P3NK-5322-02Z0

FUJITSU Network Si-R
Si-R Gシリーズ

コマンドリファレンス　V3

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。

2015年8月初版
2016年7月第2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。
Copyright FUJITSU LIMITED 2015 - 2016

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ます。

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。

ネットワーク設定を初めて行う方でも「機能説明書」に分かりやすく記載していますので、安心してお読みいただけます。

本書の構成

本書では構成定義コマンドを説明しています。

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

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戻ります。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．ログインパスワードの削除

```
# delete password admin 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。
- 版数アップによりコマンド表示項目が追加または変更となることがあります。本書での記載内容に沿った設定ができない場合は、コマンドユーザーズガイドの「1.4.4 コマンド引数補完／説明表示／形式表示機能」（P.19）の操作で表示される引数名とその説明を参照してください。

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 G110　ご利用にあたって	Si-R G110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。
コマンドユーザーズガイド	コマンドを使用して、時刻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。
コマンドリファレンス（本書）	構成定義コマンド、運用管理コマンド、およびその他の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。
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。
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。
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。
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。
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。

目次

第 1 章　パスワード情報の設定 31

1.1　パスワード情報 32
1.1.1　password format 32
1.1.2　password admin set 34
1.1.3　password user set 36
1.1.4　password aaa 38
1.1.5　password authtype 39

第 2 章　WAN 情報の設定 40

2.1　回線共通情報 41
2.1.1　wan description 41
2.1.2　wan use 42
2.1.3　wan bind 43
2.1.4　wan line 44

2.2　データ通信モジュール情報 45
2.2.1　wan modemmodule condition mode 45
2.2.2　wan modemmodule condition level 46
2.2.3　wan modemmodule condition watch 47
2.2.4　wan modemmodule condition connect mode 48
2.2.5　wan modemmodule condition history dupcut 49

2.3　SNMP 関連情報 50
2.3.1　wan snmp trap linkdown 50
2.3.2　wan snmp trap linkup 51

第 3 章　ether グループ情報の設定 52

3.1　ether グループ共通情報 53
3.1.1　ethergroup vlan mode 53

3.2　ether グループポート間アクセス制御情報 54
3.2.1　ethergroup access-control mode 54

3.3　ブリッジグループ関連情報 55
3.3.1　ethergroup bridgegroup use 55
3.3.2　ethergroup bridgegroup group 56
3.3.3　ethergroup bridgegroup control 57

第 4 章　ポート情報の設定 58

4.1　ether 共通情報 59
4.1.1　ether description 59
4.1.2　ether use 60
4.1.3　ether media 61
4.1.4　ether mode 62
4.1.5　ether duplex 63
4.1.6　ether mdi 64
4.1.7　ether flowctl 66
4.1.8　ether type 67

4.2　STP 情報 69
4.2.1　ether stp use 69
4.2.2　ether stp domain cost 70
4.2.3　ether stp domain priority 71

4.3　VLAN 関連情報 72
4.3.1　ether vlan tag 72
4.3.2　ether vlan untag 73
4.3.3　ether vlan primap mode 75
4.3.4　ether vlan primap rule 77

4.4　ポート閉塞関連情報 79

4.4.1 ether recovery . . . 79
4.5 シェーピング関連情報 . . . 81
4.5.1 ether shaping . . . 81
4.5.2 ether shaping-opt tc . . . 83
4.6 WFQ 関連情報 . . . 84
4.6.1 ether priority ip . . . 84
4.6.2 ether priority ipv6 . . . 86
4.7 MAC アドレス認証情報 . . . 88
4.7.1 ether macauth use . . . 88
4.7.2 ether macauth aaa . . . 90
4.7.3 ether macauth authenticated-mac . . . 91
4.7.4 ether macauth expire . . . 93
4.7.5 ether macauth vlan assign . . . 94
4.7.6 ether macauth vid . . . 95
4.8 IEEE802.1X 認証情報 . . . 96
4.8.1 ether dot1x use . . . 96
4.8.2 ether dot1x aaa . . . 98
4.8.3 ether dot1x quietperiod . . . 99
4.8.4 ether dot1x txperiod . . . 100
4.8.5 ether dot1x supptimeout . . . 101
4.8.6 ether dot1x maxreq . . . 102
4.8.7 ether dot1x reauthperiod . . . 103
4.8.8 ether dot1x vlan assign . . . 104
4.8.9 ether dot1x vid . . . 105
4.9 SNMP 関連情報 . . . 106
4.9.1 ether snmp trap linkdown . . . 106
4.9.2 ether snmp trap linkup . . . 107
4.10 バックアップポート関連情報 . . . 108
4.10.1 backup mode . . . 108
4.10.2 backup standby . . . 109
第 5 章 STP 情報の設定 . . . 110
5.1 STP 情報 . . . 111
5.1.1 stp mode . . . 111
5.1.2 stp age . . . 112
5.1.3 stp delay . . . 113
5.1.4 stp hello . . . 114
5.1.5 stp domain priority . . . 115
第 6 章 VLAN 情報の設定 . . . 116
6.1 VLAN 共通情報 . . . 117
6.1.1 vlan description . . . 117
6.1.2 vlan forward . . . 118
6.2 ブリッジグループ関連情報 . . . 119
