1.2 show ip ospf protocol

[機能]

OSPF 情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip ospf protocol

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

OSPF の動作状態を表示します。

[注意]

ページャー機能を使用した場合に、さかのぼって再表示するなどの動作が使用できません。
使用できない動作、入力キーについては、terminal pager コマンド (ページャー機能の設定) を参照してください。

[メッセージ]

```
<ERROR> No OSPF is configured.
```

原因： OSPF が設定されていません。または、定義が不足しており OSPF が動作していません。

対処： OSPF を設定してください。

[実行例]

以下に、実行例を示します。

(OSPF の動作状態表示の場合)

```
# show ip ospf protocol

 ospf(v2) daemon is running.                                          ---(1)
 Global statistics and variables:
 SPF schedule delay 5 secs, Hold time between next SPF 10 secs.       ---(2)
  Router ID: 192.168.100.1                                            ---(3)
  This implementation conforms to RFC2328                             ---(4)
  RFC1583Compatibility flag is enabled                                ---(5)
  AS boundary router.                                                 ---(6)
  Redistributing external routes from,                                ---(7)
    Static
    Connected
  Area border router.                                                 ---(8)
  Number of External LSA in Database is 5. Checksum Sum is 0x1fc7a    ---(9)
  Number of LSA is 5                                                  ---(10)
  Number of network route is 4                                        ---(11)
  Number of router route is 0                                         ---(12)
  Number of configured areas is 1                                     ---(13)

  Area(0.0.0.0) statistics and variables:                             ---(14)
    This area seems to be normal area                                 ---(15)
    SPF algorithm executed 14 times                                   ---(16)
    Number of LSA in Database is 4. Checksum Sum is 0x1aec1           ---(17)
    Number of fully adjacent neighbor is 0                            ---(18)
    Number of active interface is 1                                   ---(19)
    Number of interfaces attached in this area is 1                   ---(20)
    "Area" address range(for route aggregation):                      ---(21)
      192.168.0.0/255.255.0.0 (Advertise)

  Area(0.0.0.1) statistics and variables:
    This area seems to be normal area
    SPF algorithm executed 14 times
    Number of LSA in Database is 5. Checksum Sum is 0x206a2
    Number of fully adjacent neighbor is 1
    Number of full virtual adjacencies going through this area is 0    ---(22)
    Number of active interface is 1
    Number of interfaces attached in this area is 1
    "Area" address range(for route aggregation):
```

1) ospf(v2) daemon is running.

   OSPF の版数が表示されます。

2) SPF schedule delay 5 secs, Hold time between next SPF 10 secs.

   spf-delay タイマ値と spf-holdtime タイマ値が表示されます。

3) Router ID: 192.168.100.1

   ルータ ID が表示されます。

4) This implementation conforms to RFC2328

   RFC2328 に準拠していることを示します。

5) RFC1583Compatibility flag is enabled

   RFC1583 互換モードで動作していることを示します。

6) AS boundary router.

   AS 境界ルータとして動作している場合に表示されます。

7) Redistributing external routes from

   AS 内に広報する AS-External 経路の種類が表示されます。

   Static　：スタティック経路を示します。

   Connected

   ：インタフェース経路を示します。

   RIP　：RIP 経路を示します。

BGP ：BGP 経路を示します。

DNS ：DNS 経路を示します。

8) Area border router.
エリア境界ルータとして動作している場合に表示されます。

9) Number of External LSA in Database is 5. Checksum Sum is 0x1fc7a
AS-ExternalLSA の数およびそれらのチェックサム合計値が表示されます。

10) Number of LSA is 5
LSA の数が表示されます。

11) Number of network route is 4
ネットワーク経路の数が表示されます。

12) Number of router route is 0
ルータ経路の数が表示されます。

13) Number of configured areas is 1
設定されているエリアの総数が表示されます。

14) Area(0.0.0.0) statistics and variables:
Area(0.0.0.0) に関する動作状況が表示されます。

15) This area seems to be normal area
エリアの種類を表示します。

This area seems to be normal area
：通常エリアの場合に表示されます。

This area is configured as Stub, default cost is 1
：スタブエリアの場合に表示され、デフォルト経路のコストを表示します。

This area is configured as NSSA, default cost is 1
：NSSA エリアの場合に表示され、デフォルト経路のコストを表示します。

16) SPF algorithm executed
SPF 計算アルゴリズムの実行回数が表示されます。

17) Number of LSA in Database is 4. Checksum Sum is 0x1aec1
このエリアに属する LSA 数とそのチェックサム合計値が表示されます。

18) Number of fully adjacent neighbor is 0
このエリアで Full 状態になっている隣接ルータ数が表示されます。

19) Number of active interface is 1
このエリアに属しているインタフェースのうち動作状態のインタフェース数が表示されます。

20) Number of interfaces attached in this area is 1
このエリアに属するインタフェースの総数が表示されます。

21) "Area" address range(for route aggregation):
エリア内部集約経路の一覧が表示されます。

22) Number of full virtual adjacencies going through this area
エリアを経由しているバーチャルリンク数が表示されます。

35.1.3　show ip ospf database

[機能]

OSPF LSA データベース情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip ospf database
show ip ospf database self-originate
show ip ospf database lsa <type> detail
show ip ospf database lsa <type> ls-id <link_id> detail
show ip ospf database lsa <type> self-originate detail
show ip ospf database lsa <type> adv-router <router_id> detail

[オプション]

なし

OSPF データベースの全 LSA を表示します。

self-originate

OSPF データベースの自ルータが発行した LSA のみを表示します。

lsa <type> detail

OSPF データベースのうち指定された LSA 種別のみを詳細表示します。
<type>には、router、network、summary、asbr-summary、external、nssa-external を指定します。

lsa <type> ls-id <link_id> detail

OSPF データベースで指定された LSA 種別、リンク ID と一致する LSA のみを詳細表示します。

lsa <type> self-originate detail

OSPF データベースで指定された LSA 種別で自ルータ発行の LSA のみを詳細表示します。

lsa <type> adv-router <router_id> detail

OSPF データベースで指定された LSA 種別、広報元ルータ ID と一致する LSA のみを詳細表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

OSPF の LSA データベース情報を表示します。

[注意]

ページャー機能を使用した場合に、さかのぼって再表示するなどの動作が使用できません。
使用できない動作、入力キーについては、terminal pager コマンド (ページャー機能の設定) を参照してください。

[メッセージ]

```
<ERROR> No OSPF is configured.
```

原因： OSPF が設定されていません。または、定義が不足しており OSPF が動作していません。

対処： OSPF を設定してください。

```
<ERROR> No such lsa.
```

原因： リンク ID または広報元ルータ ID で指定した lsa が存在しません。

対処： 正しいリンク ID または広報元ルータ ID を指定してください。

[実行例]

以下に、実行例を示します。

・OSPF データベースの全 LSA の簡易表示の場合

```
# show ip ospf database

LSA list in the LSDB for area 0.0.0.0 (4 LSAs, Checksum Sum:0x1aec1)
                                        (1)       (2)
Type     Link ID         Advertiser      Age  Seq#     Sum
 (3)      (4)             (5)            (6)   (7)     (8)
Router   192.168.100.1   192.168.100.1   0431 80000008 6715
SumNet   192.168.110.247 192.168.100.1   0855 80000006 d483
SumNet   192.168.120.247 192.168.100.1   0644 80000001 70e2
SumNet   192.168.130.247 192.168.100.1   0823 80000001 0247

LSA list in the LSDB for area 0.0.0.1 (5 LSAs, Checksum Sum:0x204a3)
Type     Link ID         Advertiser      Age  Seq#     Sum
Router   192.168.100.1   192.168.100.1   0096 80000008 d99c
SumNet   0.0.0.0         192.168.100.1   0106 80000002 1b13
SumNet   192.168.100.247 192.168.100.1   0827 80000006 6103
SumNet   192.168.120.247 192.168.100.1   0904 80000001 8ec6
SumNet   192.168.130.247 192.168.100.1   0632 80000001 202b

LSA list in the LSDB for area 0.0.0.2 (10 LSAs, Checksum Sum:0x5dd0e)
Type     Link ID         Advertiser      Age  Seq#     Sum
Router   192.168.100.1   192.168.100.1   0638 80000004 c99c
SumNet   192.168.100.247 192.168.100.1   0848 80000006 e873
SumNet   192.168.110.247 192.168.100.1   0876 80000006 7ad7
SumNet   192.168.130.247 192.168.100.1   0639 80000001 a79b
NSSA     0.0.0.0         192.168.100.1   0106 80000002 3559
NSSA     10.255.255.255  192.168.100.1   0684 80000009 0199
NSSA     20.255.255.255  192.168.100.1   0698 80000009 7e12
NSSA     30.255.255.255  192.168.100.1   0712 80000009 fb8a
NSSA     192.168.10.255  192.168.100.1   0726 80000009 63cd
NSSA     192.168.20.255  192.168.100.1   0740 80000009 f432

LSA list in the LSDB (AS-External) (5 LSAs, Checksum Sum:0x1fc7a)
Type     Link ID         Advertiser      Age  Seq#     Sum
External 10.255.255.255  192.168.100.1   0677 80000009 a2da
External 20.255.255.255  192.168.100.1   0691 80000009 2053
External 30.255.255.255  192.168.100.1   0705 80000009 9dcb
External 192.168.10.255  192.168.100.1   0719 80000009 050f
External 192.168.20.255  192.168.100.1   0733 80000009 9673
```

1) 4 LSAs

エリアごとに広報されている LSA の個数が表示されます。

2) Checksum Sum:0x1aec1

エリアごとのチェックサム合計値が表示されます。

3) Type

LSA の種別が表示されます。

Router　：Router LSA を示します。

Network　：Network LSA を示します。

SumNet　：Summary LSA を示します。

SumRtr　：ASBR Summary LSA を示します。

External　：AS external LSA を示します。

NSSA　：NSSA AS external LSA を示します。

4) Link ID

LSA の Link State ID(ルータやネットワークの IP アドレス) が表示されます。

5) Advertiser

LSA を発行したルータのルータ ID が表示されます。

6) Age

LSA が発行されてからの経過時間が秒単位の 10 進数で表示されます。

7) Seq#

LSA の発行シーケンス番号が表示されます。

8) Sum

LSA のチェックサム値が表示されます。

・ルータリンク情報表示の場合

```
# show ip ospf database lsa router detail

LSA list in the LSDB for area 0.0.0.0 (3 LSAs, Checksum Sum:0x14bd2)

Router    Id 192.168.100.1    Router 192.168.100.1
 (1)      (2)                 (3)
Age 0098  Seq 800000d4  Sum 8b27  Length 48    Option 0x02(*|-|-|-|-|-|E|-)
(4)       (5)           (6)       (7)          (8)
  #links  2  Option (E,B)
   (9)       (10)
    Stub            Id 192.168.100.0    Data 255.255.255.0    Metric 1
    Stub            Id 192.168.130.0    Data 255.255.255.0    Metric 1
    (11)            (12)                (13)                  (14)

LSA list in the LSDB for area 0.0.0.1 (4 LSAs, Checksum Sum:0x13851)

Router    Id 192.168.100.1    Router 192.168.100.1
Age 0453  Seq 800000d1  Sum 4666  Length 36    Option 0x00(*|-|-|-|-|-|-|-)
  #links  1  Option (B)
    Stub            Id 192.168.110.0    Data 255.255.255.0    Metric 1
```

1) Router

Router LSA であることを示します。

2) Id

この LSA を生成したルータのルータ ID が表示されます。

3) Router

この LSA を発行したルータのルータ ID が表示されます。

4) Age

LSA が発行されてからの経過時間が秒単位の 10 進数で表示されます。

5) Seq

LSA の発行シーケンス番号が表示されます。

6) Sum

LSA のチェックサム値が表示されます。

7) Length

LSA の長さが表示されます。

8) Option

ルータがサポートするオプション能力 (capability) が表示されます。

9) #links

このルータのリンク数が表示されます。

10) Option

このルータの役割が表示されます。

NT ：NSSA のトランスレータであることを示します。

V ：バーチャルリンクのエンド ポイントであることを示します。

E ：AS 境界ルータであることを示します。

B ：エリア境界ルータであることを示します。

11) Stub

リンクの種類が表示されます。

Point-to-Point

：Point-to-Point 接続であることを示します。

Transit　：トランジットネットワークであることを示します。

Stub　：スタブネットワークであることを示します。

Virtual　：バーチャルリンクであることを示します。

12) ID

リンクの ID が表示されます。

13) Data

リンクデータが表示されます。

14) Metric

そのリンクのコストが表示されます。

・ネットワークリンク情報表示の場合

```
# show ip ospf database lsa network detail

LSA list in the LSDB for area 0.0.0.0 (2 LSAs, Checksum Sum:0x1aec1)

Network   Id 192.168.2.3     Router 192.168.100.1
 (1)      (2)                 (3)
Age 0905  Seq 80000006  Sum d483  Length 32    Option 0x02 (*|-|-|-|-|-|E|-)
 (4)      (5)           (6)       (7)          (8)
  Network Mask 255.255.255.0
   (9)
    Attached Router: 192.168.100.2   ---(10)
    Attached Router: 192.168.100.3

Network   Id 192.168.3.3     Router 192.168.110.1
Age 0693  Seq 80000006  Sum 70e2  Length 32    Option 0x02 (*|-|-|-|-|-|E|-)
  Network Mask 255.255.255.0
    Attached Router: 192.168.110.2
    Attached Router: 192.168.110.3
```

1) Network

   Network LSA であることを示します。

2) Id

   当該ネットワークの DR のインタフェースの IP アドレスが表示されます。

3) Router

   この LSA を発行したルータのルータ ID が表示されます。

4) Age

   LSA が発行されてからの経過時間が秒単位の 10 進数で表示されます。

5) Seq

   LSA の発行シーケンス番号が表示されます。

6) Sum

   LSA のチェックサム値が表示されます。

7) Length

   LSA の長さが表示されます。

8) Option

   ルータがサポートするオプション能力 (capability) が表示されます。

9) Network Mask

   当該ネットワークのネットワークマスクが表示されます。

10) Attached Router

    当該ネットワークに接続しているすべてのルータのルータ ID が表示されます。

・サマリリンク情報表示の場合

```
# show ip ospf database lsa summary detail

LSA list in the LSDB for area 0.0.0.0 (4 LSAs, Checksum Sum:0x1aec1)

SumNet    Id 192.168.110.0    Router 192.168.100.1
 (1)      (2)                 (3)
Age 0905  Seq 80000006  Sum d483  Length 28    Option 0x02 (*|-|-|-|-|-|E|-)
 (4)      (5)           (6)       (7)          (8)
  Network Mask 255.255.255.0
   (9)
    TOS 0  Metric 1
           (10)

SumNet    Id 192.168.120.0    Router 192.168.100.1
Age 0693  Seq 80000001  Sum 70e2  Length 28    Option 0x02(*|-|-|-|-|-|E|-)
  Network Mask 255.255.255.0
    TOS 0  Metric 1
```

1) SumNet

Summary LSA であることを示します。

2) Id

エリア外のネットワークアドレスが表示されます。

3) Router

この LSA を発行したルータのルータ ID が表示されます。

4) Age

LSA が発行されてからの経過時間が秒単位の 10 進数で表示されます。

5) Seq

LSA の発行シーケンス番号が表示されます。

6) Sum

LSA のチェックサム値が表示されます。

7) Length

LSA の長さが表示されます。

8) Option

ルータがサポートするオプション能力 (capability) が表示されます。

9) Network Mask

ネットワークマスクが表示されます。

10) Metric

(2) で示すネットワークまでのコストが表示されます。

・ASBR サマリリンク情報表示の場合

```
# show ip ospf database lsa asbr-summary detail

LSA list in the LSDB for area 0.0.0.0 (2 LSAs, Checksum Sum:0x1aec1)

SumRtr    Id 172.16.0.1       Router 192.168.100.1
 (1)      (2)                 (3)
Age 0905  Seq 80000006  Sum d483  Length 28    Option 0x02 (*|-|-|-|-|-|E|-)
 (4)      (5)           (6)       (7)          (8)
  Network Mask 0.0.0.0
   (9)
    TOS 0  Metric 10
           (10)

SumRtr    Id 172.16.1.1       Router 192.168.110.1
Age 0693  Seq 80000001  Sum 70e2  Length 28    Option 0x02 (*|-|-|-|-|-|E|-)
  Network Mask 0.0.0.0
    TOS 0  Metric 10
```

1) SumRtr

   ASBR Summary LSA であることを示します。

2) Id

   AS 境界ルータのルータ ID が表示されます。

3) Router

   この LSA を発行したルータのルータ ID が表示されます。

4) Age

   LSA が発行されてからの経過時間が秒単位の 10 進数で表示されます。

5) Seq

   LSA の発行シーケンス番号が表示されます。

6) Sum

   LSA のチェックサム値が表示されます。

7) Length

   LSA の長さが表示されます。

8) Option

   ルータがサポートするオプション能力 (capability) が表示されます。

9) Network Mask

   0.0.0.0 が表示されます。

10) Metric

    (2) で示す AS 境界ルータまでのコストが表示されます。

・AS 外部ネットワークリンク情報表示の場合

```
# show ip ospf database lsa external detail

LSA list in the LSDB (AS-External) (5 LSAs, Checksum Sum:0x2b39e)

External  Id 10.0.0.0         Router 192.168.100.1
 (1)      (2)                 (3)
Age 0468  Seq 80000011  Sum 92e2  Length 36    Option 0x02(*|-|-|-|-|-|E|-)
 (4)      (5)           (6)       (7)          (8)
  Network Mask 255.0.0.0
   (9)
    Type2 TOS 0  Metric 20  Forwarder 0.0.0.0  Tag 0
     (10)              (11)       (12)          (13)

External  Id 20.0.0.0         Router 192.168.100.1
Age 1719  Seq 80000010  Sum 125a  Length 36    Option 0x02(*|-|-|-|-|-|E|-)
  Network Mask 255.0.0.0
    Type2 TOS 0  Metric 20  Forwarder 0.0.0.0  Tag 0
```

1) External
AS external LSA であることを示します。
lsa タイプに nssa-external を指定した場合は、NSSA が表示されます。

2) Id
AS 外部のネットワークアドレスが表示されます。

3) Router
この LSA を発行したルータのルータ ID が表示されます。

4) Age
LSA が発行されてからの経過時間が秒単位の 10 進数で表示されます。

5) Seq
LSA の発行シーケンス番号が表示されます。

6) Sum
LSA のチェックサム値が表示されます。

7) Length
LSA の長さが表示されます。

8) Option
ルータがサポートするオプション能力 (capability) が表示されます。

9) Network Mask
ネットワークマスクが表示されます。

10) Type2
メトリックの種類が表示されます。

Type1　：Type1 external メトリックであることを示します。
Type2　：Type2 external メトリックであることを示します。

11) Metric
(2) で示すネットワークまでのメトリックが表示されます。

12) Forwarder
(2) で示すネットワークへ向かうデータトラフィックが転送されるアドレスが表示されます。
0.0.0.0 の場合は、LSA を生成したルータに送られます。

13) Tag
(2) で示すネットワークにつけるタグが表示されます。

35.1.4 show ip ospf interface

[機能]

OSPF インタフェース情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip ospf interface

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

OSPF に関するインタフェース情報を表示します。

[注意]

ページャー機能を使用した場合に、さかのぼって再表示するなどの動作が使用できません。
使用できない動作、入力キーについては、terminal pager コマンド (ページャー機能の設定) を参照してください。

[メッセージ]

```
<ERROR> No OSPF is configured.
```

原因： OSPF が設定されていません。または、定義が不足しており OSPF が動作していません。

対処： OSPF を設定してください。

[実行例]

以下に、実行例を示します。

```
# show ip ospf interface

lan0:                                                                  ---(1)
  Line physical status is (Up)                                         ---(2)
  Line ospf status is (DR), priority is 1, transmit delay is 10
   (3)                      (4)           (5)
  Neighbor Count is 0, Adjacent neighbor count is 0                    ---(6)
  Internet Address 192.168.100.1, Mask 255.255.255.0, Area 0.0.0.0
   (7)                            (8)                (9)
  Timer intervals(in seconds): Hello 10, Dead 40, Wait 40, Retransmit 5  ---(10)
  Router ID 192.168.100.1, Network Type BROADCAST, Cost: 10
   (11)                    (12)                   (13)
  Designated Router ID 192.168.100.1, Interface Address 192.168.100.1    ---(14)
  Backup Designated Router ID 0.0.0.0, Interface Address 0.0.0.0         ---(15)
  Next hello packet due in 00:00:08                                      ---(16)

lan1:
  Line physical status is (Up)
  Line ospf status is (DR), priority is 1, transmit delay is 10
  Neighbor Count is 0, Adjacent neighbor count is 0
  Internet Address 192.168.110.1, Mask 255.255.255.0, Area 0.0.0.1
  Timer intervals(in seconds): Hello 10, Dead 40, Wait 40, Retransmit 5
  Router ID 192.168.100.1, Network Type BROADCAST, Cost: 10
  Designated Router ID 192.168.100.1, Interface Address 192.168.110.1
  Backup Designated Router ID 0.0.0.0, Interface Address 0.0.0.0
  Next hello packet due in 00:00:08

rmt0:
  Line physical status is (Up)
  Line ospf status is (PtoP), transmit delay is 1
  Neighbor Count is 1, Adjacent neighbor count is 1
  Internet Address 172.16.1.1, Mask 255.255.255.255, Area 0.0.0.0
  Timer intervals(in seconds): Hello 10, Dead 40, Wait 40, Retransmit 5
  Router ID 255.255.255.255, Network Type POINTOPOINT, Cost: 10
  Next hello packet due in 00:00:01

VLINK0:
  Virtual Link to router 5.5.5.5 is (Up)                                 ---(17)
  Line ospf status is (PtoP), transmit delay is 1
  Transit area 0.0.0.3 via interface lan3                                ---(18)
  Timer intervals(in seconds): Hello 10, Dead 40, Retransmit 5
  Router ID 255.255.255.255, Network Type VIRTUALLINK
  Next hello packet due in 00:00:08
  Adjacency state Full                                                   ---(19)
```

1) lan0:

   インタフェース名が表示されます。

2) Line physical status is (Up)

   インタフェースの状態が表示されます。

3) Line ospf status is (DR)

   OSPF のインタフェースの状態が表示されます。

4) priority is 1

   指定ルータ優先度の値が表示されます。

5) transmit delay is 10

   LSU パケット送信遅延時間が表示されます。

6) Neighbor Count is 0, Adjacent neighbor count is 0

   隣接関係にあるルータ数および FULL 状態にあるルータ数が表示されます。

7) Internet Address 192.168.100.1

   このインタフェースの IP アドレスが表示されます。

8) Mask 255.255.255.0

   このインタフェースのネットマスク値が表示されます。

9) Area 0.0.0.0
このインタフェースが属するエリア ID が表示されます。

10) Timer intervals(in seconds)
以下のタイマに関する情報が表示されます。

Hello : Hello パケット送信間隔の時間を示します。

Dead : 隣接ルータ停止確認間隔の時間を示します。

Retransmit
: パケット再送間隔の時間を示します。

11) Router ID
ルータ ID が表示されます。

12) Network Type
ネットワークタイプが表示されます。

POINTOPOINT
: ポイントツーポイントネットワークを示します。

BROADCAST
: プロードキャストネットワークを示します。

VIRTUALLINK
: バーチャルリンクを示します。

13) Cost
インタフェースの出力コストが表示されます。

14) Designated Router ID 192.168.100.1, Interface Address 192.168.100.1
指定ルータのルータ ID とそのインタフェースアドレスが表示されます。
当該ネットワークで決定していない場合は 0.0.0.0 と表示されます。

15) Backup Designated Router ID 0.0.0.0, Interface Address 0.0.0.0
副指定ルータのルータ ID とそのインタフェースアドレスが表示されます。
当該ネットワークで決定していない場合は 0.0.0.0 と表示されます。

16) Next hello packet due in
Hello パケットが再送されるまでの時間が表示されます。
OSPF パケット送信抑止が設定されている場合は、以下が表示されます。
"No Hellos (Passive interface)"

17) Virtual Link to router 5.5.5.5 is (Up)
バーチャルリンク接続の相手装置のルータ ID とその状態が表示されます。

18) Transit area 0.0.0.3 via interface lan3
本装置とバーチャルリンク接続する相手装置間のエリア ID およびそのエリアへのインタフェース名が表示されます。

19) Adjacency state Full
相手装置と隣接関係を構築するまでの状態が表示されます。

35.1.5　show ip ospf neighbor

[機能]

OSPF 隣接情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip ospf neighbor [detail]
show ip ospf neighbor router-id <router_id> detail

[オプション]

なし

OSPF 隣接情報を表示します。

detail

OSPF 隣接情報を詳細表示します。

router-id <router_id> detail

指定した隣接ルータに関する OSPF 隣接情報を詳細表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

インタフェースごとに OSPF 隣接情報を表示します。

[注意]

ページャー機能を使用した場合に、さかのぼって再表示するなどの動作が使用できません。
使用できない動作、入力キーについては、terminal pager コマンド (ページャー機能の設定) を参照してください。

[メッセージ]

```
<ERROR> No OSPF is configured.
```

原因：　OSPF が設定されていません。または、定義が不足しており OSPF が動作していません。

対処：　OSPF を設定してください。

```
<ERROR> No such neighbor.
```

原因：　指定した隣接ルータが存在しません。

対処：　正しいルータ ID を指定してください。

[実行例]

以下に、実行例を示します。

・OSPF 隣接情報表示の場合

```
# show ip ospf neighbor

Neighbor information with all interfaces, result:

Neighbor with lan0 result:
 Neighbor ID     Pri State          Deadtime Address           DDL  ReqL  RtrL
  (1)            (2)  (3)           (4)       (5)              (6)   (7)   (8)
   192.168.100.2   1  Full/BDR      00:00:38 192.168.100.2      11     0     0
   192.168.100.3   1  Full/DR       00:00:38 192.168.100.3      11     0    10
   192.168.100.4   1  2-Way/Other   00:00:37 192.168.100.4       0     0     0
```

1) Neighbor ID

隣接ルータのルータ ID を表示します。

2) Pri

優先度 (Priority) を表示します。

3) State

隣接ルータとの状態が表示されます。

Down ：Neighbor との接続が行われていない状態を示します。

Init ：まだ隣接と双方向通信が行われていない状態を示します。

2-Way ：隣接と双方向通信可能な状態を示します。

ExStart ：隣接関係の構築を開始した状態を示します。

Exchange ：リンクステートデータベースの交換を行っている状態を示します。

Loading ：リンクステートデータベースの交換が終了し、最新情報がある場合は、その要求を行っている状態を示します。

Full ：隣接関係を構築した状態を示します。

DR ：隣接ルータが、指定ルータであることを示します。

BDR ：隣接ルータが、副指定ルータであることを示します。

Other ：隣接ルータが、指定ルータでも副指定ルータでもないことを示します。

PtoP ：隣接ルータと Point-to-Point 接続していることを示します。

4) Deadtime

隣接ルータの停止を検出するまでの残り時間が表示されます。

5) Address

隣接ルータの IP アドレスが表示されます。

6) DDL

データベースデスクリプションリスト中の LSA 数が表示されます。

7) ReqL

リンクステート要求リスト中の LSA 数が表示されます。

8) RtrL

リンクステート再送リスト中の LSA 数が表示されます。

・指定した OSPF 隣接ルータ情報表示の場合

```
# show ip ospf neighbor router-id 5.5.5.5 detail
 Neighbor 5.5.5.5, interface address 192.168.1.5            ---(1)
    In the area 0.0.0.0 via interface lan0                  ---(2)
    Neighbor priority is 1, State is Full, 11 state changes ---(3)
    DR is 192.168.1.1, BDR is 192.168.1.5                   ---(4)
    Options is 0x02 (*|-|-|-|-|-|E|-)                       ---(5)
    Dead timer due in 00:00:36                              ---(6)
    Neighbor is up for 00:03:40                             ---(7)
    Database Summary List 0                                 ---(8)
    Link State Request List 0                               ---(9)
    Link State Retransmission List 0                        ---(10)
```

1) Neighbor 5.5.5.5, interface address 192.168.1.5
   隣接ルータのルータ ID とアドレスが表示されます。

2) In the area 0.0.0.0 via interface lan0
   接続しているエリアとインタフェース名が表示されます。

3) Neighbor priority is 1, State is Full, 11 state changes
   隣接ルータの指定ルータ優先度、状態および状態の遷移回数が表示されます。

4) DR is 192.168.1.1, BDR is 192.168.1.5
   指定ルータおよび副指定ルータのアドレスが表示されます。

5) Option is 0x02 (*|-|-|-|-|-|E|-)
   Hello パケットに設定されたオプションが表示されます。

   0x02 (*|-|-|-|-|-|E|-) :
   通常エリア

   0x00 (*|-|-|-|-|-|-|-) :
   スタブエリア

   0x08 (*|-|-|-|NP|-|-|-) :
   準スタブエリア (NSSA)

6) Dead timer due in 00:00:36
   隣接ルータの停止を検出するまでの残り時間が表示されます。

7) Neighbor is up for 00:03:40
   隣接ルータと Hello パケットの交換を開始してからの経過時間が表示されます。

8) Database Summary List 0
   データベースデスクリプションリスト中の LSA 数が表示されます。

9) Link State Request List 0
   リンクステート要求リスト中の LSA 数が表示されます。

10) Link State Retransmission List 0
    リンクステート再送リスト中の LSA 数が表示されます。

35.1.6 clear ip ospf statistics

[機能]

OSPF 統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear ip ospf statistics

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

OSPF 統計情報をクリアします。

[実行例]

```
# clear ip ospf statistics
#
```

第 36 章　VPNv4 ルーティングテーブル情報の表示コマンド

36.1 VPNv4 ルーティングテーブル情報の表示

36.1.1 show ip vpnv4 route

[機能]

VPNv4 ルーティングテーブル情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip vpnv4 route [vrf <vrf_number>] [all]

[オプション]

なし

有効な VRF 経路情報を VRF 番号ごとに表示します。

vrf <vrf_number>

指定した VRF 番号の VRF 経路情報を表示します。

all

すべての VRF 経路情報を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

経路共通管理部に登録している VPNv4 経路情報を表示します。

[メッセージ]

```
<ERROR> No VRF is configured.
```

原因：VRF が設定されていません。
対処：VRF を設定してください。

```
<ERROR> No such VRF.
```

原因：指定した VRF 番号の VRF が存在しません。
対処：正しい VRF 番号を指定してください。

[実行例]

以下に、実行例を示します。

```
# show ip vpnv4 route
[VRF 0]                                                                    (1)
FP  Destination/Mask   Gateway         Distance UpTime    Interface
(2)  (3)               (4)             (5)      (6)       (7)
--- ------------------ --------------- -------- --------- ------------------
*C  10.1.1.1/32        10.1.1.1               0 00:03:51  lo0
*C  172.16.1.0/24      172.16.1.1             0 00:03:51  lan2
*C  192.168.10.0/24    192.168.10.50          0 00:02:02  lan0
*Bi 192.168.15.0/24    10.1.1.2             200 00:00:03  mpls
*S  192.168.20.0/24    192.168.10.99          1 00:02:02  lan0
```

1) [VRF 0]

VRF 番号が表示されます。

2) FP

状態フラグおよびプロトコル種別が表示されます。

以下に、表示される状態フラグを示します。

*****　：有効経路を示します。

空白　：有効でない経路を示します。

以下に、表示されるプロトコル種別を示します。

Bi　：BGP(Internal) 経路情報を示します。

S　：スタティック経路情報を示します。

C　：インタフェース経路情報を示します。

3) Destination/Mask

あて先アドレス／マスク長が表示されます。

4) Gateway

ゲートウェイアドレスが表示されます。

BGP 経路の場合、BGP 経路の NextHop アドレスが表示されます。

5) Distance

経路優先度が表示されます。

6) UpTime

経路情報更新時からの経過時間が表示されます。

01:23:45　：1 時間 23 分 45 秒経過 (経過時間が 24 時間以内の場合)

6d23h45m

：6 日と 23 時間 45 分経過 (経過時間が 7 日以内の場合)

3w6d23h　：3 週間と 6 日と 23 時間経過

7) Interface

出力インタフェース名が表示されます。使用不可能状態のインタフェースは、インタフェース名に続いて (inactive) が表示されます。

BGP 経路の場合は、"mpls"が表示されます。

36.1.2 show ip vpnv4 route summary

[機能]

VPNv4 ルーティングテーブル経路情報数の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip vpnv4 route [vrf <vrf_number>] summary [all]

[オプション]

summary

有効な VRF 経路情報数を VRF 番号ごとに表示します。

vrf <vrf_number> summary

指定した VRF 番号の VRF 経路情報数を表示します。

all

すべての VRF 経路情報数を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

経路共通管理部に登録している VPNv4 経路情報数を表示します。

[メッセージ]

```
<ERROR> No VRF is configured.
```

原因：VRF が設定されていません。
対処：VRF を設定してください。

```
<ERROR> No such VRF.
```

原因：指定した VRF 番号の VRF が存在しません。
対処：正しい VRF 番号を指定してください。

[実行例]

以下に、実行例を示します。

```
# show ip vpnv4 route summary
[VRF 0]                                                          ---(1)
Route Source    Networks
------------    --------
 (2)             (3)
Static                 0
BGP                    2 (Be:0, Bi:2)
Connected              2
Total                  4
```

1) [VRF 0]
VRF 番号が表示されます。

2) Route Source
ルーティングプロトコル種別が表示されます。

Static　：スタティック経路情報を示します。

BGP　：BGP 経路情報を示します。
External ／ Internal の経路種別ごとの数が表示されます。

Connected
：インタフェース経路情報を示します。

3) Networks
経路数が表示されます。

第 37 章　パケットの統計情報の表示、クリア操作コマンド

37.1　IPv4 パケットの統計情報の表示、クリア操作

37.1.1　show ip traffic

[機能]

IP 関連の統計情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip traffic
show ip traffic { tcp | udp | ip | icmp | igmp | ipsec | pim }

[オプション]

なし
すべての IP 統計情報を表示します。

tcp
TCP パケットの統計情報を表示します。

udp
UDP パケットの統計情報を表示します。

ip
IP パケットの統計情報を表示します。

icmp
ICMP パケットの統計情報を表示します。

igmp
IGMP パケットの統計情報を表示します。

ipsec
IPsec パケットの統計情報を表示します。

pim
PIM パケットの統計情報を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

IP 関連の統計情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show ip traffic
tcp:
        170 packets sent
                145 data packets (29694 bytes)
                1 data packet (18 bytes) retransmitted
                0 resends initiated by MTU discovery
                19 ack-only packets (10 delayed)
                0 URG only packets
                0 window probe packets
                0 window update packets
                5 control packets
        217 packets received
                145 acks (for 29706 bytes)
                1 duplicate ack
                0 acks for unsent data
                121 packets (14492 bytes) received in-sequence
                0 completely duplicate packets (0 bytes)
                0 old duplicate packets
                0 packets with some dup. data (0 bytes duped)
                3 out-of-order packets (42 bytes)
                0 packets (0 bytes) of data after window
                0 window probes
                0 window update packets
                0 packets received after close
                0 discarded for bad checksums
                0 discarded for bad header offset fields
                0 discarded because packet too short
                0 discarded for bad/no md5 signatures
        3 connection requests
        4 connection accepts
        0 bad connection attempts
        0 listen queue overflows
        6 connections established (including accepts)
        2 connections closed (including 1 drop)
                1 connection updated cached RTT on close
                1 connection updated cached RTT variance on close
                0 connections updated cached ssthresh on close
        1 embryonic connection dropped
        145 segments updated rtt (of 145 attempts)
        1 retransmit timeout
                0 connections dropped by rexmit timeout
        0 persist timeouts
                0 connections dropped by persist timeout
        22 keepalive timeouts
                0 keepalive probes sent
                0 connections dropped by keepalive
        22 correct ACK header predictions
        64 correct data packet header predictions
udp:
        250 datagrams received
        0 with incomplete header
        0 with bad data length field
        0 with bad checksum
        0 dropped due to no socket
        224 broadcast/multicast datagrams dropped due to no socket
        0 dropped due to full socket buffers
        0 not for hashed pcb
        26 delivered
        26 datagrams output
```

(続く)

(続き)

```
ip:
        467 total packets received
        0 bad header checksums
        0 with size smaller than minimum
        0 with data size < data length
        0 with ip length > max ip packet size
        0 with header length < data size
        0 with data length < header length
        0 with bad options
        0 with incorrect version number
        0 fragments received
        0 fragments dropped (dup or out of space)
        0 fragments dropped after timeout
        0 packets reassembled ok
        467 packets for this host
        0 packets for unknown/unsupported protocol
        0 packets forwarded
        0 packets not forwardable
        0 redirects sent
        197 packets sent from this host
        0 packets sent with fabricated ip header
        0 output packets dropped due to no bufs, etc.
        0 output packets discarded due to no route
        0 output datagrams fragmented
        0 fragments created
        0 datagrams that can’t be fragmented
        0 tunneling packets that can’t find gif
icmp:
        0 calls to icmp_error
        0 errors not generated ’cuz old message was icmp
        0 messages with bad code fields
        0 messages < minimum length
        0 bad checksums
        0 messages with bad length
        0 message responses generated
igmp:
        0 messages received
        0 messages received with too few bytes
        0 messages received with bad checksum
        0 membership queries received
        0 membership queries received with invalid field(s)
        0 membership reports received
        0 membership reports received with invalid field(s)
        0 membership reports received for groups to which we belong
        0 membership reports sent
ipsec:
        0 inbound packets processed successfully
        0 inbound packets violated process security policy
        0 inbound packets with no SA available
        0 invalid inbound packets
        0 discard inbound packets by interface down
        0 inbound packets failed due to insufficient memory
        0 inbound packets failed getting SPI
        0 inbound packets failed on AH replay check
        0 inbound packets failed on ESP replay check
        0 inbound packets considered authentic
        0 inbound packets failed on authentication
        0 inbound packets considered authentic(ESPinAuth)
        0 inbound packets failed on authentication(ESPinAuth)
        0 outbound packets processed successfully
        0 outbound packets violated process security policy
        0 outbound packets with no SA available
        0 invalid outbound packets
        0 outbound packets failed due to insufficient memory
        0 outbound packets with no route
        0 ipsec queue overflows
```

(続く)

(続き)

```
pim:
        0 messages received
        0 bytes received
        0 messages received with too few bytes
        0 messages received with bad checksum
        0 messages received with bad version
        0 data register messages received
        0 data register bytes received
        0 data register messages received on wrong iif
        0 bad registers received
        0 full checksum registers received
        0 data register messages sent
        0 data register bytes sent
#
```

37.1.2　clear ip traffic

[機能]

IP 関連の統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear ip traffic

[オプション]

なし

IP 関連の統計情報をクリアします。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

IP 関連の統計情報をクリアします。

[実行例]

```
# clear ip traffic
#
```

37.2 IPv6 パケットの統計情報の表示、クリア操作

37.2.1 show ipv6 traffic

[機能]

IPv6 パケットの統計情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ipv6 traffic
show ipv6 traffic { tcp | udp | ip | icmp | ipsec }

[オプション]

なし

すべての IPv6 統計情報を表示します。

tcp

TCP パケットの統計情報を表示します。

udp

UDP パケットの統計情報を表示します。

ip

IPv6 パケットの統計情報を表示します。

icmp

ICMP パケットの統計情報を表示します。

ipsec

IPsec パケットの統計情報を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

IPv6 パケットの統計情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show ipv6 traffic
tcp6:
        0 packets sent
                0 data packets (0 bytes)
                0 data packets (0 bytes) retransmitted
                0 ack-only packets (0 delayed)
                0 URG only packets
                0 window probe packets
                0 window update packets
                0 control packets
        0 packets received
                0 acks (for 0 bytes)
                0 duplicate acks
                0 acks for unsent data
                0 packets (0 bytes) received in-sequence
                0 completely duplicate packets (0 bytes)
                0 old duplicate packets
                0 packets with some dup. data (0 bytes duped)
                0 out-of-order packets (0 bytes)
                0 packets (0 bytes) of data after window
                0 window probes
                0 window update packets
                0 packets received after close
                0 discarded for bad checksums
                0 discarded for bad header offset fields
                0 discarded because packet too short
        0 connection requests
        0 connection accepts
        0 bad connection attempts
        0 connections established (including accepts)
        0 connections closed (including 0 drops)
        0 embryonic connections dropped
        0 segments updated rtt (of 0 attempts)
        0 retransmit timeouts
                0 connections dropped by rexmit timeout
        0 persist timeouts
        0 connections timed out in persist
        0 keepalive timeouts
                0 keepalive probes sent
                0 connections dropped by keepalive
        0 correct ACK header predictions
        0 correct data packet header predictions
        0 PCB cache misses
udp6:
        0 datagrams received
        0 with incomplete header
        0 with bad data length field
        0 with bad checksum
        0 with no checksum
        0 dropped due to no socket
        0 multicast datagrams dropped due to no socket
        0 dropped due to full socket buffers
        0 delivered
        0 datagrams output
```