6.2.1 vlan bridgegroup use . . . 119
6.2.2 vlan bridgegroup group . . . 120
6.2.3 vlan bridgegroup macfilter . . . 121
6.2.4 vlan bridgegroup macfilter move . . . 123
6.3 ARP 認証関連情報 . . . 124
6.3.1 vlan arpauth use . . . 124
6.3.2 vlan arpauth aaa . . . 125
6.3.3 vlan arpauth obstruction . . . 126
6.3.4 vlan arpauth dummymac . . . 127
6.3.5 vlan arpauth expire . . . 128
6.3.6 vlan arpauth overflow . . . 129
6.3.7 vlan arpauth type . . . 130
6.3.8 vlan arpauth authenticated-ip . . . 131

第 7 章　MAC 情報の設定 132
7.1　MAC 情報. 133
7.1.1　mac age 133
第 8 章　pseudo ether 情報の設定 134
8.1　pseudo ether インタフェース共通情報 135
8.1.1　pseudo-ether description 135
8.1.2　pseudo-ether use 136
8.1.3　pseudo-ether bind. 137
8.1.4　pseudo-ether startup-delay. 138
8.2　VLAN 関連情報. 139
8.2.1　pseudo-ether vlan untag 139
8.3　SNMP 関連情報. 140
8.3.1　pseudo-ether snmp trap linkdown 140
8.3.2　pseudo-ether snmp trap linkup. 141
第 9 章　lan 情報の設定 142
9.1　lan 共通情報. 143
9.1.1　lan description 143
9.1.2　lan mtu 144
9.1.3　lan shaping 145
9.1.4　lan shaping-opt tc. 147
9.2　IP 関連情報 148
9.2.1　lan ip address. 148
9.2.2　lan ip alias 150
9.2.3　lan ip dhcp service 152
9.2.4　lan ip dhcp info 153
9.2.5　lan ip dhcp macauth use 157
9.2.6　lan ip dhcp macauth db. 158
9.2.7　lan ip dhcp macauth aaa 159
9.2.8　lan ip dhcp macauth type 160
9.2.9　lan ip proxyarp 161
9.2.10　lan ip localproxyarp. 162
9.2.11　lan ip route. 163
9.2.12　lan ip rip use 165
9.2.13　lan ip rip filter act. 167
9.2.14　lan ip rip filter move 169
9.2.15　lan ip rip filter route 170
9.2.16　lan ip rip filter set metric. 172
9.2.17　lan ip ospf use 173
9.2.18　lan ip ospf cost. 174
9.2.19　lan ip ospf hello. 175
9.2.20　lan ip ospf dead. 176
9.2.21　lan ip ospf retrans 177
9.2.22　lan ip ospf delay. 178
9.2.23　lan ip ospf priority. 179
9.2.24　lan ip ospf auth type. 180
9.2.25　lan ip ospf auth textkey. 181
9.2.26　lan ip ospf auth md5key 182
9.2.27　lan ip ospf passive 183
9.2.28　lan ip nat mode 184
9.2.29　lan ip nat static. 186
9.2.30　lan ip nat static default. 188
9.2.31　lan ip nat rule 189
9.2.32　lan ip nat wellknown. 191
9.2.33　lan ip nat destination 193
9.2.34　lan ip nat appli. 195
9.2.35　lan ip filter. 196

9.2.36 lan ip filter move 200
9.2.37 lan ip filter default 201
9.2.38 lan ip tos 202
9.2.39 lan ip tos move 205
9.2.40 lan ip priority 206
9.2.41 lan ip in-policy 209
9.2.42 lan ip in-policy move 211
9.2.43 lan ip msschange 212
9.2.44 lan ip icmp redirect 213
9.2.45 lan ip multicast mode 214
9.2.46 lan ip multicast ttl threshold 215
9.2.47 lan ip multicast pim preference 216
9.2.48 lan ip multicast pim upstream type 217
9.2.49 lan ip arp cycle 218
9.2.50 lan ip arp static 219
9.2.51 lan ip ids use 220

9.3 IPv6 関連情報 221
9.3.1 lan ipv6 use 221
9.3.2 lan ipv6 ifid 222
9.3.3 lan ipv6 address 223
9.3.4 lan ipv6 ra mode 225
9.3.5 lan ipv6 ra interval 226
9.3.6 lan ipv6 ra mtu 227
9.3.7 lan ipv6 ra reachabletime 228
9.3.8 lan ipv6 ra retranstimer 229
9.3.9 lan ipv6 ra curhoplimit 230
9.3.10 lan ipv6 ra flags 231
9.3.11 lan ipv6 ra prefix 232
9.3.12 lan ipv6 ra trigger ifdown 234
9.3.13 lan ipv6 ra recv valid-lifetime 235
9.3.14 lan ipv6 route 236
9.3.15 lan ipv6 rip use 238
9.3.16 lan ipv6 rip site-local 240
9.3.17 lan ipv6 rip aggregate 241
9.3.18 lan ipv6 rip filter act 242
9.3.19 lan ipv6 rip filter move 244
9.3.20 lan ipv6 rip filter route 245
9.3.21 lan ipv6 rip filter set metric 247
9.3.22 lan ipv6 ospf use 248
9.3.23 lan ipv6 ospf cost 249
9.3.24 lan ipv6 ospf hello 250
9.3.25 lan ipv6 ospf dead 251
9.3.26 lan ipv6 ospf retrans 252
9.3.27 lan ipv6 ospf delay 253
9.3.28 lan ipv6 ospf priority 254
9.3.29 lan ipv6 ospf passive 255
9.3.30 lan ipv6 filter 256
9.3.31 lan ipv6 filter move 261
9.3.32 lan ipv6 filter default 262
9.3.33 lan ipv6 trafficclass 263
9.3.34 lan ipv6 trafficclass move 266
9.3.35 lan ipv6 priority 267
9.3.36 lan ipv6 in-policy 270
9.3.37 lan ipv6 in-policy move 272
9.3.38 lan ipv6 dhcp service 273
9.3.39 lan ipv6 dhcp duid 274
9.3.40 lan ipv6 dhcp client option na 275
9.3.41 lan ipv6 dhcp client option pd 276
9.3.42 lan ipv6 dhcp client option dns 277

9.3.43 lan ipv6 dhcp client option domain . . . 278
9.3.44 lan ipv6 dhcp client option sipserver address . . . 279
9.3.45 lan ipv6 dhcp client option sipserver domain . . . 280
9.3.46 lan ipv6 dhcp client option sntpserver . . . 281
9.3.47 lan ipv6 dhcp client option refreshtime . . . 282
9.3.48 lan ipv6 dhcp client iaid . . . 283
9.3.49 lan ipv6 dhcp client route . . . 284
9.3.50 lan ipv6 dhcp relay interface . . . 285
9.3.51 lan ipv6 dhcp relay server . . . 286
9.3.52 lan ipv6 dhcp relay source . . . 287
9.3.53 lan ipv6 dhcp server preference . . . 288
9.3.54 lan ipv6 dhcp server info address . . . 289
9.3.55 lan ipv6 dhcp server info dns . . . 291
9.3.56 lan ipv6 dhcp server info domain . . . 292
9.3.57 lan ipv6 dhcp server info prefix . . . 293
9.3.58 lan ipv6 dhcp server info sipserver address . . . 295
9.3.59 lan ipv6 dhcp server info sipserver domain . . . 296
9.3.60 lan ipv6 dhcp server info sntpserver . . . 297

9.4 VRRP 関連情報 . . . 298
9.4.1 lan vrrp use . . . 298
9.4.2 lan vrrp auth . . . 299
9.4.3 lan vrrp group id . . . 300
9.4.4 lan vrrp group ad . . . 302
9.4.5 lan vrrp group preempt . . . 303
9.4.6 lan vrrp group trigger ifdown . . . 304
9.4.7 lan vrrp group trigger route . . . 306
9.4.8 lan vrrp group trigger node . . . 308
9.4.9 lan vrrp group action . . . 310
9.4.10 lan vrrp group vaddr icmp . . . 314
9.4.11 lan vrrp group vaddr etherip . . . 315
9.4.12 lan vrrp trap . . . 316

9.5 VLAN 関連情報 . . . 317
9.5.1 lan vlan . . . 317

9.6 SNMP 関連情報 . . . 318
9.6.1 lan snmp trap linkdown . . . 318
9.6.2 lan snmp trap linkup . . . 319

第 10 章 相手情報の設定 . . . 320

10.1 相手共通情報 . . . 321
10.1.1 remote description . . . 321
10.1.2 remote name . . . 322
10.1.3 remote autodial . . . 323
10.1.4 remote mtu . . . 324
10.1.5 remote shaping . . . 325
10.1.6 remote shaping-opt tc . . . 327

10.2 接続先情報 . . . 328
10.2.1 remote ap description . . . 328
10.2.2 remote ap name . . . 329
10.2.3 remote ap move . . . 330
10.2.4 remote ap datalink type . . . 331
10.2.5 remote ap datalink bind . . . 332
10.2.6 remote ap recovery . . . 333
10.2.7 remote ap ip dns . . . 334
10.2.8 remote ap multiroute pattern . . . 336
10.2.9 remote ap multiroute pattern move . . . 339
10.2.10 remote ap limit time . . . 340
10.2.11 remote ap disconnect time . . . 341
10.2.12 remote ap disconnect packet . . . 342

10.2.13 remote ap ppp auth type. 343
10.2.14 remote ap ppp auth send. 344
10.2.15 remote ap ppp auth receive 345
10.2.16 remote ap pppoe acname 346
10.2.17 remote ap pppoe svname 347
10.2.18 remote ap dial number 348
10.2.19 remote ap called accept. 349
10.2.20 remote ap called clid 350
10.2.21 remote ap called number. 351
10.2.22 remote ap connect priority 352
10.2.23 remote ap idle 353
10.2.24 remote ap keep 354
10.2.25 remote ap ipsec type. 355
10.2.26 remote ap ipsec send spi. 357
10.2.27 remote ap ipsec send protocol 358
10.2.28 remote ap ipsec send range 360
10.2.29 remote ap ipsec send encrypt. 361
10.2.30 remote ap ipsec send auth 363
10.2.31 remote ap ipsec receive spi. 365
10.2.32 remote ap ipsec receive protocol. 366
10.2.33 remote ap ipsec receive range 367
10.2.34 remote ap ipsec receive encrypt. 368
10.2.35 remote ap ipsec receive auth. 370
10.2.36 remote ap ipsec ike protocol. 372
10.2.37 remote ap ipsec ike encrypt. 373
10.2.38 remote ap ipsec ike auth. 375
10.2.39 remote ap ipsec ike pfs. 376
10.2.40 remote ap ipsec ike lifetime. 377
10.2.41 remote ap ipsec ike lifebyte. 378
10.2.42 remote ap ipsec ike newsa initiator. 379
10.2.43 remote ap ipsec ike newsa responder. 380
10.2.44 remote ap ipsec ike range 381
10.2.45 remote ap ipsec ike anti-replay. 383
10.2.46 remote ap ipsec ike esn. 384
10.2.47 remote ap ipsec ike exchange-sa initiator 385
10.2.48 remote ap ipsec ike exchange-sa responder 386
10.2.49 remote ap ipsec extension-range. 387
10.2.50 remote ap ike port 389
10.2.51 remote ap ike shared key. 390
10.2.52 remote ap ike proposal move. 392
10.2.53 remote ap ike proposal auth-method 394
10.2.54 remote ap ike proposal encrypt 396
10.2.55 remote ap ike proposal hash. 397
10.2.56 remote ap ike proposal pfs 398
10.2.57 remote ap ike proposal lifetime. 399