(続く)

(続き)

```
ip6:
        24 total packets received
        0 with size smaller than minimum
        0 with data size < data length
        0 with bad options
        0 with incorrect version number
        0 fragments received
        0 fragments dropped (dup or out of space)
        0 fragments dropped after timeout
        0 fragments that exceeded limit
        0 packets reassembled ok
        24 packets for this host
        0 packets forwarded
        0 packets not forwardable
        0 redirects sent
        17 packets sent from this host
        0 packets sent with fabricated ip header
        0 output packets dropped due to no bufs, etc.
        0 output packets discarded due to no route
        0 output datagrams fragmented
        0 fragments created
        0 datagrams that can’t be fragmented
        0 packets that violated scope rules
        0 multicast packets which we don’t join
        Input histogram:
                ICMP6: 24
        Mbuf statistics:
                0 one mbuf
                24 one ext mbuf
                0 two or more ext mbuf
        0 packets whose headers are not continuous
        0 tunneling packets that can’t find gif
        0 packets discarded due to too many headers
        0 failures of source address selection
        source addresses on an outgoing I/F
                11 link-locals
        source addresses of same scope
                11 link-locals
        11 forward cache hit
        0 forward cache miss
icmp6:
        0 calls to icmp6_error
        0 errors not generated because old message was icmp6 error or so
        0 errors not generated because rate limitation
        Output histogram:
                echo: 5
                echo reply: 5
                multicast listener report: 1
                neighbor solicitation: 4
                neighbor advertisement: 2
        0 messages with bad code fields
        0 messages < minimum length
        0 bad checksums
        0 messages with bad length
        Input histogram:
                echo: 5
                echo reply: 15
                neighbor solicitation: 2
                neighbor advertisement: 2
        Histogram of error messages to be generated:
                0 no route
                0 administratively prohibited
                0 beyond scope
                0 address unreachable
                0 port unreachable
                0 packet too big
                0 time exceed transit
                0 time exceed reassembly
                0 erroneous header field
                0 unrecognized next header
                0 unrecognized option
                0 redirect
                0 unknown
        5 message responses generated
        0 messages with too many ND options
```

(続く)

(続き)

```
ipsec6:
        0 inbound packets processed successfully
        0 inbound packets violated process security policy
        0 inbound packets with no SA available
        0 invalid inbound packets
        0 discard inbound packets by interface down
        0 inbound packets failed due to insufficient memory
        0 inbound packets failed getting SPI
        0 inbound packets failed on AH replay check
        0 inbound packets failed on ESP replay check
        0 inbound packets considered authentic
        0 inbound packets failed on authentication
        0 inbound packets considered authentic(ESPinAuth)
        0 inbound packets failed on authentication(ESPinAuth)
        0 outbound packets processed successfully
        0 outbound packets violated process security policy
        0 outbound packets with no SA available
        0 invalid outbound packets
        0 outbound packets failed due to insufficient memory
        0 outbound packets with no route
        0 ipsec queue overflows
#
```

37.2.2 clear ipv6 traffic

[機能]

IPv6 パケットの統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear ipv6 traffic

[オプション]

なし

すべての IP 統計情報をクリアします。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

IPv6 パケットの統計情報をクリアします。

[実行例]

```
# clear ipv6 traffic
#
```

第 38 章　IP フィルタのカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

38.1 IPv4 フィルタのカウンタ・ログ・統計・状態などの表示、クリア操作

38.1.1 show ip filter

[機能]

IP フィルタテーブル表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip filter [interface <interface_name>] [all]

[オプション]

なし

すべてのインタフェースの IP フィルタテーブルを表示します。

interface <interface_name>

指定したインタフェースの IP フィルタテーブルを表示します。

all

時間切れの IP フィルタテーブルを含めて表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

IP フィルタテーブルを表示します。

[実行例]

以下に、実行例を示します。

```
# show ip filter
[lan0]---(1)
IPv4 filter
 default:spi---(2)

 static table:6---(3)
        action acl_count  dir
 [  0]    pass        1    in
 [  1]    pass       21   out
 [  2]  reject      500   rev
                    (5)   (14)
        action src IP/mask:port                                proto SYN  dir
               dst IP/mask:port                                 tos  type code
 [  3]    pass any                                                 6   Y   any
               any                                              any  any  any
 [  4]    pass any:21                                              6   N   any
               any:any                                          any  any  any
 [  5]    pass 10.0.0.0/8:5000                                    17   Y   out
  (4)     (15) (6)     (7)(8)                                  (12) (13) (14)
               192.168.1.0/24:6000                              any  any  any
               (9)       (10) (11)                              (16) (17) (18)


 dynamic table:1---(19)
       action src(dst) IP/mask:port                            proto SYN remain
              dst(src) IP/mask:port
 [  0]   pass 192.168.1.2/32:any                                  6   Y      30
              10.36.195.28/32:54063                                        (20)

 SPI table:1---(21)
       action src(dst) IP/mask:port    dst(src) IP/mask:port    proto SYN remain
 [  0]   pass 192.168.1.2/32:any                                  1   -      30
              10.36.195.28/32:any
```

1) インタフェース名
2) どの IP フィルタテーブルにも不一致時の動作
3) 静的フィルタテーブル数
4) フィルタ通番
5) ACL 番号
6) フィルタ送信元 IP アドレス
7) フィルタ送信元 IP アドレスマスク
8) フィルタ送信元ポート番号
9) フィルタ送信先 IP アドレス
10) フィルタ送信先 IP アドレスマスク
11) フィルタ送信先ポート番号
12) フィルタプロトコル番号
13) フィルタ TCP 接続要求を含むかどうか
14) パケットの入出力方向

any: 入力パケットと出力パケットの両方に対してフィルタ動作を行います。

in: 入力パケットに対してだけフィルタ動作を行います。

out: 出力パケットに対してだけフィルタ動作を行います。

rev: 入力パケットと出力パケットの両方に対してフィルタ動作を行います。
ただし、入力パケットについては、以下のものを逆転した条件でフィルタ動作をします。
・送信元 IP アドレス/マスクとあて先 IP アドレス/マスク
・送信元ポート番号とあて先ポート番号

15) フィルタ動作

16) TOS 値

17) ICMP TYPE

18) ICMP CODE

19) 動的フィルタテーブル数

20) フィルタテーブルタイマ [*10 秒]
オプションに all を指定した場合は時間切れのテーブルに関しては expire と表示します。

21) SPI フィルタテーブル数

38.1.2　show ip filter statistics

[機能]

IP フィルタの統計情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip filter statistics [interface <interface_name>]

[オプション]

なし

すべてのインタフェースの IP フィルタ統計情報を表示します。

interface <interface_name>

指定したインタフェースの統計情報を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

IP フィルタの統計情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show ip filter statistics
[lan0]---(1)
IPv4 filter
  packet                 in          out
  pass(static)          358---(2)      2---(3)
  pass(dynamic)           0---(4)      0---(5)
  pass(SPI)               1---(6)      1---(7)
  reject                  0---(8)      0---(9)
  total                 359---(10)     3---(11)

[all]
IPv4 filter
  lack of memory                       0---(12)
  SPI table limit over                 0---(13)
```

1) インタフェース名
2) 入力側で静的フィルタで透過したパケット数
3) 出力側で静的フィルタで透過したパケット数
4) 入力側で動的フィルタで透過したパケット数
5) 出力側で動的フィルタで透過したパケット数
6) 入力側で SPI フィルタで透過したパケット数
7) 出力側で SPI フィルタで透過したパケット数
8) 入力側で遮断したパケット数

9) 出力側で遮断したパケット数

10) 入力側で処理したパケット数

11) 出力側で処理したパケット数

12) メモリ不足で SPI フィルタテーブルを確保できなかった回数

13) テーブル数が最大値に達していて SPI フィルタテーブルを確保できなかった回数

38.1.3　show ip filter summary

[機能]

IP フィルタのフィルタテーブル数の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip filter summary [interface <interface_name>] [total] [all]

[オプション]

なし

すべてのインタフェースのフィルタテーブル数と装置全体のフィルタテーブル数を表示します。

interface <interface_name>

指定したインタフェースのフィルタテーブル数を表示します。

total

装置全体のフィルタテーブル数を表示します。

all

時間切れのフィルタテーブルを含めたフィルタテーブル数を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

IP フィルタのフィルタテーブル数を表示します。

[実行例]

以下に、実行例を示します。

```
# show ip filter summary
[lan0]---(1)
IPv4 filter
  static table                          1---(2)
  dynamic table                         0---(3)
  SPI table                             1---(4)

[all]
IPv4 filter
  static table                          1---(5)
  dynamic table                         0---(6)
  SPI table                             1---(7)
```

1) インタフェース名
2) 静的フィルタテーブル数
3) 動的フィルタテーブル数
4) SPI フィルタテーブル数
5) 装置全体の静的フィルタテーブル数

6) 装置全体の動的フィルタテーブル数

7) 装置全体の SPI フィルタテーブル数

38.1.4　clear ip filter statistics

[機能]

IP フィルタの統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear ip filter statistics

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

IP フィルタ統計情報をクリアします。

[実行例]

```
# clear ip filter statistics
#
```

38.2 IPv6 フィルタのカウンタ・ログ・統計・状態などの表示、クリア操作

38.2.1 show ipv6 filter

[機能]

IPv6 フィルタテーブル表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ipv6 filter [interface <interface_name>] [all]

[オプション]

なし

すべてのインタフェースの IP フィルタテーブルを表示します。

interface <interface_name>

指定したインタフェースの IP フィルタテーブルを表示します。

all

時間切れの IP フィルタテーブルを含めて表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

IPv6 フィルタテーブルを表示します。

[実行例]

以下に、実行例を示します。

```
# show ipv6 filter
[lan0]---(1)
IPv6 filter
 default:spi---(2)

 static table:6---(3)
        action acl_count  dir
 [  0]    pass        1    in
 [  1]    pass       21   out
 [  2]  reject      500   rev
                    (5)   (14)
        action src IP/prefixlen:port                          proto SYN  dir
               dst IP/prefixlen:port                           tos  type code
 [  3]    pass any:any                                            6   Y   out
               any:21                                          any  any  any
 [  4]    pass any:21                                             6   N    in
               any:any                                        0-10 any  any
 [  5]    pass 2001:200:1::/64:any                               58   Y   rev
  (4)     (15) (6)         (7) (8)                            (12) (13) (14)
               2001:200:2::/64:6000                           any  1-10   0
               (9)        (10) (11)                           (21) (16) (17)

 dynamic table:1---(18)
        action src IP/prefixlen:port                         proto SYN remain
               dst IP/prefixlen:port
 [  0]    pass 2001:200:1::88/128:49165                          6   Y     30
               2001:200:2::27/128:21512                                   (19)

 SPI table:1---(20)
        action src IP/prefixlen:port                         proto SYN remain
               dst IP/prefixlen:port
 [  0]    pass 2001:200:1::88/128:22                             1   -     30
               2001:200:2::27/128:12431
```

1) インタフェース名
2) どの IP フィルタテーブルにも不一致時の動作
3) 静的フィルタテーブル数
4) フィルタ通番
5) ACL 番号
6) フィルタ送信元 IP アドレス
7) フィルタ送信元 IP アドレスマスク
8) フィルタ送信元ポート番号
9) フィルタ送信先 IP アドレス
10) フィルタ送信先 IP アドレスマスク
11) フィルタ送信先ポート番号
12) フィルタプロトコル番号
13) フィルタ TCP 接続要求を含むかどうか
14) パケットの入出力方向

any: 入力パケットと出力パケットの両方に対してフィルタ動作を行います。

in: 入力パケットに対してだけフィルタ動作を行います。

out: 出力パケットに対してだけフィルタ動作を行います。

rev: 入力パケットと出力パケットの両方に対してフィルタ動作を行います。
ただし、入力パケットについては、以下のものを逆転した条件でフィルタ動作をします。
送信元 IP アドレス/マスクとあて先 IP アドレス/マスク
送信元ポート番号とあて先ポート番号

15) フィルタ動作

16) ICMP TYPE

17) ICMP CODE

18) 動的フィルタテーブル数

19) フィルタテーブルタイマ [*10 秒]
オプションに all を指定した場合は時間切れのテーブルに関しては expire と表示します。

20) SPI フィルタテーブル数

21) Traffic Class 値

38.2.2　show ipv6 filter statistics

[機能]

IPv6 フィルタの統計情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ipv6 filter statistics [interface <interface_name>]

[オプション]

なし

すべてのインタフェースの IP フィルタ統計情報を表示します。

interface <interface_name>

指定したインタフェースの統計情報を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

IP フィルタの統計情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show ipv6 filter statistics
[lan0]---(1)
IPv6 filter
  packet                 in          out
  pass(static)          358---(2)      2---(3)
  pass(dynamic)           0---(4)      0---(5)
  pass(SPI)               1---(6)      1---(7)
  reject                  0---(8)      0---(9)
  total                 359---(10)     3---(11)

[all]
IPv6 filter
  lack of memory                       0---(12)
  SPI table limit over                 0---(13)
```

1) インタフェース名
2) 入力側で静的フィルタで透過したパケット数
3) 出力側で静的フィルタで透過したパケット数
4) 入力側で動的フィルタで透過したパケット数
5) 出力側で動的フィルタで透過したパケット数
6) 入力側で SPI フィルタで透過したパケット数
7) 出力側で SPI フィルタで透過したパケット数
8) 入力側で遮断したパケット数

9) 出力側で遮断したパケット数

10) 入力側で処理したパケット数

11) 出力側で処理したパケット数

12) メモリ不足で SPI フィルタテーブルを確保できなかった回数

13) テーブル数が最大値に達していて SPI フィルタテーブルを確保できなかった回数

38.2.3　show ipv6 filter summary

[機能]

IPv6 フィルタのフィルタテーブル数の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ipv6 filter summary [interface <interface_name>] [total] [all]

[オプション]

なし

すべてのインタフェースのフィルタテーブル数と装置全体のフィルタテーブル数を表示します。

interface <interface_name>

指定したインタフェースの統計情報を表示します。

total

装置全体のフィルタテーブル数を表示します。

all

時間切れのフィルタテーブルを含めたフィルタテーブル数を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

IPv6 フィルタのフィルタテーブル数を表示します。

[実行例]

以下に、実行例を示します。

```
# show ipv6 filter summary
[lan0]---(1)
IPv6 filter
  static table                          1---(2)
  dynamic table                         0---(3)
  SPI table                             1---(4)

[all]
IPv6 filter
  static table                          1---(5)
  dynamic table                         0---(6)
  SPI table                             1---(7)
```

1) インタフェース名
2) 静的フィルタテーブル数
3) 動的フィルタテーブル数
4) SPI フィルタテーブル数
5) 装置全体の静的フィルタテーブル数

6) 装置全体の動的フィルタテーブル数

7) 装置全体の SPI フィルタテーブル数

38.2.4　clear ipv6 filter statistics

[機能]

IPv6 フィルタの統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear ipv6 filter statistics

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

IPv6 フィルタ統計情報をクリアします。

[実行例]

```
# clear ipv6 filter statistics
#
```

第 39 章　IDS のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

39.1　IPv4 IDS のカウンタ・ログ・統計・状態などの表示、クリア操作

39.1.1　show ip ids statistics

[機能]

IDS の統計情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip ids statistics [interface <interface_name>]

[オプション]

なし

すべてのインタフェースの IDS 統計情報を表示します。

interface <interface_name>

指定したインタフェースの統計情報を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

IDS の統計情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show ip ids statistics
[lan0]---(1)
IPv4 IDS
  event                              in
  Unknown IP protocol                 0 ---(2)
  Land attack                         0 ---(3)
  Short IP header                     0 ---(4)
  Malformed IP packet                 0 ---(5)
  IP option
  Malformed IP option                 0 ---(6)
  Security IP option                  0 ---(7)
  Loose routing IP option             0 ---(8)
  Record route IP option              0 ---(9)
  Stream ID IP option                 0 ---(10)
  Strict routing IP option            0 ---(11)
  Timestamp IP option                 0 ---(12)
  ICMP
  ICMP source quench                  0 ---(13)
  ICMP timestamp request              0 ---(14)
  ICMP timestamp reply                0 ---(15)
  ICMP information request            0 ---(16)
  ICMP information reply              0 ---(17)
  ICMP address mask request           0 ---(18)
  ICMP address mask reply             0 ---(19)
  UDP
  UDP short header                    0 ---(20)
  UDP bomb                            0 ---(21)
  TCP
  TCP no bits set                     0 ---(22)
  TCP SYN and FIN                     0 ---(23)
  TCP FIN and no ACK                  0 ---(24)
  FTP
  FTP improper port                   0 ---(25)
```

1) インタフェース名
2) Protocol フィールドが 134 以上のとき
3) 始点 IP アドレスと終点 IP アドレスが同じとき
4) Ip ヘッダの長さが length フィールドの長さよりも長いとき
5) length フィールドと実際のパケットの長さが違うとき
6) オプションヘッダの解析を行うとオプションヘッダの領域に過剰または不足があった場合。
7) Security and handling restriction header を受信したとき
8) Loose source routing header を受信したとき
9) Record route header を受信したとき
10) Stream identifier header を受信したとき
11) Strict source routing header を受信したとき
12) Internet timestamp header を受信したとき
13) source quench を受信したとき
14) timestamp request を受信したとき
15) timestamp reply を受信したとき
16) information request を受信したとき
17) information reply を受信したとき
18) address mask request を受信したとき
19) address mask reply を受信したとき
20) UDP の length フィールドの値が 8 よりも小さいとき

21) UDP ヘッダの length フィールドの値が小さ過ぎる時
22) フラグに何もセットされていないとき
23) SYN と FIN が同時にセットされているとき
24) ACK のない FIN を受信したとき
25) PORT や PASV コマンドで指定されるポート番号が 1024～65535 の範囲でないとき

39.1.2 clear ip ids statistics

[機能]

IDS の統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear ip ids statistics

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

IDS 統計情報をクリアします。

[実行例]

```
# clear ip ids statistics
#
```

第 40 章　NAT のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

40.1 NAT のカウンタ・ログ・統計・状態などの表示

40.1.1 show ip nat interface

[機能]

NAT 変換テーブルの表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip nat [interface <interface_name>] [all]

[オプション]

なし

すべてのインタフェースの NAT 変換テーブルを表示します。

interface <interface_name>

指定したインタフェースの NAT 変換テーブルを表示します。

all

時間切れの NAT 変換テーブルを含めて表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

NAT 変換テーブルの情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show ip nat
[rmt0]  ---(1)
ap 0: ap-001
-(2)- -(3)--
dynamic NAT table queue
table:3   ---(4)
index  GlobalAddr/Port       PrivateAddr/Port      DestAddr/Port         remain
       GlobalAddr:Icmp_Id    PrivateAddr:Icmp_Id   DestAddr
[   0] 10.36.195.136/10031   192.168.1.2/1055      10.36.195.1/80             2
-(5)-- ------(6)------ -(7)- ----(8)---- -(9)-     -----(10)----- -(11)-  -(12)-
[   1] 10.36.195.136/10030   192.168.1.2/1054      10.36.195.1/80             2
[   2] 10.36.195.136/10029   192.168.1.2/1053      10.36.195.1/80             2

application table queue
table:1
index  GlobalAddr/Port       PrivateAddr/Port      DestAddr/Port         remain
[   0] 10.36.195.136/10010   192.168.1.2/1034      10.36.195.28/49167        30

static NAT table queue
table:3
index  GlobalAddr/Port       PrivateAddr/Port      DestAddr/Port         remain
       GlobalAddr:Icmp_Id    PrivateAddr:Icmp_Id   DestAddr
[   0] 10.36.195.255/0       10.36.195.255/0       0.0.0.0/0                  0
[   1] 10.36.195.0/0         10.36.195.0/0         0.0.0.0/0                  0
[   2] 10.36.195.136:0       10.36.195.136:0       0.0.0.0                    0

address table queue
table:1
index  GlobalAddr            PrivateAddr           DestAddr              remain
[   0] 10.36.195.136         192.168.1.2           0.0.0.0                   30
```

1) インタフェース名
2) 接続先定義番号
3) 接続先名
4) 変換テーブル数
5) 変換テーブル通番
6) グローバル IP アドレス
7) グローバルポート番号、またはグローバル ICMP_ID
8) プライベート IP アドレス
9) プライベートポート番号、またはプライベート ICMP_ID
10) 相手側 IP アドレス
11) 相手側ポート番号
12) テーブル解放残時間 [*10 秒]
    オプションに all を指定した場合は時間切れのテーブルに関しては expire と表示します。

40.1.2 show ip nat statistics

[機能]

NAT の統計情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip nat statistics

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

NAT の統計情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show ip nat statistics
            to Global   to Private
translate         85 ---(1)    63 ---(2)
error              0 ---(3)     0 ---(4)

             fragment
translate          0 ---(5)
error              0 ---(6)

              current         peak
nat table         12 ---(7)    12 ---(8)

error accounting
  lack of memory                0 ---(9)
  table not found               0 ---(10)
  too small packet              0 ---(11)
  other reason                  0 ---(12)
```

1) プライベート→グローバル変換回数
2) グローバル→プライベート変換回数
3) プライベート→グローバルエラー発生回数
4) グローバル→プライベートエラー発生回数
5) フラグメントパケットの正常変換回数
6) フラグメントパケットのエラー発生回数
7) 現在使用中の NAT 変換テーブル個数
8) NAT 変換テーブルのピークホールド個数 (NAT モジュールで確保した NAT 変換テーブル個数)
9) メモリ枯渇回数

10) 変換テーブルにないパケットの受信回数

11) 異常に短いパケットの受信回数

12) その他のエラー回数

40.1.3 show ip nat summary

[機能]

NAT 変換テーブル数の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip nat summary [interface <interface_name>] [all]

[オプション]

なし

すべてのインタフェースの NAT 変換テーブル数を表示します。

interface <interface_name>

指定したインタフェースの NAT 変換テーブル数を表示します。

all

時間切れの NAT 変換テーブル数を含めて表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

NAT 変換テーブル数を表示します。

[実行例]

以下に、実行例を示します。

```
# show ip nat summary
[rmt0]  ---(1)
ap 0: ap-001
-(2)- -(3)--
dynamic NAT table queue
table:3   ---(4)
application table queue
table:1
static NAT table queue
table:3
address table queue
table:1
```

1) インタフェース名
2) 接続先定義番号
3) 接続先名
4) 変換テーブル数

40.2　NAT のカウンタ・ログ・統計などのクリア

40.2.1　clear ip nat statistics

[機能]

NAT の統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear ip nat statistics

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

NAT 統計情報をクリアします。

[実行例]

```
# clear ip nat statistics
#
```

第 41 章　マルチキャストのカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

41.1　マルチキャストのカウンタ・ログ・統計・状態などの表示

41.1.1　show ip multicast group

[機能]

マルチキャストグループ情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip multicast group [interface <interface_name>] [group <group_address>]

[オプション]

なし

マルチキャストグループの情報を表示します。

interface <interface_name>

指定されたインタフェースのマルチキャストグループの情報を表示します。

group <group_address>

指定されたグループアドレスのマルチキャストグループの情報を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

マルチキャスト経路共通管理部が保持しているマルチキャストグループの情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show ip multicast group

Interface Querier           Uptime        QTimer Expire Flags
lan0      me                0000.00:00:00     45      0 QUERIER
----      -------           ------------- ------ ------ -------
 (1)        (2)                 (3)        (4)    (5)    (6)
     Group             Reporter          Uptime
     239.255.255.10    192.168.1.100     0000.00:03:27
     239.255.255.11    192.168.1.100     0000.00:01:24
     --------------    -------------     -------------
           (7)              (8)               (9)
Interface Querier           Uptime        QTimer Expire Flags
lan1      192.168.2.2       0000.00:01:23     55    160
     Group             Reporter          Uptime
     239.255.255.12    192.168.2.100     0000.00:00:21

Total Multicast Groups: 3   ---(10)

#
```

1)　インタフェース名

2)　IGMP General Query の送信者 (自分自身の場合は me と表示)

3) IGMP Query を受け取ってからの経過時間 (自身が Querier の場合は常に 0)

4) IGMP General Query 発行用のタイマ

5) Other Querier Present Interval のタイムアウトまでの時間

6) フラグ情報

フラグの内容を以下に説明します。

QUERIER

IGMP Querier である

7) グループアドレス

224.0.0.0/24 のグループはローカル・ネットワーク用に予約されているため、マルチキャスト・パケット転送の対象外になります。

8) IGMP Membership Report の送信者

9) IGMP Membership Report を受信してからの経過時間

10) IGMP で管理されているグループの総数

41.1.2　show ip multicast interface

[機能]

マルチキャストインタフェース情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip multicast interface [interface <interface_name>]

[オプション]

なし

マルチキャストインタフェース情報を表示します。

interface <interface_name>

指定されたインタフェースの情報を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

マルチキャスト経路共通管理部が保持しているマルチキャストインタフェース情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show ip multicast interface

Interface Thresh Address           Subnet           Flags       Neighbors
lan0           1 192.168.1.1       192.168.1        PIM         192.168.1.2
                                                                192.168.1.5
                                                                192.168.1.10
lan1           1 192.168.2.1       192.168.2        DR NO-NBR
lan2           1 192.168.10.1      192.168.10       DR NO-NBR
register       1 192.168.1.1
--------  ------ -------------     ----------       ---------   ------------
   (1)      (2)       (3)             (4)              (5)           (6)
Total Interfaces: 3   ---(7)
Total Neighbors: 3   ---(8)

#
```

インタフェース情報

1) インタフェース名

   PIM-SM では、PIM Register パケットの送受信を行うためのインタフェースとして、仮想的に register インタフェースを作成します。

2) TTL しきい値

3) インタフェースの IP アドレス

4) インタフェースのサブネットワークアドレス

5) フラグ情報

フラグの内容を以下に説明します。

DISABLED
非動作状態

DOWN インタフェースダウン

DR 代表ルータ (DR:Designated Router) として動作

PIM PIM プロトコルが動作中

P2P Point-to-Point インタフェース

NO-NBR 隣接ルータが存在しない

6) 隣接ルータ

7) インタフェースの総数

8) 隣接ルータの総数

41.1.3　show ip multicast interface statistics

[機能]

マルチキャストインタフェースの統計情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip multicast interface statistics [interface <interface_name>]

[オプション]

なし

マルチキャストインタフェースの統計情報を表示します。

interface <interface_name>

指定されたインタフェースの統計情報を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

マルチキャストインタフェースの統計情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show ip multicast interface statistics

Interface  Incoming  Outgoing
lan0             23         0
lan1              0        23
register          0         0
--------   --------  --------
   (1)        (2)       (3)
Total Interfaces: 3   ---(4)

#
```

インタフェース情報

1) インタフェース名

   PIM-SM では、PIM Register パケットの送受信を行うためのインタフェースとして、仮想的に register インタフェースを作成します。

2) 入力パケット数

3) 出力パケット数

4) インタフェースの総数

41.1.4 show ip multicast pimsm rp

[機能]

PIM-SM のランデブーポイント情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip multicast pimsm rp [address <ip_address>]

[オプション]

なし

PIM-SM のランデブーポイント情報を表示します。

address <ip_address>

指定された IP アドレスのランデブーポイントの情報を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

マルチキャスト経路共通管理部が保持している PIM-SM のランデブーポイント情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show ip multicast pimsm rp

Current BSR address: 192.168.1.1   ---(1)
RP-address      Incoming   Group prefix   Priority   Holdtime
192.168.1.1     lan0       224/4                 0         95
192.168.10.1    lan3       224.255/16            0         20
------------    --------   ------------   --------   --------
    (2)            (3)          (4)          (5)        (6)
Total RPs: 2   ---(7)

#
```

1) BSR アドレス
2) RP アドレス
3) 入力インタフェース
4) マルチキャスト・グループ
5) プライオリティ
6) 生存時間
7) RP の総数

41.1.5　show ip multicast protocol

[機能]

マルチキャストプロトコル情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip multicast protocol

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

動作中のマルチキャストプロトコルの情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show ip multicast protocol
PIM-SM   ---(1)

#
```

1)　動作中のマルチキャスト・ルーティングプロトコルです。

not running
マルチキャストが動作していません。

PIM-DM　PIM-DM が動作中です。

PIM-SM　PIM-SM が動作中です。

41.1.6 show ip multicast route

[機能]

マルチキャストルーティングテーブル情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip multicast route [source <ip_address>] [group <group_address>]

[オプション]

なし

マルチキャストルーティングテーブルの情報を表示します。

source <ip_address>

指定された送信元アドレスのマルチキャストルーティングテーブルの情報を表示します。any を指定すると、アドレスは不定 ((*,G) エントリの場合) となります。

group <group_address>

指定されたグループアドレスのマルチキャストルーティングテーブルの情報を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

マルチキャスト経路共通管理部が保持している
マルチキャストルーティングテーブルの情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show ip multicast route

Source          Group           RP-addr         Flags
any             239.255.20.1    192.168.2.1     WC
-----------     ------------    -----------     --
    (1)               (2)             (3)        (4)
    Incoming     : lan0            ---(5)
    Upstream     : 192.168.1.1     ---(6)
    Preference   : 0 (0x00000000)  ---(7)
    Metric       : 0 (0x00000000)  ---(8)
    Entry Timer  :    200    ---(9)
    J/P Timer    :     30    ---(10)
    RegSup Timer :      0    ---(11)
    Assert Timer :      0    ---(12)
    Interface Join Prune Leave Assert Out JoinTimer PruneTimer
    lan0       OFF   OFF   OFF    OFF OFF         0          0
    lan1       OFF   OFF    ON    OFF  ON         0          0
    lan2       OFF   OFF   OFF    OFF OFF         0          0
    register   OFF   OFF   OFF    OFF OFF         0          0
    --------  ---- ----- ----- ------ ---      ----       ----
      (13)    (14)  (15)  (16)  (17)  (18)     (19)       (20)

Total Groups: 1                 ---(21)
Total Cache MIRRORs: 1          ---(22)
Total Multicast Routing Tables: 1   ---(23)

#
```

1) マルチキャスト・パケットの送信元アドレス
   不定の場合 ((*,G) エントリの場合) には any となります。
2) マルチキャスト・グループ
3) RP アドレス (PIM-SM の場合のみ)
4) フラグ情報
   フラグの内容を以下に説明します。

   SPT　SPT への経路 (PIM-SM の場合のみ)
   SPT フラグが立つのは、RP 経由のツリーと SPT の分岐点となるルータです。分岐点が最終ホップのルータよりも上流にある場合は、最終ホップのルータは SPT への切り替えが行われたことを知る手段がないため、SPT フラグは立ちません。

   WC　ワイルド・カードを含むエントリ

   RP　RP への経路 (PIM-SM の場合のみ)

   CACHE　カーネルにルーティングテーブルが登録されている

   ASSERTED
   Assert タイマが動作している
   冗長なネットワーク構成により複数の転送経路が存在する場合は、PIM Assert メッセージにより片側の経路が刈り取られます。この際、転送経路が変わる場合があるため、下流のルータは上流側のネットワーク上で発生した PIM Assert を追随してアップストリーム・ルータを切り替え、Assert タイマを動作させます。Assert タイマの満了時には、アップストリーム・ルータを再び基に戻します。

   SG　(S,G) エントリ (PIM-SM の場合のみ)

5) 入力インタフェース
6) アップストリーム・ルータ
   上流側のパケットの転送者となっているルータです。
7) プリファレンス値
8) メトリック値

9) ルーティングテーブルの生存時間

10) Join/Prune タイマ (PIM-SM の場合のみ)

11) Register-Suppression タイマ (PIM-SM の場合のみ)

12) Assert タイマ

13) インタフェース名

PIM-SM では、PIM Register パケットの送受信を行うためのインタフェースとして、仮想的に register インタフェースを作成します。

14) インタフェース情報 (Join 状態フラグ)

15) インタフェース情報 (Prune 状態フラグ)

16) インタフェース情報 (グループ参加者の存在フラグ)

17) インタフェース情報 (Assert 状態フラグ)

18) 出力先インタフェース

19) Join タイマ (PIM-SM の場合のみ)

20) Prune タイマ (PIM-DM の場合のみ)

21) マルチキャスト・ルーティングを行っているグループの総数

(*,G) または (S,G) エントリが存在しているグループの総数です。

22) CACHE フラグが立っているマルチキャスト・ルーティングテーブルの総数

23) ルーティングテーブルの総数

(*,G)、(S,G) エントリの総数です。

41.1.7　show ip multicast route kernel

[機能]

IP カーネルのマルチキャストルーティングテーブルの表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip multicast route kernel [source <ip_address>] [group <group_address>]
show ip multicast route kernel summary

[オプション]

なし

IP カーネルのマルチキャストルーティングテーブルの情報を表示します。

source <ip_address>

指定された送信元アドレスのマルチキャストルーティングテーブルの情報を表示します。

group <group_address>

指定されたグループアドレスのマルチキャストルーティングテーブルの情報を表示します。

summary

IP カーネルのマルチキャストルーティングテーブルのエントリ数を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

IP カーネルのマルチキャストルーティングテーブルの、現在の状態を表示します。

[実行例]

以下に、実行例を示します。
実行例 (ルーティングテーブル情報表示の場合)

```
# show ip multicast route kernel

Source          Group           Incoming  Outgoings
192.168.2.2     239.255.30.1    lan0      lan1 lan2 lan3 lan4 lan10 rmt0
                                          rmt1 rmt2 rmt3 rmt998 rmt999
192.168.2.2     239.255.30.2    lan0      lan1 lan2
192.168.2.2     239.255.30.3    lan1      lan2
------------    ------------    --------  -------------------
     (1)             (2)            (3)           (4)

Total Multicast Routing Tables: 3   --- (5)

#
```

1)　マルチキャスト・パケットの送信元のアドレス

2)　マルチキャスト・グループ

3) 入力インタフェース

マルチキャスト・ルーティングテーブルは、マルチキャスト・パケットの到達時に一時的に作成されます。この際、入力インタフェースは空欄となっています。

その後、マルチキャスト・ルーティングテーブルは入力インタフェースと出力インタフェースの決定後に有効になり、マルチキャスト・パケットの転送に利用されますが、転送に利用されない場合は、そのまま削除されます。

4) 出力インタフェースの一覧

出力インタフェースが多数存在する場合は、適当な位置で折り返して表示します。

5) マルチキャスト・ルーティングテーブルの総数

実行例 (ルーティングテーブル数表示の場合)

```
# show ip multicast route kernel summary
    Entry:3    --- (6)

#
```

6) マルチキャスト・ルーティングテーブルの総数

41.1.8　show ip multicast route kernel statistics

[機能]

IP カーネルのマルチキャストルーティングテーブルの統計情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip multicast route kernel statistics [source <ip_address>] [group <group_address>]

[オプション]

なし

IP カーネルのマルチキャストルーティングテーブルの統計情報を表示します。

source <ip_address>

指定された送信元アドレスのマルチキャストルーティングテーブルの統計情報を表示します。

group <group_address>

指定されたグループアドレスのマルチキャストルーティングテーブルの統計情報を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

IP カーネルのマルチキャストルーティングテーブルの、統計情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show ip multicast route kernel statistics

Source          Group             Packets
192.168.2.2     239.255.30.1            7
192.168.2.2     239.255.30.2            5
192.168.2.2     239.255.30.3            3
------------    ------------      -------
     (1)             (2)             (3)

Total Multicast Routing Tables  3   --- (4)

#
```

1) マルチキャスト・パケットの送信元のアドレス
2) マルチキャスト・グループ
3) パケット数
4) マルチキャスト・ルーティングテーブルの総数

41.1.9 show ip multicast statistics

[機能]

マルチキャストパケットの統計情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip multicast statistics

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

マルチキャストパケットの統計情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show ip multicast statistics
multicast forwarding: ---(1)
          0 multicast forwarding cache lookups
          0 multicast forwarding cache misses
          0 upcalls to multicast daemon
          0 upcall queue overflows
          0 upcalls dropped due to full socket buffer
          0 cache cleanups
          0 datagrams with no route for origin
          0 datagrams arrived with bad tunneling
          0 datagrams could not be tunneled
          0 datagrams arrived on wrong interface
          0 datagrams selectively dropped
          0 datagrams dropped due to queue overflow
          0 datagrams dropped for being too large
```

1) マルチキャスト・ルーティングテーブル統計情報

41.2　マルチキャストのカウンタ・ログ・統計などのクリア

41.2.1　clear ip multicast interface statistics

[機能]

マルチキャストインタフェースの統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear ip multicast interface statistics

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

マルチキャストインタフェースの統計情報をクリアします。

[実行例]

以下に、実行例を示します。

```
# clear ip multicast interface statistics
#
```

41.2.2 clear ip multicast route kernel statistics

[機能]

IP カーネルのマルチキャストルーティングテーブルの統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear ip multicast route kernel statistics

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

IP カーネルのマルチキャストルーティングテーブルの統計情報をクリアします。

[実行例]

以下に、実行例を示します。

```
# clear ip multicast route kernel statistics
#
```

41.2.3　clear ip multicast statistics

[機能]

マルチキャストパケットの統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear ip multicast statistics

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

マルチキャストパケットの統計情報をクリアします。

[実行例]

以下に、実行例を示します。

```
# clear ip multicast statistics
#
```

第 42 章　DHCP のカウンタ・ログ・統計・状態などの表示コマンド

42.1　IPv4 DHCP のカウンタ・ログ・統計・状態などの表示

42.1.1　show ip dhcp

[機能]

IPv4 DHCP 運用状況の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ip dhcp [interface <interface_name>]

[オプション]

なし

すべてのインタフェースの DHCP 運用状況を表示します。

interface <interface_name>

指定したインタフェースについての DHCP 運用状況を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

DHCP の以下の機能の運用状況を表示します。

IPv4 DHCP サーバの運用状況表示

リース可能アドレスレンジ、リース中のアドレスとリース先情報およびリース期間を表示します。

IPv4 DHCP リレーエージェントの運用状況表示

中継先 DHCP サーバアドレスを表示します。

IPv4 DHCP クライアントの運用状況表示

クライアント状態、リース開始時刻／終了時刻、サーバから獲得したオプション情報を表示します。
また、指定されたインタフェースで IPv4 DHCP サーバ、リレーエージェント、クライアントのどれも動作していない場合は何も表示されません。
また、インタフェースの指定がない場合は、すべてのインタフェースの DHCP 情報が表示されます。

[実行例]

以下に、実行例を示します。

IPv4 DHCP サーバの場合

```
# show ip dhcp interface lan0

[lan0] IPv4 DHCP Server Informations

Lease IP Address          : 192.168.1.2  [Range: 253] --- (1)
Subnet Mask               : 255.255.255.0 --- (2)
Default Router Address    : 192.168.1.1 --- (3)
TIME Server Address       : 192.168.1.1 --- (4)
NTP Server Address        : 192.168.1.1 --- (5)
DNS Server Address        : 192.168.1.1 --- (6)
Domain Name               : fujitsu.com --- (7)
Lease Time                : 0001.00:00:00 --- (8)