10.2.58 remote ap ike proposal prf 400
10.2.59 remote ap ike retry. 401
10.2.60 remote ap ike idtype. 402
10.2.61 remote ap ike eap auth send. 403
10.2.62 remote ap ike ts multi 404
10.2.63 remote ap ike name local. 405
10.2.64 remote ap ike name remote 407
10.2.65 remote ap ike release 408
10.2.66 remote ap ike initial 409
10.2.67 remote ap ike mode 410
10.2.68 remote ap ike bind 412
10.2.69 remote ap ike nat-traversal use. 414
10.2.70 remote ap ike certificate remote. 416
10.2.71 remote ap ike certificate local. 417
10.2.72 remote ap ike certificate key 418

10.2.73 remote ap ike certificate expired 419
10.2.74 remote ap ike certificate send 420
10.2.75 remote ap ike certificate request 421
10.2.76 remote ap ike local-idtype 422
10.2.77 remote ap ike remote-idtype. 423
10.2.78 remote ap ike remote-id-send. 424
10.2.79 remote ap ike dpd use 425
10.2.80 remote ap ike dpd idle 426
10.2.81 remote ap ike dpd retry. 427
10.2.82 remote ap ike dpd anti-replay 428
10.2.83 remote ap dvpn client 429
10.2.84 remote ap dvpn remotenet. 430
10.2.85 remote ap dvpn remoteid. 432
10.2.86 remote ap tunnel local 433
10.2.87 remote ap tunnel remote. 435
10.2.88 remote ap tunnel mtu. 437
10.2.89 remote ap overlap to. 438
10.2.90 remote ap overlap nexthop 439
10.2.91 remote ap overlap nexthop6 440
10.2.92 remote ap sessionwatch address 441
10.2.93 remote ap sessionwatch interval. 443
10.2.94 remote ap sessionwatch ttl 445
10.2.95 remote ap sessionwatch mode. 446
10.2.96 remote ap sessionwatch recovery. 447
10.2.97 remote ap sessionwatch error-wait 448
10.2.98 remote ap snmp trap linkdown. 449
10.2.99 remote ap snmp trap linkup 450

10.3 PPP 関連情報 451
10.3.1 remote ppp ipcp vjcomp 451
10.3.2 remote ppp ipcp iphc. 452
10.3.3 remote ppp ipv6cp iphc 453

10.4 IP 関連情報. 454
10.4.1 remote ip address local 454
10.4.2 remote ip address remote. 455
10.4.3 remote ip route 456
10.4.4 remote ip rip use. 458
10.4.5 remote ip rip filter act. 460
10.4.6 remote ip rip filter move. 462
10.4.7 remote ip rip filter route 463
10.4.8 remote ip rip filter set metric 465
10.4.9 remote ip ospf use 466
10.4.10 remote ip ospf cost. 467
10.4.11 remote ip ospf hello. 468
10.4.12 remote ip ospf dead. 469
10.4.13 remote ip ospf retrans 470
10.4.14 remote ip ospf delay. 471
10.4.15 remote ip ospf auth type. 472
10.4.16 remote ip ospf auth textkey. 473
10.4.17 remote ip ospf auth md5key 474
10.4.18 remote ip ospf passive 475
10.4.19 remote ip ospf multicast. 476
10.4.20 remote ip ospf checkmtu. 477
10.4.21 remote ip nat mode 478
10.4.22 remote ip nat static. 480
10.4.23 remote ip nat static default. 482
10.4.24 remote ip nat rule 483
10.4.25 remote ip nat wellknown. 485
10.4.26 remote ip nat destination 487
10.4.27 remote ip nat appli. 488

10.4.28 remote ip filter . . . 489
10.4.29 remote ip filter move . . . 493
10.4.30 remote ip filter default . . . 494
10.4.31 remote ip tos . . . 495
10.4.32 remote ip tos move . . . 498
10.4.33 remote ip priority . . . 499
10.4.34 remote ip in-policy . . . 502
10.4.35 remote ip in-policy move . . . 504
10.4.36 remote ip msschange . . . 505
10.4.37 remote ip multicast mode . . . 506
10.4.38 remote ip multicast ttl threshold . . . 507
10.4.39 remote ip multicast pim preference . . . 508
10.4.40 remote ip multicast pim upstream type . . . 509
10.4.41 remote ip dvpn . . . 510
10.4.42 remote ip dvpn move . . . 512
10.4.43 remote ip ids use . . . 513

10.5 IPv6 関連情報 . . . 514
10.5.1 remote ipv6 use . . . 514
10.5.2 remote ipv6 ifid . . . 515
10.5.3 remote ipv6 address . . . 516
10.5.4 remote ipv6 ra mode . . . 518
10.5.5 remote ipv6 ra interval . . . 519
10.5.6 remote ipv6 ra mtu . . . 520
10.5.7 remote ipv6 ra reachabletime . . . 521
10.5.8 remote ipv6 ra retranstimer . . . 522
10.5.9 remote ipv6 ra curhoplimit . . . 523
10.5.10 remote ipv6 ra flags . . . 524
10.5.11 remote ipv6 ra prefix . . . 525
10.5.12 remote ipv6 ra trigger ifdown . . . 527
10.5.13 remote ipv6 ra recv valid-lifetime . . . 528
10.5.14 remote ipv6 route . . . 529
10.5.15 remote ipv6 rip use . . . 531
10.5.16 remote ipv6 rip site-local . . . 533
10.5.17 remote ipv6 rip aggregate . . . 534