Active Client List:
No. IP address          MAC address       Lease remain
--- ----------          -----------       ------------
(9) (10)                (11)              (12)
001 192.168.1.2         00:00:00:00:00:00 0000.23:59:00
002 192.168.1.3         00:00:00:00:00:00 0000.23:59:00
003 192.168.1.4         00:00:00:00:00:00 0000.23:59:00
004 192.168.1.5         00:00:00:00:00:00 0000.23:59:00
005 192.168.1.6         00:00:00:00:00:00 0000.23:59:00
:

#
```

1) 配布 IP アドレス先頭 [配布アドレス数]
2) 配布サブネットマスク
3) 配布デフォルトルータアドレス
4) 配布タイムサーバアドレス
5) 配布 NTP サーバアドレス
6) 配布 DNS サーバアドレス
7) 配布ドメイン名
8) リース時間
9) 通番
10) IP アドレス
11) MAC アドレス
12) 残りリース時間

IPv4 DHCP リレーエージェントの場合

```
# show ip dhcp

[lan0] IPv4 DHCP Relay Agent Information

Forwarding DHCP Server: 192.168.3.1 --- (1)

#
```

1) DHCP サーバアドレス

IPv4 DHCP クライアントの場合

```
# show ip dhcp

[lan0] IPv4 DHCP Client Informations

Leased IP Address         : 192.168.1.2 --- (1)
Subnet Mask               : 255.255.255.0 --- (2)
Default Router Address    : 192.168.1.1 --- (3)
DHCP Server Address       : 192.168.1.1 --- (4)
TIME Server Address       : 192.168.1.X --- (5)
NTP Server Address        : 192.168.1.X --- (6)
DNS Server Address        : 192.168.1.1 --- (7)
Domain Name               : fujitsu.com --- (8)
Lease Time                : 0001.00:00:00 --- (9)
Renewal Time              : 0000.12:00:00 --- (10)
Rebinding Time            : 0000.18:00:00 --- (11)
Lease Expire              : Tue Dec  1 14:00:13 1998 --- (12)
Client Status             : BOUND --- (13)

#
```

1) 獲得 IP アドレス
2) 獲得サブネットマスク
3) 獲得デフォルトルータアドレス
4) 獲得 DHCP サーバアドレス
5) 獲得タイムサーバアドレス
6) 獲得 NTP サーバアドレス
7) 獲得 DNS サーバアドレス
8) 獲得ドメイン名
9) リース時間
10) リース更新時間 (T1)
11) リース更新時間 (T2)
12) リース有効期限
13) DHCP クライアント状態

42.2 IPv6 DHCP のカウンタ・ログ・統計・状態などの表示

42.2.1 show ipv6 dhcp

[機能]

IPv6 DHCP 運用状況の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ipv6 dhcp [interface <interface_name>]

[オプション]

なし

すべてのインタフェースの IPv6 DHCP 運用状況を表示します。

interface <interface_name>

指定したインタフェースについての DHCP 運用状況を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

DHCP の以下の機能の運用状況を表示します。

IPv6 DHCP サーバの運用状況表示

配布プレフィックス情報、リース中のプレフィックス情報とリース先情報およびリース期間を表示します。

IPv6 DHCP クライアント の運用状況表示

IPv6 DHCP クライアント状態、リース開始時刻／終了時刻、サーバから獲得したオプション情報を表示します。

また、指定されたインタフェースで IPv6 DHCP サーバ、クライアントのどちらも動作していない場合は何も表示されません。
また、インタフェースの指定がない場合は、すべてのインタフェースの DHCP 情報が表示されます。

[実行例]

以下に、実行例を示します。

IPv6 DHCP サーバの場合

```
# show ipv6 dhcp

[rmt0] IPv6 DHCP Server Informations

Server DUID               : 0003 0001 0200 0eff fe58 a00b       .. .. .. .. .X .. ---(1)
Server Preference         : 0 ---(2)
DNS Server Address        : 2001:db8::1 ---(3)
                            2001:db8::3 ---(4)
Active Client
-------------------------------------------------------------------------------
Client DUID             : ffff                                  .. ---(5)
IAID                    : 2 ---(6)
Prefix/Prefixlen        : 2001:db8::/48 ---(7)
Preferred Lifetime      : infinity ---(8)
Valid Lifetime          : infinity ---(9)
Delegated Time          : Wed May 26 09:56:28 2004 ---(10)
Lease remain            : infinity ---(11)
#
```

1) サーバ DUID
2) サーバプリファレンス値
3) 配布 DNS サーバアドレス
4) 配布セカンダリ DNS サーバアドレス
5) クライアント DUID
6) IAID
7) 配布プレフィックス
8) Preferred Lifetime
9) Valid Lifetime
10) 配布時間
11) リース有効期限

IPv6 DHCP クライアントの場合

```
# show ipv6 dhcp
[rmt0] IPv6 DHCP Client Informations

Client Status             : ACTIVE ---(1)
IAID                      : 2 ---(2)
Client DUID               : ffff                                .. ---(3)
Server DUID               : 0003 0001 0200 0eff fe58 a00b       .. .. .. .. .X .. ---(4)
Server Preference         : 0 ---(5)
DNS Server Address        : 2001:db8::1 ---(6)
                            2001:db8::3 ---(7)
Delegated Time            : Wed May 26 09:56:28 2004 ---(8)
Uptime                    : 0000.00:00:41 ---(9)
T1 (Renewal Time)         : infinity ---(10)
T2 (Rebind Time)          : infinity ---(11)
Preferred Lifetime        : infinity ---(12)
Valid Lifetime            : infinity ---(13)
Prefix/Prefixlen          : 2001:db8::/48 ---(14)

Assign Interface List
-------------------------------------------------------------------------------
I/F Name                  Prefix/Prefixlen
rmt1                      2001:db8:0:1::/64 ---(15)
rmt2                      2001:db8:0:2::/64
rmt3                      2001:db8:0:2::/64
#
```

1) クライアント状態
2) IAID
3) クライアント DUID

4) サーバ DUID
5) サーバプリファレンス値
6) 獲得 DNS サーバアドレス
7) 獲得セカンダリ DNS サーバアドレス
8) 獲得時間
9) 経過時間
10) T1 時間
11) T2 時間
12) Preferred Lifetime
13) Valid Lifetime
14) 獲得プレフィックス
15) 割り当てプレフィックス情報

第 43 章　動的 VPN の状態などの表示、情報の削除コマンド

43.1 動的 VPN の情報交換クライアントの状態などの表示

43.1.1 show dvpn client user

[機能]

動的 VPN の情報交換クライアントユーザ情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show dvpn client user
show dvpn client user summary

[オプション]

なし

すべてのユーザ情報を表示します。

summary

ユーザ合計数を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

動的 VPN の情報交換クライアントユーザ情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show dvpn client user
No.(1)  Status(2) User ID (3)
  Pri(4)Trs(5)    Server (6)
              (7) Elapsed Time   Expire (8)
------  ---------------------------------------------------------------------
[0001]  IDLE      IPsecIKE)20010db8000000000000000000000000/64@fujitsu.com
    1   UDP       [2001:db8::1]:5060
                  0000.00:00:45  3600
[0002]  REGISTER  IPsecIKE)c0a80100/24@fujitsu.com
    2   UDP       192.168.1.1:5061
                  0000.00:00:45  3600
[0003]  REGISTER  TOKYO@fujitsu.com
    1   UDP       dvpnserver.fujitsu.com:5061
                  0000.00:00:00  3600

Total Users      3  (9)
#

# show dvpn client user summary
Total Users      3
#
```

1) No.

ユーザの番号が表示されます。

2) Status

ユーザの登録状態が表示されます。

INIT　：初期化中

REGISTER

：登録中

IDLE　：登録済

UPDATE

：更新中

DELETE

：削除中

3) User ID

ユーザ ID が表示されます。

4) Pri

プライオリティが表示されます。

5) Trs

トランスポート種別が表示されます。

UDP　：UDP で通信

6) Server

ユーザを登録したサーバ、ポート番号を表示します。

7) Elapsed Time

ユーザをサーバに登録してからの経過時間が表示されます。

8) Expire

ユーザの有効時間が秒単位で表示されます。

9) Total Users

ユーザの合計数が表示されます。

43.1.2 show dvpn client session

[機能]

動的 VPN の情報交換クライアントのセッション情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show dvpn client session
show dvpn client session summary

[オプション]

なし

すべてのセッション情報を表示します。

summary

セッション合計数を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

動的 VPN の情報交換クライアントのセッション情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show dvpn client session
No.(1)  Status (2)    Elapsed Time   Expire (4)
        User Agent Client (5) (3)
        User Agent Server (6)
------  ------------------------------------------------------------
[0001]  CONNECTED     0000.00:00:30  300
       *IPsecIKE)20010db8000000000000000000000000/64@fujitsu.com
        IPsecIKE)20010db8000000001000000000000000/64@fujitsu.com
[0002]  INVITE        0000.00:00:00    0
        TOKYO@fujitsu.com
       *KAWASAKI@fujitsu.com
[0003]  CONNECTED     0000.00:00:45  300
       *IPsecIKE)c0a80100/24@fujitsu.com
        IPsecIKE)c0a80200/24@fujitsu.com

Total Sessions      2   (7)
#

# show dvpn client session summary
Total Sessions      2
#
```

1) No.

セッションの番号が表示されます。

2) Status

セッションの状態が表示されます。

INVITE　：INVITE 転送中

re-INVITE

：re-INVITE 転送中

INVITE_RECV

：INVITE 受信中

RESPONSE

：RESPONSE 転送中

ACK　：ACK 転送中

CANCEL

：CANCEL 転送中

BYE　：BYE 転送中

CONNECTED

：接続中

RECONNECT

：再接続中

3) Elapsed Time
セッションの経過時間が表示されます。

4) Expire
セッションの有効時間が秒単位で表示されます。

5) User Agent Client
セッションの発呼側ユーザ ID が表示されます。
本装置のユーザの場合は、ユーザ ID の前に*が表示されます。

6) User Agent Server
セッションの着呼側ユーザ ID かが表示されます。
本装置のユーザの場合は、ユーザ ID の前に*が表示されます。

7) Total Sessions
セッションの合計数が表示されます。

43.2　動的 VPN サーバの状態などの表示

43.2.1　show dvpn server

[機能]

動的 VPN サーバ情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show dvpn server

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

動的 VPN サーバ情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show dvpn server
Domain Name    : fujitsu.com     (1)
Status         : ACTIVE          (2)
Authenticate   : ON              (3)
Total Users    : 2               (4)
Total Sessions : 1               (5)

#
```

1) Domain Name
管理するドメイン名が表示されます。

2) Status

ACTIVE　: 動作中

INACTIVE
: 停止中

3) Authenticate
認証使用状況が表示されます。

ON　: 認証を行います

OFF　: 認証を行いません

4) Total Users
登録されているユーザの合計数が表示されます。

5) Total Sessions

セッションの合計数が表示されます。

43.2.2 show dvpn server user

[機能]

動的 VPN サーバに登録されているユーザ情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show dvpn server user
show dvpn server user summary

[オプション]

なし

すべてのユーザ情報を表示します。

summary

ユーザ合計数を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

動的 VPN サーバに登録されているユーザ情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show dvpn server user
No.(1)  User Name (2)                                                  (7)
  Pri(3)Trs Contact (4) (5)                            (6) Elapsed Time   Expire
------  ---------------------------------------------------------------------
[0001]  IPsecIKE)20010db8000000000000000000000000/64
    1   UDP [2001:db8::1]:5061 0000.00:00:45  3600
    2   UDP [2001:db8::2]:5061 0000.00:00:30  3600
[0002]  IPsecIKE)c0a80100/24
    1   UDP 192.168.1.1:5060                              0000.00:00:45  3600
    2   UDP 192.168.1.2:5060                              0000.00:00:30  3600
[0003]  TOKYO
    2   UDP [2001:db8::3]:5060 0000.00:00:45  3600

Total Users      3  (8)
#

# show dvpn server user summary
Total Users      3
#
```

1) No.

ユーザの番号が表示されます。

2) User Name

登録されているユーザ名が表示されます。

3) Pri
登録されているプライオリティを表示します。

4) Trs
登録されているトランスポート種別を表示します。

UDP　　：UDP で通信

5) Contact
登録されているユーザの Contact アドレス、ポート番号を表示します。

6) Elapsed Time
ユーザを登録してからの経過時間が表示されます。

7) Expire
ユーザの登録有効時間が秒単位で表示されます。

8) Total Users
ユーザの合計数が表示されます。

43.2.3 show dvpn server session

[機能]

動的 VPN サーバのセッション情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show dvpn server session
show dvpn server session summary

[オプション]

なし

すべてのセッション情報を表示します。

summary

セッション合計数を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

動的 VPN サーバ機能が管理しているセッション情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show dvpn server session
No.(1)  Status (2)    Elapsed Time   Expire (4)
  Pri(5)User Agent Client (6)  (3)
  Pri(5)User Agent Server (7)
------  ------------------------------------------------------------
[0001]  CONNECTED     0000.00:00:30  300
    1   IPsecIKE)20010db8000000000000000000000000/64
    1   IPsecIKE)20010db8000000001000000000000000/64
[0002]  INVITE        0000.00:00:00    0
    1   TOKYO
   10   KAWASAKI
[0003]  CONNECTED     0000.00:00:30  300
    1   IPsecIKE)c0a80100/24
    1   IPsecIKE)c0a80200/24

Total Sessions      2   (8)
#

# show dvpn server session summary
Total Sessions      2
#
```

1) No.

セッションの番号が表示されます。

2) Status

セッションの状態が表示されます。

INVITE　：INVITE 転送状態

re-INVITE

：re-INVITE 転送状態

ACK WAIT

：ACK 待ち状態

CANCEL

：CANCEL 転送状態

BYE　：BYE 転送状態

CONNECTED

：接続状態

END　：セッション終了状態

3) Elapsed Time
セッションの経過時間が表示されます。

4) Expire
セッションの有効時間が秒単位で表示されます。

5) Pri
登録されているプライオリティを表示します。

6) User Agent Client
発呼側ユーザ名が表示されます。

7) User Agent Server
着呼側ユーザ名が表示されます。

8) Total Sessions
セッションの合計数が表示されます。

43.3 動的 VPN サーバの情報の削除

43.3.1 clear dvpn server user

[機能]

動的 VPN サーバに登録されているユーザ情報の削除

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear dvpn server user

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

動的 VPN サーバに登録されているすべてのユーザ情報を削除します。

[実行例]

以下に、実行例を示します。

```
# clear dvpn server user
#
```

43.3.2　clear dvpn server session

[機能]

動的 VPN サーバのセッション情報の削除

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear dvpn server session

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

動的 VPN サーバ機能が管理しているすべてのセッション情報を削除します。

[実行例]

以下に、実行例を示します。

```
# clear dvpn server session
#
```

第 44 章　IPsec/IKE のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

44.1　IPsec/IKE のカウンタ・ログ・統計・状態などの表示、クリア操作

44.1.1　show ipsec sa

[機能]

システムの IPsec SA 情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ipsec sa
show ipsec sa [<protocol>]

[オプション]

なし

IPsec/IKE SA 情報を表示します。

<protocol>

ike　IKE SA 情報を表示します。

protocol　IPsec SA および SPD 情報を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

IPsec/IKE SA 情報を表示します。

[実行例]

以下に、IPsec/IKE SA 情報の実行例を示します。

(1)　オプションなし

```
# show ipsec sa
[IPsec SA Information]
[1]     Remote Name(ISP-0), rmt0, ap0
        Side(Initiator), Gateway(192.168.2.1, 192.168.1.1), OUT
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=171237444(0x0a34e044)
        Created(Jun 26 17:59:03 2006), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(4096Kbyte), Current(2528Kbyte), Remain(1568Kbyte)

[2]     Remote Name(ISP-0), rmt0, ap0
        Side(Initiator), Gateway(192.168.1.1, 192.168.2.1), IN
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=181913669(0x0ad7c845)
        Created(Jun 26 17:59:03 2006), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(4096Kbyte), Current(2528Kbyte), Remain(1568Kbyte)

[3]     Remote Name(ISP-1), rmt1, ap0
        Side(Initiator), Gateway(2001:db8:1111:2::66, 2001:db8:1111:1::66), OUT
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=171237446(0x0a34e046)
        Created(Jun 26 17:59:03 2006), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(4096Kbyte), Current(2528Kbyte), Remain(1568Kbyte)

[4]     Remote Name(ISP-1), rmt1, ap0
        Side(Initiator), Gateway(2001:db8:1111:1::66, 2001:db8:1111:2::66), IN
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=181913671(0x0ad7c847)
        Created(Jun 26 17:59:03 2006), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(4096Kbyte), Current(2528Kbyte), Remain(1568Kbyte)

[5]     Remote Name(ISP-2), rmt2, ap0
        Side(Responder), Gateway(172.168.1.1, 172.168.2.1), OUT
        Protocol(ESP), Enctype(3des-cbc), Authtype(hmac-sha1), PFS(modp1024)
        Status(mature), Spi=6576585(0x006459c9)
        Created(Jun 26 17:59:03 2006), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(0Kbyte), Current(1Kbyte), Remain(0Kbyte)

[6]     Remote Name(ISP-2), rmt2, ap0
        Side(Responder), Gateway(172.168.2.1, 172.168.1.1), IN
        Protocol(ESP), Enctype(3des-cbc), Authtype(hmac-sha1), PFS(modp1024)
        Status(mature), Spi=68728918(0x0418b856)
        Created(Jun 26 17:59:03 2006), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(0Kbyte), Current(1Kbyte), Remain(0Kbyte)

[7]     Remote Name(), rmt3, ap0, tmp0
        Side(Responder), Gateway(201.1.0.1, 201.1.0.2), OUT
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=171237446(0x0a34e048)
        Created(Jun 26 17:59:03 2006), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(4096Kbyte), Current(2528Kbyte), Remain(1568Kbyte)

[8]     Remote Name(), rmt3, ap0, tmp0
        Side(Responder), Gateway(201.1.0.2, 201.1.0.1), IN
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=181913671(0x0ad7c849)
        Created(Jun 26 17:59:03 2006), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(4096Kbyte), Current(2528Kbyte), Remain(1568Kbyte)
```

(続く)

```
[9]     Remote Name(), rmt4, ap0, tmp1
        Side(Responder), Gateway(2001:db8:2:2::66, 2001:db8:2:1::66), OUT
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=171237446(0x0a34e048)
        Created(Jun 26 17:59:03 2006), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(4096Kbyte), Current(2528Kbyte), Remain(1568Kbyte)

[10]    Remote Name(), rmt4, ap0, tmp1
        Side(Responder), Gateway(2001:db8:2:1::66, 2001:db8:2:2::66), IN
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=181913671(0x0ad7c849)
        Created(Jun 26 17:59:03 2006), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(4096Kbyte), Current(2528Kbyte), Remain(1568Kbyte)

[11]    Remote Name(), rmt5, ap0, tmp2
        Side(Responder), Gateway(200.1.0.1, 200.1.1.1), OUT
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=171237446(0x0a34e048)
        Created(Jun 26 17:59:03 2006), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(0Kbyte), Current(1Kbyte), Remain(0Kbyte)

[12]    Remote Name(), rmt5, ap0, tmp2
        Side(Responder), Gateway(200.1.1.1, 200.1.0.1), IN
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=181913671(0x0ad7c849)
        Created(Jun 26 17:59:03 2006), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(0Kbyte), Current(1Kbyte), Remain(0Kbyte)

[IKE SA Information]
[1]     Destination(192.168.1.1.500), Source(192.168.2.1.500), rmt0
        Cookies(2ee33635dcc2a837:ece2a45bc12889ef)
        Side(Initiator), Status(ESTABLISHED), Exchangetype(AGGRESSIVE)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        Created(Jun 26 17:59:03 2006)
        Lifetime(86400sec), Current(10sec), Remain(86390sec)

[2]     Destination(2001:db8:1111:1::66.500), Source(2001:db8:1111:2::66.500), rmt1
        Cookies(6ee33635dcc2a837:dce2a45bc12889ef)
        Side(Initiator), Status(ESTABLISHED), Exchangetype(AGGRESSIVE)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        Created(Jun 26 17:59:03 2006)
        Lifetime(86400sec), Current(10sec), Remain(86390sec)

[3]     Destination(172.168.1.1.10100), Source(172.168.2.1.4500), rmt2
        Cookies(6cdcdb0f5cca5ba8:8eea7fd95adc032d)
        Side(Responder), Status(ESTABLISHED), Exchangetype(AGGRESSIVE)
        Enctype(3des-cbc), Hashtype(hmac-sha1), PFS(modp1024)
        Created(Jun 26 17:59:03 2006)
        Lifetime(86400sec), Current(10sec), Remain(86390sec)
        NAT-T VendorID(0x7d9419a65310ca6f2c179d9215529d56)

[4]     Destination(201.1.0.1.500), Source(201.1.0.2.500), rmt3, tmp0
        Cookies(47de2fca62f00cfe:a28fa385e74a9855)
        Side(Responder), Status(ESTABLISHED), Exchangetype(AGGRESSIVE)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        Created(Jun 26 17:59:03 2006)
        Lifetime(86400sec), Current(10sec), Remain(86390sec)
```

(続く)

(続き)

```
[5]     Destination(2001:db8:2:1::66.500), Source(2001:db8:2:2::66.500), rmt4, tmp1
        Cookies(76b6e510a6836813:ad12e09555ad6245)
        Side(Responder), Status(ESTABLISHED), Exchangetype(AGGRESSIVE)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        Created(Jun 26 17:59:03 2006)
        Lifetime(86400sec), Current(10sec), Remain(86390sec)

[6]     Destination(200.1.0.1.10010), Source(200.1.1.1.4500), rmt5, tmp2
        Cookies(6cdcdb0f5cca5ba8:8eea7fd95adc032d)
        Side(Responder), Status(ESTABLISHED), Exchangetype(AGGRESSIVE)
        Enctype(3des-cbc), Hashtype(hmac-sha1), PFS(modp1024)
        Created(Jun 26 17:59:03 2006)
        Lifetime(86400sec), Current(10sec), Remain(86390sec)
        NAT-T VendorID(0x4a131c81070358455c5728f20e95452f)
```

(2) ike オプション指定

```
# show ipsec sa ike
[1]     Destination(192.168.1.1.500), Source(192.168.2.1.500), rmt0
        Cookies(2ee33635dcc2a837:ece2a45bc12889ef)
        Side(Initiator), Status(ESTABLISHED), Exchangetype(AGGRESSIVE)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        Created(Jun 26 17:59:03 2006)
        Lifetime(86400sec), Current(10sec), Remain(86390sec)

[2]     Destination(2001:db8:1111:1::66.500), Source(2001:db8:1111:2::66.500), rmt1
        Cookies(6ee33635dcc2a837:dce2a45bc12889ef)
        Side(Initiator), Status(ESTABLISHED), Exchangetype(AGGRESSIVE)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        Created(Jun 26 17:59:03 2006)
        Lifetime(86400sec), Current(10sec), Remain(86390sec)

[3]     Destination(172.168.1.1.10100), Source(172.168.2.1.4500), rmt2
        Cookies(6cdcdb0f5cca5ba8:8eea7fd95adc032d)
        Side(Responder), Status(ESTABLISHED), Exchangetype(AGGRESSIVE)
        Enctype(3des-cbc), Hashtype(hmac-sha1), PFS(modp1024)
        Created(Jun 26 17:59:03 2006)
        Lifetime(86400sec), Current(10sec), Remain(86390sec)
        NAT-T VendorID(0x7d9419a65310ca6f2c179d9215529d56)

[4]     Destination(201.1.0.1.500), Source(201.1.0.2.500), rmt3, tmp0
        Cookies(47de2fca62f00cfe:a28fa385e74a9855)
        Side(Responder), Status(ESTABLISHED), Exchangetype(AGGRESSIVE)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        Created(Jun 26 17:59:03 2006)
        Lifetime(86400sec), Current(10sec), Remain(86390sec)

[5]     Destination(2001:db8:2:1::66.500), Source(2001:db8:2:2::66.500), rmt4, tmp1
        Cookies(76b6e510a6836813:ad12e09555ad6245)
        Side(Responder), Status(ESTABLISHED), Exchangetype(AGGRESSIVE)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        Created(Jun 26 17:59:03 2006)
        Lifetime(86400sec), Current(10sec), Remain(86390sec)

[6]     Destination(200.1.0.1.10010), Source(200.1.1.1.4500), rmt5, tmp2
        Cookies(6cdcdb0f5cca5ba8:8eea7fd95adc032d)
        Side(Responder), Status(ESTABLISHED), Exchangetype(AGGRESSIVE)
        Enctype(3des-cbc), Hashtype(hmac-sha1), PFS(modp1024)
        Created(Jun 26 17:59:03 2006)
        Lifetime(86400sec), Current(10sec), Remain(86390sec)
        NAT-T VendorID(0x4a131c81070358455c5728f20e95452f)
```

(3)　protocol オプション指定

```
# show ipsec sa protocol
[1]     Remote Name(ISP-0), rmt0, ap0
        Side(Initiator), Gateway(192.168.2.1, 192.168.1.1), OUT
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=171237444(0x0a34e044)
        Created(Jun 26 17:59:03 2006), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(4096Kbyte), Current(2528Kbyte), Remain(1568Kbyte)

[2]     Remote Name(ISP-0), rmt0, ap0
        Side(Initiator), Gateway(192.168.1.1, 192.168.2.1), IN
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=181913669(0x0ad7c845)
        Created(Jun 26 17:59:03 2006), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(4096Kbyte), Current(2528Kbyte), Remain(1568Kbyte)

[3]     Remote Name(ISP-1), rmt1, ap0
        Side(Initiator), Gateway(2001:db8:1111:2::66, 2001:db8:1111:1::66), OUT
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=171237446(0x0a34e046)
        Created(Jun 26 17:59:03 2006), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(4096Kbyte), Current(2528Kbyte), Remain(1568Kbyte)

[4]     Remote Name(ISP-1), rmt1, ap0
        Side(Initiator), Gateway(2001:db8:1111:1::66, 2001:db8:1111:2::66), IN
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=181913671(0x0ad7c847)
        Created(Jun 26 17:59:03 2006), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(4096Kbyte), Current(2528Kbyte), Remain(1568Kbyte)

[5]     Remote Name(ISP-2), rmt2, ap0
        Side(Responder), Gateway(172.168.1.1, 172.168.2.1), OUT
        Protocol(ESP), Enctype(3des-cbc), Authtype(hmac-sha1), PFS(modp1024)
        Status(mature), Spi=6576585(0x006459c9)
        Created(Jun 26 17:59:03 2006), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(0Kbyte), Current(1Kbyte), Remain(0Kbyte)

[6]     Remote Name(ISP-2), rmt2, ap0
        Side(Responder), Gateway(172.168.2.1, 172.168.1.1), IN
        Protocol(ESP), Enctype(3des-cbc), Authtype(hmac-sha1), PFS(modp1024)
        Status(mature), Spi=68728918(0x0418b856)
        Created(Jun 26 17:59:03 2006), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(0Kbyte), Current(1Kbyte), Remain(0Kbyte)

[7]     Remote Name(), rmt3, ap0, tmp0
        Side(Responder), Gateway(201.1.0.1, 201.1.0.2), OUT
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=171237446(0x0a34e048)
        Created(Jun 26 17:59:03 2006), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(4096Kbyte), Current(2528Kbyte), Remain(1568Kbyte)

[8]     Remote Name(), rmt3, ap0, tmp0
        Side(Responder), Gateway(201.1.0.2, 201.1.0.1), IN
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=181913671(0x0ad7c849)
        Created(Jun 26 17:59:03 2006), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(4096Kbyte), Current(2528Kbyte), Remain(1568Kbyte)

[9]     Remote Name(), rmt4, ap0, tmp1
        Side(Responder), Gateway(2001:db8:2:2::66, 2001:db8:2:1::66), OUT
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=171237446(0x0a34e048)
        Created(Jun 26 17:59:03 2006), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(4096Kbyte), Current(2528Kbyte), Remain(1568Kbyte)
```

(続く)

(続き)

```
[10]    Remote Name(), rmt4, ap0, tmp1
        Side(Responder), Gateway(2001:db8:2:1::66, 2001:db8:2:2::66), IN
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=181913671(0x0ad7c849)
        Created(Jun 26 17:59:03 2006), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(4096Kbyte), Current(2528Kbyte), Remain(1568Kbyte)

[11]    Remote Name(), rmt5, ap0, tmp2
        Side(Responder), Gateway(200.1.0.1, 200.1.1.1), OUT
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=171237446(0x0a34e048)
        Created(Jun 26 17:59:03 2006), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(0Kbyte), Current(1Kbyte), Remain(0Kbyte)

[12]    Remote Name(), rmt5, ap0, tmp2
        Side(Responder), Gateway(200.1.1.1, 200.1.0.1), IN
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=181913671(0x0ad7c849)
        Created(Jun 26 17:59:03 2006), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(0Kbyte), Current(1Kbyte), Remain(0Kbyte)
```

IPsec SA/SPD 情報

```
[1]     Remote Name(ISP-0), rmt0, ap0, tmp0
---     ------------------  ----  ---  ----
(1)          (2)            (5)   (6)  (7)
[1]     Destination(192.168.2.20/24), Source(192.168.1.10/24), rmt0, ap0, tmp0
---     ---------------------------  ------------------------  ----  ---  ----
(1)          (3)                          (4)                    (5)   (6)  (7)
        Side(Initiator), Gateway(192.168.2.1, 192.168.1.1), OUT
        ---------------  --------------------------------  ---
             (8)            (9)                             (10)
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        -------------  ----------------  ------------------  ------------
             (11)           (12)             (13)               (14)
        Status(mature), Spi=171237444(0x0a34e044)
        --------------  -------------------------
             (15)           (16)
        Created(Apr 26 17:59:03 2004), NewSA(23040sec, 3276Kbyte)
        ----------------------------  ---------------------------
             (17)                          (18)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        ------------------  ---------------  ----------------
             (19)                (20)              (21)
        Lifebyte(4096Kbyte), Current(2528Kbyte), Remain(1568Kbyte)
        -------------------  ------------------  -----------------
             (22)                (23)              (24)
```

1) IPsec SA/SPD 表示番号

2) IPsec 対象区間のネットワーク名 (IPsec 対象範囲が any4 または any6 の場合)

3) IPsec 対象あて先 IP アドレス (IPsec 対象範囲の指定がある場合)

4) IPsec 対象送信元 IP アドレス (IPsec 対象範囲の指定がある場合)

5) IPsec 対象区間のインタフェース名

6) IPsec 対象区間の接続先定義番号

7) IPsec 対象区間のテンプレート定義番号 (IPsec のテンプレートを使用している場合)

8) ネゴシエーションサイド

   Initiator: イニシエータ

   Responder: レスポンダ

   Manual : 手動鍵設定 ((18)/(19)/(21)/(22)/(24) は、—で表示されます)

9) IPsec 対象パケットをセキュア/アンセキュア化する送信元 IP アドレスおよびあて先 IP アドレス (IKE セッション)

10) ポリシの方向
OUT: 出力用ポリシ
IN : 入力用ポリシ

11) 使用するセキュリティプロトコル

12) 暗号アルゴリズム
※ AES-CBC の場合、"aes-cbc"に続く数字は鍵長を表しています。

13) 認証アルゴリズム

14) PFS 使用時の DH(Diffie-Hellman) グループ

15) IPsec SA の状態
larval: IPsec SA 作成中状態 (ネゴシエーション中の状態)
mature: IPsec SA 作成完了状態 (ネゴシエーションが完了し、IPsec SA が作成された状態)
dying : SA の更新時間 (softtime) に到達した状態
※ IPsec 通信に使用されるのは、mature または dying の状態の IPsec SA となります。

16) SPI 値

17) IPsec SA 作成時間 (秒)

18) IPsec SA の更新を開始する時間 (秒) および有効パケット量 (キロバイト)

19) IPsec SA 有効時間 (秒)

20) IPsec SA 作成からの経過時間 (秒)

21) IPsec SA 削除までの残存時間 (秒)

22) IPsec SA 有効パケット量 (キロバイト)

23) IPsec SA 作成からの転送バイト数 (キロバイト)
出力時: 暗号化/認証後のパケット長の累計
入力時: 復号化/認証前のパケット長の累計

24) IPsec SA 削除までの残バイト数 (キロバイト)

IKE SA 情報

```
[1]     Destination(192.168.1.1.500), Source(192.168.2.1.500), rmt0, tmp0
---     ----------------------------  -----------------------  ----  ----
(1)          (2)                          (3)                  (4)   (5)
        Cookies(2ee33635dcc2a837:ece2a45bc12889ef)
        ------------------------------------------
             (6)
        Side(Initiator), Status(ESTABLISHED), Exchangetype(AGGRESSIVE)
        ---------------  -------------------  ------------------------
             (7)              (8)                  (9)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        ----------------  ------------------  ------------
             (10)             (11)                 (12)
        Created(Apr 26 17:59:03 2004)
        -----------------------------
             (13)
        Lifetime(86400sec), Current(10sec), Remain(86390sec)
        ------------------  --------------  ----------------
             (14)             (15)              (16)
        NAT-T VendorID(0x7d9419a65310ca6f2c179d9215529d56)
        --------------------------------------------------
             (17)
```

1) IKE SA 表示番号
2) IKE あて先 IP アドレス
3) IKE 送信元 IP アドレス
4) IPsec 対象区間のインタフェース名
5) IPsec 対象区間のテンプレート定義番号 (IPsec のテンプレートを使用している場合)
6) クッキー (Initiator:Responder)
7) ネゴシエーションサイド
   Initiator: イニシエータ
   Responder: レスポンダ
8) IKE SA のネゴシエーション状態
   MSG1RECEIVED
   MSG1SENT
   MSG2RECEIVED
   MSG2SENT
   MSG3RECEIVED
   MSG3SENT
   MSG4RECEIVED
   ESTABLISHED
   EXPIRED
   ※ ESTABLISHED は、Phase1 のネゴシエーションが完了した状態を意味します。
   EXPIRED は、IKE SA 情報の削除待ちを意味します。
   その他は、Phase1 のネゴシエーション中の状態を意味します。
9) 交換モード
   BASE: Base モード (未サポート)
   MAIN: Main モード
   AUTH ONLY: Authentication Only モード (未サポート)
   AGGRESSIVE: Aggressive モード
10) 暗号アルゴリズム
   ※ AES-CBC の場合、"aes-cbc"に続く数字は鍵長を表しています。
11) 認証アルゴリズム
12) PFS グループ
13) IKE SA 作成時間
14) IKE SA 有効時間 (秒)
15) IKE SA 作成からの経過時間 (秒)
16) IKE SA 削除までの残存時間 (秒)
17) NAT トラバーサルのバージョン (NAT トラバーサル機能により NAT 装置を検出している場合)
   ※以下の表のハッシュ値で表示します。

VID文字列	ハッシュ値
RFC 3947	0x4a131c81070358455c5728f20e95452f
draft-ietf-ipsec-nat-t-ike-03	0x7d9419a65310ca6f2c179d9215529d56
draft-ietf-ipsec-nat-t-ike-02\n	0x90cb80913ebb696e086381b5ec427b1f
draft-ietf-ipsec-nat-t-ike-02	0xcd60464335df21f87cfdb2fc68b6a448

44.1.2　show ike statistics

[機能]

IKE 統計情報表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ike statistics
show ike statistics interface [interface <interface_name>]

[オプション]

なし

IKE ネゴシエーションパケットの統計情報を表示します。

interface

全リモート・インタフェースについての IKE 統計情報を表示します。

interface interface <interface_name>

指定された名のリモート番号のリモート・インタフェースについての IKE 統計情報を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

IKE ネゴシエーションパケットの統計情報を表示します。

[注意]

テンプレート機能より割り当てられたインタフェースを使用する場合、テンプレートが切断された時に、インタフェース IKE 統計情報がクリアされます。

[実行例]

以下に、IKE ネゴシエーションパケットの統計情報の実行例を示します。

```
# show ike statistics
received isakmp packet:
 0 isakmp packet received error                              --- (1)
 0 total isakmp packet received                              --- (2)
       0 invalid IP address                                  --- (3)
       0 invalid ISAKMP header                               --- (4)
       0 invalid ISAKMP packet                               --- (5)
       0 possible attack                                     --- (6)
received isakmp packet exchange type:
       0 Base Exchange                                       --- (7)
       0 Identity Protection Exchange                        --- (8)
       0 Authentication Only Exchange                        --- (9)
       0 Aggressive Exchange                                 --- (10)
               0 unsupported NAT Traversal version           --- (11)
               0 invalid Security Association                --- (12)
               0 invalid Key Exchange                        --- (13)
               0 invalid Identification                      --- (14)
               0 invalid Certificate                         --- (15)
               0 invalid Certificate Request                 --- (16)
               0 invalid Hash                                --- (17)
               0 invalid Signature                           --- (18)
               0 invalid Nonce                               --- (19)
               0 invalid Notification                        --- (20)
               0 invalid Delete                              --- (21)
               0 invalid Vendor ID                           --- (22)
               0 invalid NAT Discovery                       --- (23)
               0 invalid NAT Original Address                --- (24)
               0 invalid Next Payload type                   --- (25)
       0 Informational Exchange                              --- (26)
               0 Notification                                --- (27)
                       0 No Proposal Chosen                  --- (28)
                       0 Initial Contact                     --- (29)
                       0 others Notify Message               --- (30)
                       0 invalid Notify Message type         --- (31)
               0 there is no valid ISAKMP-SA                 --- (32)
               0 invalid Security Association
               0 invalid Key Exchange
               0 invalid Identification
               0 invalid Certificate
               0 invalid Certificate Request
               0 invalid Hash
               0 invalid Signature
               0 invalid Nonce
               0 invalid Notification
               0 invalid Delete
                       0 invalid received delete message     --- (33)
               0 invalid Vendor ID
               0 invalid NAT Discovery
               0 invalid NAT Original Address
               0 invalid Next Payload type
```

(続く)

(続き)

```
        0 Quick Mode Exchange                                   --- (34)
                0 there is no valid ISAKMP-SA                   --- (35)
                0 invalid Security Association
                0 invalid Key Exchange
                0 invalid Identification
                0 invalid Certificate
                0 invalid Certificate Request
                0 invalid Hash
                0 invalid Signature
                0 invalid Nonce
                0 invalid Notification
                0 invalid Delete
                0 invalid Vendor ID
                0 invalid NAT Discovery
                0 invalid NAT Original Address
                0 invalid Next Payload type
        0 New group  Exchange                                   --- (36)
        0 Acknowledged Informational Exchange                   --- (37)
        0 invalid Exchange type                                 --- (38)
sent isakmp packet:
 0 isakmp packet send error                                     --- (39)
 0 total isakmp packet sent                                     --- (40)
sent isakmp packet phase1:
        0 isakmp phase1 packet resent                           --- (41)
        0 phase1 give up                                        --- (42)
sent isakmp packet phase2:
        0 isakmp phase2 packet resent                           --- (43)
        0 phase2 give up                                        --- (44)
sent isakmp packet information:
        0 No Proposal Chosen                                    --- (45)
        0 Initial Contact                                       --- (46)
        0 others Notify Message                                 --- (47)
others:
        0 phase1 count > phase1_max                             --- (48)
        0 encrypting failed                                     --- (49)
        0 decrypting failed                                     --- (50)
        0 failed to create inbound IPsec SA                     --- (51)
        0 failed to create outbound IPsec SA                    --- (52)
        0 IKE SA information no entry                           --- (53)
        0 IPsec SA information no entry                         --- (54)
        0 shared key no entry                                   --- (55)
        0 IPsec remote interface Down                           --- (56)
        0 invalid remote address                                --- (57)
        0 invalid local address                                 --- (58)
        0 failed to allocate buffer                             --- (59)
        0 radius/aaa authentication succeeded                   --- (60)
        0 radius/aaa authentication failed                      --- (61)
        0 access interface allocation failed                    --- (62)
        0 other                                                 --- (63)
#
```

1) パケット受信エラー数
2) 受信パケットの合計数
3) 無効な IP アドレス受信数
4) 無効な ISAKMP ヘッダ受信数
5) 無効な ISAKMP パケット受信数
6) 自装置に対して攻撃していると思われるパケットの受信数
7) Base 交換受信数
8) Identity 交換受信数
9) Authentication Only 交換受信数
10) Aggressive 交換受信数
11) 未サポートの NAT トラバーサルバージョン受信数
12) SA ペイロード受信失敗数

13) 鍵交換ペイロード受信失敗数
14) ID ペイロード受信失敗数
15) 証明書ペイロード受信失敗数
16) 証明書要求ペイロード受信失敗数
17) ハッシュペイロード受信失敗数
18) 署名ペイロード受信失敗数
19) Nonce ペイロード受信失敗数
20) 通知ペイロード受信失敗数
21) 削除ペイロード受信失敗数
22) ベンダ ID ペイロード受信失敗数
23) NAT ディスカバリペイロード受信失敗数
24) NAT オリジナルアドレスペイロード受信失敗数
25) 無効なペイロードタイプ受信数
26) Informational 交換受信数
27) 通知ペイロード受信数
28) SA Proposal が受け入れられない通知メッセージ受信数
29) 初めての SA 確立通知メッセージ受信数
30) その他の通知メッセージ受信数
31) 無効な通知メッセージの受信数
32) ISAKMP SA がない Informational 受信数
33) 無効な削除メッセージ受信数
34) Quick Mode 受信数
35) ISAKMP SA がない Quick Mode 受信数
36) New group Mode 受信数
37) Acknowledged Informational 受信数
38) 無効な交換タイプ受信数
39) パケット送信エラー数
40) 送信パケットの合計数
41) Phase1 パケット再送数
42) Phase1 ネゴシエーション失敗数
43) Phase2 パケット再送数
44) Phase2 ネゴシエーション失敗数
45) SA Proposal が受け入れられない通知メッセージ送信数
46) 初めての SA 確立通知メッセージ送信数
47) その他の通知メッセージ送信数
48) 装置内での ISAKMP SA 最大数超過数
49) ISAKMP パケット暗号化失敗数
50) ISAKMP パケット復号化失敗数
51) 受信用 IPsec SA 作成失敗数

52)　送信用 IPsec SA 作成失敗数

53)　IKE SA 情報検索失敗数

54)　IPsec SA 情報検索失敗数

55)　共有鍵検索失敗

56)　IPsec 用相手情報接続先名回線閉塞時ネゴシエーション中止数

57)　相手側アドレス不正数

58)　自側アドレス不正数

69)　領域獲得失敗数

60)　RADIUS/AAA 認証成功数

61)　RADIUS/AAA 認証失敗数

62)　アクセスインタフェース獲得失敗数

63)　その他のエラー数

以下に、全リモート・インタフェース IKE 統計情報簡易表示の実行例を示します。

```
# show ike statistics interface
[rmt0]:                                                  --- (1)
 0 total Phase1 packet received                          --- (2)
       0 invalid Payload                                 --- (3)
 0 total Phase1 packet sent                              --- (4)
       0 isakmp phase1 packet resent                     --- (5)
       0 phase1 give up                                  --- (6)
 0 total Phase2 packet received                          --- (7)
       0 invalid Payload                                 --- (8)
 0 total Phase2 packet sent                              --- (9)
       0 isakmp phase2 packet resent                     --- (10)
       0 phase2 give up                                  --- (11)
 0 total Informational packet received                   --- (12)
       0 invalid Payload                                 --- (13)
 0 total Informational packet sent                       --- (14)
[rmt1]:
 0 total Phase1 packet received
       0 invalid Payload
 0 total Phase1 packet sent
       0 isakmp phase1 packet resent
       0 phase1 give up
 0 total Phase2 packet received
       0 invalid Payload
 0 total Phase2 packet sent
       0 isakmp phase2 packet resent
       0 phase2 give up
 0 total Informational packet received
       0 invalid Payload
 0 total Informational packet sent
[rmt2]:
 0 total Phase1 packet received
       0 invalid Payload
 0 total Phase1 packet sent
       0 isakmp phase1 packet resent
       0 phase1 give up
 0 total Phase2 packet received
       0 invalid Payload
 0 total Phase2 packet sent
       0 isakmp phase2 packet resent
       0 phase2 give up
 0 total Informational packet received
       0 invalid Payload
 0 total Informational packet sent
#
```

1)　Remote インタフェース

2)　Phase1 受信合計数

3) Phase1 無効ペイロード 受信数
4) Phase1 送信合計数
5) Phase1 再送数
6) Phase1 ネゴシエーション失敗数
7) Phase2 受信合計数
8) Phase2 無効ペイロード 受信数
9) Phase2 送信合計数
10) Phase2 再送数
11) Phase2 ネゴシエーション失敗数
12) 通知メッセージ受信合計数
13) 通知メッセージ無効ペイロード 受信数
14) 通知メッセージ送信合計数

44.1.3　clear ike statistics

[機能]

IKE 統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear ike statistics

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

IKE ネゴシエーションパケットの統計情報をクリアします。

[実行例]

```
# clear ike statistics
#
```

第 45 章　VRRP のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

45.1　VRRP のカウンタ・ログ・統計・状態などの表示

45.1.1　show vrrp

[機能]

VRRP 機能の各種情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show vrrp [interface <interface_name> [vrid <vrid>]] [brief]

[オプション]

なし

稼働しているすべての VRRP グループ詳細情報を表示します。

interface <interface_name>

指定した LAN インタフェースの VRRP グループを表示します。

範囲	機種
lan0～lan19	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
lan0～lan9	Si-R180

interface <interface_name> vrid <vrid>

指定した<vrid>である VRRP グループを表示します。

- VRID
  VRRP グループの VRID を、1～255 の 10 進数値で指定します。

brief

VRID とグループの状態を簡易表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

interface <interface_name> vrid <vrid>と指定した場合は、指定 LAN インタフェースの指定 VRRP グループ詳細情報を表示します。
interface <interface_name>だけを指定した場合は、指定 LAN インタフェースに設定されたすべての VRRP グループ詳細情報を表示します。
interface <interface_name> vrid <vrid>をすべて指定しない場合は、全 VRRP グループの詳細情報を表示します。
brief オプションを指定することによって、VRID とグループの状態を簡易表示します。
interface <interface_name> vrid <vrid> brief と指定することによって、ヘッダのない VRID とグループの状態を簡易表示します。

[実行例]

以下に、各オプションごとの実行例を示します。

brief

定義されている VRID の一覧とそのグループの状態を簡易表示します。グループの状態として、Master/Backup/Initialize/Initialize:Disabled があります。

- Master
  マスタルータとして仮想ルータの IP アドレスあてのパケットをフォワーディングしている状態。
- Backup
  バックアップルータとしてマスタルータのダウンに備えている状態。
- Initialize
- Initialize:Disabled
  マスタルータまたはバックアップルータになることができない状態。
  Disabled は手動停止コマンドが投入された状態を示します。

```
# show vrrp brief
[LAN 0]
  VRID  Status
    10  Master
    20  Backup
[LAN 1]
  VRID  Status
    25  Backup
    40  Initialize
#
```

interface <interface_name> vrid <vrid> brief

VRID とそのグループの状態をヘッダなしで簡易表示します。

```
# show vrrp interface lan0 vrid 10 brief
    10  Master
#
```

オプションなし

オプションなしの場合は、本装置にて稼働しているすべての VRRP グループ詳細情報を表示します。

```
# show vrrp
[LAN 0]                                                                  --- (1)
  State              : OK                                                --- (2)
  Authentication Type: None                                              --- (3)
  Authentication Pass: ""                                                --- (4)
  Interface statistics information:
      0          Bad checksum packets                                    --- (5)
      0          VRRP Version illegal packets                            --- (6)
      0          VRID illegal packets                                    --- (7)

  VRID 10                                                                --- (8)
    Master(PRI 254 now 254/PREEMPT ON)                                   --- (9)
    Now Master : Me                                                      --- (10)
    Virtual MAC Address : 00:00:5E:00:01:0A                              --- (11)
    Virtual Router IP Address:
        10.124.2.126                                                     --- (12)
    VRRP advertisement interval 1                                        --- (13)
    Shutdown interface trigger:
        lan1   reduce 200  OFF                                           --- (14)
        rmt11  reduce 100  OFF
    Shutdown route trigger:
        default            lan0   reduce 255  OFF                        --- (15)
        10.232.79.200/32   rmt1   reduce 100  OFF
    Shutdown node trigger:
        192.168.100.100    lan0   reduce 255  OFF                        --- (16)
        10.232.79.193      rmt1   reduce 100  OFF
    Group statistics information:
        1          become master-router                                  --- (17)
        0          received VRRP advertisement packets                   --- (18)
        0          VRRP advertisement interval configuration mismatched packets --- (19)
        0          Authentication failed packets                         --- (20)
        0          TTL illegal packets                                   --- (21)
        0          received priority 0 advertisement packets             --- (22)
        0          sent priority 0 advertisement packets                 --- (23)
        0          VRRP type illegal packets                             --- (24)
        0          Virtual router IP address configuration mismatched packets   --- (25)
        0          Authentication type illegal packets                   --- (26)
        0          Authentication type mismatch packets                  --- (27)
        0          Length illegal packets                                --- (28)

  VRID 20
    Backup(PRI 100 now 50/PREEMPT OFF)
    Now Master : 10.124.2.100 Priority 255
    Virtual MAC Address : 00:00:5E:00:01:14
    Virtual Router IP Address:
        10.124.2.138
        10.124.2.139
    VRRP advertisement interval 1
    Shutdown interface trigger:
        rmt3  reduce  50  ON
    Action:
        backup diallock remote 2                  OFF                        --- (29)
        master online remote 6 ap 0               Thu Apr  7 11:00:32 2005
        master offline template interface rmt4    Thu Apr  7 11:00:32 2005
    Group statistics information:
        0          become master-router
        6130       received VRRP advertisement packets
        0          VRRP advertisement interval configuration mismatched packets
        0          Authentication failed packets
        0          TTL illegal packets
        0          received priority 0 advertisement packets
        0          sent priority 0 advertisement packets
        0          VRRP type illegal packets
        0          Virtual router IP address configuration mismatched packets
        0          Authentication type illegal packets
        0          Authentication type mismatch packets
        0          Length illegal packets
#
```

1) 情報を表示する LAN インタフェース

2) LAN インタフェースの状態 : OK/NG

3) LAN インタフェースの VRRP-AD 認証方法

4) LAN インタフェースの VRRP-AD 認証パスワード

5) 受信 VRRP-AD のチェックサム異常数

6) 受信 VRRP-AD の VRRP バージョン異常数

7) 受信 VRRP-AD の VRID 異常数

8) VRID

9) VRRP グループ状態 (設定優先度、現在の優先度/プリエンプトモード)
VRRP グループ状態 : 現在の VRRP グループの状態
(Master/Backup/Initialize/Initialize:Disabled)

- Master
  マスタルータとして仮想ルータの IP アドレスあてのパケットをフォワーディングしている状態。
- Backup
  バックアップルータとしてマスタルータのダウンに備えている状態。
- Initialize
- Initialize:Disabled
  マスタルータまたはバックアップルータになることができない状態。
  Disabled は手動停止コマンドが投入された状態を示します。
  設定優先度 : 構成定義で設定された優先度
  現在の優先度 : トリガイベントの減算値を含めた現在の優先度
  プリエンプトモード : 構成定義で設定されたプリエンプトモード (ON/OFF)

10) 現在のマスタルータの実 IP アドレスと優先度 (本装置がマスタルータである場合は"Me" を表示)

11) 仮想 MAC アドレス

12) 仮想ルータの IP アドレス

13) VRRP-AD の送信間隔

14) インタフェースダウントリガと適用状態

15) ルートダウントリガと適用状態

16) ノードダウントリガと適用状態

17) マスタルータになった回数

18) VRRP-AD の総受信数

19) 受信 VRRP-AD の送信間隔異常数

20) 受信 VRRP-AD の認証パスワード異常数

21) 受信 VRRP-AD の TTL 異常数

22) 優先度 0 の VRRP-AD 総受信数

23) 優先度 0 の VRRP-AD 総送信数

24) 受信 VRRP-AD のタイプ異常数

25) 受信 VRRP-AD のバックアップ IP アドレス構成異常数

26) 受信 VRRP-AD の認証タイプ異常数

27) 受信 VRRP-AD の認証タイプ不一致数

28) 受信 VRRP-AD のヘッダ長異常数

29) VRRP 状態変化に対するアクションと適用状態

45.2　VRRP のカウンタ・ログ・統計などのクリア

45.2.1　clear vrrp statistics

[機能]

VRRP 統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear vrrp statistics

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

全 VRRP グループの統計情報をクリアします。

[実行例]

```
# clear vrrp statistics
#
```

第 46 章　ブリッジのカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

46.1　ブリッジのカウンタ・ログ・統計・状態などの表示

46.1.1　show bridge

[機能]

ブリッジに関する状態および統計情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show bridge
show bridge group [<group_id>]
show bridge summary

[オプション]

なし

学習テーブルの内容を表示します。

group [<group_id>]

表示するブリッジグループを指定します。
group_id を省略時は、すべてのグループをグループ順にソートして表示します。

範囲	機種
0〜19	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
0〜7	Si-R180

summary

学習テーブルの割り当て状況を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

ブリッジに関する状態、または統計情報を表示します。

[実行例]

学習テーブルの内容を表示する場合

```
# show bridge
Codes: D - Dynamic entry, S - Static entry
Address                Group    Interface      Status Remain time
-------                -----    ---------      ------ -----------
  (1)                   (2)        (3)           (4)       (5)
00:e0:00:78:2f:7a          0         lan0           S    infinity
00:a0:c9:13:f3:37          0         lan0           D         164
00:a0:c9:f0:20:e9          0         lan1           D         196
00:b0:d0:6f:94:78          0         lan1           D         196
00:0c:6e:63:25:77          1         lan2           D         204
00:04:96:1a:a7:b0          1         lan3           D         300
```

1) 学習テーブルに登録されている MAC アドレス

2) グループ識別子

3) エントリされた端末が存在するインタフェース名

4) 学習テーブルの状態
以下のどれかが表示されます。

D	動的学習テーブル
S	静的学習テーブル

5) 残り生存時間 (秒)
学習テーブルの割り当て状況を表示する場合

```
#show bridge summary
Registered station blocks : 6                                --- (1)
Free station blocks : 1018                                   --- (2)
Max allocated blocks : 6                                     --- (3)
Learned count : 6                                            --- (4)
Deleted count : 0                                            --- (5)
Expired count : 0                                            --- (6)
```

1) 使用中の学習テーブル数

2) 未使用の学習テーブル数

3) 過去に割り当てられた学習テーブルの最大値

4) 学習テーブルにエントリした回数

5) 学習テーブルに空きがないために削除された学習テーブル数

6) 寿命によって削除された学習テーブル数

46.1.2　show bridge status

[機能]

ブリッジのインタフェース状態および統計情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show bridge status
show bridge status interface <interface_name>
show bridge status group [<group_id>]

[オプション]

なし

全インタフェースの状態や入出力パケット数を表示します。

interface <interface_name>

指定したインタフェースの状態や入出力パケット数を表示します。

group [<group_id>]

表示するブリッジグループを指定します。
group_id を省略時は、すべてのグループをグループ順にソートして表示します。

範囲	機種
0〜19	Si-R570　Si-R370　Si-R240　Si-R220B
0〜7	Si-R180

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

ブリッジのインタフェース状態と統計情報を表示します。

[実行例]

インタフェースごとの状態と入出力パケット数を表示する場合

```
# show bridge status
Name    Group   Status  IPv4    IPv6    D_if            In    Out
----    -----   ------  ----    ----    ---             --    ---
(1)     (2)      (3)    (4)     (5)     (6)             (7)   (8)

lan0    0       valid   Bridge  Routing *                0     2
lan1    0       valid   Bridge  Routing                  0     1
lan2    1       valid   Bridge  Routing *                0     0
lan3    1       valid   Bridge  Routing                  0     0
rmt0    1       valid   Bridge  Routing                  0     0
```

1)　インタフェース名
lan、または rmt インタフェース名が表示されます。

2) グループ識別子

3) ブリッジの状態

以下のどれかが表示されます。

valid ブリッジは有効

invalid ブリッジは無効

4) IPv4 転送方式

以下のどれかが表示されます。

Bridge ブリッジで転送

Routing ルーティングで転送

5) IPv6 転送方式

以下のどれかが表示されます。

Bridge ブリッジで転送

Routing ルーティングで転送

6) 代表インタフェース

レイヤ 3 代表インタフェースには * が表示されます。

7) 入力パケット数

8) 出力パケット数

46.2　ブリッジのカウンタ・ログ・統計などのクリア

46.2.1　clear bridge statistics

[機能]

ブリッジ関連の統計情報クリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear bridge statistics

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

ブリッジ関連の統計情報をクリアします。

[実行例]

```
# clear bridge statistics
#
```

46.3 スパニングツリーのカウンタ・ログ・統計・状態などの表示

46.3.1 show spanning-tree

[機能]

スパニングツリー情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show spanning-tree
show spanning-tree root
show spanning-tree bridge
show spanning-tree active
show spanning-tree interface <interface_name>
show spanning-tree detail
show spanning-tree brief

[オプション]

なし

すべてのスパニングツリー情報を簡易表示します。

root

ルートブリッジのスパニングツリー情報だけを表示します。

bridge

装置のスパニングツリーブリッジ情報だけを表示します。

active

動作しているインタフェースのスパニングツリー情報だけを表示します。

interface <interface_name>

指定したインタフェースのスパニングツリー情報だけを表示します。

detail

すべてのスパニングツリー情報を詳細表示します。

brief

すべてのスパニングツリー情報を簡易表示します。

[動作モード]

運用管理モード (一般ユーザクラス／管理者クラス)
構成定義モード (管理者クラス)

[説明]

スパニングツリー機能の状態を表示します。

[実行例]

ルートブリッジのスパニングツリー情報を表示する場合

```
# show spanning-tree root
Root ID    Priority    32768                                        ---(1)
           Address     00:00:0e:a8:0b:5a                            ---(2)
           Cost        110                                          ---(3)
           Port        lan0                                         ---(4)
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
           ----------------  --------------  --------------------
                 (5)               (6)                (7)
```

1) ブリッジ優先度

   ルートブリッジの優先度が表示されます。

2) MAC アドレス

   ルートブリッジの MAC アドレスが表示されます。

3) ルートパスコスト

   ルートブリッジまでのパスコスト値が表示されます。

4) ルートポート

   ルートポートのインタフェース名が表示されます

5) 構成情報 BPDU 送出間隔

   構成情報 BPDU の送出間隔 (秒) が表示されます。

6) 最大待ち合わせ時間 (秒)

   構成情報 BPDU の最大待ち合わせ時間 (秒) が表示されます。

7) 最大中継遅延時間 (秒)

   最大中継遅延時間 (秒) が表示されます。

装置のスパニングツリーブリッジ情報を表示する場合

```
# show spanning-tree bridge
Bridge ID  Priority    32768                                       ---(1)
           Address     00:00:0e:a8:0b:5a                           ---(2)
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
           ----------------  --------------  --------------------
                 (3)               (4)                (5)
           Aging Time 300sec
           ----------------
                 (6)
```

1) ブリッジ優先度

   本装置のブリッジ識別子に用いるブリッジ優先度が表示されます。

2) MAC アドレス

   本装置のブリッジ識別子に用いる MAC アドレスが表示されます。

3) 構成情報 BPDU 送出間隔

   構成情報 BPDU の送出間隔 (秒) が表示されます。

4) 最大待ち合わせ時間

   構成情報 BPDU の最大待ち合わせ時間 (秒) が表示されます。

5) 最大中継遅延時間

   最大中継遅延時間 (秒) が表示されます。

6) 学習テーブルの最大生存時間

学習テーブルの最大生存時間 (秒) が表示されます。

指定したインタフェースのスパニングツリー情報を表示する場合

```
# show spanning-tree interface lan0
lan0 is Forwarding
------------------
       (1)
    Port path cost 10(auto), Port priority 128, Port Identifier 128.1
    ----------------------   -----------------  ----------------------
             (2)                   (3)                 (4)
    Port role is Root
    -----------------
           (5)
    Designated root has priority 32768, address 00:00:0e:a8:0b:5a
    ----------------------------------  -------------------------
             (6)                                  (7)
    Designated bridge has priority 32768, address 00:e0:00:26:09:8b
    -----------------------------------  -------------------------
             (8)                                  (9)
    Designated port id is 128.2, Designated path cost 100
    ---------------------------  ------------------------
             (10)                      (11)
    BPDU statistics:
      Config BPDU: sent 1, sent error 0
                   ------  ------------
                    (12)       (13)
                   received 901, discarded 0
                  -------------  -----------
                      (14)          (15)
      TCN BPDU:    sent 0, sent error 0
                   ------  ------------
                    (16)       (17)
                   received 0, discarded 0
                   ----------  -----------
                      (18)         (19)
      Other error: bad protocol 0, bad version 0
                   --------------  -------------
                       (20)            (21)
                   bad BPDU type 0
                   ---------------
                        (22)
```

1) インタフェース名とポート状態

ポート状態は以下のどれかが表示されます。

Disabled STP は無効

Blocking Blocking 状態

Listening Listening 状態

Learning Learning 状態

Forwarding

Forwarding 状態

2) ポートパスコスト

該当ポートのパスコスト値が表示されます。

3) ポート優先度

該当ポートの優先度が表示されます。

4) ポート識別子

ポート識別子 (ポート優先度. ポート番号) が表示されます。

5) ポート役割

ポートの役割状態が以下のどれかで表示されます。

Disabled　STP は無効

Root　ルートポート

Designated
代表ポート

Blocking　ブロッキングポート

6) ルートブリッジ優先度
ルートブリッジの優先度が表示されます。

7) ルートブリッジ MAC
ルートブリッジの MAC アドレスが表示されます。

8) 代表ブリッジ優先度
代表ブリッジの優先度が表示されます。

9) 代表ブリッジ MAC
代表ブリッジの MAC アドレスが表示されます。

10) 代表ポート識別子
代表ポートの識別子 (ポート優先度. ポート番号) が表示されます。

11) 代表ポートパスコスト
代表ポートのパスコスト値が表示されます。

12) 構成 BPDU 送信回数
構成 BPDU の送信回数が表示されます。

13) 構成 BPDU 送信エラー回数
構成 BPDU の送信エラー回数が表示されます。

14) 構成 BPDU 受信回数
構成 BPDU の受信回数が表示されます。

15) 構成 BPDU 受信破棄回数
構成 BPDU の受信破棄回数が表示されます。

16) TCN BPDU 送信回数
TCN BPDU の送信回数が表示されます。

17) TCN BPDU 送信エラー回数
TCN PDU の送信エラー回数が表示されます。

18) TCN PDU 受信回数
TCN BPDU の受信回数が表示されます。

19) TCN BPDU 受信破棄回数
TCN BPDU の受信破棄回数が表示されます。

20) プロトコルバージョンエラー回数
プロトコルバージョンのエラーによる破棄回数が表示されます。

21) バージョンエラー回数
バージョンのエラーによる破棄回数が表示されます。

22) BPDU タイプエラー回数
BPDU のタイプエラーによる破棄回数が表示されます。

すべてのスパニングツリー情報を詳細表示する場合

```
# show spanning-tree detail
IEEE compatible spanning tree protocol is being executed.
  Bridge Identifier has priority 32768, address 00:e0:00:00:d7:e0
  -----------------------------------  -------------------------
            (1)                                (2)
  Configured hello time 2, max age 20, forward delay 15, aging time 300
  -----------------------  ----------  ----------------  --------------
            (3)              (4)            (5)              (6)
  Current root has priority 32768, address 00:00:0e:a8:0b:5a
  ------------------------------  -------------------------
            (7)                                (8)
  Root port is lan0, cost of root path is 110
  -----------------  ------------------------
        (9)                 (10)

lan0 is Forwarding
------------------
           (11)
    Port path cost 10(auto), Port priority 128, Port Identifier 128.1
    ----------------------   ----------------  ----------------------
             (12)                  (13)               (14)
    Port role is Root
    -----------------
           (15)
    Designated root has priority 32768, address 00:00:0e:a8:0b:5a
    ----------------------------------  -------------------------
             (16)                                (17)
    Designated bridge has priority 32768, address 00:e0:00:26:09:8b
    -----------------------------------  ------------------------
             (18)                                (19)
    Designated port id is 128.2, Designated path cost 100
    ---------------------------  ------------------------
             (20)                     (21)
    BPDU statistics:
      Config BPDU: sent 1, sent error 0
                   ------  ------------
                    (22)       (23)
                   received 901, discarded 0
                  -------------  -----------
                      (24)          (25)
      TCN BPDU:    sent 0, sent error 0
                   ------  ------------
                    (26)       (27)
                   received 0, discarded 0
                   ----------  -----------
                      (28)         (29)
      Other error: bad protocol 0, bad version 0
                   --------------  -------------
                       (30)            (31)
                   bad BPDU type 0
                   ---------------
                        (32)
```

(続く)

(続き)

```
lan1 is Forwarding
------------------
           (11)
    Port path cost 10(auto), Port priority 128, Port Identifier 128.2
    ----------------------   -----------------  ----------------------
             (12)                   (13)               (14)
    Port role is Designated
    -----------------------
           (15)
    Designated root has priority 32768, address 00:00:0e:a8:0b:5a
    ---------------------------------  -------------------------
             (16)                                  (17)
    Designated bridge has priority 32768, address 00:e0:00:26:09:8b
    -----------------------------------  -------------------------
             (18)                                 (19)
    Designated port id is 128.2, Designated path cost 100
    ---------------------------  ------------------------
             (20)                      (21)
    BPDU statistics:
      Config BPDU: sent 2, sent error 0
                   ------  ------------
                    (22)       (23)
                   received 501, discarded 0
                  -------------  -----------
                      (24)          (25)
      TCN BPDU:    sent 0, sent error 0
                   ------  ------------
                    (26)       (27)
                   received 0, discarded 0
                   ----------  -----------
                      (28)         (29)
      Other error: bad protocol 0, bad version 0
                   --------------  -------------
                       (30)            (31)
                   bad BPDU type 0
                   ---------------
                        (32)
```

1) ブリッジ優先度

本装置のブリッジ識別子に用いるブリッジ優先度が表示されます。

2) MAC アドレス

本装置のブリッジ識別子に用いる MAC アドレスが表示されます。

3) 構成情報 BPDU 送出間隔

構成情報 BPDU の送出間隔 (秒) が表示されます。

4) 最大待ち合わせ時間

構成情報 BPDU の最大待ち合わせ時間 (秒) が表示されます。

5) 最大中継遅延時間

最大中継遅延時間 (秒) が表示されます。

6) 学習テーブルの最大生存時間

学習テーブルの最大生存時間 (秒) が表示されます。

7) ルートブリッジ優先度

ルートブリッジの優先度が表示されます。

8) ルートブリッジ MAC

ルートブリッジの MAC アドレスが表示されます。

9) ルートポート

ルートポートのインタフェース名が表示されます

10) ルートパスコスト

ルートブリッジまでのパスコスト値が表示されます。

11) インタフェース名とポート状態
ポート状態は以下のどれかが表示されます。

Disabled STP は無効

Blocking Blocking 状態

Listening Listening 状態

Learning Learning 状態

Forwarding
Forwarding 状態

12) ポートパスコスト
該当ポートのパスコスト値が表示されます。

13) ポート優先度
該当ポートの優先度が表示されます。

14) ポート識別子
ポート識別子 (ポート優先度. ポート番号) が表示されます。

15) ポート役割
ポートの役割状態が以下のどれかで表示されます。

Disabled STP は無効

Root ルートポート

Designated
代表ポート

Blocking ブロッキングポート

16) ルートブリッジ優先度
ルートブリッジの優先度が表示されます。

17) ルートブリッジ MAC
ルートブリッジの MAC アドレスが表示されます。

18) 代表ブリッジ優先度
代表ブリッジの優先度が表示されます。

19) 代表ブリッジ MAC
代表ブリッジの MAC アドレスが表示されます。

20) 代表ポート識別子
代表ポートの識別子 (ポート優先度. ポート番号) が表示されます。

21) 代表ポートパスコスト
代表ポートのパスコスト値が表示されます。

22) 構成 BPDU 送信回数
構成 BPDU の送信回数が表示されます。

23) 構成 BPDU 送信エラー回数
構成 BPDU の送信エラー回数が表示されます。

24) 構成 BPDU 受信回数
構成 BPDU の受信回数が表示されます。

25) 構成 BPDU 受信破棄回数

構成 BPDU の受信破棄回数が表示されます。

26) TCN BPDU 送信回数

TCN BPDU の送信回数が表示されます。

27) TCN BPDU 送信エラー回数

TCN PDU の送信エラー回数が表示されます。

28) TCN PDU 受信回数

TCN BPDU の受信回数が表示されます。

29) TCN BPDU 受信破棄回数

TCN BPDU の受信破棄回数が表示されます。

30) プロトコルバージョンエラー回数

プロトコルバージョンのエラーによる破棄回数が表示されます。

31) バージョンエラー回数

バージョンのエラーによる破棄回数が表示されます。

32) BPDU タイプエラー回数

BPDU のタイプエラーによる破棄回数が表示されます。

すべてのスパニングツリー情報を簡易表示する場合

```
# show spanning-tree brief
Spanning tree enabled protocol IEEE
Root ID    Priority    32768                                          ---(1)
           Address     00:00:0e:a8:0b:5a                              ---(2)
           Cost        110                                            ---(3)
           Port        1 (lan0)                                       ---(4)
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
           ----------------  --------------  --------------------
                 (5)              (6)               (7)

Bridge ID  Priority    32768                                          ---(8)
           Address     00:e0:00:00:d7:e0                              ---(9)
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
           ----------------  --------------  --------------------
                 (10)              (11)               (12)
          Aging Time 300 sec
           ----------------
                 (13)

Interface       Port ID  Cost        Status(Role)            Sent
                                     Designated Bridge ID    Received
--------------- -------- ----------- ----------------------- ----------
lan0            128.1            10* Forwarding(Root)                10
----            -----           ---- ------------------             ---
(14)             (15)           (16)       (17)                    (18)
                128.2           100  32768 00:e0:00:26:09:8b        29
                -----           ---- ------------------             ---
                 (19)           (20)       (21)                    (22)
lan1            128.2            10* Forwarding(Designated)          7
----            -----           ---- ------------------             ---
(14)             (15)           (16)       (17)                    (18)
                128.2           100  32768 00:e0:00:26:09:8b       291
                -----           ---- ------------------             ---
                 (19)           (20)       (21)                    (22)
```

1) ルートブリッジ優先度

ルートブリッジ識別子のブリッジ優先度が表示されます。

2) ルートブリッジ MAC アドレス

ルートブリッジ識別子の MAC アドレスが表示されます。

3) ルートパスコスト
ルートブリッジまでのパスコスト値が表示されます。

4) ポート番号とインタフェース名
ポート番号とインタフェース名が表示されます。

5) 構成情報 BPDU 送出間隔
構成情報 BPDU の送出間隔 (秒) が表示されます。

6) 最大待ち合わせ時間
構成情報 BPDU の最大待ち合わせ時間 (秒) が表示されます。

7) 最大中継遅延時間
最大中継遅延時間 (秒) が表示されます。

8) 自装置ブリッジ優先度
本装置のブリッジ識別子に用いるブリッジ優先度が表示されます。

9) 自装置 MAC アドレス
本装置のブリッジ識別子に用いる MAC アドレスが表示されます。

10) 構成情報 BPDU 送出間隔
構成情報 BPDU の送出間隔 (秒) が表示されます。

11) 最大待ち合わせ時間
構成情報 BPDU の最大待ち合わせ時間 (秒) が表示されます。

12) 最大中継遅延時間
最大中継遅延時間 (秒) が表示されます。

13) 学習テーブルの最大生存時間
学習テーブルの最大生存時間 (秒) が表示されます。

14) インタフェース名
インタフェース名が表示されます。

15) ポート識別子
ポート識別子が表示されます。

16) ポートパスコスト
ポートのパスコスト (自動計算された場合は数字のあとに"*"が表示されます) が表示されます。

17) ポート状態と役割が表示されます。
ポート状態は以下のどれかが表示されます。

Disabled STP は無効

Blocking Blocking 状態

Listening Listening 状態

Learning Learning 状態

Forwarding
Forwarding 状態

ポートの役割状態が以下のどれかが表示されます。

Root ルートポート

Designated
代表ポート

Blocking　ブロッキングポート

18) BPDU 送信回数
BPDU 送信回数 (すべてのタイプの BPDU の合計値) が表示されます。

19) 代表ブリッジポート識別子
代表ブリッジのポート識別子が表示されます。

20) 構成 BPDU の代表パスコスト
構成 BPDU の代表パスコストが表示されます。

21) 代表ブリッジ識別子
代表ブリッジ識別子 (優先度と MAC アドレス) が表示されます。

22) BPDU 受信回数
BPDU 受信回数 (すべてのタイプの BPDU の合計値) が表示されます。

46.4 スパニングツリーのカウンタ・ログ・統計のクリア

46.4.1 clear spanning-tree statistics

[機能]

スパニングツリー関連の統計情報クリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear spanning-tree statistics

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

スパニングツリー関連の統計情報をクリアします。

[実行例]

```
# clear spanning-tree statistics
#
```

第 47 章　MPLS のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

47.1 MPLS のカウンタ・ログ・統計・状態などの表示

47.1.1 show mpls

[機能]

MPLS インタフェース情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show mpls [interface <interface_name>]

[オプション]

なし

すべてのインタフェースの情報を表示します。

interface <interface_name>

指定したインタフェースの情報を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

MPLS のインタフェース情報を表示します。

[実行例]

以下に、実行例を示します。
MPLS を使用するすべてのインタフェースの統計情報を表示する場合 (オプションなし)

```
# show mpls
[Data for Interface Table]
I/F     USE
---     ---
(1)     (2)
lan0    Enabled
lan1    Disabled
rmt0    Enabled
```

特定のインタフェースの情報を表示する場合 (interface <interface_name>を指定)

```
# show mpls interface lan0
[Data for Interface Table]
I/F     USE
---     ---
(1)     (2)
lan0    Enabled
```

1) インタフェース名
2) MPLS の有効／無効

47.1.2　show mpls ftn

[機能]

MPLS FTN テーブル情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show mpls ftn [address <ip_address>[/<mask>]] [detail]

[オプション]

なし

すべての FTN テーブルの情報を表示します。

address <ip_address>/<mask>

指定した IPv4 ネットワークアドレスにマッチする FTN テーブルの情報を表示します。
<ip_address>/<mask>には、IPv4 アドレスとマスクビット数またはマスク値の組み合わせを指定します。
/<mask> を省略時は、ホストアドレスとみなします。

detail

FTN テーブルの情報を統計情報を含めて詳細表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

MPLS の FTN テーブル情報を表示します。

[実行例]

以下に、実行例を示します。
FTN テーブルのすべての情報を表示する場合 (オプションなし)

```
# show mpls ftn
[Data for FTN Table]
PREFIX              NH ADDR          OUT I/F      LABEL   OPCODE
------              -------          -------      ------  ------
 (1)                 (2)              (3)          (4)     (5)
100.232.1.0/24      100.232.2.1      rmt0         19      PUSH
192.168.3.0/24      192.168.5.1      lan1         18      PUSH
192.168.4.0/24      192.168.2.1      lan0         17      PUSH
```

FTN テーブルのすべての情報を統計情報を含めて表示する場合 (detail 指定時)

```
# show mpls ftn detail
[Data for FTN Table]
PREFIX              NH ADDR          OUT I/F      LABEL   OPCODE      PACKETS    OCTETS
------              -------          -------      -----   ------      -------    ------
 (1)                  (2)              (3)         (4)     (5)          (6)        (7)
100.232.1.0/24      100.232.2.1      rmt0         19      PUSH              0         0
192.168.3.0/24      192.168.5.1      lan1         18      PUSH             29      2162
192.168.4.0/24      192.168.2.1      lan0         17      PUSH              0         0
```

1) プレフィックス

ftn を指定した場合はプレフィックス順に表示します。

2) 次ホップアドレス

インタフェース経路は 0.0.0.0 と表示されます。

3) 出力インタフェース名

4) 出力ラベル (出力ラベル値がない場合は ‘-‘を表示)

5) ラベルオペレーションコード

以下のどれかが表示されます。

PUSH : プレフィックスに該当する IP パケットに出力ラベルを PUSH して出力インタフェース名のインタフェースに出力します。

DLVR-VPN :

プレフィックスに該当する IP パケットを出力インタフェース名のインタフェースにそのまま出力します。

6) エントリを使用して送出したパケット数

7) エントリを使用して送出したオクテット数

エントリが存在しない場合

```
# show mpls ftn
[Data for FTN Table]
No Entry.
```

47.1.3　show mpls ilm

[機能]

MPLS ILM テーブル情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show mpls ilm [address <ip_address>[/<mask>]] [detail]

[オプション]

なし

すべての ILM テーブルの情報を表示します。

address <ip_address>/<mask>

指定した IPv4 ネットワークアドレスにマッチする ILM テーブルの情報を表示します。
<address>/<mask>には、IPv4 アドレスとマスクビット数またはマスク値の組み合わせを指定します。
/<mask> を省略時は、ホストアドレスとみなします。

detail

ILM テーブルの情報を統計情報を含めて表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

MPLS の ILM テーブル情報を表示します。

[実行例]

以下に、実行例を示します。
ILM テーブルの情報を表示する場合 (オプションなし)

```
# show mpls ilm
[Data for ILM Table]
PREFIX              IN-LABEL  OUT-LABEL  NH ADDR          OUT I/F      OPCODE
------              --------  ---------  -------          -------      ------
 (1)                 (2)        (3)       (4)              (5)          (6)
192.168.4.0/24      17         -         192.168.3.1      lan1         POP
192.168.1.0/24      18         -         192.168.2.2      lan0         POP
```

ILM テーブルの情報を統計情報を含めて表示する場合 (detail 指定時)

```
# show mpls ilm detail
[Data for ILM Table]
PREFIX              IN-LABEL  OUT-LABEL  NH ADDR          OUT I/F  OPCODE    PACKETS    OCTETS
------              --------  ---------  -------          -------  ------    -------    ------
 (1)                 (2)        (3)       (4)              (5)      (6)       (7)        (8)
192.168.4.0/24      17         -         192.168.3.1      lan1     POP            0         0
192.168.1.0/24      18         -         192.168.2.2      lan0     POP          211     15613
```

1) プレフィックス
2) 入力ラベル
   ilm を指定した場合は入力ラベル順に表示します。

3) 出力ラベル (出力ラベル値がない場合は ‘-‘を表示)

4) 次ホップアドレス

インタフェース経路は 0.0.0.0 と表示されます。

5) 出力インタフェース名

6) ラベルオペレーションコード

以下のどれかが表示されます。

POP : 入力ラベルに該当する MPLS パケットからラベルを POP して出力インタフェース名のインタフェースに出力します。

SWAP : 入力ラベルに該当する MPLS パケットのラベルを出力ラベルに SWAP して出力インタフェース名のインタフェースに出力します。

POP-VPN :

入力ラベルに該当する MPLS パケットから VPN ラベルを POP して出力インタフェースの VRF インタフェースに出力します。

7) エントリを使用して送出したパケット数

8) エントリを使用して送出したオクテット数

エントリが存在しない場合

```
# show mpls ilm
[Data for ILM Table]
No Entry.
```

47.1.4　show mpls ldp

[機能]

LDP インタフェース情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show mpls ldp [interface <interface_name>] [detail]

[オプション]

なし

すべてのインタフェースの情報を表示します。

interface <interface_name>

指定したインタフェースの情報を表示します。

detail

インタフェースの情報を詳細に表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

LDP のインタフェース情報を表示します。

[実行例]

以下に、実行例を示します。
インタフェースの LDP 情報を表示する場合 (オプションなし)

```
# show mpls ldp
Name       LDP Identifier  Label-switching
----       -------------   ---------------
(1)              (2)           (3)
lan0       192.168.2.1:0   Enabled
lan1       192.168.2.1:0   Enabled
```

インタフェースの LDP 情報を表示する場合 (interface <interface_name>指定時)

```
# show mpls ldp interface lan1
Name       LDP Identifier  Label-switching
----       -------------   ---------------
(1)              (2)           (3)
lan1       192.168.2.1:0   Enabled
```