10.5.18 remote ipv6 rip filter act . . . 535
10.5.19 remote ipv6 rip filter move . . . 537
10.5.20 remote ipv6 rip filter route . . . 538
10.5.21 remote ipv6 rip filter set metric . . . 540
10.5.22 remote ipv6 ospf use . . . 541
10.5.23 remote ipv6 ospf cost . . . 542
10.5.24 remote ipv6 ospf hello . . . 543
10.5.25 remote ipv6 ospf dead . . . 544
10.5.26 remote ipv6 ospf retrans . . . 545
10.5.27 remote ipv6 ospf delay . . . 546
10.5.28 remote ipv6 ospf passive . . . 547
10.5.29 remote ipv6 ospf checkmtu . . . 548
10.5.30 remote ipv6 filter . . . 549
10.5.31 remote ipv6 filter move . . . 554
10.5.32 remote ipv6 filter default . . . 555
10.5.33 remote ipv6 trafficclass . . . 556
10.5.34 remote ipv6 trafficclass move . . . 559
10.5.35 remote ipv6 priority . . . 560
10.5.36 remote ipv6 in-policy . . . 563
10.5.37 remote ipv6 in-policy move . . . 565
10.5.38 remote ipv6 dhcp service . . . 566
10.5.39 remote ipv6 dhcp duid . . . 567
10.5.40 remote ipv6 dhcp client option na . . . 568
10.5.41 remote ipv6 dhcp client option pd . . . 569
10.5.42 remote ipv6 dhcp client option dns . . . 570

10.5.43 remote ipv6 dhcp client option domain . . . 571
10.5.44 remote ipv6 dhcp client option sipserver address . . . 572
10.5.45 remote ipv6 dhcp client option sipserver domain . . . 573
10.5.46 remote ipv6 dhcp client option sntpserver . . . 574
10.5.47 remote ipv6 dhcp client option refreshtime . . . 575
10.5.48 remote ipv6 dhcp client iaid . . . 576
10.5.49 remote ipv6 dhcp client route . . . 577
10.5.50 remote ipv6 dhcp relay interface . . . 578
10.5.51 remote ipv6 dhcp relay server . . . 579
10.5.52 remote ipv6 dhcp relay source . . . 580
10.5.53 remote ipv6 dhcp server preference . . . 581
10.5.54 remote ipv6 dhcp server info dns . . . 582
10.5.55 remote ipv6 dhcp server info domain . . . 583
10.5.56 remote ipv6 dhcp server info prefix . . . 584
10.5.57 remote ipv6 dhcp server info sipserver address . . . 586
10.5.58 remote ipv6 dhcp server info sipserver domain . . . 587
10.5.59 remote ipv6 dhcp server info sntpserver . . . 588
10.5.60 remote ipv6 dvpn . . . 589
10.5.61 remote ipv6 dvpn move . . . 591

10.6 ブリッジグループ関連情報 . . . 592
10.6.1 remote bridgegroup use . . . 592
10.6.2 remote bridgegroup group . . . 593
10.6.3 remote bridgegroup macfilter . . . 594
10.6.4 remote bridgegroup macfilter move . . . 596

10.7 SNMP 関連情報 . . . 597
10.7.1 remote snmp trap linkdown . . . 597
10.7.2 remote snmp trap linkup . . . 598

第 11 章 着信デフォルト情報の設定 . . . 599

11.1 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 . . . 600
11.1.1 answer accept . . . 600
11.1.2 answer ppp auth type . . . 601
11.1.3 answer ppp auth receive add . . . 602

第 12 章 テンプレート情報の設定 . . . 603

12.1 テンプレート共通情報 . . . 604
12.1.1 template description . . . 604
12.1.2 template name . . . 605
12.1.3 template mtu . . . 606
12.1.4 template idle . . . 607
12.1.5 template interface pool . . . 608
12.1.6 template aaa . . . 609
12.1.7 template datalink type . . . 610
12.1.8 template combine use . . . 611

12.2 IP 関連情報 . . . 612
12.2.1 template ip dns . . . 612
12.2.2 template ip nat mode . . . 614
12.2.3 template ip nat static . . . 616
12.2.4 template ip nat static default . . . 618
12.2.5 template ip nat rule . . . 619
12.2.6 template ip nat wellknown . . . 621
12.2.7 template ip nat destination . . . 623
12.2.8 template ip nat appli . . . 624
12.2.9 template ip filter . . . 625
12.2.10 template ip filter move . . . 629
12.2.11 template ip filter default . . . 630
12.2.12 template ip tos . . . 631
12.2.13 template ip tos move . . . 634
12.2.14 template ip msschange . . . 635

12.2.15 template ip ids use . . . 636
12.2.16 template ip in-policy . . . 637
12.2.17 template ip in-policy move . . . 639

12.3 IPv6 関連情報 . . . 640
12.3.1 template ipv6 use . . . 640
12.3.2 template ipv6 ifid . . . 641
12.3.3 template ipv6 filter . . . 642
12.3.4 template ipv6 filter move . . . 647
12.3.5 template ipv6 filter default . . . 648
12.3.6 template ipv6 trafficclass . . . 649
12.3.7 template ipv6 trafficclass move . . . 652
12.3.8 template ipv6 priority . . . 653
12.3.9 template ipv6 in-policy . . . 656
12.3.10 template ipv6 in-policy move . . . 658

12.4 動的 VPN 関連情報 . . . 659
12.4.1 template dvpn client . . . 659
12.4.2 template dvpn server address . . . 660
12.4.3 template dvpn server auth . . . 662
12.4.4 template dvpn expire register . . . 663
12.4.5 template dvpn expire session . . . 664
12.4.6 template dvpn ua . . . 665
12.4.7 template dvpn domain . . . 667
12.4.8 template dvpn localnet . . . 668
12.4.9 template dvpn localid . . . 670
12.4.10 template dvpn interface . . . 671
12.4.11 template dvpn global . . . 672

12.5 IPsec 関連情報 . . . 673
12.5.1 template ipsec ike protocol . . . 673
12.5.2 template ipsec ike encrypt . . . 674
12.5.3 template ipsec ike auth . . . 675
12.5.4 template ipsec ike pfs . . . 676
12.5.5 template ipsec ike lifetime . . . 677
12.5.6 template ipsec ike lifebyte . . . 678
12.5.7 template ipsec ike newsa initiator . . . 679
12.5.8 template ipsec ike newsa responder . . . 680
12.5.9 template ipsec ike anti-replay . . . 681
12.5.10 template ipsec ike exchange-sa initiator . . . 682
12.5.11 template ipsec ike exchange-sa responder . . . 683

12.6 IKE 関連情報 . . . 684
12.6.1 template ike shared key . . . 684
12.6.2 template ike proposal move . . . 686
12.6.3 template ike proposal auth-method . . . 687
12.6.4 template ike proposal encrypt . . . 688
12.6.5 template ike proposal hash . . . 689
12.6.6 template ike proposal pfs . . . 690
12.6.7 template ike proposal lifetime . . . 691
12.6.8 template ike retry . . . 692
12.6.9 template ike idtype . . . 693
12.6.10 template ike name local . . . 694
12.6.11 template ike release . . . 695
12.6.12 template ike mode . . . 696
12.6.13 template ike nat-traversal use . . . 697
12.6.14 template ike certificate local . . . 699
12.6.15 template ike certificate key . . . 700
12.6.16 template ike certificate expired . . . 701
12.6.17 template ike certificate send . . . 702
12.6.18 template ike certificate request . . . 703
12.6.19 template ike dpd use . . . 704

12.6.20 template ike dpd idle . . . 705
12.6.21 template ike dpd retry . . . 706
12.6.22 template ike dpd anti-replay . . . 707

12.7 トンネル関連情報 . . . 708
12.7.1 template tunnel local . . . 708

12.8 セッション監視関連情報 . . . 710
12.8.1 template sessionwatch address . . . 710
12.8.2 template sessionwatch interval . . . 712

12.9 SNMP 関連情報 . . . 714
12.9.1 template snmp trap linkdown . . . 714
12.9.2 template snmp trap linkup . . . 715

第 13 章 IP 関連情報の設定 . . . 716

13.1 IP 関連情報 . . . 717
13.1.1 ip arp age . . . 717
13.1.2 ip arp verify mode . . . 718

第 14 章 動的 VPN 情報の設定 . . . 719

14.1 動的 VPN サーバ情報 . . . 720
14.1.1 dvpn server use . . . 720
14.1.2 dvpn server domain . . . 721
14.1.3 dvpn server auth use . . . 722
14.1.4 dvpn server auth aaa . . . 723

14.2 動的 VPN クライアント情報 . . . 724
14.2.1 dvpn client encode . . . 724
14.2.2 dvpn client server address . . . 725
14.2.3 dvpn client server auth . . . 727
14.2.4 dvpn client expire register . . . 728
14.2.5 dvpn client expire session . . . 729
14.2.6 dvpn client ua . . . 730
14.2.7 dvpn client domain . . . 732
14.2.8 dvpn client localnet . . . 733
14.2.9 dvpn client localid . . . 735
14.2.10 dvpn client interface . . . 736
14.2.11 dvpn client global . . . 737
14.2.12 dvpn client priority . . . 738
14.2.13 dvpn client ip route distance . . . 739
14.2.14 dvpn client ipv6 route distance . . . 740

第 15 章 ルーティングプロトコル情報の設定 . . . 741

15.1 ルーティングマネージャ情報 . . . 742
15.1.1 routemanage ip distance . . . 742
15.1.2 routemanage ip redist rip . . . 744
15.1.3 routemanage ip redist bgp . . . 746
15.1.4 routemanage ip redist ospf . . . 747
15.1.5 routemanage ip ecmp mode . . . 749
15.1.6 routemanage ip ecmp ospf . . . 750
15.1.7 routemanage ipv6 distance . . . 751
15.1.8 routemanage ipv6 redist rip . . . 753
15.1.9 routemanage ipv6 redist bgp . . . 755
15.1.10 routemanage ipv6 redist ospf . . . 756

15.2 RIP 情報 . . . 758
15.2.1 rip ip timers basic . . . 758
15.2.2 rip ip timers jitter . . . 759
15.2.3 rip ip multipath . . . 760
15.2.4 rip ip redist . . . 761
15.2.5 rip ip redist move . . . 763
15.2.6 rip ip neighbor . . . 764

15.2.7 rip ip gwfilter 765