1) インタフェース名
2) LDP-ID(LDP ROUTER-ID:LABEL-SPACE)
3) MPLS の有効/無効

インタフェースの LDP 情報を表示する場合 (detail を指定した時)

```
#show mpls ldp detail
[Interface lan0]
Status                  : Enabled                  (1)
Primary IP Address      : 10.1.201.2               (2)
Interface Type          : Ethernet                 (3)
Hello Interval          : 5                        (4)
Hold Time               : 15                       (5)
Keepalive Interval      : 60                       (6)
Keepalive Timeout       : 180                      (7)
Advertisement Mode      : Downstream Unsolicited   (8)
Label Retention Mode    : Liberal                  (9)

[Interface lan1]
Status                  : Enabled                  (1)
Primary IP Address      : 10.1.202.2               (2)
Interface Type          : Ethernet                 (3)
Hello Interval          : 5                        (4)
Hold Time               : 15                       (5)
Keepalive Interval      : 60                       (6)
Keepalive Timeout       : 180                      (7)
Advertisement Mode      : Downstream Unsolicited   (8)
Label Retention Mode    : Liberal                  (9)
```

インタフェースの LDP 情報を表示する場合 (interface <interface_name> detail を指定した時)

```
# show mpls ldp interface lan0
Status                  : Enabled                  (1)
Primary IP Address      : 10.1.201.2               (2)
Interface Type          : Ethernet                 (3)
Hello Interval          : 5                        (4)
Hold Time               : 15                       (5)
Keepalive Interval      : 60                       (6)
Keepalive Timeout       : 180                      (7)
Advertisement Mode      : Downstream Unsolicited   (8)
Label Retention Mode    : Liberal                  (9)
```

1) LDP の動作状態
2) インタフェースの IP アドレス
3) インタフェース種別
   以下のどれかが表示されます。

   Ethernet :
   Ethernet MPLS mode

   ATM SHIM :
   RFC3031/3032 ATM MPLS mode

   PPP : PPP MPLS mode

4) Hello の送信インターバルの値 (秒)
5) Hello のホールドタイマーの値 (秒)
   ホールドタイマーが無限秒である場合は infinity と表示されます。
6) KeepAlive の送信インターバルの値 (秒)
7) KeepAlive タイムアウトの値 (秒)
8) ラベル広報モード (Advertise)
   以下のどれかが表示されます。

   Downstream Unsolicited :
   Downstream Unsolicited Label advertisement mode

Downstream on Demand :

Downstream on Demand Label advertisement mode

9) ラベル保持モード (Retention)

以下が表示されます。

Liberal : Liberal Label retention mode

Conservative :

Conservative Label retention mode

47.1.5 show mpls ldp adjacency

[機能]

LDP 近隣情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show mpls ldp adjacency

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

LDP の近隣関係に関する情報を表示します。

[実行例]

以下に実行例を示します。

```
# show mpls ldp adjacency
IP Address              Name  Holdtime        LDP ID
----------              ----  --------        ------
   (1)                   (2)   (3)             (4)
192.168.2.2             lan0  15              192.168.1.1:0
192.168.3.1             lan1  15              192.168.3.1:0
```

1) 近隣関係にある相手 LSR の IP アドレス
2) インタフェース名
3) Holdtime (秒)
4) 相手 LSR の LDP-ID(LDP ROUTER-ID:LABEL-SPACE)

47.1.6　show mpls ldp fec

[機能]

LDP FEC テーブル情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show mpls ldp fec

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

LDP FEC テーブル情報を表示します。

[実行例]

以下に実行例を示します。

```
# show mpls ldp fec
Codes  Prefix             Session            Out Label          Nexthop Addr
-----  ------             -------            ----------         ------------
  (1)    (2)                (3)                (4)                (5)
NL>    192.168.1.0/24     192.168.2.2        18                 192.168.2.2
E >    192.168.2.0/24     non-existent       none               none
E >    192.168.3.0/24     non-existent       none               none
NL>    192.168.4.0/24     192.168.3.1        23                 192.168.3.1

Total/MAX FEC Entries : 4 / 362
                        ---  ---
                        (6)  (7)
```

1) コード
以下のどれかが表示されます。

E :　この FEC の出口 (Egress)

N :　この FEC の出口ではない (Non-Egress)

L :　この FEC に対しラベルで受信

> :　この FEC に対しこのルートを使用

2) プレフィックス
3) LDP セッションの相手 LSR の IP アドレス
4) 出力ラベル
5) 次ホップアドレス
6) 現在 FEC 数の合計
7) 装置の最大 FEC 数

47.1.7 show mpls ldp session

[機能]

LDP セッション情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show mpls ldp session [address <ip_address>] [detail]

[オプション]

なし

すべての LDP セッションの情報を表示します。

address <ip_address>

指定した相手 LSR に関連した LDP セッションの情報を表示します。
<ip_address>には、相手 LSR を IPv4 アドレスで指定します。

detail

LDP セッションの情報を詳細に表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

LDP セッションに関する情報を表示します。

[実行例]

以下に実行例を示します。
LDP セッションの情報を表示する場合 (オプションなし)

```
# show mpls ldp session
IP Address      Name       Role    State           KeepAlive    Retention/Advertise
----------      ----       ----    -----           ---------    -------------------
  (1)            (2)       (3)      (4)            (5)          (6)
192.168.2.2      lan0      Passive OPERATIONAL     180          Liberal/DU
192.168.3.1      lan1      Active  OPERATIONAL     180          Conservative/DoD
```

LDP セッションの情報を表示する場合 (address <ip_address>指定時)

```
# show mpls ldp session address 192.168.3.1
IP Address      Name       Role    State           KeepAlive    Retention/Advertise
----------      ----       ----    -----           ---------    -------------------
  (1)            (2)       (3)      (4)            (5)          (6)
192.168.3.1      lan1      Active  OPERATIONAL     180          Conservative/DoD
```

1) LDP セッションを確立している相手 LSR の IP アドレス
2) インタフェース名
3) ロール
以下のどれかが表示されます。

Active :　アクティブロール

Passive :　パッシブロール

4) LDP セッションの状態
以下のどれかが表示されます。
NON_EXISTENT
INITIALIZED
OPENSENT
OPENREC
OPERATIONAL

5) KeepAlive タイムアウトの値 (秒)

6) ラベル保持モード /ラベル広報モード
ラベル保持モード (Retention)
以下のどれかが表示されます。

Liberal :　Liberal Label retention mode

Conservative :
Conservative Label retention mode

ラベル広報モード (Advertise)
以下のどれかが表示されます。

DU :　Downstream Unsolicited Label advertisement mode

DoD :　Downstream on Demand Label advertisement mode

LDP セッションの情報を表示する場合 (detail 指定時)

```
# show mpls ldp session detail
[Session peer address 10.1.201.1]
 Session state         : OPERATIONAL                                    (1)
 Session role          : Active                                         (2)
 TCP Connection        : Established                                    (3)
 IP Address for TCP    : 10.1.201.1                                     (4)
 Interface being used  : lan0                                           (5)
 Peer LDP ID           : 10.4.1.2:0                                     (6)
 Adjacencies           : 10.1.201.1                                     (7)
 Advertisement mode    : Downstream Unsolicited                         (8)
 Label retention mode  : Liberal                                        (9)
 Keepalive Timeout     : 180                                            (10)
 Reconnect Interval    : 15                                             (11)
 Address List received : 10.1.201.1                                     (12)
 Received Labels :       Fec             Label           Maps To        (13)
                 IPV4:10.0.0.6/32        19              16
                 IPV4:10.1.101.2/32      20              18
 Sent Labels :   Fec                     Label           Maps To        (14)
                 IPV4:10.0.0.6/32        16              19
                 IPV4:10.0.0.201/32      17              none
                 IPV4:10.1.101.2/32      18              20
                 IPV4:10.1.201.0/24      impl-null       none
                 IPV4:10.1.201.2/32      19              none
                 IPV4:192.168.201.0/24   impl-null       none

[Session peer address 10.1.202.1]
 Session state         : OPERATIONAL                                    (1)
 Session role          : Active                                         (2)
 TCP Connection        : Established                                    (3)
 IP Address for TCP    : 10.1.202.1                                     (4)
 Interface being used  : lan0                                           (5)
 Peer LDP ID           : 10.4.2.2:0                                     (6)
 Adjacencies           : 10.1.202.1                                     (7)
 Advertisement mode    : Downstream Unsolicited                         (8)
 Label retention mode  : Liberal                                        (9)
 Keepalive Timeout     : 180                                            (10)
 Reconnect Interval    : 15                                             (11)
 Address List received : 10.1.202.1                                     (12)
 Received Labels :       Fec             Label           Maps To        (13)
                 IPV4:10.0.0.9/32        19              16
                 IPV4:10.1.102.2/32      20              18
 Sent Labels :   Fec                     Label           Maps To        (14)
                 IPV4:10.0.0.9/32        16              19
                 IPV4:10.0.0.202/32      17              none
                 IPV4:10.1.102.2/32      18              20
                 IPV4:192.168.101.0/24   impl-null       none
```

LDP セッションの情報を表示する場合 (address <ip_address> detail 指定時)

```
# show mpls ldp session address 10.1.201.1 detail
 Session state         : OPERATIONAL                                    (1)
 Session role          : Active                                         (2)
 TCP Connection        : Established                                    (3)
 IP Address for TCP    : 10.1.201.1                                     (4)
 Interface being used  : lan0                                           (5)
 Peer LDP ID           : 10.4.1.2:0                                     (6)
 Adjacencies           : 10.1.201.1                                     (7)
 Advertisement mode    : Downstream Unsolicited                         (8)
 Label retention mode  : Liberal                                        (9)
 Keepalive Timeout     : 180                                            (10)
 Reconnect Interval    : 15                                             (11)
 Address List received : 10.1.201.1                                     (12)
 Received Labels :       Fec             Label           Maps To        (13)
                 IPV4:10.0.0.6/32        19              16
                 IPV4:10.1.101.2/32      20              18
 Sent Labels :   Fec                     Label           Maps To        (14)
                 IPV4:10.0.0.6/32        16              19
                 IPV4:10.0.0.201/32      17              none
                 IPV4:10.1.101.2/32      18              20
                 IPV4:10.1.201.0/24      impl-null       none
                 IPV4:10.1.201.2/32      19              none
                 IPV4:192.168.201.0/24   impl-null       none
```

1) LDP セッションの状態
以下のどれかが表示されます。
NON_EXISTENT
INITIALIZED
OPENSENT
OPENREC
OPERATIONAL

2) ロール
以下のどれかが表示されます。

Active :　アクティブロール

Passive :　パッシブロール

3) TCP コネクションの状態
以下のどれかが表示されます。
Established
Not Established

4) TCP で使用する相手 LSR の IP アドレス

5) インタフェース名

6) 相手 LSR の LDP-ID(LDP ROUTER-ID:LABEL-SPACE)

7) 近隣関係にある相手 LSR の IP アドレス

8) ラベル広報モード (Advertise)
以下のどれかが表示されます。

Downstream Unsolicited :
Downstream Unsolicited Label advertisement mode

Downstream on Demand :
Downstream on Demand Label advertisement mode

9) ラベル保持モード (Retention)
以下が表示されます。

Liberal :　Liberal Label retention mode

Conservative :
Conservative Label retention mode

10) KeepAlive タイムアウトの値 (秒)

11) 再接続のインターバルの値 (秒)

12) 受信した Address List の値

13) セッションで受信した FEC とラベル値とラベルマッピングしたラベル値

14) セッションで送信した FEC とラベル値とラベルマッピングしたラベル値

47.1.8 show mpls ldp summary

[機能]

LDP の状態の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show mpls ldp summary

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

LDP の状態を表示します。

[実行例]

以下に実行例を示します。

```
# show mpls ldp summary
Router ID                : 10.1.201.2                                (1)
LDP Version              : 1                                         (2)
Label Control Mode       : Independent                               (3)
Request Retry            : On                                        (4)
Transport Address data   : 10.1.201.2 (platform wide)                (5)
Import routes            : connected, RIP, OSPF                      (6)
```

1) 装置の ROUTER-ID

2) LDP のバージョン (常に 1)

3) LDP 配布制御方式
以下のどれかが表示されます。

Independent :

Independent Label Distribution Control

Ordered :

Ordered Label Distribution Control

4) Label Request の再送 (常に On)

5) トランスポートアド レス

6) 経路の使用の有無
以下のどれかが 1 つ以上表示されます。

connected :

connected 経路を用いてラベル広報を行う

static :　static 経路を用いてラベル広報を行う

RIP :　RIP 経路を用いてラベル広報を行う

OSPF :　OSPF 経路を用いてラベル広報を行う

BGP :　BGP 経路を用いてラベル広報を行う

none :　経路を用いてラベル広報を行いません

47.1.9 show mpls ldp vc

[機能]

LDP VC 情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show mpls ldp vc

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

LDP VC に関する情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show mpls ldp vc
Transport Client     VC     VC       Local       Remote      Destination
VC ID     I/F        State  Type     VC Label    VC Label    Address
--------  ----       ----   -----    ---------   ---------   -----------
 (1)      (2)       (3)     (4)        (5)         (6)          (7)
1         lan1       UP     ethernet 16          17          10.1.201.2
2         lan2       UP     ethernet 17          18          10.1.201.2
```

1) VC ID
2) VC インタフェース名
3) VC の状態
   以下のどれかが表示されます。

   UP : VC インタフェース UP

   DOWN : VC インタフェース DOWN

4) VC Type
   VC ラベル交換に使用したインタフェースの種類を表示します。
   以下のどれかが表示されます。

   ethernet : Ethernet

   vlan : Ethernet VLAN

5) 自側 VC ラベル (受信用)
6) 相手側 VC ラベル (送信用)
7) VC 相手の IP アドレス

47.1.10　show mpls statistics

[機能]

MPLS インタフェース統計情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show mpls statistics [interface <interface_name>]

[オプション]

なし

すべてのインタフェースの統計情報を表示します。

interface <interface_name>

指定したインタフェースの統計情報を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

MPLS のインタフェース統計情報を表示します。

[実行例]

以下に、実行例を示します。
インタフェースの統計情報を表示する場合 (オプションなし)

```
# show mpls statistics
[Data for Interface Table]
I/F     USE      IN-PACKET  OUT-PACKET   Error (   TTL  LABEL  SHORT  ENTRY)
---     ---      ---------  ----------   -----     ---  -----  ----- ------
(1)     (2)         (3)        (4)        (5)      (6)   (7)    (8)    (9)
lan0    Enabled      11136       11123      13 (     6      4      0      8)
lan1    Disabled         0           0       0 (     0      0      0      0)
rmt0    Enabled      28748       98983      16 (     2      4      6      3)
```

インタフェースの統計情報を表示する場合 (interface <interface_name>指定時)

```
# show mpls statistics interface lan0
[Data for Interface Table]
I/F     USE      IN-PACKET  OUT-PACKET   Error (   TTL  LABEL  SHORT  ENTRY)
---     ---      ---------  ----------   -----     ---  -----  ----- ------
(1)     (2)         (3)        (4)        (5)      (6)   (7)    (8)    (9)
lan0    Enabled      11136       11123      13 (     6      4      0      8)
```

1) インタフェース名
2) MPLS の有効／無効
3) 入力 MPLS パケット数
4) 出力 MPLS パケット数
5) エラー破棄パケット総数

6) TTL Expire 検出数

7) 不正ラベル検出数

8) 不正長のパケット検出数

9) ILM 未登録検出数

47.1.11　show mpls summary

[機能]

MPLS の状態の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show mpls summary

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

MPLS の状態を表示します。

[実行例]

以下に、実行例を示します。

```
# show mpls summary
[Status of MPLS Forwarder]
MPLS Forwarder           : Enabled          (1)
Number of Interface      : 2                (2)
Number of Entry          :
  FTN                    : 6                (3)
  ILM                    : 8                (4)
  VRF                    : 2                (5)
IP Propagate TTL         : Off              (6)
```

1) MPLS の有効／無効
   Enabled の場合に有効、Disabled の場合に無効であることを表します。
2) インタフェース数
   MPLS で使用するインタフェース数を表示します。
3) FTN エントリ数
   MPLS 中の FTN のエントリ数を表示します。
4) ILM エントリ数
   MPLS 中の ILM のエントリ数を表示します。
5) VRF エントリ数
   MPLS 中の VRF のエントリ数を表示します。
6) TTL 継承動作
   On の場合に継承する、Off の場合に継承しないことを表します。

47.1.12 show mpls vc

[機能]

MPLS VC テーブル情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show mpls vc [detail]
show mpls vc vcid <vc_id> [detail]
show mpls vc interface <interface_name> [detail]

[オプション]

なし

すべての VC 情報を表示します。

vcid <vc_id>

指定した VC ID の VC 情報を表示します。

interface <interface_name>

指定したインタフェースの VC 情報を表示します。

detail

VC 情報を詳細に表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

MPLS の VC テーブル情報を表示します。

[実行例]

以下に、実行例を示します。
すべての VC 情報を表示する場合 (オプションなし)

```
# show mpls vc
[Data for VC]

VC I/F  VC ID    NH ADDR          OUT I/F       OUTLABEL  INLABEL
------  -------  ---------------  -----------   --------  --------
 (1)     (2)         (3)             (4)          (5)      (6)
lan1    1        10.56.11.21      16/lan0       21        22
lan2    2        10.56.11.21      16/lan0       22        23
```

1) VC インタフェース名
2) VC 識別子
3) 次ホップアドレス
   インタフェース経路は 0.0.0.0 と表示されます。

4) 出力インタフェース名

LSP に送出する場合は LSP ラベル/インタフェース名 の形式で、それ以外の場合はインタフェース名だけ表示されます。

5) 出力ラベル

VC LSP が確立できていなく、出力ラベルが存在しない場合は N/A と表示されます。

6) 入力ラベル

VC LSP が確立できていなく、入力ラベルが存在しない場合は N/A と表示されます。

すべての VC 情報を詳細に表示する場合 (detail 指定時)

```
# show mpls vc detail
[Data for VC]
VC Interface             : lan1              (1)
Virtual Circuit ID       : 1                 (2)
In Label                 : 22                (3)
Nexthop Address          : 10.56.11.21       (4)
Out Interface            : 16/lan0           (5)
Out Label                : 21                (6)
PACKET RESULT            :
  in packet              : 450               (7)
  in octet               : 17622             (8)
  out packet             : 28                (9)
  out octet              : 2134              (10)

[Data for VC]
VC Interface             : lan2              (1)
Virtual Circuit ID       : 2                 (2)
In Label                 : 23                (3)
Nexthop Address          : 10.56.11.21       (4)
Out Interface            : 16/lan0           (5)
Out Label                : 22                (6)
PACKET RESULT            :
  in packet              : 221               (7)
  in octet               : 8166              (8)
  out packet             : 455               (9)
  out octet              : 16521             (10)
```

1) VC 識別子

2) VC インタフェース名

3) 入力ラベル

VC LSP が確立できていなく、入力ラベルが存在しない場合は N/A と表示されます。

4) 次ホップアドレス

インタフェース経路は 0.0.0.0 と表示されます。

5) 出力インタフェース名

LSP に送出する場合は LSP ラベル/インタフェース名 の形式で、それ以外の場合はインタフェース名だけ表示されます。

6) 出力ラベル

VC LSP が確立できていなく、出力ラベルが存在しない場合は N/A と表示されます。

7) VC で受信したパケット数

8) VC で受信したオクテット数

9) VC で送出したパケット数

10) VC で送出したオクテット数

47.1.13 show mpls vrf

[機能]

MPLS VRF テーブル情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show mpls vrf [vrf <vrf_number>] [address <ip_address>[/<mask>]] [detail]

[オプション]

なし

すべての VRF 定義番号のすべての VRF テーブルの情報を表示します。

vrf <vrf_number>

指定した VRF 定義番号の VRF テーブルの情報を表示します。

address <ip_address>/<mask>

指定した IPv4 ネットワークアドレスにマッチする VRF テーブルの情報を表示します。
<ip_address>/<mask>には、IPv4 アドレスとマスクビット数またはマスク値の組み合わせを指定します。

detail

VRF テーブルの情報を統計情報を含めて表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

MPLS の VRF テーブル情報を表示します。

[実行例]

以下に、実行例を示します。
すべての VRF テーブルの情報を表示する場合 (オプションなし)

```
# show mpls vrf
[Data for VRF Table # 2 ]
                     ---
                     (1)
PREFIX               NH ADDR          OUT I/F      LABEL   OPCODE
------               -------          -------      ------  ------
 (2)                  (3)              (4)          (5)     (6)
192.168.100.0/24     10.56.11.21      16/lan0      21      PUSH-VPN
192.168.130.0/24     10.56.11.77      17/lan0      22      PUSH-VPN
192.168.160.0/24     192.168.2.1      lan1         -       DLVR-VPN
                                            :
[Data for VRF Table # 1 ]
PREFIX               NH ADDR          OUT I/F      LABEL   OPCODE
192.168.4.0/24       192.168.2.1      lan0         17      PUSH
192.168.120.0/24     10.56.11.21      16/lan0      25      PUSH-VPN
```

すべての VRF テーブルの情報を詳細に表示する場合 (detail 指定時)

```
# show mpls vrf detail
[Data for VRF Table # 2 ]
                      ---
                      (1)
PREFIX              NH ADDR          OUT I/F      LABEL   OPCODE      PACKETS    OCTETS
------              -------          -------      ------  ------      -------    ------
 (2)                 (3)              (4)          (5)     (6)          (7)        (8)
192.168.100.0/24    10.56.11.21      16/lan0      21      PUSH-VPN         13      1104
192.168.130.0/24    10.56.11.77      17/lan0      22      PUSH-VPN         26      2006
192.168.160.0/24    192.168.2.1      lan1         -       DLVR-VPN          0         0
                                          :
[Data for VRF Table # 1 ]
PREFIX              NH ADDR          OUT I/F      LABEL   OPCODE      PACKETS    OCTETS
192.168.4.0/24      192.168.2.1      lan0         17      PUSH              0         0
192.168.120.0/24    10.56.11.21      16/lan0      25      PUSH-VPN          0         0
```

1) VRF 定義番号

2) プレフィックス

vrf を指定した場合はプレフィックス順に表示します。

3) 次ホップアドレス

インタフェース経路は 0.0.0.0 と表示されます。

4) 出力インタフェース名

LSP に送出する場合は LSP ラベル/インタフェース名 の形式で、それ以外の場合はインタフェース名だけ表示されます。

5) 出力ラベル (出力ラベル値がない場合は ‘-‘を表示)

6) ラベルオペレーションコード

以下のどれかが表示されます。

PUSH : プレフィックスに該当する IP パケットに出力ラベルを PUSH して出力インタフェース名のインタフェースに出力します。

PUSH-VPN :

プレフィックスに該当する IP パケットに VPN ラベルを PUSH して次ホップアドレスに該当する FTN エントリを再検索し、FTN エントリの内容に従って出力します。

DLVR-VPN :

プレフィックスに該当する IP パケットを出力インタフェース名のインタフェースにそのまま出力します。

7) エントリを使用して送出したパケット数

8) エントリを使用して送出したオクテット数

エントリが存在しない場合

```
# show mpls vrf
[Data for VRF Table # 2 ]
No Entry.
                                          :
[Data for VRF Table # 1 ]
No Entry.
```

47.2 MPLS のカウンタ・ログ・統計などのクリア

47.2.1 clear mpls statistics

[機能]

MPLS インタフェース統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear mpls statistics [interface <interface_name>]

[オプション]

なし

すべてのインタフェースの統計情報をクリアします。

interface <interface_name>

指定したインタフェースの統計情報をクリアします。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

MPLS インタフェース統計情報をクリアします。

[実行例]

```
# clear mpls statistics
#
```

47.2.2　clear mpls statistics ftn

[機能]

MPLS FTN テーブル統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear mpls statistics ftn [address <ip_address>[/<mask>]]

[オプション]

なし

すべての FTN テーブルの統計情報をクリアします。

address <ip_address>/<mask>

指定した IPv4 ネットワークアドレスにマッチする FTN テーブルの統計情報をクリアします。
<ip_address>/<mask>には、IPv4 アドレスとマスクビット数またはマスク値の組み合わせを指定します。
/<mask> を省略時は、ホストアドレスとみなします。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

MPLS FTN テーブル情報の中の統計情報をクリアします。

[実行例]

```
# clear mpls statistics ftn
#
```

47.2.3 clear mpls statistics ilm

[機能]

MPLS ILM テーブル統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear mpls statistics ilm [address <ip_address>[/<mask>]]

[オプション]

なし

すべての ILM テーブルの統計情報をクリアします。

address <ip_address>/<mask>

指定した IPv4 ネットワークアドレスにマッチする ILM テーブルの統計情報をクリアします。
<ip_address>/<mask>には、IPv4 アドレスとマスクビット数またはマスク値の組み合わせを指定します。
/<mask> を省略時は、ホストアドレスとみなします。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

MPLS ILM テーブル情報の中の統計情報をクリアします。

[実行例]

```
# clear mpls statistics ilm
#
```

47.2.4　clear mpls statistics vc

[機能]

MPLS VC テーブル統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear mpls statistics vc
clear mpls statistics vc vcid <vc_id>
clear mpls statistics vc interface <interface_name>

[オプション]

なし

すべての VC 統計情報をクリアします。

vcid <vc_id>

指定した VC ID の VC 統計情報をクリアします。

interface <interface_name>

指定したインタフェースの VC 統計情報をクリアします。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

MPLS VC テーブル情報の中の統計情報をクリアします。

[実行例]

```
# clear mpls statistics vc
#
```

47.2.5 clear mpls statistics vrf

[機能]

MPLS VRF テーブル統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear mpls statistics vrf [vrf <vrf_number>] [address <ip_address>[/<mask>]]

[オプション]

なし

すべての VRF 定義番号のすべての VRF テーブルの統計情報をクリアします。

vrf <vrf_number>

指定した VRF 定義番号の VRF テーブルの統計情報をクリアします。

address <ip_address>/<mask>

指定した IPv4 ネットワークアドレスにマッチする VRF テーブルの統計情報をクリアします。
<ip_address>/<mask>には、IPv4 アドレスとマスクビット数
またはマスク値の組み合わせを指定します。
/<mask> を省略時は、ホストアドレスとみなします。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

MPLS VRF テーブル情報の中の統計情報をクリアします。

[実行例]

```
# clear mpls statistics vrf
#
```

第 48 章　MAC アドレス認証のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

48.1 MAC アドレス認証のカウンタ・ログ・統計・状態などの表示

48.1.1 show macauth

[機能]

MAC アドレス認証管理テーブルの表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show macauth [interface <interface_name>]

[オプション]

なし

すべてのインタフェースの MAC アドレス認証管理テーブルを表示します。

interface <interface_name>

指定したインタフェースの MAC アドレス認証管理テーブルを表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

MAC アドレス認証結果を保持する、MAC アドレス認証管理テーブルの情報を表示します。
MAC アドレス認証管理テーブルは、認証結果保持時間のあいだ有効であり、保持時間を経過すると認証結果にかかわらず破棄されます。

[実行例]

以下に、実行例を示します。

```
# show macauth interface lan0
[lan0]
total table entry     : 6
                       ---(1)
success state entry   : 2
                       ---(2)
no table count        : 0
                       ---(3)
no memory count       : 0
                       ---(4)

MAC address             aaa   auth_state   remain_time      discard
-----------------------------------------------------------------------
00:00:0e:00:00:00         1   success      0000.00:10:29    0
-----------------(5)    --(6) -------(7)   -------------(8) --(9)
00:00:0e:00:00:01         1   success      0000.00:04:38    0
00:00:0e:00:00:02         1   success      0000.00:10:42    0
00:00:0e:00:00:03         1   failure      0000.00:02:11    1234567890
00:00:0e:00:00:04         1   auth...      0000.00:00:00    3
00:00:0e:00:00:05         1   error        0000.00:00:00    0

#
```

(1) total table entry

MAC アドレス認証管理テーブル数。

(2) success state entry

認証成功状態の MAC アドレス認証管理テーブル数。

(3) no table count

MAC アドレス認証管理テーブル不足発生回数。

(4) no memory count

メモリ資源不足発生回数。

(5) MAC address

MAC アドレス認証管理テーブルに登録されている MAC アドレス。

(6) aaa

認証先データベースのグループ ID。

(7) auth_state

MAC アドレス認証管理テーブルで管理される MAC アドレス認証状態。

```
auth...         認証中
success         認証成功
failure         認証失敗
error           認証エラー(lan macauth security normal指定でパケット通過)
```

(8) remain_time

認証結果保持残り時間。

(9) discard

MAC アドレス認証管理テーブル保持中に破棄したパケット数。

48.2 MAC アドレス認証のカウンタ・ログ・統計などのクリア

48.2.1 clear macauth statistics

[機能]

MAC アドレス認証管理テーブルの統計情報クリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear macauth statistics

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

MAC アドレス認証管理テーブルで保持する統計情報をクリアします。

[実行例]

以下に、実行例を示します。

```
# clear macauth statistics
#
```

第 49 章　SNMP 統計情報の表示、クリア操作コマンド

49.1 SNMP 統計情報の表示

49.1.1 show snmp statistics

[機能]

SNMP 機能の統計情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show snmp statistics

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

SNMP の統計情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show snmp statistics
SNMP statistics information:
           0 Input Packets                                --- (1)
           0 Output Packets                               --- (2)
           0 Input Bad Versions                           --- (3)
           0 Input Bad Community Names                    --- (4)
           0 Input Bad Community Uses                     --- (5)
           0 Input ASN Parse Errors                       --- (6)
           0 Input Too Bigs                               --- (7)
           0 Input No Such Names                          --- (8)
           0 Input Bad Values                             --- (9)
           0 Input Read Only                              --- (10)
           0 Input Gen Errors                             --- (11)
           0 Input Total Request Vars                     --- (12)
           0 Input Total Set Vars                         --- (13)
           0 Input Get Requests                           --- (14)
           0 Input Get Next                               --- (15)
           0 Input Set Requests                           --- (16)
           0 Input Get Responses                          --- (17)
           0 Input Traps                                  --- (18)
           0 Output Too Bigs                              --- (19)
           0 Output No Such Names                         --- (20)
           0 Output Bad Values                            --- (21)
           0 Output Gen Errors                            --- (22)
           0 Output Get Requests                          --- (23)
           0 Output Get Next                              --- (24)
           0 Output Set Requests                          --- (25)
           0 Output Get Responses                         --- (26)
           0 Output Traps                                 --- (27)
#
```

1) SNMP 受信メッセージの総数

2) SNMP 送信メッセージの総数
3) 未サポート SNMP メッセージ受信の総数
4) 未使用コミュニティの SNMP 受信メッセージの総数
5) コミュニティでは許されていないオペレーションを示す受信メッセージの総数
6) ASN.1 エラーの受信メッセージの総数
7) エラーステータスが tooBig の受信 PDU の総数
8) エラーステータスが noSuchName の受信 PDU の総数
9) エラーステータスが badValue の受信 PDU の総数
10) エラーステータスが readOnly の受信 PDU の総数
11) エラーステータスが genErr の受信 PDU の総数
12) MIB の収集が成功した MIB オブジェクトの総数
13) MIB の設定が成功した MIB オブジェクトの総数
14) 受信した GetRequestPDU の総数
15) 受信した GetNextRequestPDU の総数
16) 受信した SetRequestPDU の総数
17) 受信した GetResponsePDU の総数
18) 受信したトラップ PDU の総数
19) エラーステータスが tooBig の送信 PDU の総数
20) エラーステータスが noSuchName の送信 PDU の総数
21) エラーステータスが badValue の送信 PDU の総数
22) エラーステータスが genErr の送信 PDU の総数
23) 送信した GetRequestPDU の総数
24) 送信した GetNextRequestPDU の総数
25) 送信した SetRequestPDU の総数
26) 送信した GetResponsePDU の総数
27) 送信したトラップ PDU の総数

49.2 SNMP 統計などのクリア

49.2.1 clear snmp statistics

[機能]

SNMP 統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear snmp statistics

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

SNMP の統計情報をクリアします。

[実行例]

```
# clear snmp statistics
#
```

第 50 章　NETTIME(time/sntp) サーバ、クライアントの統計情報表示、クリア操作コマンド

50.1 NETTIME(time/sntp) 統計情報の表示

50.1.1 show nettime statistics

[機能]

NETTIME(time/sntp) 機能の統計情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show nettime statistics [<mode> [<protocol>]]

[オプション]

なし

稼働しているすべての情報を表示します。

<mode>

表示するモードを指定します。

- server
  サーバ機能 (時刻情報提供側) の情報を表示します。
- client
  クライアント機能 (時刻情報取得側) の情報を表示します。

<protocol>

表示するプロトコルを指定します。

- time
  TIME プロトコルの情報を表示します。
- sntp
  簡易 NTP プロトコルの情報を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

NETTIME(time/sntp) の統計情報を表示します。

[実行例]

以下に、各オプションごとの実行例を示します。

<mode> <protocol>

稼動している指定したモードのプロトコルのみ表示します。

```
# show nettime statistics client time
NETTIME client statistics information:
[time tcp]
           0 request transmission error
           0 transmitted synchronized request
           0 received response
           0   received invalid packet
           0     received clock not synchronized
           0 local clock updated
[time tcp6]
           0 request transmission error
           0 transmitted synchronized request
           0 received response
           0   received invalid packet
           0     received clock not synchronized
           0 local clock updated
#
```

オプションなし

オプションなしの場合は、本装置にて稼働しているすべての NETTIME 情報を表示します。

```
# show nettime statistics
NETTIME server statistics information:
 [sntp udp]
           0 received synchronized request                   --- (1)
           0   received invalid packet                       --- (2)
           0 request discard (clock not synchronized)        --- (3)
           0 response transmission error                     --- (4)
           0 transmitted response                            --- (5)
 [sntp udp6]
           0 received synchronized request
           0   received invalid packet
           0 request discard (clock not synchronized)
           0 response transmission error
           0 transmitted response
 [time tcp]
           0 received synchronized request
           0   received invalid packet
           0 request discard (clock not synchronized)
           0 response transmission error
           0 transmitted response
 [time udp]
           0 received synchronized request
           0   received invalid packet
           0 request discard (clock not synchronized)
           0 response transmission error
           0 transmitted response
 [time tcp6]
           0 received synchronized request
           0   received invalid packet
           0 request discard (clock not synchronized)
           0 response transmission error
           0 transmitted response
 [time udp6]
           0 received synchronized request
           0   received invalid packet
           0 request discard (clock not synchronized)
           0 response transmission error
           0 transmitted response
NETTIME client statistics information:
 [sntp udp]
           0 request transmission error                      --- (6)
           0 transmitted synchronized request                --- (7)
           0 received response                               --- (8)
           0   received invalid packet                       --- (9)
           0     received clock not synchronized             --- (10)
           0 local clock updated                             --- (11)
 [sntp udp6]
           0 request transmission error
           0 transmitted synchronized request
           0 received response
           0   received invalid packet
           0     received clock not synchronized
           0 local clock updated
#
```

- server

1) 時刻同期要求パケットを受信した総数

2) 1) の内時刻同期要求パケットが不正であった総数

3) 本装置が時刻同期していないために時刻同期要求を破棄した総数

4) 応答送信に失敗した総数

5) 応答を送信した総数

- client

6) 時刻同期要求パケット送信に失敗した総数

7) 時刻同期要求パケットを送信した総数

8) サーバからの応答を受信した総数

9) 8) の内応答パケットが不正であった総数

10) 9) の内サーバ側の時刻が同期していないために応答が無効となった総数

11) 応答により本装置の時刻を更新した総数

50.2 NETTIME(time/sntp) 統計などのクリア

50.2.1 clear nettime statistics

[機能]

NETTIME(time/sntp) 統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear nettime statistics [<mode>]

[オプション]

なし

すべての NETTIME(time/sntp) 統計情報をクリアします。

<mode>

クリアするモードを指定します。

- server
  サーバ機能の統計情報をクリアします。
- client
  クライアント機能の統計情報をクリアします。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

NETTIME(time/sntp) の統計情報をクリアします。

[実行例]

```
# clear nettime statistics
#
```

第 51 章　UPnP のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

51.1 UPnP のカウンタ・ログ・統計・状態などの表示、クリア

51.1.1 show upnp

[機能]

UPnP 状態情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show upnp

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

UPnP 変数名と現在値を表示します。

[実行例]

```
# show upnp

UPnP external interface : lan0                                          (1)

UPnP variable name:          Value                                      (2)
DefaultConnectionService
WANAccessType                Ethernet
Layer1UpstreamMaxBitRate     100000000
Layer1DownstreamMaxBitRate   100000000
PhysicalLinkStatus           Up
ConnectionType               IP_ROUTED
PossibleConnectionTypes      IP_ROUTED
ConnectionStatus             Connected
Uptime                       1234
LastConnectionError          ERROR_NONE
RSIPAvailable                FALSE
NATEnabled                   TRUE
ExternalIPAddress            123.45.67.89
PortMappingNumberOfEntries   3
PortMappingEnabled           TRUE
#
```

1) 外部インタフェース名

2) UPnP 変数名、現在値

DefaultConnectionService

初期値は空白 (UPnP クライアントが設定)

WANAccessType

常に Ethernet

Layer1UpstreamMaxBitRate

上り回線速度 (bps)

Layer1DownstreamMaxBitRate

下り回線速度

PhysicalLinkStatus

物理リンク状態 (Up:接続、Down:切断)

ConnectionType

常に IP_ROUTED

PossibleConnectionTypes

常に IP_ROUTED

ConnectionStatus

接続状態 (Connected:接続、Disconnected:切断)

Uptime　接続経過時間 (秒)

LastConnectionError

接続異常要因

RSIPAvailable

常に FALSE

NATEnabled

常に TRUE

ExternalIPAddress

外部 IP アドレス

PortMappingNumberOfEntries

ポートマッピング登録数 (※)

PortMappingEnabled

常に TRUE

51.1.2 show upnp statistics

[機能]

UPnP 統計情報情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show upnp statistics

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

UPnP 制御名と UPnP クライアントからの要求回数を表示します。

[実行例]

```
# show upnp statistics

UPnP action name:            Requested count                              (1)
SetDefaultConnectionService  0
GetDefaultConnectionService  0
GetCommonLinkProperties      0
SetConnectionType            0
GetConnectionTypeInfo        0
RequestConnection            0
ForceTermination             0
GetStatusInfo                1
GetNATRSIPStatus             1
GetGenericPortMappingEntry   0
GetSpecificPortMappingEntry  0
AddPortMapping               4
DeletePortMapping            4
GetExternalIPAddress         7
#
```

1) UPnP 制御名、UPnP クライアントからの要求回数

SetDefaultConnectionService

DefaultConnectionService 設定

GetDefaultConnectionService

DefaultConnectionService 取得

GetCommonLinkProperties

WANAccessType,Layer1Up/DownstreamMaxBitRate,PhysicalLinkStatus 取得

SetConnectionType

ConnectionType 設定

GetConnectionTypeInfo

ConnectionType,PossibleConnectionTypes 取得

RequestConnection

接続要求 (非サポート)

ForceTermination

切断要求 (非サポート)

GetStatusInfo

ConnectionStatus,LastConnectionError,Uptime 取得

GetNATRSIPStatus

NATRSIPAvailable,NATEnabled 取得

GetGenericPortMappingEntry

PortMapping 取得 (番号指定)

GetSpecificPortMappingEntry

PortMapping 取得 (条件指定)

AddPortMapping

PortMapping 登録 (※)

DeletePortMapping

PortMapping 削除 (※)

GetExternalIPAddress

ExternalIPAddress 取得

※ AddPortMapping と DeletePortMapping の差が PortMappingNumberOfEntries の数になるとは限りません。同じ内容を再登録したり、存在しない内容を削除することがあるためです。

51.1.3 show upnp portmapping

[機能]

UPnP ポートマッピング情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show upnp portmapping

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

UPnP クライアントによって設定されたポートマッピング情報を表示します。

[実行例]

```
# show upnp portmapping

Number of UPnP portmappings : 3                                          (1)

date  time     external      internal     protocol lease description
(2)               (3)          (4)            (5)   (6) (7)
09/20 17:35:18 0.0.0.0:5091  192.168.0.2:5091  UDP     0 VoIP (192.168.0.2:5091)
09/20 17:35:20 0.0.0.0:5090  192.168.0.2:5090  UDP     0 VoIP (192.168.0.2:5090)
09/20 17:35:22 0.0.0.0:5060  192.168.0.2:5060  UDP     0 VoIP (192.168.0.2:5060)
#
```