15.2.8 rip ip gwfilter move. 766
15.2.9 rip ipv6 timers basic. 767
15.2.10 rip ipv6 multipath 768
15.2.11 rip ipv6 redist. 769
15.2.12 rip ipv6 redist move. 771

15.3 BGP 情報 772
15.3.1 bgp as 772
15.3.2 bgp id 773
15.3.3 bgp ip network route. 774
15.3.4 bgp ip network igp 775
15.3.5 bgp ip aggregate. 776
15.3.6 bgp ip redist. 777
15.3.7 bgp ip redist move 779
15.3.8 bgp ipv6 network route 780
15.3.9 bgp ipv6 network igp. 781
15.3.10 bgp ipv6 aggregate 782
15.3.11 bgp ipv6 redist. 783
15.3.12 bgp ipv6 redist move. 785

15.4 BGP 相手側情報 786
15.4.1 bgp neighbor address. 786
15.4.2 bgp neighbor as 787
15.4.3 bgp neighbor timers 788
15.4.4 bgp neighbor ebgp-multihop 789
15.4.5 bgp neighbor family 790
15.4.6 bgp neighbor source 791
15.4.7 bgp neighbor authentication 792
15.4.8 bgp neighbor graceful-restart family. 793
15.4.9 bgp neighbor graceful-restart stale-timer. 794
15.4.10 bgp neighbor community 795
15.4.11 bgp neighbor ip medmetric 796
15.4.12 bgp neighbor ip asprepend 797
15.4.13 bgp neighbor ip localpref 798
15.4.14 bgp neighbor ip nexthopself. 799
15.4.15 bgp neighbor ip default-originate 800
15.4.16 bgp neighbor ip filter act 801
15.4.17 bgp neighbor ip filter move. 803
15.4.18 bgp neighbor ip filter as 804
15.4.19 bgp neighbor ip filter route. 805
15.4.20 bgp neighbor ip filter set medmetric. 807
15.4.21 bgp neighbor ip filter set asprepend. 809
15.4.22 bgp neighbor ip filter set localpref. 811
15.4.23 bgp neighbor ip filter set community. 813
15.4.24 bgp neighbor ipv6 medmetric. 814
15.4.25 bgp neighbor ipv6 asprepend. 815
15.4.26 bgp neighbor ipv6 localpref. 816
15.4.27 bgp neighbor ipv6 nexthopself 817
15.4.28 bgp neighbor ipv6 default-originate. 818
15.4.29 bgp neighbor ipv6 filter act. 819
15.4.30 bgp neighbor ipv6 filter move 821
15.4.31 bgp neighbor ipv6 filter as. 822
15.4.32 bgp neighbor ipv6 filter route 823
15.4.33 bgp neighbor ipv6 filter set medmetric 825
15.4.34 bgp neighbor ipv6 filter set asprepend 826
15.4.35 bgp neighbor ipv6 filter set localpref 828
15.4.36 bgp neighbor ipv6 filter set community 830

15.5 OSPF 情報 831
15.5.1 ospf ip id 831
15.5.2 ospf ipv6 id. 832

15.6 OSPF エリア情報 833
15.6.1 ospf ip area id 833
15.6.2 ospf ip area type 834
15.6.3 ospf ip area defcost 835
15.6.4 ospf ip area range 836
15.6.5 ospf ip area type3-lsa 838
15.6.6 ospf ip area type3-lsa move 840
15.6.7 ospf ipv6 area id 841
15.6.8 ospf ipv6 area type 842
15.6.9 ospf ipv6 area defcost 843
15.6.10 ospf ipv6 area range 844
15.6.11 ospf ipv6 area inter-area-prefix 846
15.6.12 ospf ipv6 area inter-area-prefix move 848
15.7 ASBR 情報 849
15.7.1 ospf ip definfo 849
15.7.2 ospf ip summary 850
15.7.3 ospf ip redist 851
15.7.4 ospf ip redist move 853
15.7.5 ospf ipv6 definfo 854
15.7.6 ospf ipv6 redist 855
15.7.7 ospf ipv6 redist move 857

第 16 章 ブリッジグループ情報の設定 858

16.1 ブリッジグループ情報 859
16.1.1 bridgegroup ip routing 859
16.1.2 bridgegroup ip policy 860
16.1.3 bridgegroup ipv6 routing 861
16.1.4 bridgegroup ipv6 policy 862
16.1.5 bridgegroup vlan tag transmit 863
16.1.6 bridgegroup inter-remote 864

第 17 章 マルチキャスト情報の設定 865

17.1 マルチキャスト情報 866
17.1.1 multicast ip igmp report 866
17.1.2 multicast ip pimsm candrp mode 867
17.1.3 multicast ip pimsm candrp address 868
17.1.4 multicast ip pimsm candrp priority 869
17.1.5 multicast ip pimsm candbsr mode 870
17.1.6 multicast ip pimsm candbsr address 871
17.1.7 multicast ip pimsm candbsr priority 872
17.1.8 multicast ip pimsm staticrp address 873
17.1.9 multicast ip pimsm spt mode 874
17.1.10 multicast ip pimsm spt rate 875
17.1.11 multicast ip pimsm register checksum 876
17.1.12 multicast ip route static 877

第 18 章 UPnP 情報の設定 879

18.1 UPnP 情報 880
18.1.1 upnp use 880
18.1.2 upnp portmapping lease 882

第 19 章 ACL 情報の設定 883

19.1 ACL 情報 884
19.1.1 acl description 884
19.1.2 acl mac 885
19.1.3 acl ip 887
19.1.4 acl ipv6 889
19.1.5 acl tcp 891
19.1.6 acl udp 893

19.1.7 acl icmp. 894

第 20 章 ポリシーグループ定義情報の設定. 896

20.1 ポリシーグループ定義情報. 897
20.1.1 policy-group pattern. 897
20.1.2 policy-group pattern move. 899
20.1.3 policy-group interface 900
20.1.4 policy-group nexthop. 901
20.1.5 policy-group nexthop6. 902