1) ポートマッピング数
2) 作成日時
3) 外部アドレス:外部ポート
4) 内部アドレス:内部ポート
5) プロトコル種別 (TCP か UDP)
6) 有効期間 (秒)
7) 説明

51.1.4　clear upnp statistics

[機能]

UPnP 統計情報のクリア

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear upnp statistics

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

UPnP 統計情報をクリアします。

[実行例]

```
# clear upnp statistics
#
```

51.1.5 clear upnp portmapping

[機能]

UPnP ポートマッピングエントリの削除

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear upnp portmapping

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

UPnP クライアントが設定したポートマッピングエントリをすべて削除します。
ポートマッピングを設定した UPnP クライアントが動作している場合、UPnP クライアントを再起動する必要があります。

[実行例]

```
# clear upnp portmapping
#
```

第 52 章　ポリシーグループの状態の表示コマンド

52.1 ポリシーグループの状態の表示

52.1.1 show policy-group

[機能]

ポリシーグループ情報表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show policy-group [policy <policy-group_number>]

[オプション]

なし

すべてのポリシーグループ情報を表示します。

<policy-group_number>

- ポリシーグループ番号
  表示するポリシーグループ番号を、10 進数値で指定します。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B Si-R220B
0〜49	Si-R180

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

ポリシーグループについての情報を表示します。

[注意]

policy-group 情報が何も設定されていないポリシーグループ情報は表示しません。

[実行例]

以下に、実行例を示します。

```
# show policy-group
    group_number  out_interface   status         since
    [    0]       lan0            up             Jun 26 10:52:46 2006
       (1)        (2)             (4)          (5)
    [    1]       lan2            watch failed   Feb 11 11:22:16 2006
    [    3]       rmt5            inactive       -
    [    4]       lan5            force-down     Jun 22 20:18:33 2006
# show policy-group policy 3
    group_number  out_interface   status         since
    [    3]       rmt5            inactive       -
# show policy-group policy 5
#
```

1) ポリシールールグループ番号

2) 転送先インタフェース

3) 転送先 nexthop(IPv4)

4) 転送先状態

up　利用可能

force-down

閉塞中

watch failed

監視失敗

inactive　構成定義不備

down　送出先回線ダウン

5) 状態遷移時刻

「status」が現在の状態に変化した時刻を表示します。

ただし、「status」が「inactive」「down」の場合は表示しません。

第 53 章　SSH ホスト認証用公開鍵の表示コマンド

53.1　SSH ホスト認証用公開鍵の表示

53.1.1　show ssh server key

[機能]

SSH ホスト認証用公開鍵の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show ssh server key {dsa|rsa}

[オプション]

dsa

本装置の SSH ホスト認証用 DSA 公開鍵を表示します。

rsa

本装置の SSH ホスト認証用 RSA 公開鍵を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

本装置の SSH ホスト認証用公開鍵を表示します。
SSH プロトコルバージョン 2(SSH2) のホスト認証で使用されます。
SSH ホスト認証には DSA 公開鍵暗号方式または RSA 公開鍵暗号方式が使用され、どちらの公開鍵を表示するかを指定してください。
あらかじめ ssh クライアントまたは sftp クライアントにホスト認証用公開鍵を設定しておく必要がある場合に、本コマンドで表示された内容を設定してください。

[注意]

serverinfo ssh コマンドおよび serverinfo sftp コマンドで SSH 関連機能をすべて無効にしてある場合は、SSH ホスト認証用公開鍵が生成されていないため、何も表示されません。
ただし、一度有効にしたあとに無効にした場合は、SSH ホスト認証用公開鍵が生成されているため表示されます。

[実行例]

・DSA 公開鍵を表示する場合

```
# show ssh server key dsa
ssh-dss AzaCJB5CpVUXI1LXjzNVo1kt/LHGhWlOleJQDj11tGeeAAAFKoNjMatP
i8JWtZhrgldtxVVmBAIAB3Nc3MAAAAAkgFa0nu7HMPdQAAAIA4sIwVzNfTpxNtjJ
Qx1gJHrDjybKeBMmpnJ/RtGTJfvZW5T/aDc/aoB7PdF+appeXx9U8FsQF+EaMNfq
P3lK2u3XAEoAzLa0JQCo6VjoDQh15YIzKFo2AVaK4lCeS3q81q8A4+jttJ0Dt0U0
rVucQoOq+BdIgaCMDuaqmJQAotGvZvZQ/RMTSh6pMh+z9DdB1DLnPNxEyt61Sftz
Vk+rjgZ29In2V7ai4yuOfIhNL61ybOrrfoZ9YQW4P9rJuDxhvn2xvZQ/RMTSh6pM
6WIwA9mlzAst/YBxbb9JcO7uPVhN8M624q8yKsQaMClW1AAAWOO+ZkaqccWLy9GU
xPksjfC+N7O22akmykT8V6iMh4+7iAIBJYE6pWpsQU5nFP9rJuDx5R/QV4Ql77od
96vNtgwv/hSseRFjyqrGxKewMb11FNjzWSAUyzW0p+GLR/mqBCFavMRl4toxEsP3
UDNRpGpFdw== root@localhost    --- (1)
#
```

1)　本装置のホスト認証用 DSA 公開鍵

・RSA 公開鍵を表示する場合

```
# show ssh server key rsa
ssh-rsa AA94UAATdVfYAAxsAArx3AAIF7QAsTsTwAEeKogAFAlNoAA0OAAAAj3F
AAD3C1yc2EAAAABIwAAAHsMXKAAB+shGQAHDmIABBSpjAARVYAAERAAJZ/IAAAAB
0AB9QAB+2kSY6AAUAygACvAAB3NzaA7wtAAJ/kAADRQgABwmQAThHAAUtOySgAEJ
JMBAAX4= root@localhost    --- (1)
#
```

1)　本装置のホスト認証用 RSA 公開鍵

第 54 章　AAA の状態の表示コマンド

54.1 AAA の状態の表示

54.1.1 show aaa radius client server-info

[機能]

RADIUS クライアント機能のサーバ情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show aaa radius client server-info [group <group_id>]

[オプション]

なし

AAA グループすべてのサーバ情報を表示します。

group <group_id>

指定したグループに関するサーバ情報を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

RADIUS サーバの状態を表示します。

[実行例]

以下に実行例を示します。

```
# show aaa radius client server-info group 0
[aaa group 0]
Type No.  Server Address                          Port  Pri  State  recover
---- ---- ------------------------------------  ----  ---  -----  -------
(1)  (2)            (3)                           (4)   (5)   (6)    (7)
Auth   0  192.168.0.101                           1812   10  dead   293/300
Auth   1  192.168.0.100                           1812   20  alive     -
Acct   0  192.168.0.100                           1813    0  alive     -
```

1) サーバの種別

- Auth
  認証サーバ
- Acct
  アカウンティングサーバ

2) サーバ定義番号

3) サーバ IP アドレス

4) サーバポート番号

5) 優先度

6)　サーバの状態

- alive
  使用可能
- dead
  応答不能により使用不可

7)　復旧残り時間／復旧待機時間

第 55 章　ソケット状態の表示コマンド

55.1　ソケット状態の表示

55.1.1　show socket

[機能]

ソケット状態の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show socket [{ ip | ipv6 }]

[オプション]

なし

IPv4/IPv6 双方のソケットの状態を表示します。

ip

IPv4 のソケットの状態を表示します。

ipv6

IPv6 のソケットの状態を表示します。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

アプリケーション層ソフトウェアが利用しているソケットの状態を表示します。

[実行例]

以下に、実行例を示します。

```
# show socket
Active sockets for IPv4 (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        State
----- ------ ------  -------------          ---------------        -------
 (1)   (2)    (3)         (4)                      (5)               (6)

tcp        0      0  *.22                   *.*                    LISTEN
tcp        0      0  127.0.0.1.2600         127.0.0.1.1025         ESTABLISHED
tcp        0      0  127.0.0.1.1025         127.0.0.1.2600         ESTABLISHED
tcp        0      0  *.37                   *.*                    LISTEN
tcp        0      0  *.21                   *.*                    LISTEN
tcp        0      0  *.80                   *.*                    LISTEN
tcp        0      0  *.23                   *.*                    LISTEN
tcp        0      0  127.0.0.1.61225        *.*                    LISTEN
tcp        0      0  127.0.0.1.2600         *.*                    LISTEN
udp        0      0  127.0.0.1.2611         *.*
udp        0      0  *.68                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.67                   *.*
```

(続く)

(続き)

```
udp        0      0  127.0.0.1.2645         *.*
udp        0      0  *.67                   *.*
udp        0      0  *.53                   *.*
udp        0      0  *.67                   *.*
udp        0      0  127.0.0.1.52000        *.*
udp        0      0  *.67                   *.*
udp        0      0  *.67                   *.*
udp        0      0  127.0.0.1.2642         *.*
udp        0      0  *.37                   *.*
udp        0      0  *.67                   *.*
udp        0      0  127.0.0.1.2639         *.*
udp        0      0  127.0.0.1.2638         *.*
udp        0      0  127.0.0.1.161          *.*
udp        0      0  127.0.0.1.8900         *.*
udp        0      0  127.0.0.1.2631         *.*
udp        0      0  *.123                  *.*
udp        0      0  *.67                   *.*
udp        0      0  127.0.0.1.2633         *.*
udp        0      0  127.0.0.1.2632         *.*
udp        0      0  127.0.0.1.2634         *.*
udp        0      0  127.0.0.1.2635         *.*
udp        0      0  127.0.0.1.2637         *.*
udp        0      0  *.500                  *.*
udp        0      0  127.0.0.1.2628         *.*
udp        0      0  127.0.0.1.2629         *.*
udp        0      0  127.0.0.1.2621         *.*
udp        0      0  127.0.0.1.2623         *.*
udp        0      0  127.0.0.1.2627         *.*
udp        0      0  127.0.0.1.2624         *.*
udp        0      0  127.0.0.1.2625         *.*
udp        0      0  127.0.0.1.2622         *.*
udp        0      0  *.*                    *.*
Active sockets for IPv6 (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        State
tcp6       0      0  *.22                   *.*                    LISTEN
tcp6       0      0  *.37                   *.*                    LISTEN
tcp6       0      0  *.80                   *.*                    LISTEN
tcp6       0      0  *.23                   *.*                    LISTEN
tcp6       0      0  *.21                   *.*                    LISTEN
udp6       0      0  *.53                   *.*
udp6       0      0  *.547                  *.*
udp6       0      0  *.37                   *.*
udp6       0      0  *.123                  *.*
udp6       0      0  *.500                  *.*
#
```

1) プロトコル

tcp または udp が表示されます。

IPv6 の場合は tcp6 または udp6 になります。

2) 読みだし待ちデータ量

装置が受信したデータのうち、アプリケーション層ソフトウェアから読みだし待ちとなっているデータ量が表示されます。

3) 送達確認待ちデータ量

アプリケーション層ソフトウェアから送信されたデータのうち、送達確認がとれていないデータ量が表示されます。

4) 自側アドレス. ポート番号

自側アドレスとポート番号が表示されます。指定がない場合は * が表示されます。

5) 相手アドレス. ポート番号

相手アドレスとポート番号が表示されます。未定の場合は * が表示されます。

6) プロトコル内部状態

- プロトコルが tcp の場合に、以下のどれかが表示されます。

CLOSED セッション未確立
CLOSE_WAIT セッション切断後、アプリケーション層ソフトウェアからの close 処理待ち
CLOSING アプリケーション層ソフトウェアから close 処理要求され、FIN 交換後の ACK 受信待ち
ESTABLISHED セッション確立状態
FIN_WAIT_1 FIN 送信後の ACK 受信待ち
FIN_WAIT_2 FIN 受信待ち
LAST_ACK FIN 交換後の ACK 受信待ち
LISTEN セッション受け付け可能
SYN_RCVD SYN-ACK 送信後の ACK 受信待ち
SYN_SENT SYN 送信後の SYN-ACK 受信待ち
TIME_WAIT セッション切断後の保持中

第 56 章　トレースの表示、クリア操作コマンド

56.1 トレースの表示

56.1.1 show trace ppp

[機能]

PPP フレームトレースの表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show trace ppp

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

PPP フレームトレース情報を表示します。

[実行例]

以下に、実行例を示します。

```
# show trace ppp

[001] internet.ISP     : PPP session start                02.08.07 09:55:01.697
-(1)- ----(2)-----       ------(3)--------                ----------(4)--------
        port=slot:mb, line:0 (lan0)
             ---------(5)----------

[002] internet.ISP     : Send LCP       Configure-Request 02.08.07 09:55:01.697
                        -(6)- -(7)-     -------(8)-------
        port=slot:mb, line:0 (lan0)
        data=c021 0100 000a 0506 f01e 028e
             -----------(9)---------------

[003] internet.ISP     : Recv LCP       Configure-Request 02.08.07 09:55:02.116
        port=slot:mb, line:0 (lan0)
        data=c021 0101 001c 0802 0702 0206 0000 0000
             0104 05ae 0506 b104 7cbb 0304 c023

[004] internet.ISP     : Send LCP       Configure-Reject  02.08.07 09:55:02.116
        port=slot:mb, line:0 (lan0)
        data=c021 0401 000e 0802 0702 0206 0000 0000

[005] internet.ISP     : Recv LCP       Configure-Nak     02.08.07 09:55:02.116
        port=slot:mb, line:0 (lan0)
        data=c021 0300 0008 0104 05ae
```

1) ログ番号

ログ番号が、001～999 の 10 進数値で表示されます。

2) 接続先名

この PPP セッションが利用した接続先名が<ネットワーク名>.<接続先名>の形式で表示されます。

3) ネゴシエーション開始

ネゴシエーション開始時に表示されます。

4) 採取時間

情報を採取した時間が表示されます。

5) 回線識別子

以下の形式で通信に利用した回線が表示されます。

slot:<slot 番号> line:<line 番号> (<回線固有情報>)

<slot 番号>

通信に利用した物理回線のスロット番号が表示されます。

(※ Si-R220B Si-R180 では必ず"mb"(基本ボード) が表示されます。)

(※ 2 および 3 が表示されるのは Si-R570 のみです。)

・mb

基本ボード

・0

slot 0

・1

slot 1

・2

slot 2

・3

slot 3

<line 番号>

通信に利用した物理回線の回線番号が表示されます。

回線固有情報

利用する回線に応じた内容が表示されます。

・HSD の場合 (※ Si-R260B Si-R240 Si-R180 では使用できません)

表示されません。

・ISDN の場合 (※ Si-R260B Si-R240 Si-R180 では使用できません)

チャネル名が表示されます。

・PPPoE の場合

利用した lan 定義が表示されます。

6) 送受信

以下のどれかが表示されます。

- Send
- Recv

7) プロトコル種別

PPP のプロトコル種別として、以下のプロトコルが表示されます。

プロトコル種別の前に「MP:」が付加されている場合、そのパケットが MP によってカプセル化されていることを示します。

(※ Si-R260B Si-R240 Si-R180 では MP を使用できません。また CCP,ICCP,BAP,BACP,BCP,MPLSCP は未サポートです。)

Oxc021 LCP : Link Control Protocol

Oxc023 PAP : Password Authentication Protocol

Oxc223 CHAP : Challenge-Handshake Authentication Protocol

Ox8021 IPCP : Internet Protocol Control Protocol

Ox8031 BCP : Bridge Control Protocol

Ox8057 IPV6CP : IPv6 Control Protocol

Ox80fd CCP : Compression Control Protocol

Ox80fb ICCP : Individual Compression Control Protocol

Oxc02d BAP : Bandwidth Allocation Protocol

Oxc02b BACP : Bandwidth Allocation Control Protocol

Oxc029 CBCP : Callback Control Protocol

0x8281 MPLSCP : MPLS Control Protocol

8) コード種別

各プロトコルのコードの内容が以下の文字列で表示されます。

- プロトコル種別が LCP、CCP、ICCP、IPCP、IPV6CP、BCP、MPLSCP の場合

  Ox01 Configure-Request

  Ox02 Configure-Ack

  Ox03 Configure-Nak

  Ox04 Configure-Reject

  Ox05 Terminate-Request

  Ox06 Terminate-Ack

  Ox07 Code-Reject

- プロトコル種別が LCP の場合

  Ox08 Protocol-Reject

  Ox09 Echo-Request

  Ox0a Echo-Reply

  Ox0b Discard-Request

- プロトコル種別が CCP、ICCP の場合

  Ox0e Reset-Request

  Ox0f Reset-Act

- プロトコル種別が PAP の場合

  Ox01 Authenticate-Request

  Ox02 Authenticate-Ack

  Ox03 Authenticate-Nak

- プロトコル種別が CHAP の場合

  Ox01 Challenge

  Ox02 Response

  Ox03 Success

  Ox04 Failure

- プロトコル種別が BAP の場合

  Ox01 Call-Request

  Ox02 Call-Response

  Ox03 Callback-Request

  Ox04 Callback-Response

  Ox05 Link-Drop-Request

  Ox06 Link-Drop-Response

  Ox07 Call-Status-Ind

  Ox08 Call-Status-Rsp

- プロトコル種別が CBCP の場合

  Ox01 Callback-Request

  Ox02 Callback-Response

  Ox03 Callback-Ack

9) data=

送受信したパケットの内容が、16 進数値で表示されます。最大 108 バイト分までが表示され、それよりあとは表示されません。

56.1.2 show trace pppoe

[機能]

PPPoE フレームトレースの表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show trace pppoe

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

PPPoE のフレームトレースを表示します。

[注意]

PPPoE フレームトレース情報は、本装置を再起動するとクリアされます。

[実行例]

以下に、実行例を示します。

```
# show trace pppoe
[01] Internet.ISP      : PPPoE Discovery Stage start      00.01.02 09:19:54.225
---- ------------        ---------------------------      ---------------------
(1)      (2)                 (3)                                     (4)

[02] Internet.ISP      : Send PADI                len=35  00.01.02 09:19:54.275
                         ---- ----                ------
                         (5)  (6)                  (7)

        data=ffff ffff ffff 0000 0eaa 010c 8863 1109 --- (8)
             0000 000f 0101 0000 0103 0007 0000 0eaa
             010c 01

[03] Internet.ISP      : Recv PADO                len=62  00.01.02 09:19:54.325
        data=0000 0eaa 010c 0003 e48a 0c1c 8863 1107
             0000 002a 0101 0000 0103 0007 0000 0eaa
             010c 0101 0200 0372 6173 0104 0010 4c3b
             69dc e7d6 949a 90d6 86b5 8bdf 5ce5

[04] Internet.ISP      : Send PADR                len=62  00.01.02 09:19:54.445
        data=0003 e48a 0c1c 0000 0eaa 010c 8863 1119
             0000 002a 0101 0000 0103 0007 0000 0eaa
             010c 0101 0200 0372 6173 0104 0010 4c3b
             69dc e7d6 949a 90d6 86b5 8bdf 5ce5

[05] Internet.ISP      : Recv PADS                len=62  00.01.02 09:19:54.495
        data=0000 0eaa 010c 0003 e48a 0c1c 8863 1165
             0003 002a 0101 0000 0103 0007 0000 0eaa
             010c 0101 0200 0372 6173 0104 0010 4c3b
             69dc e7d6 949a 90d6 86b5 8bdf 5ce5

[06] Internet.ISP      : Send PADT                len=20  00.01.02 09:21:16.099
        data=0003 e48a 0c1c 0000 0eaa 010c 8863 11a7
             0003 0000
```

1) ログ番号

ログ番号が 01～99 の 10 進数値で表示されます。

2) 接続先名

この PPPoE セッションが利用した接続先名が<ネットワーク名>.<接続先名>の形式で表示されます。

3) ネゴシエーション開始

ネゴシエーション開始時に表示されます。

4) pppoetrace 採取時刻

pppoetrace 採取時刻が表示されます。

5) 送受信

以下のどれかが表示されます。

- Send
- Recv

6) コード種別

PPPoE フレームのコードの内容として、以下のコードが表示されます。

- PADI

  PPPoE Active Discovery Initiation

- PADO

  PPPoE Active Discovery Offer

- PADR

  PPPoE Active Discovery Request

- PADS

  PPPoE Active Discovery Session-confirmation

- PADT

  PPPoE Active Discovery Terminate

- SESS

  Session Stage

7) フレーム長

   送受信したフレーム長が 10 進数値で表示されます。

8) data=

   送受信したフレームの内容を 16 進数値で表示します。最大 128 バイト分まで表示され、それよりあとは表示されません。

56.1.3　show trace ike

[機能]

IKE トレース情報表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show trace ike

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

IKE ネゴシエーションパケットのトレース情報を表示します。
以下に機種ごとのトレース表示最大数を示します。

表示最大数	機種
300	Si-R570　Si-R370
30	Si-R260B　Si-R240　Si-R220B　Si-R180

[注意]

IKE フレームトレース情報は、本装置を再起動するとクリアされます。

[実行例]

以下に、IKE トレース情報の実行例を示します。

```
# show trace ike
[1]  ISAKMP Send                                Aug  7 10:26:26 2002
---  -----------                                --------------------
(1)     (2)                                             (3)
        Local  Address:(192.168.1.1)
        ----------------------------
                (4)
        Remote Address:(192.168.2.1)
        ----------------------------
                (5)
        Cookies:(22f2b428fb243bba:0000000000000000)
        -------------------------------------------
                                (6)
        Exchange Type: Aggressive          Len:215(0xd7)
        -------------------------          -------------
                           (7)                 (8)
        data=22f2 b428 fb24 3bba 0000 0000 0000 0000 --- (9)
             0110 0400 0000 0000 0000 00d7 0400 0038
             0000 0001 0000 0001 0000 002c 0101 0001
             0000 0024 0101 0000 8001 0001 8002 0001
             8003 0001 8004 0001 800b 0001 000c 0004
             0001 5180 0a00 0064 1d9b dedd 0bd7 55bf
             d1d1 0ba1 3595 fa9e 421e 790e 4e9b c95c
             dc1e 07bc e220 2179 095c 11f8 4138 a44a


[2]  ISAKMP Receive                             Aug  7 10:26:27 2002
        Cookies:(22f2b428fb243bba:5b504feebef8c495)
        Exchange Type: Aggressive          Len:255(0xff)
        data=22f2 b428 fb24 3bba 5b50 4fee bef8 c495
             0110 0400 0000 0000 0000 00ff 0400 0038
             0000 0001 0000 0001 0000 002c 0101 0001
             0000 0024 0101 0000 8001 0001 8002 0001
             8003 0001 8004 0001 800b 0001 000c 0004
             0001 5180 0a00 0064 05ab 21eb 7d9c 2261
             80b8 ca00 9647 fdc1 ea94 1d0b 1740 ba33
             5f64 a095 fb90 ac52 e533 e820 7da5 ceca


[3]  ISAKMP Send                                Aug  7 10:26:27 2002
        Cookies:(22f2b428fb243bba:5b504feebef8c495)
        Exchange Type: Aggressive          Len:48(0x30)
        data=22f2 b428 fb24 3bba 5b50 4fee bef8 c495
             0810 0400 0000 0000 0000 0030 0000 0014
             0d89 bb75 240e 3028 294d 41af 7c86 0d15


[4]  ISAKMP Send(Before Encrypt)                Aug  7 10:26:27 2002
        Cookies:(22f2b428fb243bba:5b504feebef8c495)
        Exchange Type: Informational       Len:76(0x4c)
        data=22f2 b428 fb24 3bba 5b50 4fee bef8 c495
             0810 0501 774d 2a19 0000 004c 0b00 0014
             81de 9a99 455f a72d 9b54 c631 2909 3d1b
             0000 001c 0000 0001 0110 6002 22f2 b428
             fb24 3bba 5b50 4fee bef8 c495


[5]  ISAKMP Send                                Aug  7 10:26:27 2002
        Cookies:(22f2b428fb243bba:5b504feebef8c495)
        Exchange Type: Informational       Len:84(0x54)
        data=22f2 b428 fb24 3bba 5b50 4fee bef8 c495
             0810 0501 774d 2a19 0000 0054 ebbb fd4a
             474c 9cf7 6a1f daaa c622 7389 5d0d 2787
             d87b ca80 af88 338f 2dca 3147 c9d2 5656
             2602 59c8 f6e1 6c61 d8a3 0ae3 4d79 7ffa
             ac57 7db9
```

(続く)

(続き)

```
[6]  ISAKMP Send(Before Encrypt)                Aug  7 10:26:27 2002
        Cookies:(22f2b428fb243bba:5b504feebef8c495)
        Exchange Type: Quick               Len:148(0x94)
        data=22f2 b428 fb24 3bba 5b50 4fee bef8 c495
             0810 2001 4730 70fb 0000 0094 0100 0014
             fd3b 2b24 f778 8e08 a7c8 bbb2 b7bc 0914
             0a00 0030 0000 0001 0000 0001 0000 0024
             0103 0401 03ff 7c4b 0000 0018 0102 0000
             8001 0001 8002 7080 8004 0001 8005 0001
             0500 0014 f7c2 d1ab d5c6 d3e4 5929 38ae
             91f9 5354 0500 0010 0400 0000 0000 0000


[7]  ISAKMP Send                                Aug  7 10:26:27 2002
        Cookies:(22f2b428fb243bba:5b504feebef8c495)
        Exchange Type: Quick               Len:156(0x9c)
        data=22f2 b428 fb24 3bba 5b50 4fee bef8 c495
             0810 2001 4730 70fb 0000 009c 789e 35b5
             fb49 2b8a 3ebd 5663 81ab 4c78 e4cf 864c
             b968 1d8e 6238 d076 b095 0b17 af03 33e0
             2735 f9ba 13dd 2000 3efb bc65 1e8b b482
             3be8 48ac ebab 6548 3394 512e 6a27 5f37
             c16a 97a8 4a65 40fa 06b1 3eef 1ea2 8e0d
             9a87 b933 6bed 117b ec8b 0b35 e227 32c4


[8]  ISAKMP Receive                             Aug  7 10:26:27 2002
        Cookies:(22f2b428fb243bba:5b504feebef8c495)
        Exchange Type: Quick               Len:156(0x9c)
        data=22f2 b428 fb24 3bba 5b50 4fee bef8 c495
             0810 2001 4730 70fb 0000 009c f14e ecb1
             938f 88aa bafe 127d dea8 0a24 5a45 2d47
             c50e 36dc f77e dccc 6d20 4395 c1f1 574d
             76c0 a67c 53e3 b7e8 9a6b 276a aea5 585d
             87f0 6db3 9a77 227c 8696 4105 296b 83e9
             e0fc f516 3ead f907 96a4 2910 c2a9 0ca7
             fa1e 92a5 ce82 3af0 16e0 9ee1 cea3 4f2d


[9]  ISAKMP Receive(After Decrypt)              Aug  7 10:26:27 2002
        Cookies:(22f2b428fb243bba:5b504feebef8c495)
        Exchange Type: Quick               Len:156(0x9c)
        data=22f2 b428 fb24 3bba 5b50 4fee bef8 c495
             0810 2001 4730 70fb 0000 009c 0100 0014
             d4d3 5742 a8e3 f18a 76c4 94f7 d080 e877
             0a00 0030 0000 0001 0000 0001 0000 0024
             0103 0401 0efd a61d 0000 0018 0102 0000
             8001 0001 8002 7080 8004 0001 8005 0001
             0500 0014 c538 a8b4 8271 1754 da9e 84c4
             fcb6 d999 0500 0010 0400 0000 0000 0000


[10]  ISAKMP Send(Before Encrypt)               Aug  7 10:26:27 2002
        Cookies:(22f2b428fb243bba:5b504feebef8c495)
        Exchange Type: Quick               Len:48(0x30)
        data=22f2 b428 fb24 3bba 5b50 4fee bef8 c495
             0810 2001 4730 70fb 0000 0030 0000 0014
             9b63 756e 00c2 1d9c e7f0 94ef b608 5817


[11]  ISAKMP Send                               Aug  7 10:26:27 2002
        Cookies:(22f2b428fb243bba:5b504feebef8c495)
        Exchange Type: Quick               Len:52(0x34)
        data=22f2 b428 fb24 3bba 5b50 4fee bef8 c495
             0810 2001 4730 70fb 0000 0034 6062 6bca
             2665 5bd9 f8d6 4f97 4245 3ea1 939d 0665
             1259 cdca
#
```

1) ログ番号

ログ番号が、10 進数で表示されます。

2) 送受信

以下のどれかが表示されます。

ISAKMP Send : 送信フレーム

ISAKMP Receive : 受信フレーム

ISAKMP Send(Before Encrypt) : 暗号化前の送信フレーム

ISAKMP Receive(After Decrypt) : 復号化後の受信フレーム

3) IKE トレース採取時間

IKE トレース採取時間が表示されます。

4) Local Address

IKE ネゴシエーションを行う、自装置 IPv4 または IPv6 アドレスが表示されます。

IPv4 アドレスで、可変 IP アドレス Aggressive モード Initiator の設定を行っている場合、IKE ネゴシエーションパケット送信時 (ISAKMP Send および ISAKMP Send(Before Encrypt)) に 0.0.0.0 と表示されることがあります。

5) Remote Address

IKE ネゴシエーションを行う、相手装置 IPv4 または IPv6 アドレスが表示されます。

6) Cookies

Cookie を (Initiator 側 Cookie:Responder 側 Cookie) の形式で表示されます。

7) Exchange Type

以下の Exchange Type が表示されます。

NONE : 交換なし

Base : Base モード

Identity Protection : Identity Protection モード

Authentication Only : Authentication Only モード

Aggressive : Aggressive モード

Informational : Informational モード

Quick : Quick モード

New group : New group モード

Acknowledged Informational : Acknowledged Informational モード

8) Len

ISAKMP パケット長が表示されます。

9) data=

送受信したパケットの内容が、16 進数で表示されます。最大 320 バイトまでが表示されます。

56.1.4　show trace modem

[機能]

モデム／データ通信カード 制御トレースの表示

[適用機種]

			Si-R 240	Si-R 220B	

[入力形式]

show trace modem

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス／管理者クラス)
構成定義モード (管理者クラス)

[説明]

モデム／データ通信カード の発着呼トレースデータを表示します。

[注意]

モデム／データ通信カード 制御トレース情報は、本装置を再起動するとクリアされます。

[実行例]

以下に、実行例を示します。

```
# show trace modem

[01]  Slot 0 : Slot Status                                  06.03.02 21:19:07.939
        sig_on=()
        PC-Slot In

[02]  Slot 0 : Send                                         06.03.02 21:19:07.943
(1)-  (2)---   (3)-                                         ----------(4)--------
        sig_on=(ER,RS)
        -------(5)----
        data=4154 5a0d 0a                                   ATZ..
        ----(6)----------                                   -(7)-

[03]  Slot 0 : Change Signal                                06.03.02 21:19:08.272
        sig_on=(CS,ER,RS)
        CS OFF -> ON

[04]  Slot 0 : Change Signal                                06.03.02 21:19:08.461
        sig_on=(ER,RS)
        CS ON -> OFF

[05]  Slot 0 : Change Signal                                06.03.02 21:19:08.461
        sig_on=(CS,ER,RS)
        CS OFF -> ON

[06]  Slot 0 : Change Signal                                06.03.02 21:19:12.566
        sig_on=(DR,CS,ER,RS)
        DR OFF -> ON

[07]  Slot 0 : Recv                                         06.03.02 21:19:12.567
        sig_on=(DR,CS,ER,RS)
        data=4154 5a                                        ATZ

[08]  Slot 0 : Recv                                         06.03.02 21:19:12.578
        sig_on=(DR,CS,ER,RS)
        data=4f4b                                           OK

[09]  Slot 0 : Send                                         06.03.02 21:19:14.578
        sig_on=(DR,CS,ER,RS)
        data=4154 4530 4050 5346 543d 300d 0a               ATE0@PSFT=0..

[10]  Slot 0 : Recv                                         06.03.02 21:19:14.582
        sig_on=(DR,CS,ER,RS)
        data=4154 4530 4050 5346 543d 30                    ATE0@PSFT=0

[11]  Slot 0 : Recv                                         06.03.02 21:19:14.584
        sig_on=(DR,CS,ER,RS)
        data=4f4b                                           OK

[12]  Slot 0 : Send                                         06.03.02 21:23:38.113
        sig_on=(DR,CS,ER,RS)
        data=4154 442a 3939 230d 0a                         ATD*99#..

[13]  Slot 0 : Change Signal                                06.03.02 21:24:05.922
        sig_on=(CD,DR,CS,ER,RS)
        CD OFF -> ON

[14]  Slot 0 : Change Signal                                06.03.02 21:33:33.074
        sig_on=(CD,DR,CS,ER,RS)
        ER ON -> OFF (Disconnect)

[15]  Slot 0 : Change Signal                                06.03.02 21:33:38.075
        sig_on=(CD,DR,RS)
        CS ON -> OFF

[16]  Slot 0 : Change Signal                                06.03.02 21:33:38.075
        sig_on=(DR,RS)
        CD ON -> OFF

[17]  Slot 0 : Recv                                         06.03.02 21:33:38.075
        sig_on=(DR,RS)
        data=4e4f 2043 4152 5249 4552                       NO CARRIER

[18]  Slot 0 : Change Signal                                06.03.02 21:33:38.075
        sig_on=(DR,CS,RS)
        CS OFF -> ON
#
```

1) ログ番号

ログ番号が、01～99 の 10 進数値で表示されます。

2) スロット番号

データ通信カードの場合のみ PC カードスロットのスロット番号が表示されます。

3) 送受信

以下のどれかが表示されます。

Send　ルータがモデム／データ通信カードへデータを送信したことを示します。

Recv　ルータがモデム／データ通信カードからデータを受信したことを示します。

Change Signal

RS-232C インタフェース信号が変更されたことを示します。

Slot Status

PC カードスロットでカードの挿抜が行われた事を示します。

4) 採取時間

情報を採取した時間が表示されます。

5) 信号状態

RS-232C インタフェース信号が ON の信号が表示されます。

信号の内容を以下に説明します。

CS　モデム／データ通信カードがデータ受信可能であることを示します。

ER　ルータが通信可能であることを示します。

RS　ルータがデータ受信可能であることを示します。または、ルータがデータ送信を要求していることを示します。

CI　着信を検出したことを示します。

CD　キャリアが検出され、接続状態であることを示します。

DR　モデム／データ通信カードが送受信可能であることを示します。

6) data=

送受信したデータの内容が、16 進数値で表示されます。最大 128 バイト分までが表示され、それよりあとは表示されません。

(※ Si-R240 ではルータから切断を行った場合、ER ON -> OFF (Disconnect) と表示されます。)

7) ASCII 表示

6) のデータが ASCII 文字で表示されます。

56.1.5 show trace ssh

[機能]

SSH サーバ機能のトレース情報の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

show trace ssh

[オプション]

なし

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

SSH サーバ機能のトレース情報を表示します。

[注意]

SSH サーバ機能のトレース情報は、本装置を再起動するとクリアされます。

[実行例]

```
# show trace ssh
[1] sshd        Thu Sep 30 14:34:37 2004
--- ----        ------------------------
(1)  (2)                    (3)
        This platform does not support both privilege separation and
        ------------------------------------------------------------
                                    (4)
compression
-----------
    (4)
[2] sshd        Thu Sep 30 14:34:37 2004
        Compression disabled
[3] sshd        Thu Sep 30 14:34:37 2004
        info1: sshd version OpenSSH_3.9p1
[4] sshd        Thu Sep 30 14:34:37 2004
        info1: private host key: #0 type 0 RSA1
[5] sshd        Thu Sep 30 14:34:37 2004
        info1: read PEM private key done: type RSA
[6] sshd        Thu Sep 30 14:34:37 2004
        info1: private host key: #1 type 1 RSA
[7] sshd        Thu Sep 30 14:34:37 2004
        info1: read PEM private key done: type DSA
[8] sshd        Thu Sep 30 14:34:37 2004
        info1: private host key: #2 type 2 DSA
[9] sshd        Thu Sep 30 14:34:37 2004
        info1: Bind to port 22 on 0.0.0.0.
[10] sshd       Thu Sep 30 14:34:37 2004
        Server listening on 0.0.0.0 port 22.
[11] sshd       Thu Sep 30 14:34:37 2004
        info1: Bind to port 22 on ::.
[12] sshd       Thu Sep 30 14:34:37 2004
        Server listening on :: port 22.
[13] sshd       Thu Sep 30 14:34:37 2004
        Generating 768 bit RSA key.
[14] sshd       Thu Sep 30 14:34:38 2004
        RSA key generation complete.
```

1) トレース番号

トレース番号が、10 進数で表示されます。

2) スレッド名

スレッド名が表示されます。

3) トレース採取時間

トレース採取時間が表示されます。

4) トレース内容

トレースの内容が表示されます。

56.2 トレースのクリア

56.2.1 clear trace ssh

[機能]

SSH サーバ機能トレース情報の消去

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

clear trace ssh

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

SSH サーバ機能のトレース情報を消去します。

[注意]

SSH サーバ機能のトレース情報は、本装置を再起動するとクリアされます。

[実行例]

```
# clear trace ssh
#
```

第 57 章　回線制御コマンド

57.1 回線制御

57.1.1 addlink

[機能]

MP 使用時のチャネル数増加

[適用機種]

Si-R 570	Si-R 370			Si-R 220B	

[入力形式]

addlink remote <remote_number> ap <ap_number>
addlink access-point <ap_name>

[オプション]

remote <remote_number> ap <ap_number>

構成定義の<remote_number>および<ap_number>で指定した接続先について、チャネル数増加を実施します。<remote_number>および<ap_number>で指定可能な範囲は以下のとおりです。

<remote_number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R220B

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R220B

access-point <ap_name>

<ap_name>で指定される接続先について、チャネル数増加を実施します。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

MP 通信中に、チャネル数増加を指示します。

[実行例]

```
# addlink remote 0 ap 0
#
```

57.1.2 dellink

[機能]

MP 使用時のチャネル数減少

[適用機種]

Si-R 570 | Si-R 370 | | | Si-R 220B | |

[入力形式]

dellink remote <remote_number> ap <ap_number>
dellink access-point <ap_name>

[オプション]

<remote_number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R220B

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R220B

<ap_name>

- 接続先名
  接続先の名前を指定します。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

MP 通信中に、チャネル数減少を指示します。

[実行例]

```
# dellink remote 0 ap 0
#
```

57.1.3 offline

[機能]

切断、または閉塞の実施

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

offline lan [<lan_number>]
offline switch [<switch_number> [port <port_number>]]
offline remote [<remote_number> [ap <ap_number>]]
offline access-point <ap_name>
offline template interface <interface_name>
offline template <template_number> [uid <user_id>]
offline policy-group [<policy-group_number>]

[オプション]

lan

すべての LAN を閉塞 (リンクダウン) します。

lan <lan_number>

指定された LAN を閉塞 (リンクダウン) します。
複数の LAN を指定する場合は、", "(カンマ) で区切って指定します。また、範囲指定する場合は、「2-4」のように"-"(ハイフン) を使用して指定します。

switch

すべてのスイッチポート (SW1〜SW4) を閉塞 (リンクダウン) します。

switch <switch_number>

指定されたスイッチの全ポートを閉塞 (リンクダウン) します。

switch <switch_number> port <port_number>

指定されたスイッチポートを閉塞 (リンクダウン) します。
複数のスイッチポートを指定する場合は、", "(カンマ) で区切って指定します。
また、範囲指定する場合は、「2-4」のように"-"(ハイフン) を使用して指定します。

remote

すべての接続先 (template で通信している接続先を含みます) を切断および閉塞 (通信禁止) します。

remote <remote_number>

指定された相手定義のすべての接続先を切断および閉塞 (通信禁止) します。
指定可能な範囲は以下のとおりです。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B Si-R240 Si-R220B
0〜49	Si-R180

複数の相手定義番号を指定する場合は、", "(カンマ) で区切って指定します。
また、範囲指定する場合は、「2-4」のように"-"(ハイフン) を使用して指定します。

remote <remote_number> ap <ap_number>

指定された接続先を切断、または閉塞 (通信禁止) します。<remote_number>で指定可能な範囲は上記のとおりです。また、<ap_number>で指定可能な範囲は以下のとおりです。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B　Si-R240　Si-R220B
0〜49	Si-R180

複数の接続先定義番号を指定する場合は、", "(カンマ) で区切って指定します。
また、範囲指定する場合は、「2-4」のように"-"(ハイフン) を使用して指定します。

access-point <ap_name>

指定された接続先を切断、または閉塞 (通信禁止) します。

template interface <interface_name>

<interface_name>で指定された、template で通信している接続を切断します。

template <template_number>

指定された template を利用して通信しているすべての接続先を切断します。

template <template_number> uid <user_id>

template で接続した相手で、指定された template で指定された<user_id>を利用している接続を切断します。指定可能な範囲は以下のとおりです。

<template_number>

- テンプレート定義番号

  テンプレート定義の通し番号を、10 進数値で指定します。

範囲	機種
0〜5	Si-R570　Si-R370
0〜2	Si-R240　Si-R220B
0〜1	Si-R260B　Si-R180

<user_id>

- ユーザ ID

  テンプレート着信の通信状態で表示される着信した接続先のユーザ ID を指定します。最大 145 文字まで指定可能です。

policy-group

すべてのポリシーグループを無効にします。

policy-group <policy-group_number>

- ポリシーグループ番号

  無効にするポリシーグループ番号を、10 進数値で指定します。

  <policy-group_number>で指定可能な範囲は以下のとおりです。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B　Si-R220B
0〜49	Si-R180

複数のポリシーグループ番号を指定する場合は、", "(カンマ) で区切って指定します。また、範囲指定する場合は、「2-4」のように"-"(ハイフン) を使用して指定します。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

切断、または通信閉塞を行います。

[注意]

"switch"オプションは Si-R180 で指定が可能です。
"policy-group"オプションでポリシーグループを閉塞した場合でも、接続先監視は行います。

[実行例]

```
# offline remote 0 ap 0
#
```

57.1.4　online

[機能]

接続、または閉塞解除の実施

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

online lan [<lan_number>]
online switch [<switch_number> [port <port_number>]]
online remote [<remote_number> [ap <ap_number> [id <id> <password>]]]
online access-point <ap_name>
online template <template_number> uid <user_id>
online policy-group [<policy-group_number>]

[オプション]

lan

すべての LAN を閉塞解除します。

lan <lan_number>

指定された LAN を閉塞解除します。
複数の LAN を指定する場合は、", "(カンマ) で区切って指定します。また、範囲指定する場合は、「2-4」のように"-"(ハイフン) を使用して指定します。

switch

すべてのスイッチポート (SW1～SW4) を閉塞解除します。

switch <switch_number>

指定されたスイッチの全ポートを閉塞解除します。

switch <switch_number> port <port_number>

指定されたスイッチポートを閉塞解除します。
複数のスイッチポートを指定する場合は、", "(カンマ) で区切って指定します。
また、範囲指定する場合は、「2-4」のように"-"(ハイフン) を使用して指定します。

remote

すべての接続先を閉塞解除します。

remote <remote_number>

指定された相手定義のすべての接続先を閉塞解除します。
指定可能な範囲は以下のとおりです。

範囲	機種
0～999	Si-R570
0～499	Si-R370
0～99	Si-R260B　Si-R240　Si-R220B
0～49	Si-R180

複数の相手定義番号を指定する場合は、", "(カンマ) で区切って指定します。
また、範囲指定する場合は、「2-4」のように"-"(ハイフン) を使用して指定します。

remote <remote_number> ap <ap_number> id <id> <password>

指定された接続先を接続、または閉塞解除します。<remote_number>で指定可能な範囲は上記のとおりです。また、<ap_number>で指定可能な範囲は以下のとおりです。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B Si-R240 Si-R220B
0〜49	Si-R180

複数の接続先定義番号を指定する場合は、", "(カンマ) で区切って指定します。
また、範囲指定する場合は、「2-4」のように"-"(ハイフン) を使用して指定します。
複数指定した場合は閉塞解除のみを行います。

<id>

送信認証 ID(最大 64 文字)
<remote_number>、<ap_number>で複数の接続先を指定していない場合に有効です。

<password>

送信認証パスワード (最大 64 文字)
<remote_number>、<ap_number>で複数の接続先を指定していない場合に有効です。

access-point <ap_name>

指定された接続先を接続、または閉塞解除します。

template <template_number> uid <user_id>

指定された template を使用して<user_id>に対して接続します。
指定可能な範囲は以下のとおりです。

<template_number>

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。

範囲	機種
0〜5	Si-R570 Si-R370
0〜2	Si-R240 Si-R220B
0〜1	Si-R260B Si-R180

<user_id>

- ユーザ ID
  接続相手が動的 VPN サーバに登録しているユーザ ID を指定します。
  最大 145 文字まで指定可能です。
  動的 VPN 接続では、以下の形式で指定してください。

  <user_id>
  : ユーザ名 (最大 64 文字)@ドメイン名 (最大 80 文字)

policy-group

すべてのポリシーグループを有効にします。

policy-group <policy-group_number>

- ポリシーグループ番号

  有効にするポリシーグループ番号を、10 進数値で指定します。

  <policy-group_number>で指定可能な範囲は以下のとおりです。

範囲	機種
0〜999	Si-R570
0〜499	Si-R370
0〜99	Si-R260B　Si-R220B
0〜49	Si-R180

  複数のポリシーグループ番号を指定する場合は、", "(カンマ) で区切って指定します。また、範囲指定する場合は、「2-4」のように"-"(ハイフン) を使用して指定します。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

接続、または閉塞解除を行います。

[注意]

"switch"オプションは Si-R180 で指定が可能です。

[実行例]

```
# online remote 0 ap 0
#
```

第 58 章　VRRP 制御コマンド

58.1　VRRP 制御

58.1.1　vrrp action

[機能]

VRRP の手動停止および再開始

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

vrrp action [interface <interface_name>] [vrid <vrid>] disable
(VRRP グループの手動停止)
vrrp action [interface <interface_name>] [vrid <vrid>] enable
(VRRP グループ手動停止状態からの開始)

[オプション]

interface <interface_name>

コマンド適用対象の LAN インタフェースを指定します。

範囲	機種
lan0～lan19	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
lan0～lan9	Si-R180

interface <interface_name>を省略時は、すべての LAN インタフェースが対象となります。

vrid <vrid>

コマンド適用対象の VRRP グループを指定します。
vrid <vrid>を省略時は、指定された LAN インタフェースに設定されているすべての VRRP グループが対象となります。

- VRID
  対象の LAN インタフェースに設定されている VRRP グループの VRID を、1～255 の 10 進数値で指定します。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

本装置 VRRP グループの動作を、手動にて停止状態にしたり、停止状態にした VRRP グループを再開始したりすることができます。
停止状態にした場合の VRRP グループ状態は Initial 状態となります。
再開始を実行した場合であっても VRRP グループが定義された LAN が異常である場合は再開始しません。異常復旧により開始します。
また、手動停止していない VRRP グループを指定した場合は要求を無視します。(コマンド適用の意味がない状態)

[メッセージ]

コマンドが正常に実行された場合は以下のメッセージを出力します。

```
vrrp: command accepted vrid<vrid>
```

vrid<vrid>
コマンドが適用された VRRP グループを示します。
指定された本装置 VRRP グループがすでにコマンド適用状態であったり、コマンド適用の意味がない状態である場合は、要求は無視され以下のエラーメッセージを出力します。
なお、VRID が指定されなかった場合はエラーメッセージは出力しません。

```
<ERROR> vrrp: not command accept vrid<vrid>
```

vrid<vrid>
コマンドが適用されなかった VRRP グループを示します。
また、有効ではない VRRP グループが指定された場合は以下のエラーメッセージを出力します。

```
<ERROR> vrrp: Bad vrid<vrid> provided
```

vrid<vrid>
有効ではない VRRP グループを示します。

[注意]

VRRP グループを手動停止した状態にて構成定義変更の反映を行うと停止状態が解除される場合があります。

[実行例]

lan0 の VRID が 10 である VRRP グループを停止し、その後再開始する場合の実行例を示します。

```
# vrrp action interface lan0 vrid 10
vrrp: command accepted vrid10
# vrrp action interface lan0 vrid 10
vrrp: command accepted vrid10
#
```

58.1.2　vrrp preempt-permit

[機能]

VRRP プリエンプトモードの制御

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

vrrp preempt-permit [interface <interface_name>] [vrid <vrid>] [interval <interval>]

[オプション]

interface <interface_name>

コマンド適用対象の LAN インタフェースを指定します。

範囲	機種
lan0～lan19	Si-R570　Si-R370　Si-R260B　Si-R240　Si-R220B
lan0～lan9	Si-R180

interface <interface_name>を省略時は、すべての LAN インタフェースが対象となります。

vrid <vrid>

コマンド適用対象の VRRP グループを指定します。
vrid <vrid>を省略時は、指定された LAN インタフェースに設定されているすべての VRRP グループが対象となります。

- VRID
  対象の LAN インタフェースに設定されている VRRP グループの VRID を、1～255 の 10 進数値で指定します。

interval <interval>

- プリエンプトモード ON 時間
  プリエンプトモードを ON にする時間を、0～900 の範囲で指定します。単位は秒です。
  省略時は、VRRP グループに設定された VRRP-AD 送信間隔の 3 倍+5 秒の時間を指定したものとみなされます。
  また、VRRP-AD 送信間隔の 3 倍+5 より小さい値を指定しても VRRP-AD 送信間隔の 3 倍+5 秒を指定されたものとして動作します。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

VRRP グループの動作を、一時的にプリエンプトモードが ON に設定されたものとして動作させます。
これにより、プリエンプトモードが OFF に設定された本装置 VRRP グループが現在のマスタルータより優先度の高いバックアップルータである場合、マスタルータに状態を切り戻すことができます。
現在のマスタルータの優先度のほうが高い場合は、要求は無視されます。(コマンド適用の意味がない状態)

[メッセージ]

コマンドが正常に実行された場合は以下のメッセージを出力します。

```
vrrp: command accepted vrid<vrid>
```

vrid<vrid>
コマンドが適用された VRRP グループを示します。
指定された本装置 VRRP グループがすでにコマンド適用状態であったり、コマンド適用の意味がない状態である場合は、要求は無視され以下のエラーメッセージを出力します。
なお、VRID が指定されなかった場合はエラーメッセージは出力しません。

```
<ERROR> vrrp: not command accept vrid<vrid>
```

vrid<vrid>
コマンドが適用されなかった VRRP グループを示します。
また、有効ではない VRRP グループが指定された場合は以下のエラーメッセージを出力します。

```
<ERROR> vrrp: Bad vrid<vrid> provided
```

vrid<vrid>
有効ではない VRRP グループを示します。

[実行例]

現在はマスタルータとして動作している待機設定ルータで lan0 の VRID が 10 である VRRP グループを、優先度の高い仮想ルータへきり戻しを行う場合の実行例を示します。

```
# vrrp preempt-permit interface lan0 vrid 10
vrrp: command accepted vrid10
#
```

第 59 章　動的 VPN サーバ制御コマンド

59.1 動的 VPN サーバ制御

59.1.1 dvpnserver disable

[機能]

動的 VPN サーバの手動停止

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

dvpnserver disable

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

本装置動的 VPN サーバの動作を、手動にて停止状態にすることができます。

[実行例]

動的 VPN サーバを手動で停止する場合の実行例を示します。

```
# dvpnserver disable
#
```

59.1.2　dvpnserver enable

[機能]

動的 VPN サーバの再開始

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

dvpnserver enable

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

本装置動的 VPN サーバの動作を、再開始することができます。

[実行例]

動的 VPN サーバを再開始する場合の実行例を示します。

```
# dvpnserver enable
#
```

第 60 章　RADIUS 制御コマンド

60.1　RADIUS 制御

60.1.1　radius recovery

[機能]

RADIUS サーバの復旧

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

radius recovery group <group_id> auth <number>
radius recovery group <group_id> accounting <number>

[オプション]

<group_id>

- グループ ID

  コマンド 適用対象の AAA グループの ID を指定します。

auth <number>

- 認証サーバ定義番号

  コマンド 適用対象の認証サーバの定義番号を指定します。

accounting <number>

- アカウンティングサーバ定義番号

  コマンド 適用対象のアカウンティングサーバの定義番号を指定します。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

RADIUS サーバで dead 状態になったサーバを alive 状態に復旧させます。

[実行例]

```
# radius recovery group 1 auth 2
#
```

第 61 章　データ通信カードの PIN 制御コマンド

61.1　データ通信カードの PIN 制御

61.1.1　pinctl change

[機能]

PIN コードを変更する

[適用機種]

			Si-R 240		

[入力形式]

pinctl change

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

PIN コードを変更します。
旧 PIN コードと新 PIN コードを尋ねられますので、旧 PIN コードを入力したあとに新 PIN コードを入力してください。
PIN コードは、4〜8 文字以内の数字で指定します。

[注意]

PIN コードに対応しているデータ通信カード (Vodafone VC701SI) のみ有効です。
PIN コードを変更する際にはあらかじめ、pinctl use コマンドを実行し、PIN 照合する指定にしてください。
原則として PIN コード認証に連続して 3 回失敗すると、PIN ロック状態になります。
ただし、前回認証に失敗した PIN コードを再度入力した場合は、SIM に対して認証を行いません。
結果として、PIN コード認証に連続して 3 回以上失敗した場合でも PIN ロック状態にならない場合があります。
WAN 情報でデータ通信カードを使用する設定をしていない場合、PIN 制御コマンドがエラー終了します。

[メッセージ]

```
old PIN:
```

旧 PIN コードを入力してください。

```
new PIN:
```

新 PIN コードを入力してください。

```
new PIN(again):
```

新 PIN コードを再度入力してください。

```
<ERROR> unavailable wan 0
```

WAN 情報でデータ通信カードを使用する設定をしていないため、PIN 制御を行うことができません。

```
<ERROR> difference new PIN and new PIN(again)
```

新 PIN コードと再度入力した新 PIN コードが異なっています。

```
<ERROR> PIN Authentication failed
```

旧 PIN コードの認証に失敗したため、PIN コードを変更できませんでした。
正しい PIN コードを入力してください。

```
<ERROR> PIN LOCK
```

連続して旧 PIN コードの認証に失敗したため、PIN ロック状態になりました。

```
<ERROR> PIN LOCKED
```

PIN ロック状態です。

```
<ERROR> Unsupported card
```

PIN コードに対応したカードではありません。

```
<ERROR> BUSY
```

通信中または PIN ロックを解除できない状態で、現在 PIN に関する操作ができません。

```
<ERROR> PIN NOUSE
```

データ通信カードが PIN 照合しない設定のため、PIN コードを変更できませんでした。

[実行例]

```
# pinctl change
old PIN:
new PIN:
new PIN(again):
#
```

61.1.2　pinctl unlock

[機能]

PIN ロックを解除する

[適用機種]

Si-R 240

[入力形式]

pinctl unlock

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

PIN ロックを解除します。
PUK コード (ロック解除コード) と新 PIN コードを尋ねられますので、PUK コードを入力したあとに、新 PIN コードを入力してください。
PIN/PUK コードは、4〜8 文字以内の数字で指定します。

[注意]

PIN コードに対応しているデータ通信カード (Vodafone VC701SI) のみ有効です。
原則として PUK コード認証に連続して 10 回失敗すると、ロック状態を解除できなくなります。
ただし、前回認証に失敗した PUK コードを再度入力した場合は、SIM に対して認証を行いません。
結果として、PUK コード認証に連続して 10 回以上失敗した場合でもロック状態を解除できる場合があります。
WAN 情報でデータ通信カードを使用する設定をしていない場合、PIN 制御コマンドがエラー終了します。

[メッセージ]

```
PUK:
```

PUK コードを入力してください。

```
new PIN:
```

新しい PIN コードを入力してください。

```
new PIN(again):
```

新 PIN コードを再度入力してください。

```
<ERROR> unavailable wan 0
```

WAN 情報でデータ通信カードを使用する設定をしていないため、PIN 制御を行うことができません。

```
<ERROR> Illegal PUK
```

PUK コード長が誤っている、または数字以外が入力されました。

```
<ERROR> Illegal PIN
```

PIN コード長が誤っている、または数字以外が入力されました。

```
<ERROR> PUK Authentication failed
```

PUK コードの認証に失敗したため、PIN ロックが解除されませんでした。

```
<ERROR> PUK LOCKED
```

PIN ロック解除コードの認証に失敗したために、ロック状態を解除する事ができなくなりました。

```
<ERROR> Unsupported card
```

PIN コードに対応したカードではありません。

```
<ERROR> BUSY
```

通信中または PIN ロックを解除できない状態で、現在 PIN に関する操作ができません。

```
<ERROR> PIN NOT LOCKED
```

PIN ロック状態ではありません。

[実行例]

```
# pinctl unlock
PUK:
new PIN:
new PIN(again):
#
```

61.1.3　pinctl use

[機能]

PIN コードを照合する指定をする

[適用機種]

Si-R 240

[入力形式]

pinctl use

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

データ通信カード内の SIM に対して PIN コードを照合する指定を行います。
PIN コードを尋ねられますので、入力してください。
PIN コードは、4〜8 文字以内の数字で指定します。

[注意]

PIN コードに対応しているデータ通信カード (Vodafone VC701SI) のみ有効です。
原則として PIN コード認証に連続して 3 回失敗すると、PIN ロック状態になります。
ただし、前回認証に失敗した PIN コードを再度入力した場合は、SIM に対して認証を行いません。
結果として、PIN コード認証に連続して 3 回以上失敗した場合でも PIN ロック状態にならない場合があります。
WAN 情報でデータ通信カードを使用する設定をしていない場合、PIN 制御コマンドがエラー終了します。

[メッセージ]

```
PIN:
```

PIN コードを入力してください。

```
<ERROR> unavailable wan 0
```

WAN 情報でデータ通信カードを使用する設定をしていないため、PIN 制御を行うことができません。

```
<ERROR> Illegal PIN
```

PIN コード長が誤っている、または数字以外が入力されました。

```
<ERROR> PIN Authentication failed
```

PIN コードの認証に失敗したため、PIN コードを照合する設定ができませんでした。

正しい PIN コードを入力してください。

```
<ERROR> PIN LOCK
```

連続して PIN コードの認証に失敗したため、PIN ロック状態になりました。

```
<ERROR> PIN LOCKED
```

PIN ロック状態です。

```
<ERROR> Unsupported card
```

PIN コードに対応したカードではありません。

```
<ERROR> BUSY
```

通信中または PIN ロックを解除できない状態で、現在 PIN に関する操作ができません。

```
<ERROR> PIN Authentication not execed
```

PIN 照合する指定の状態で PIN 照合する指定を行いました。

[実行例]

```
# pinctl use
PIN:
#
```

61.1.4　pinctl nouse

[機能]

PIN コードを照合しない指定をする

[適用機種]

Si-R 240

[入力形式]

pinctl nouse

[オプション]

なし

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

データ通信カード内の SIM に対して PIN コードを照合しない指定を行います。
PIN コードを尋ねられますので、入力してください。
PIN コードは、4〜8 文字以内の数字で指定します。

[注意]

PIN コードに対応しているデータ通信カード (Vodafone VC701SI) のみ有効です。
原則として PIN コード認証に連続して 3 回失敗すると、PIN ロック状態になります。
ただし、前回認証に失敗した PIN コードを再度入力した場合は、SIM に対して認証を行いません。
結果として、PIN コード認証に連続して 3 回以上失敗した場合でも PIN ロック状態にならない場合があります。
WAN 情報でデータ通信カードを使用する設定をしていない場合、PIN 制御コマンドがエラー終了します。

[メッセージ]

```
PIN:
```

PIN コードを入力してください。

```
<ERROR> unavailable wan 0
```

WAN 情報でデータ通信カードを使用する設定をしていないため、PIN 制御を行うことができません。

```
<ERROR> Illegal PIN
```

PIN コード長が誤っている、または数字以外が入力されました。

```
<ERROR> PIN Authentication failed
```

PIN コードの認証に失敗したため、PIN コードを照合しない設定ができませんでした。

正しい PIN コードを入力してください。

```
<ERROR> PIN LOCK
```

連続して PIN コードの認証に失敗したため、PIN ロック状態になりました。

```
<ERROR> PIN LOCKED
```

PIN ロック状態です。

```
<ERROR> Unsupported card
```

PIN コードに対応したカードではありません。

```
<ERROR> BUSY
```

通信中または PIN ロックを解除できない状態で、現在 PIN に関する操作ができません。

```
<ERROR> PIN Authentication not execed
```

PIN 照合しない指定の状態で PIN 照合しない指定を行いました。

[実行例]

```
# pinctl nouse
PIN:
#
```

第 62 章　その他のコマンド

62.1 その他

62.1.1 ping

[機能]

ICMP エコー要求パケットの送信

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

ping <ip_address>
[source <ip_address>] [repeat [<count>]] [size <data_size>]
[tos <tos>] [ttl <ttl>] [timeout <timeout>] [df]
ping <host_name> [{v4|v6}]
[source <ip_address>] [repeat [<count>]] [size <data_size>]
[tos <tos>] [ttl <ttl>] [timeout <timeout>] [df]

[オプション]

<ip_address>

- 送出先 IP アドレス

  送信先の IPv4 アドレス、または IPv6 アドレスを指定します。

  IPv6 リンクローカルアドレスを指定する場合、アドレスに続けて"%<interface>" を指定して、どのインタフェースを使用するのか指定してください。たとえば、"fe80::1%lan0"のように指定します。

  <ip_address>か<host_name>のどちらか一方を指定する必要があります。

<host_name>

- 送信先ホスト名

  送出先のホスト名を指定します。

  ホスト名を指定した場合は、ホストデータベース情報に該当ホスト名が登録されているか、本装置が DNS サーバを使用可能な状態でなければなりません。

  <ip_address>か<host_name>のどちらか一方を指定する必要があります。

{v4|v6}

- 送出先ホスト名の IP バージョン指定

  <host_name>指定時に、<host_name>から解決した送出先 IP アドレスのバージョンを指定します。省略時は v4 とみなされます。解決した IP アドレスのバージョンと本指定が一致しない場合はエラーとなります。

source <ip_address>

- 送信元 IP アドレス

  送信元 IP アドレスを指定します。装置に定義されていないアドレスは指定できません。

  送信先 IP アドレスとバージョンが一致しない場合はエラーとなります。

repeat [<count>]

- 繰り返し回数

  繰り返し回数を 0〜65535 の 10 進数で指定します。<count>を省略時は、0 を指定したものとみなされます。

size <data_size>

- データサイズ
  送信する IP ヘッダを含むパケット長を、46〜9600 の 10 進数値 (単位:バイト) で指定します。
  省略時は、46 バイトを指定したものとみなされます。

tos <tos>

- TOS 値
  TOS 値を、0〜ff の 16 進数で指定します。省略時は、0 を指定したものとみなされます。

ttl <ttl>

- TTL 値
  TTL 値を、0〜255 の 10 進数で指定します。省略時は、128 を指定したものとみなされます。

timeout <timeout>

- 応答監視時間
  応答監視時間を、1〜300 の 10 進数値 (単位：秒) で指定します。
  省略時は、1 秒を指定したものとみなされます。
  ただし、repeat を省略時は 20 秒を指定したものとみなされます。

df

- フラグメント禁止
  送信するパケットに Don’t Fragment bit を設定して経路の途中でフラグメントされないようにします。
  送出先 IP アドレスが IPv6、または送出先ホスト名の IP バージョン指定が v6 の場合は本指定は無視されます。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

指定したホスト (IP アドレスまたはホスト名) に対して、ICMP ECHO_REQUEST を送信し、ICMP ECHO_RESPONSE の受信を確認します。

[実行例]

a) オプションなし (IP アドレス指定のみ)

```
# ping 192.168.1.1
192.168.1.1 is alive.
#
```

b) ホスト名指定

```
# ping jp.fujitsu.com
192.168.1.2 is alive.
#
```

c) ホスト名指定 (IPv6)

```
# ping jp.fujitsu.com v6
fe80:::fffe:c100:e00:5555:80c2 is alive.
#
```

d) 繰り返し (3 回指定)

```
# ping 192.168.1.1 repeat 3
PING 192.168.1.1: 56 data bytes.
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.768 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.736 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.736 ms

----192.168.1.1 PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms)  min/ave/max = 0.736/0.746/0.768
#
```

62.1.2　traceroute

[機能]

ネットワーク経路の表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

traceroute <ip_address> [source <src_ip_address>] [size <data_size>]
[timeout <timeout>] [mpls] [df]
traceroute <host_name> [{v4 | v6}] [source <src_ip_address>] [size <data_size>]
[timeout <timeout>] [mpls] [df]

[オプション]

<ip_address>

- 送出先 IP アドレス

  送出先の IPv4 アドレス、または IPv6 アドレスを指定します。

  <ip_address>か<host_name>のどちらか一方を指定する必要があります。

<host_name>

- 送出先ホスト名

  送出先のホスト名を指定します。

  ホスト名を指定した場合は、ホストデータベース情報に該当ホスト名が登録されているか、本装置が DNS サーバを使用可能な状態でなければなりません。

  <ip_address>か<host_name>のどちらか一方を指定する必要があります。

{ v4 | v6 }

- 送出先ホスト名の IP バージョン指定

  <host_name>指定時に、<host_name>から解決した送出先 IP アドレスのバージョンを指定します。省略時は v4 とみなされます。解決した IP アドレスのバージョンと本指定が一致しない場合はエラーとなります。

source <src_ip_address>

- 送信元 IP アドレス

  送信元 IP アドレスを指定します。装置に定義されていないアドレスは指定できません。

  送信先 IP アドレスとバージョンが一致しない場合はエラーとなります。

size <data_size>

- データサイズ

  送信する IP ヘッダを含むパケット長を、46〜9600 の 10 進数値 (単位:バイト) で指定します。

  省略時は、46 バイトを指定したものとみなされます。

  送出先 IP アドレスが IPv6、または送出先ホスト名の IP バージョン指定が v6 の場合は 46〜59 までの指定は自動的に 60 となります。

timeout <timeout>

- 応答監視時間

  応答監視時間を、1〜300 の 10 進数値 (単位：秒) で指定します。

  省略時は、20 秒を指定したものとみなされます。

mpls

- MPLS ラベル表示
  応答に MPLS のラベル情報が含まれる場合に、情報を表示します。
  送出先 IP アドレスが IPv6、または送出先ホスト名の IP バージョン指定が v6 の場合は本指定は無視されます。

df

- フラグメント禁止
  送信するパケットに Don't Fragment bit を設定して経路の途中でフラグメントされないようにします。
  送出先 IP アドレスが IPv6、または送出先ホスト名の IP バージョン指定が v6 の場合は本指定は無視されます。

[動作モード]

運用管理モード (一般ユーザクラス／管理者クラス)
構成定義モード (管理者クラス)

[説明]

ネットワーク経路を表示します。
指定した host(IP アドレスまたはホスト名) に対して、IP データグラムヘッダの生存時間 (TTL / HopLimit) の値を 1 から 1 つずつ単調に増加させながら試験パケットを送信し、時間超過またはあて先到達不能の ICMP パケット受信によって、host までの経路情報を表示します。
traceroute で表示される文字には以下の意味があります。

[あて先が IPv4 アドレスの場合]

xx.xxx ms ： ラウンドトリップタイム
!N ： あて先到達不能 (ネットワークへの経路なし)
!H ： あて先到達不能 (ホストへの経路なし)
!P ： あて先到達不能 (プロトコル到達不能)
!F ： あて先到達不能 (フラグメントが必要)
!S ： ソースルートルーティング失敗
! ： TTL 値が異常
* ： プローブのタイムアウト

[あて先が IPv6 アドレスの場合]

xx.xxx ms ： ラウンドトリップタイム
!N ： あて先到達不能 (ネットワークへの経路なし)
!A ： あて先到達不能 (アドレスへの経路なし)
!S ： あて先到達不能 (近隣ではない)
!P ： あて先到達不能 (管理上の理由)
! ： HopLimit 値が異常
* ： プローブのタイムアウト
また、traceroute は以下のエラーを報告します。

```
traceroute: unknown host <host_name>
```

<host_name>で指定した送出先ホスト名から送出先 IP アドレスが解決できない。

```
traceroute: can't assign source address
```

送信元 IP アドレスの割り当てに失敗した。
(装置に存在しないアドレスを指定した場合など)

[実行例]

実行例 1

host から応答がある場合の実行例を示します。

```
# traceroute 192.168.1.1
traceroute to 192.168.1.1 from 192.168.5.2, 30 hops max, 46 byte packets
1     192.168.5.1             20.000 ms  20.000 ms  20.000 ms
2     192.168.1.1             41.000 ms  41.000 ms  41.000 ms
#
```

実行例 2

host から応答がない場合の実行例を示します。

```
# traceroute 192.168.1.1
traceroute to 192.168.1.1 from 192.168.5.2, 30 hops max, 46 byte packets
1    *  *  *
2    *  *  *
3    *  *  *
4    *  *  *
       :
30   *  *  *
#
```

実行例 3

応答に MPLS のラベル情報が含まれる場合の実行例を示します。

```
# traceroute 10.1.101.2 mpls
traceroute to 10.1.101.2 from 10.1.201.2, 30 hops max, 46 byte packets
1    10.1.201.1              1.000 ms  1.000 ms  1.000 ms Label1=17 ExpBits1=0
2    10.4.1.1                1.000 ms  1.000 ms  2.000 ms Label1=29 ExpBits1=0
3    10.5.1.1                2.000 ms  1.000 ms  2.000 ms Label1=16 ExpBits1=0
4    10.1.101.2              2.000 ms  2.000 ms  2.000 ms Label1=18 ExpBits1=0
#
```

62.1.3 telnet

[機能]

telnet サーバへの接続

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

telnet <host> [<port>] [{ipv4|ipv6}] [escape {<char>|none}] [srcaddr <srcaddr>] [tos <tos>]

[オプション]

<host>

接続先ホスト (telnet サーバ) を、以下の形式で指定します。

- ホスト名
- IPv4 アドレス
- IPv6 アドレス
  リンクローカルアドレスを指定する場合、アドレスに続けて"%<interface>" を指定して、どのインタフェースを使用するのか指定してください。たとえば、"fe80::1%lan0"のように指定します。

<port>

ポート番号を 1〜65535 の範囲の 10 進数で指定します。
省略時は、telnet ポート番号である 23 を指定したものとみなされます。

ipv4

IPv4 アドレスで telnet 接続する場合に指定します。
<host>にホスト名を指定した場合、そのホストに IPv4 と IPv6 の両方のアドレスがあるときには IPv4 アドレスで接続します。

ipv6

IPv6 アドレスで telnet 接続する場合に指定します。
<host>にホスト名を指定した場合、そのホストが IPv4 と IPv6 の両方のアドレスを持っていたときに IPv6 アドレスを使用します。
ipv4 も ipv6 も省略したときは、<host>がアドレス指定であればそのアドレスで、ホスト名指定であれば、そのホストに IPv4 アドレスまたは IPv6 アドレスのどちらかがあるときにはそのアドレスで、両方のアドレスがある場合は IPv6 アドレスで接続します。

escape {<char>|none}

エスケープ文字を指定します。エスケープ文字を使用しない場合は "none" を指定します。
telnet 接続中にエスケープ文字キーに続けて"q"キーを入力すると、telnet 接続を強制的に切断することができます。
エスケープ文字としてコントロール文字を指定する場合、"^"に続けて文字を指定します。たとえば、CTRL+A であれば"^A"を指定します。
"none"以外の文字列を指定した場合、最初の文字をエスケープ文字に指定したものとみなされます。
省略時は、"^]"(CTRL+]) を指定したものとみなされます。

srcaddr <srcaddr>

ソースアドレス (本ルータのアドレス) を、以下の形式で指定します。

- IPv4 アドレス
- IPv6 アドレス
  <host>で指定するアドレスと同じバージョンおよび同じスコープ (範囲) のアドレスを指定してください。
  省略時は、適切なアドレスが設定されます。

tos <tos>

TOS 値を 0〜ff の範囲の 16 進数で指定します。
<host>が IPv6 アドレスの場合は指定できません。
省略時は、0 を指定したものとみなされます。

[動作モード]

運用管理モード (一般ユーザクラス/管理者クラス)
構成定義モード (管理者クラス)

[説明]

telnet サーバが動作しているホストやルータに接続して、遠隔操作することができます。
telnet サーバから以下の情報を求められた場合は、本装置の情報 (括弧内の値) を通知します。

- 端末タイプ (VT100)
- 通信速度 (9600bps)
- 画面サイズ (画面行数、画面桁数)

[実行例]

以下に、実行例を示します。

```
# telnet 192.168.1.2                    他ルータにtelnet接続
Trying 192.168.1.2...                   接続手続き中
Connected to 192.168.1.2.               接続完了
Escape character is '^]'                エスケープ文字表示
Login:                                  他ルータのユーザ名入力
Password:                               他ルータのパスワード入力
login OK.                               他ルータにログイン成功
# exit                                  他ルータのプロンプト表示、exit実行
Connection closed by foreign host.      切断
#                                       本ルータのプロンプト表示
```

62.1.4 pwconv

[機能]

暗号化パスワードの表示

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

pwconv {common|unique}

[オプション]

common

共通パスワードを表示するときに指定します。

unique

装置固有パスワードを表示するときに指定します。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

平文パスワードを入力すると、暗号化パスワードに変換された結果が表示されます。
構成定義を設定する際に、平文パスワードを画面に表示したくない場合や、構成定義の作成を外部に委託するときに平文パスワードを伝えたくない場合などに、本コマンドで表示された暗号化パスワードを利用できます。
コマンドを実行すると以下のようなプロンプトが表示されますので、平文パスワードを 2 回入力してください。入力したパスワードは表示されません。2 回入力した平文パスワードが同一であれば暗号化パスワードに変換された結果が表示されます。同一でない場合はエラーメッセージが表示されます。

```
Password:
Retype password:
```

[注意]

コマンドを実行してから Password: のプロンプトが表示されるまでに入力した場合は入力した内容が表示されます。
平文パスパスワードの前後の空白はないものとして処理されます。平文パスワードに空白を含む場合はダブルクォートで囲んで入力してください。
平文パスワードとして何も入力しなかった場合や空白だけの平文パスワードを入力した場合はエラーメッセージが表示されます。
コマンドを連続実行した場合、セキュリティの観点から暗号化パスワードを表示する際に最大 3 秒間待たされることがあります。
装置固有パスワードを表示した場合、表示された暗号化パスワードは本コマンドを実行した装置個体でのみ使用できます。
TPM(Trusted Platform Module) を実装している装置で装置固有パスワードを表示した場合、TPM を利用した装置固有パスワードとなりますが、TPM でハードウェアエラーが発生した場合は以下のエラーメッセージを表示してコマンドが異常終了します。

```
<ERROR> detected HARD ERROR, cannot execute
```

[実行例]

```
# pwconv unique
Password:               平文パスワードを入力
Retype password:        再度、平文パスワードを入力
0oxLSOCZwI69dsGBz.      装置固有パスワードが表示される
#
```

62.1.5 dnconv

[機能]

電話番号変更処理の実施

[適用機種]

Si-R 570	Si-R 370		Si-R 240	Si-R 220B	

[入力形式]

dnconv <index>

[オプション]

<index>

一括変更処理の対象とする、電話番号変更予約情報を指定します。

- 0〜3
  電話番号変更予約情報 (dnconvinfo) の登録番号を指定します。
- all
  登録されている電話番号変更情報 (dnconvinfo) すべてを対象とする場合に指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

電話番号変更予約情報に従って、構成定義情報に登録されている電話番号を一括変更します。

[注意]

本コマンドでは、電話番号一括変更処理後の構成定義情報の保存 (save)、およびシステムのリセット (reset) は行いません。

[実行例]

- 特定の電話番号変更予約情報の一括変更処理

```
# dnconv 1
 ....
# dnconv 3
 ....
# save
# reset
```

- すべての電話番号変更予約情報の一括変更処理

```
# dnconv all
 ....
# save
# reset
```

62.1.6　rpon

[機能]

リモートパワーオン機能のための MagicPacket の送信

[適用機種]

Si-R 570 | Si-R 370 | Si-R 260B | Si-R 240 | Si-R 220B | Si-R 180

[入力形式]

rpon <host_number>

[オプション]

<host_number>

- ホストデータベース定義番号
  MagicPacket 送出先のホストデータベース定義番号を指定します。
- all
  ホストデータベースに登録されたリモートパワーオン対象の全ホストを指定します。

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

ホストデータベース定義番号により指定されたホストに対して、MagicPacket を送出します。
<host_number>が指定されないか、有効範囲から外れているか、またはそのホスト情報に MAC アドレスが設定されていない場合はなにもしません。
<hosts_number>に all が指定されている場合は、MAC アドレスが設定されておりリモートパワーオン非対象ホストではない全ホストに対して MagicPacket を送出します。

[実行例]

```
# rpon 2
#
```

62.1.7 diag

[機能]

メモリの診断

[適用機種]

Si-R 570

[入力形式]

diag [memory <kind>]

[オプション]

なし

すべての診断を実行

memory <kind>

- mainmemory
  装置本体のメモリ診断
- optioncard
  オプションカード内のメモリ診断
  対象となるオプションカードは以下のとおりです。
  - ATM25M 拡張モジュール H1
  - ATM155M 拡張モジュール H1
  - BRI4 ポート拡張モジュール H1

[動作モード]

運用管理モード (管理者クラス)
構成定義モード (管理者クラス)

[説明]

コマンド投入時、装置にリブートがかかり、再起動時に指定された診断を行います。
診断結果は、装置本体の CHECK ランプの表示内容にて判断します。診断結果が正常の場合は消灯、異常の場合は橙点灯します。

[注意]

diag コマンド投入によって、装置が再起動されます。
診断対象となるデバイスが正しく実装されていない場合、再起動亜度の信 d 何が行われませんので show system status コマンドの表示情報にてデバイスが正しく実装されていることを事前に確認してください。
装置本体の CHECK ランプが橙点灯している状態で、diag コマンドを投入すると、診断結果にかかわらず CHECK ランプが橙点灯しますので、clear logging error コマンドを投入して、事前にエラーログをクリアしておいてください。
診断正常終了後、運用を開始される場合は、装置本体の電源再投入、または、reset コマンドにて再起動を実施してください。

[実行例]

```
Si-R570# diag
Login :
```

第 63 章　commit コマンド 実行時の影響について

各構成定義コマンド で構成定義を変更後に commit コマンド を実行した時の影響について以下に示します。
なお、各構成定義コマンド の変更／追加／削除のそれぞれについて、影響は同じです。

種別	コマンド名	commit実行時影響
WAN情報	wan	(3)
ATM情報	atm	(3)
スイッチ情報	switch	(3)
LAN情報	lan bind	(3)
	lan mode	(3)
	lan mdi	(3)
	lan flowctl	(3)
	lan type	(3)
	lan mtu	(1)
	lan shaping	(2)
	lan backup	(3)
	lan recovery	(3)
	lan ip address	(1)
	lan ip alias	(1)
	lan ip dhcp service	(1)
	lan ip dhcp info	(1)
	lan ip proxyarp	(1)
	lan ip localproxyarp	(1)
	lan ip route	(1)
	lan ip rip use	(1)-1
	lan ip rip filter	(1)-1 ※1
	lan ip ospf use	(1)-1
	lan ip ospf cost	(1)
	lan ip ospf hello	(1)
	lan ip ospf dead	(1)
	lan ip ospf retrans	(1)
	lan ip ospf delay	(1)
	lan ip ospf priority	(1)
	lan ip ospf auth	(1)
	lan ip ospf passive	(1)
	lan ip vrf	(1)※3
	lan ip nat	(1)
	lan ip filter	(1)
	lan ip tos	(1)
	lan ip priority	(1)
	lan ip in-policy	(1)
	lan ip icmp	(1)
	lan ip multicast	(1)
	lan ip arp cycle	(3)
	lan ip arp static	(1)
	lan ip ids	(1)
	lan ip6 use	(1)
	lan ip6 ifid	(1)
	lan ip6 address	(1)
	lan ip6 ra	(1)
	lan ip6 route	(1)
	lan ip6 rip use	(1)-1
	lan ip6 rip site-local	(1)-1 ※1
	lan ip6 rip aggregate	(1)-1 ※1
	lan ip6 rip filter	(1)-1 ※1
	lan ip6 filter	(1)
	lan ip6 priority	(1)
	lan ip6 trafficclass	(1)
	lan ip6 in-policy	(1)
	lan bridge use	(3)
	lan bridge group	(1)
	lan bridge static	(1)
	lan bridge stp	(1)
	lan bridge filter	(1)
	lan bridge priority	(1)
	lan vrrp use	(3)
	lan vrrp auth	(1)
	lan vrrp group id	(3)
	lan vrrp group ad	(1)
	lan vrrp group preempt	(1)
	lan vrrp group trigger	(1)
	lan vrrp group action	(1)
	lan vrrp group vaddr	(1)
	lan mpls	(1)
	lan vlan bind	(2)
	lan vlan tag	(2)

LAN情報	lan macauth use	(2)
	lan macauth expire	(2)
	lan macauth aaa	(2)
	lan macauth security	(2)
相手情報	remote name	(2)
	remote autodial	(2)
	remote mtu	(1)
	remote shaping	(2)
	remote ap name	(2)
	remote ap move	(2)
	remote ap datalink	(3)
	remote ap ip	(2)
	remote ap multiroute	(2)
	remote ap limit	(2)
	remote ap disconnect	(1)
	remote ap ppp	(2)
	remote ap dial	(2)
	remote ap called	(2)
	remote ap connect	(7)
	remote ap idle	(2)
	remote ap step	(2)
	remote ap step2	(2)
	remote ap step3	(2)
	remote ap keep	(2)
	remote ap fr	(2)
	remote ap atm	(3)
	remote ap ipsec	(2)
	remote ap ike	(2)
	remote ap dvpn	(2)
	remote ap tunnel	(2)
	remote ap overlap	(2)
	remote ap sessionwatch	(1)
	remote ap mpls	(2)
	remote ppp	(2)
	remote ip address	(1)
	remote ip route	(1)
	remote ip rip use	(1)-1
	remote ip rip filter	(1)-1 ※1
	remote ip ospf use	(1)-1
	remote ip ospf cost	(1)
	remote ip ospf hello	(1)
	remote ip ospf dead	(1)
	remote ip ospf retrans	(1)
	remote ip ospf delay	(1)
	remote ip ospf auth	(1)
	remote ip ospf passive	(1)
	remote ip ospf multicast	(1)
	remote ip ospf checkmtu	(1)
	remote ip nat	(1)
	remote ip filter	(1)
	remote ip tos	(1)
	remote ip priority	(1)
	remote ip clp	(1)
	remote ip msschange	(1)
	remote ip multicast	(1)
	remote ip exp	(1)
	remote ip ids	(1)
	remote ip in-policy	(1)
	remote ip6 use	(1)
	remote ip6 ifid	(1)
	remote ip6 address	(1)
	remote ip6 ra	(1)
	remote ip6 route	(1)
	remote ip6 rip use	(1)-1
	remote ip6 rip site-local	(1)-1 ※1
	remote ip6 rip aggregate	(1)-1 ※1
	remote ip6 rip filter	(1)-1 ※1
	remote ip6 filter	(1)
	remote ip6 priority	(1)
	remote ip6 trafficclass	(1)
	remote ip6 exp	(1)
	remote ip6 clp	(1)
	remote ip6 in-policy	(1)

相手情報	remote bridge use remote bridge group remote bridge static remote bridge stp use remote bridge stp cost remote bridge stp priority remote bridge filter remote bridge priority remote mpls	(2) (1) (1) (2) (1) (1) (1) (1) (1)
SERIAL情報	serial	(3)
着信デフォルト情報	answer	(2)-2
テンプレート情報	template name template mtu template idle template interface pool template aaa template datalink template ppp template ip dns template ip address remote pool template ip filter template ip tos template ip priority template ip msschange template ip ids template ip in-policy template ip6 use template ip6 ifid template ip6 filter template ip6 priority template ip6 trafficclass template ip6 in-policy template combine template tunnel template sessionwatch template dvpn template ipsec template ike	(6) (7) (7) (8) (9) (6) (7) (7) (8) (1) (1) (1) (1) (1) (1) (7) (7) (1) (1) (1) (1) (6) (10) (10) (11) (10) (10)
動的VPN情報	dvpn server dvpn client	(1) (12)
AAA情報	aaa	(1)
ルーティング プロトコル情報	routemanage ip distance routemanage ip redist rip routemanage ip redist bgp routemanage ip redist bgp vrf routemanage ip redist ospf routemanage ip ecmp routemanage interface routemanage ip6 distance routemanage ip6 redist rip bgp as bgp id bgp vrf bgp mpls-resolution bgp network route bgp network igp bgp aggregate bgp full-route bgp redist bgp neighbor address bgp neighbor as bgp neighbor timers bgp neighbor medmetric bgp neighbor asprepend bgp neighbor localpref bgp neighbor nexthopself bgp neighbor ebgp-multihop bgp neighbor enforce-multihop bgp neighbor default-originate bgp neighbor family bgp neighbor source bgp neighbor filter bgp neighbor authentication	(1) ※1 (1) (1) (1) (1) (1) (1) (1) ※1 (1) (4) (4) (1) ※3 (4) (1) (1)-1 ※2 (1) (1)-1 ※3 (1) (1)-1 ※3 (1)-1 ※3 (1)-1 ※3 (1)-1 ※3 (1)-1 ※3 (1)-1 ※3 (1)-1 ※3 (1)-1 ※3 (1)-1 ※3 (1)-1 ※3 (1)-1 ※3 (1)-1 ※3 (1) ※5

ルーティング プロトコル情報	ospf ip id ospf ip area id ospf ip area type ospf ip area defcost ospf ip area range ospf ip area type3-lsa ospf ip area vlink id ospf ip area vlink hello ospf ip area vlink dead ospf ip area vlink retrans ospf ip area vlink delay ospf ip area vlink auth ospf ip definfo ospf ip summary ospf ip redist rip ip timers rip ip multipath rip ip redist rip ip neighbor rip ip gwfilter rip ip6 timers rip ip6 multipath rip ip6 redist	(4) (1)-1　※4 (1)-1　※4 (1) (1)-1 (1) (1)-1　※4 (1) (1) (1) (1) (1) (1) (1)-1 (1)-1 (1) (1) (1)-1 (1)-1 (1)-1 (1) (1) (1)-1
ブリッジ情報	bridge age bridge stp bridge ip routing bridge ip policy bridge ip6 routing bridge ip6 policy bridge vlan bridge inter-remote	(1) (1) (2)-1 (1) (2)-1 (1) (1) (1)
MPLS情報	mpls	(1)
マルチキャスト情報	multicast	(1)
ACL情報	acl	(1)
ポリシーグループ情報	policy-group	(1)
装置情報	snmp syslog time proxydns host password set schedule dnconvinfo updateinfo macauth password addact watchdog service consoleinfo telnetinfo sysdown mflag sysname loopback ip address loopback ip ospf loopback mpls serverinfo	(1) (1) (1) (1) (1) (0) (1) (1) (1) (1) (1) (5) (1) (1) (1) (1) (5) (1) (1)-1 (1) (1)

(0)　コマンドを実行すると、その直後から有効になります。

(1)　該当箇所の該当機能だけ停止／再開になります。

(1)-1　(1) に加え、該当経路の追加・削除が行われるため、本装置や隣接ルータでの経路変更がともないます。

(2)　該当論理インタフェースでの通信が中断されます。

(2)-1

(2) で該当論理インタフェースとはブリッジが有効で PPP で接続されているインタフェースです。

(2)-2 (2) で該当論理インタフェースとはすべての ISDN のインタフェースです。

(3) 該当物理回線が切断されます。

(4) 該当ルーティングプロトコルが再起動されます。

(5) 変更した定義を有効にするには、装置の再起動 (リセット) が必要となります。

(6) 該当テンプレートで着信した接続がすべて切断されます。

(7) 現在接続中の回線は設定変更前のままの定義で接続が保持されます。
設定変更後の新しい設定は定義変更後の接続から有効になります。

(8) 設定範囲の先頭を変更した場合は該当テンプレートで着信した接続がすべて切断されます。
設定範囲を縮小した場合は、該当テンプレートて着信した接続がすべて切断されます。
設定範囲の先頭を変更しなかった場合で、設定範囲を拡大したときだけ接続が維持されます。

(9) 該当テンプレートで AAA を利用中の場合 (template combine use aaa で動作中) には該当テンプレートで着信した接続がすべて切断されます。

(10) 該当テンプレートで IPsec を利用中の場合 (template datalink type ipsec で動作中) には該当テンプレートで着信した接続がすべて切断されます。

(11) 該当テンプレートで動的 VPN を利用中の場合 (template combine use dvpn で動作中) には該当テンプレートで接続がすべて切断されます。

(12) 相手情報が参照する場合は、(2) テンプレート情報が参照する場合は、(11) と同等です。
なお、dvpn client encode のみの変更は、(1) となります。

※ 1 設定以前の送受信経路に対しては適用されません。

※ 2 BGP ネットワークで設定されている経路が一時的に削除される場合があります。

※ 3 設定変更時、該当する BGP セッションが一時的に切断されます。

※ 4 設定変更時、該当するエリア全体の経路の変更をともなうため、その間通信に影響します。

※ 5 設定のあり・なしを変更した場合に、該当する BGP セッションが一時的に切断されます。

第 64 章　運用管理コマンド の仕様変更について (V30)

V30 で運用管理コマンド の仕様が変更されました。
以下に V30 および V21 のコマンド 入力形式の対応を示します。

モード 操作コマンド /ターミナル操作コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	管理者クラスに移行する	admin	対応コマンドなし
2	管理者クラスに移行する	su	対応コマンドなし
3	クラス、モード、構成定義階層を戻る、または、ログアウトする	exit	exit
4	構成定義モードに移行する	configure	対応コマンドなし
5	運用管理モードに戻る	end	対応コマンドなし
6	運用管理モードに戻る	quit	対応コマンドなし
7	構成定義階層を最上位階層に移動する	top	対応コマンドなし
8	構成定義階層をひとつ上位階層に移動する	up	対応コマンドなし
9	クラス、モード、構成定義階層を戻る	!	対応コマンドなし
10	ページャー機能の設定	terminal pager {enable|disable}	page <mode>
11	ターミナル画面サイズの設定	terminal window [column <column>] [line <line>]	env LINES=
12	漢字コードの設定	terminal charset {EUC|SJIS}	env KANJI=
13	入力プロンプト文字列の設定	terminal prompt login "<prompt>" terminal prompt user "<prompt>" terminal prompt admin "<prompt>"	env PROMPT=
14	コマンド実行日時表示機能の設定	terminal timestamp {enable|disable}	env TIMESTAMP=
15	操作エラーベル機能の設定	terminal bell {enable|disable}	env NOBELL=
16	コマンド実行履歴機能の設定	terminal logging line <line>	env HISTSIZE=
17	ターミナル情報の表示	show terminal	env
18	コマンド実行履歴の表示	show logging command [brief]	history [-t]
19	コマンド実行履歴の消去	clear logging command	history clear
20	コマンドエイリアス情報の設定	alias <alias> "<command>"	対応コマンドなし
21	コマンドエイリアス情報の表示	show alias [<name>]	対応コマンドなし
22	コマンドエイリアス情報の削除	clear alias [<name>]	対応コマンドなし

システム操作および表示コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	静的なシステム情報の表示	show system information	date, idinfo, sysinfo
2	動的なシステム情報の表示	show system status	date, uptime, sysinfo
3	解析情報の一括表示	show tech-support	tech-support tech-support [-c <count>] [-i <time>]
4	エラーログの表示	show logging error	elog
5	エラーログのクリア	clear logging error	elog -d
6	システムログ情報の表示	show logging syslog	dsplog
7	全統計情報のクリア	clear statistics	clear statistics
8	現在の装置の日付、時刻の表示	show date	date
9	現在の装置の日付、時刻の表示/設定	date [<YYYY/MM/DD.hh:mm:ss>]	date [<yymmddHHMMSS>]
10	リモートホストの日付、時刻を本装置に設定	rdate	rdate
11	装置の再起動	reset reset clear reset {config1|config2}	reset reset clear reset {config1|config2}
12	ファームウェアの更新	update	update

構成定義情報操作および表示コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	編集中構成定義情報の表示	show candidate-config [<config>] show candidate-config all [<config>]	show [<コマンド名>] show -a [<コマンド名>]
2	動作中構成定義情報の表示	show running-config [<config>] show running-config all [<config>]	show -r [<コマンド名>] show -a -r [<コマンド名>]
3	起動用構成定義情報の表示	show startup-config [<config>]	対応コマンドなし
4	構成定義情報の差分の表示	diff <src_filename> <dst_filename>	diff <config1> <config2>
5	編集中構成定義情報の削除	delete <config>	delete <コマンド名>
6	構成定義の読み込み	load running-config load startup-config load config1 load config2	load running 対応コマンドなし load config1 load config2
7	構成定義情報の保存	save save {config1|config2}	save save {config1|config2}
8	構成定義情報の動的反映	commit	enable enable all　(※V30ではreset)
9	構成定義情報の変更破棄	discard	対応コマンドなし

Ethernet のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	Ethernet物理ポートの情報の表示	show ether [slot <slot> [line <line>]]	stlan [<slot> [<port>]] laninfo [number]
2	Ethernet物理ポートの統計情報の表示	show ether statistics [slot <slot> [line <line>]]	stlan [<slot> [<port>]]
3	Ethernet物理ポートの統計情報のクリア	clear ether statistics [slot <slot> [line <line>]]	stlan clear

ISDN 回線のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	ISDN回線状態の表示	show isdn	lineis, apstat
2	ISDNのアカウントの表示	show isdn account	isdnstat -{D|d|r} [<index>]
3	ISDN回線の統計情報の表示	show isdn statistics circuit	stins [<slot> [<line> [<channel>]]]
4	PIAFS統計情報の表示	show isdn statistics piafs	stpiafs
5	ISDNのアカウント情報のクリア	clear isdn account	isdnstat clear -{D|d|r} [<index>]
6	ISDN回線の統計情報のクリア	clear isdn statistics circuit	stins clear
7	PIAFS統計情報のクリア	clear isdn statistics piafs	stpiafs clear

フレームリレーのカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	フレームリレー回線状態の表示	show fr	lineis, apstat, frstat
2	フレームリレー回線の統計情報の表示	show fr statistics circuit	stins [<slot> [<line> [<channel>]]]
3	フレームリレー回線のPVC統計情報の表示	show fr statistics vc	frstat
4	フレームリレー回線の統計情報のクリア	clear fr statistics circuit	stins clear
5	フレームリレー回線のPVC統計情報のクリア	clear fr statistics vc	frstat clear

専用線のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	専用線状態の表示	show hsd	lineis, apstat
2	専用線の統計情報の表示	show hsd statistics circuit	stins [<slot> [<line> [<channel>]]]
3	専用線の統計情報のクリア	clear hsd statistics circuit	stins clear

ATM 回線のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	ATM回線状態の表示	show atm [brief]	lineis, apstat, statm
2	ATM統計情報の表示	show atm statistics circuit [slot <slot>]	statm [<slot> [<vpi_value> <vci_value>]]
3	VC統計情報の表示	show atm statistics vc	statm [<slot> [<vpi_value> <vci_value>]]
4	ATM回線のLLC/SNAPごとの統計情報表示	show atm statistics llc-snap	対応コマンドなし
5	ATM統計情報のクリア	clear atm statistics	statm clear

モデム接続のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	モデム回線状態の表示	show modem	lineis, apstat
2	モデムのアカウントの表示	show modem account	mdmstat -{D|d|r}
3	モデムのアカウントのクリア	clear modem account	mdmstat clear [-{D|d|r}]

インタフェースのカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	インタフェース情報の表示	show interface [interface <interface_name>]	対応コマンドなし
2	インタフェース情報の簡易表示	show interface brief [interface <interface_name>]	対応コマンドなし
3	インタフェースエントリ数の表示	show interface summary	対応コマンドなし
4	インタフェース情報の詳細表示	show interface detail [interface <interface_name>]	netstat -i -d -b
5	インタフェース統計情報の表示	show interface statistics [interface <interface_name>]	netstat -i -d -b
6	接続先情報の表示	show access-point	apstat
		show access-point remote <remote_number> [ap <ap_number>]	apstat <remote_number> [<ap_number>]
		show access-point access-point <ap_name>	apstat <ap_name>
7	テンプレート着信の通信状態	show template [interface <interface_name>]	tempstat -i [-I <interface>] [-t <temp_no>]
8	テンプレート着信の統計情報の表示	show template statistics	tempstat -s [-t <temp_no>]
9	テンプレート着信の通信状態と統計情報の表示	show template	tempstat
		show template statistic	
10	インタフェースの統計情報のクリア	clear interface statistics [interface <interface_name>]	netstat clear -i
11	テンプレート着信の統計情報クリア	clear template statistics	tempstat clear [-t <temp_no>]

ARP エントリの表示、削除

項	機能	入力形式(V30)	入力形式(V21)
1	ARPエントリの表示	show arp show arp <ip_address>	arp [-a] arp <address>
2	ARPエントリの表示	show arp summary	対応コマンドなし
3	ARPエントリの削除	clear arp clear arp <ip_address>	arp -d {all|-a} arp -d <address>

Neighbor Cache テーブルエントリの表示、削除

項	機能	入力形式(V30)	入力形式(V21)
1	Neighbor Cacheテーブルエントリの表示	show ndp [<ipv6_address>] show ndp summary	対応コマンドなし
2	Neighbor Cacheエントリの削除	clear ndp [<ipv6_address>]	対応コマンドなし

ルーティングテーブル情報・統計などの表示、クリア操作コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	ルーティングテーブル情報の表示	show ip route [all]	routestat ip route
		show ip route connected [all]	routestat ip route connected
		show ip route static [all]	routestat ip route static
		show ip route rip [all]	routestat ip route rip
		show ip route bgp [all]	routestat ip route bgp
		show ip route ospf [all]	routestat ip route ospf
		show ip route dns [all]	routestat ip route dns
		show ip route ike [all]	対応コマンドなし
		show ip route destination <ip_address>/<mask> [all]	routestat ip route <ip_address>/<mask>
		show ip route destination <ip_address>/<mask> longer-prefixes [all]	routestat ip route <ip_address>/<mask> inexact
2	ルーティングテーブルの経路情報数の表示	show ip route summary [all]	routestat ip route summary
3	IPカーネルのルーティングテーブルの表示	show ip route kernel	netstat -r -f inet
		show ip route kernel longest-match <ip_address>	対応コマンドなし
		show ip route kernel summary	対応コマンドなし
4	ECMP統計情報の表示	show ip route kernel ecmp statistics	netstat -e [-f inet]
5	ECMP統計情報のクリア	clear ip route kernel ecmp statistics	netstat clear -e
6	IPv6ルーティングテーブル情報の表示	show ipv6 route [all]	routestat ip6 route
		show ipv6 route connected [all]	routestat ip6 route connected
		show ipv6 route static [all]	routestat ip6 route static
		show ipv6 route rip [all]	routestat ip6 route rip
		show ipv6 route dns [all]	routestat ip6 route dns
		show ipv6 route dhcp [all]	routestat ip6 route dhcp
		show ipv6 route ike [all]	対応コマンドなし
		show ipv6 route destination <prefix>/<prefixlen> [all]	routestat ip6 route <prefix>/<prefixlen>
		show ipv6 route destination <prefix>/<prefixlen> longer-prefixes [all]	routestat ip6 route <prefix>/<prefixlen> [inexact]
7	IPv6ルーティングテーブルの経路数の表示	show ipv6 route summary [all]	routestat ip6 route summary
8	IPv6カーネルのルーティングテーブルの表示	show ipv6 route kernel	netstat -r -f inet6
		show ipv6 route kernel longest-match <ipv6_address>	対応コマンドなし
		show ipv6 route kernel summary	対応コマンドなし

RIP 情報の表示、クリア操作コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	RIP経路情報の表示	show ip rip route	routestat ip rip
2	RIPプロトコル情報の表示	show ip rip protocol	routestat ip rip proto
3	RIP統計情報のクリア	clear ip rip statistics	routestat clear
4	IPv6 RIP経路情報の表示	show ipv6 rip route	routestat ip6 rip
5	IPv6 RIPプロトコル情報の表示	show ipv6 rip protocol	routestat ip6 rip proto

BGP 情報の表示、クリア操作コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	BGP経路情報の表示	show ip bgp route	routestat bgp
		show ip bgp route address <ip_address>/<mask> detail	routestat bgp [<address>/<mask>
		show ip bgp route address <ip_address>/<mask> longer-prefixes	routestat bgp [<address>/<mask> [inexact]]
4	BGP経路情報数の表示	show ip bgp route summary	対応コマンドなし
5	BGPセッションの状態表示	show ip bgp status	routestat bgp summary
6	BGP隣接情報の表示	show ip bgp neighbors [address <ip_address>]	routestat bgp nbr [<neighbor>]
7	BGP VPNv4経路情報の表示	show ip bgp vpnv4 route [vrf <vrf_number>]	routestat bgp vrf [<vrf_number>]
8	BGP統計情報のクリア	clear ip bgp statistics	routestat clear

OSPF 情報の表示、クリア操作コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	OSPF経路情報の表示	show ip ospf route	routestat ip ospf
2	OSPF情報の表示	show ip ospf protocol	routestat ip ospf proto
3	OSPF LSAデータベース情報の表示	show ip ospf database	routestat ip ospf lsa
4	OSPF LSAデータベース情報の表示	show ip ospf database self-originate	routestat ip ospf lsa self
5	OSPF LSAデータベース情報の表示	show ip ospf database lsa <type> detail	routestat ip ospf lsa router routestat ip ospf lsa net routestat ip ospf lsa sum routestat ip ospf lsa asbr routestat ip ospf lsa asex routestat ip ospf lsa nssa
6	OSPF LSAデータベース情報の表示	show ip ospf database lsa <type> ls-id <link_id> detail	routestat ip ospf lsa router <link_id> routestat ip ospf lsa net <link_id> routestat ip ospf lsa sum <link_id> routestat ip ospf lsa asbr <link_id> routestat ip ospf lsa asex <link_id> routestat ip ospf lsa nssa <link_id>
7	OSPF LSAデータベース情報の表示	show ip ospf database lsa <type> self-originate detail	routestat ip ospf lsa router self routestat ip ospf lsa net <link_id> self routestat ip ospf lsa sum <link_id> self routestat ip ospf lsa asbr <link_id> self routestat ip ospf lsa asex <link_id> self routestat ip ospf lsa nssa <link_id> self
8	OSPF LSAデータベース情報の表示	show ip ospf database lsa <type> adv-router <router_id> detail	routestat ip ospf lsa net <link_id> adv <router_id> routestat ip ospf lsa sum <link_id> adv <router_id> routestat ip ospf lsa asbr <link_id> adv <router_id> routestat ip ospf lsa asex <link_id> adv <router_id> routestat ip ospf lsa nssa <link_id> adv <router_id>
9	OSPFインタフェース情報の表示	show ip ospf interface	routestat ip ospf if
10	OSPF隣接ルータ情報の表示	show ip ospf neighbor	routestat ip ospf nbr
11	OSPF隣接ルータ情報の表示	show ip ospf neighbor router-id <router_id> detail	routestat ip ospf nbr <router_id>
12	OSPF統計情報のクリア	clear ip ospf statistics	routestat clear

VPNv4 ルーティングテーブル情報の表示

項	機能	入力形式(V30)	入力形式(V21)
1	VPNv4 ルーティングテーブル情報の表示	show ip vpnv4 route [vrf <vrf_number>] [all]	routestat ip route vrf [<vrf_number>]
2	VPNv4 ルーティングテーブル経路情報数の表示	show ip vpnv4 route [vrf <vrf_number>] summary [all]	対応コマンドなし

パケットの統計情報の表示、クリア操作コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	IPパケットの統計情報の表示	show ip traffic	netstat -s
		show ip traffic {tcp|udp|ip|icmp|igmp|ipsec|pim}	netstat -s -p {tcp|udp|ip|icmp|igmp|ipsec|pim}
2	IPパケットの統計情報のクリア	clear ip traffic	netstat clear -s
3	IPv6パケットの統計情報の表示	show ipv6 traffic	netstat -s
		show ipv6 traffic {ip|icmp|tcp|udp|ipsec}	netstat -s -p {tcp6|udp6|ip6|icmp6|ipsec6}
4	IPv6パケットの統計情報のクリア	clear ipv6 traffic	netstat clear -s

IP フィルタのカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	IPフィルタテーブル表示	show ip filter [interface <interface_name>] [all]	filterstat -t -f inet [<interface>]
2	IPフィルタの統計情報の表示	show ip filter statistics [interface <interface_name>]	filterstat -s -f inet [<interface>]
3	IPフィルタのフィルタテーブル数の表示	show ip filter summary [interface <interface_name>] [total] [all]	対応コマンドなし
4	IPフィルタの統計情報のクリア	clear ip filter statistics	filterstat clear
5	IPv6フィルタテーブル表示	show ipv6 filter [interface <interface_name>] [all]	filterstat -t -f inet6 [<interface>]
6	IPv6フィルタの統計情報の表示	show ipv6 filter statistics [interface <interface_name>]	filterstat -s -f inet6 [<interface>]
7	IPv6フィルタのフィルタテーブル数の表示	show ipv6 filter summary [interface <interface_name>] [total] [all]	対応コマンドなし
8	IPv6フィルタの統計情報のクリア	clear ipv6 filter statistics	filterstat clear

IDS のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	IDSの統計情報の表示	show ip ids statistics [interface <interface_name>]	対応コマンドなし
2	IDSの統計情報のクリア	clear ip ids statistics	対応コマンドなし

NAT のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	NAT変換テーブルの表示	show ip nat interface [<interface_name>] [all]	natstat -t [<interface>]
2	NATの統計情報の表示	show ip nat statistics	natstat または natstat -s
3	NAT変換テーブル数の表示	show ip nat summary [interface <interface_name>] [all]	対応コマンドなし
4	NATの統計情報のクリア	clear ip nat statistics	natstat clear

マルチキャストのカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	マルチキャストグループ情報の表示	show ip multicast group [interface <interface_name>] [group <group_address>]	mcstat group
2	マルチキャストインタフェース情報の表示	show ip multicast interface [interface <interface_name>]	mcstat interface
3	マルチキャストインタフェースの統計情報の表示	show ip multicast interface statistics [interface <interface_name>]	netstat -g
4	PIM-SM のランデブーポイント情報の表示	show ip multicast pimsm rp [address <ip_address>]	mcstat rp
5	マルチキャストプロトコル情報の表示	show ip multicast protocol	mcstat protocol
6	マルチキャストルーティングテーブル情報の表示	show ip multicast route [source <ip_address>] [group <group_address>]	mcstat route
7	IPカーネルのマルチキャストルーティングテーブルの表示	show ip multicast route kernel [source <ip_address>] [group <group_address>]	netstat -g
		show ip multicast route kernel summary	対応コマンドなし
8	IPカーネルのマルチキャストルーティングテーブルの統計情報の表示	show ip multicast route kernel statistics [source <ip_address>] [group <group_address>]	netstat -g
9	マルチキャストパケットの統計情報の表示	show ip multicast statistics	netstat -sg
10	マルチキャストインタフェースの統計情報のクリア	clear ip multicast interface statistics	netstat clear -g
11	IPカーネルのマルチキャストルーティングテーブルの統計情報のクリア	clear ip multicast route kernel statistics	netstat clear -g
12	マルチキャストパケットの統計情報のクリア	clear ip multicast statistics	netstat clear -sg

DHCP のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	IPv4 DHCP運用状況の表示	show ip dhcp [interface <interface_name>]	dhcpstat -f inet [-I <interface>]
2	IPv6 DHCP運用状況の表示	show ipv6 dhcp [interface <interface_name>]	dhcpstat -f inet6 [-I <interface>]

動的 VPN の状態などの表示コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	動的VPNの情報交換クライアントユーザ情報の表示	show dvpn client user	対応コマンドなし
		show dvpn client user summary	
2	動的VPNの情報交換クライアントのセッション情報の表示	show dvpn client session	
		show dvpn client session summary	対応コマンドなし
3	動的VPNサーバ情報の表示	show dvpn server	対応コマンドなし
4	動的VPNサーバに登録されているユーザ情報の表示	show dvpn server user	対応コマンドなし
		show dvpn server user summary	
5	動的VPNサーバのセッション情報の表示	show dvpn server session	
		show dvpn server session summary	対応コマンドなし

IPsec/IKE のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	システムのIPsec SA情報の表示	show ipsec sa	ipsecstat
		show ipsec sa ike	ipsecstat isakmp
		show ipsec sa protocol	ipsecstat ipsec
2	IKE統計情報表示	show ike statistics	ikestat
		show ike statistics interface [interface <interface_name>]	ikestat -i [<interface>]
3	IKE統計情報のクリア	clear ike statistics	ikestat clear

VRRP のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	VRRP機能の各種情報の表示	show vrrp [interface <interface_name> [vrid <VRID>]] [brief]	vrrpstat [[-g] [<lan_number> [<vrid>]]] vrrpstat -G <lan_number> <vrid>
2	VRRP統計情報のクリア	clear vrrp statistics	vrrpstat clear

ブリッジのカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	ブリッジに関する状態および統計情報の表示	show bridge	bridgestat -l
		show bridge group [<group_id>]	bridgestat -l -g [<group_id>]
		対応コマンドなし	bridgestat -l -I <interface>
		show bridge summary	bridgestat -t
2	ブリッジのインタフェース状態および統計情報の表示	show bridge status	bridgestat -I
		show bridge status interface <interface_name>	bridgestat -i -I <interface>
		show bridge status group [<group_id>]	bridgestat -i -g [<group_id>]
3	ブリッジ関連の統計情報クリア	clear bridge statistics	bridgestat clear [-I <interface>]
4	スパニングツリー情報の表示	show spanning-tree	bridgestat -s
		show spanning-tree root	対応コマンドなし
		show spanning-tree bridge	対応コマンドなし
		show spanning-tree active	対応コマンドなし
		show spanning-tree interface <interface_name>	bridgestat -s -I <interface>
		show spanning-tree detail	対応コマンドなし
		show spanning-tree brief	bridgestat -s
5	スパニングツリー関連の統計情報クリア	clear spanning-tree statistics	対応コマンドなし

MPLS のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	MPLSインタフェース情報の表示	show mpls [interface <interface_name>]	mplsstat status
2	MPLS FTNテーブル情報の表示	show mpls ftn [address <ip_address>[/<mask>]] [detail]	mplsstat ftn [<address>[/<mask>]] [detail]
3	MPLS ILMテーブル情報の表示	show mpls ilm [address <ip_address>[/<mask>]] [detail]	mplsstat ilm [<address>[/<mask>]] [detail]
4	LDPインタフェース情報の表示	show mpls ldp [interface <interface_name>] [detail]	ldpstat interface [{<interface> | detail}]
5	LDP近隣情報の表示	show mpls ldp adjacency	ldpstat adjacency
6	LDP FECテーブル情報の表示	show mpls ldp fec	ldpstat fec
7	LDPセッション情報の表示	show mpls ldp session [address <ip_address>] [detail]	ldpstat session [{<address> | detail}]
8	LDPの状態の表示	show mpls ldp summary	ldpstat [status]
9	LDP VC情報の表示	show mpls ldp vc	ldpstat vc
10	MPLSインタフェース統計情報の表示	show mpls statistics [interface <interface_name>]	mplsstat interface [{<interface> | detail}]
11	MPLSの状態の表示	show mpls summary	mplsstat status
12	MPLS VCテーブル情報の表示	show mpls vc [detail]	mplsstat vc [detail]
		show mpls vc vcid <vc_id> [detail]	mplsstat vc <vc_id> [detail]
		show mpls vc interface <interface_name> [detail]	mplsstat vc <interface> [detail]
13	MPLS VRFテーブル情報の表示	show mpls vrf [vrf <vrf_number>] [address <ip_address>[/<mask>]] [detail]	mplsstat vrf [<vrf_number>] [<address>[/<mask>]] [detail]
14	MPLSインタフェース統計情報のクリア	clear mpls statistics [interface <interface_name>]	mplsstat clear
15	MPLS FTNテーブル統計情報のクリア	clear mpls statistics ftn [address <ip_address>[/<mask>]]	mplsstat clear ftn [<address>[/<mask>]]
16	MPLS ILMテーブル統計情報のクリア	clear mpls statistics ilm [address <ip_address>[/<mask>]]	mplsstat clear ilm [<address>[/<mask>]]
17	MPLS VCテーブル統計情報のクリア	clear mpls statistics vc	mplsstat clear vc
		clear mpls statistics vc vcid <vc_id>	mplsstat clear vc <vc_id>
		clear mpls statistics vc interface <interface_name>	mplsstat clear vc <interface>
18	MPLS VRFテーブル統計情報のクリア	clear mpls statistics vrf [vrf <vrf_number>] [address <ip_address>[/<mask>]]	mplsstat clear vrf [<vrf_number>] [<address>[/<mask>]]

UPnP のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	UPnP状態情報の表示	show upnp	upnpstat
2	UPnP統計情報情報の表示	show upnp statistic	upnpstat statistic
3	UPnPポートマッピング情報の表示	show upnp portmapping	upnpstat portmapping
4	UPnP統計情報のクリア	clear upnp statistic	upnpstat clear
5	UPnPポートマッピングエントリの削除	clear upnp portmapping	upnpctl clear portmapping

SSH ホスト認証用公開鍵の表示

項	機能	入力形式(V30)	入力形式(V21)
1	SSHホスト認証用公開鍵の表示	show ssh server key {dsa|rsa}	sshkey {dsa|rsa}

ソケット状態の表示

項	機能	入力形式(V30)	入力形式(V21)
1	ソケット状態の表示	show socket [{ ip | ipv6 }]	netstat

トレースの表示、クリア操作コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	PPPフレームトレースの表示	show trace ppp	ppptrace
2	PPPoEフレームトレースの表示	show trace pppoe	pppoetrace
3	IKEトレース情報表示	show trace ike	iketrace
4	IKEトレース情報の消去	対応コマンドなし	iketrace clear
5	モデム制御トレースの表示	show trace modem	mdmtrace
6	SSHサーバ機能のトレース情報の表示	show trace ssh	sshtrace
7	SSHサーバ機能トレース情報の消去	clear trace ssh	sshtrace clear

回線制御コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	MP使用時のチャネル数増加	addlink remote <remote_number> ap <ap_number> addlink access-point <ap_name>	addlink <remote_number> <ap_number> addlink <ap_name>
2	MP使用時のチャネル数減少	dellink remote <remote_number> ap <ap_number> dellink access-point <ap_name>	dellink <remote_number> <ap_number> dellink <ap_name>
3	切断、または閉塞の実施	offline lan [<lan_number>] offline remote [<remote_number> ap <ap_number>] offline access-point <ap_name> offline template interface <interface_name> offline template <template_number> [uid <user_id>]	close <lan_number> disconnect <remote_number> <ap_number> disconnect <ap_name> disconnect template <ifname> disconnect template <template_number> [<user_id>]
4	接続、または閉塞解除の実施	online lan [<lan_number>] online remote [<remote_number> ap <ap_number>] [id <id> <password>]] online access-point <ap_name> online template <template_number> uid <user_id>	open <lan_number> connect <remote_number> <ap_number> [<id> <password>] connect <ap_name> 対応コマンドなし

VRRP 制御コマンド

項	機能	入力形式(V30)	入力形式(V21)
1	VRRPの手動停止および再開始	vrrp action [interface <interface_name>] [vrid <VRID>] disable vrrp action [interface <interface_name>] [vrid <VRID>] enable	対応コマンドなし 対応コマンドなし
2	VRRPプリエンプトモードの制御	vrrp preempt-permit [interface <interface_name>] [vrid <vrid>] [interval <interval>]	vrrpctl preempt on {<lan_number>|all} [{<vrid>|all} [<interval>]]

その他のコマンド

項	機能	入力形式(V30)	入力形式(V21)
1	ICMPエコー要求パケットの送信	IPアドレス指定： ping <ip_address>[%<interface_name>] [source <ip_address>] [repeat [<count>]] [size <dec>] [tos <hex>] [ttl <dec>] [timeout <dec>] [df] ホスト名指定： ping <host_name> [{ v4 | v6 }] [source <ip_address>] [repeat [<count>]] [size <dec>] [tos <hex>] [ttl <dec>] [timeout <dec>] [df]	ping [-{r|v|rv}] [-S <src_addr>] [-T <ttl>] <host> [<timeout>] ping -s [-{r|v|rv}] [-S <src_addr>] [-T <ttl>] <host> [<packetsize> [<count>]] ping6 <address>[%<interface>]
2	ネットワーク経路の表示	IPアドレス指定： traceroute <ip_address> [source <src_ip_address>] [size <data_size>] [timeout <timeout>] [mpls] [df] ホスト名指定： traceroute <host_name> [v4 | v6] [source <src_ip_address>] [size <data_size>] [timeout <timeout>] [mpls] [df]	traceroute [-S <src_addr>] [-M] <host> [<data_size>]
3	telnetサーバへの接続	telnet <host> [<port>] [{ipv4|ipv6}] [escape {<char>|none}] [addr <addr>] [tos <tos>]	telnet [{-e <escape_char>|-E}] [-S <src_addr>] [-T <tos>] [{-4|-6}] <host> [<port>]
4	電話番号変更処理の実施	dnconv <index>	dnconv <index>
5	リモートパワーオン機能のためのMagicPacketの送信	rpon <host_number>	rpon <host_number>

第 65 章　V30 との非互換について

以下の内容について V30 と比較して非互換があります。

65.1　remote ap/template ipsec ike encrypt/ike proposal encrypt コマンドについて

remote ap/template ipsec ike encrypt/ike proposal encrypt コマンドの AES-CBC の指定方法が以下に変更になります。なお、V30 以前の構成定義はそのまま使用可能ですが、自動的に新しいフォーマットに変換されます。

V30以前でのフォーマット	本バージョンでのフォーマット
aes-cbc	aes-cbc-128

65.2 template sessionwatch コマンド について

template sessionwatch コマンド の指定方法が以下に変更になります。なお、V30 の構成定義はそのまま使用可能ですが、自動的に新しいフォーマットに変換されます。

V30 での指定方法

```
template [<number>] sessionwatch 192.168.1.1
```

本バージョンでの指定方法

```
template [<number>] sessionwatch address 192.168.1.1
```

65.3　RADIUS クライアント機能のサーバ定義について

RADIUS クライアント機能のサーバ定義で、1 サーバのみを定義していたものを、複数サーバ指定できるように変更します。なお、V30 の構成定義はそのまま使用可能ですが、自動的に新しいフォーマットに変換されます。

V30 での指定方法

```
aaa [<number>] radius client server-info auth address 192.168.1.1
aaa [<number>] radius client server-info auth secret sharedpass
aaa [<number>] radius client server-info auth port 1812
aaa [<number>] radius client server-info accounting address 192.168.1.1
aaa [<number>] radius client server-info accounting secret sharedpass
aaa [<number>] radius client server-info accounting port 1813
```

本バージョンでの指定方法

```
aaa [<number>] radius client server-info auth [<number>] address 192.168.1.1
aaa [<number>] radius client server-info auth [<number>] secret sharedpass
aaa [<number>] radius client server-info auth [<number>] port 1812
aaa [<number>] radius client server-info accounting [<number>] address 192.168.1.1
aaa [<number>] radius client server-info accounting [<number>] secret sharedpass
aaa [<number>] radius client server-info accounting [<number>] port 1813
```

Si-R シリーズ　コマンドリファレンス

P3NK-2192-01Z0

発行日　　2006年9月

発行責任　　富士通株式会社

• 本書の一部または全部を無断で他に転載しないよう、お願いいたします。
• 本書は、改善のために予告なしに変更することがあります。
• 本書に記載されたデータの使用に起因する第三者の特許権、その他の権利、損害については、 弊社はその責を負いません。