20.1.6 policy-group sessionwatch address. 903
20.1.7 policy-group sessionwatch interval 905
20.1.8 policy-group sessionwatch ttl. 907
20.1.9 policy-group sessionwatch recovery 908
20.1.10 policy-group sessionwatch error-wait. 909

第 21 章 AAA 情報の設定. 910

21.1 グループ ID 情報 911
21.1.1 aaa name. 911

21.2 AAA ユーザ情報 912
21.2.1 aaa user id 912
21.2.2 aaa user password. 913
21.2.3 aaa user called number 915
21.2.4 aaa user ip address local. 916
21.2.5 aaa user ip address remote 917
21.2.6 aaa user ip route. 918
21.2.7 aaa user ipv6 ifid 920
21.2.8 aaa user ipv6 route 921
21.2.9 aaa user sessionwatch. 923
21.2.10 aaa user ipsec ike range. 924
21.2.11 aaa user ipsec extension-range 926
21.2.12 aaa user ike shared key. 928
21.2.13 aaa user supplicant vid. 930
21.2.14 aaa user supplicant mac. 931
21.2.15 aaa user user-role 932

21.3 RADIUS 情報. 933
21.3.1 aaa radius service 933
21.3.2 aaa radius auth source 935
21.3.3 aaa radius auth message-authenticator. 936
21.3.4 aaa radius accounting source. 937
21.3.5 aaa radius server client-info secret. 938
21.3.6 aaa radius server client-info address. 939
21.3.7 aaa radius client server-info auth secret. 940
21.3.8 aaa radius client server-info auth address 941
21.3.9 aaa radius client server-info auth port 942
21.3.10 aaa radius client server-info auth deadtime. 943
21.3.11 aaa radius client server-info auth priority. 944
21.3.12 aaa radius client server-info auth source 945
21.3.13 aaa radius client server-info accounting secret. 946
21.3.14 aaa radius client server-info accounting address. 947
21.3.15 aaa radius client server-info accounting port 948
21.3.16 aaa radius client server-info accounting deadtime 949
21.3.17 aaa radius client server-info accounting priority 950
21.3.18 aaa radius client server-info accounting source. 951
21.3.19 aaa radius client retry. 952
21.3.20 aaa radius client nas-identifier. 953
21.3.21 aaa radius client security 954

第 22 章 認証情報の設定 955

22.1 IEEE802.1X 情報. 956

22.1.1 dot1x use . . . 956
22.2 MAC アドレス認証情報 . . . 957
22.2.1 macauth use . . . 957
22.2.2 macauth password . . . 958
22.2.3 macauth type . . . 959
22.3 ARP 認証情報 . . . 960
22.3.1 arpauth use . . . 960
22.3.2 arpauth password . . . 961
第 23 章 トラッキング定義情報の設定 . . . 962
23.1 トラッキング定義情報 . . . 963
23.1.1 tracking trigger node . . . 963
23.1.2 tracking action . . . 964
23.2 ノードトリガ定義情報 . . . 965
23.2.1 node-trigger address . . . 965
23.2.2 node-trigger interval . . . 967
23.2.3 node-trigger ttl . . . 968
23.2.4 node-trigger recovery . . . 969
23.2.5 node-trigger error-wait . . . 970
23.2.6 node-trigger tos . . . 971
23.2.7 node-trigger error-mode . . . 972
23.2.8 node-trigger error-retry . . . 973
第 24 章 メモリ予兆監視情報の設定 . . . 974
24.1 メモリ予兆監視情報 . . . 975
24.1.1 sysmemwatch mode . . . 975
24.1.2 sysmemwatch threshold . . . 976
24.1.3 sysmemwatch interval . . . 977
第 25 章 装置情報の設定 . . . 978
25.1 SNMP 情報 . . . 979
25.1.1 snmp service . . . 979
25.1.2 snmp agent contact . . . 980
25.1.3 snmp agent sysname . . . 981
25.1.4 snmp agent location . . . 982
25.1.5 snmp agent ip address . . . 983
25.1.6 snmp agent ipv6 address . . . 984
25.1.7 snmp agent engineid . . . 985
25.1.8 snmp manager . . . 986
25.1.9 snmp trap coldstart . . . 988
25.1.10 snmp trap linkdown . . . 989
25.1.11 snmp trap linkup . . . 990
25.1.12 snmp trap authfail . . . 991
25.1.13 snmp trap vrrpnewmaster . . . 992
25.1.14 snmp trap vrrpauthfail . . . 993
25.1.15 snmp trap vrrpprotoerror . . . 994
25.1.16 snmp trap noserror . . . 995
25.1.17 snmp user name . . . 996
25.1.18 snmp user address . . . 997
25.1.19 snmp user notification . . . 998
25.1.20 snmp user auth . . . 999
25.1.21 snmp user priv . . . 1000
25.1.22 snmp user write . . . 1001
25.1.23 snmp user read . . . 1002
25.1.24 snmp user notify . . . 1003
25.1.25 snmp view subtree . . . 1004
25.2 システムログ情報 . . . 1006
25.2.1 syslog server address . . . 1006

25.2.2 syslog server pri . . . 1007
25.2.3 syslog pri . . . 1008
25.2.4 syslog facility . . . 1009
25.2.5 syslog security . . . 1010
25.2.6 syslog dupcut . . . 1011
25.2.7 syslog command-logging . . . 1012
25.2.8 syslog header . . . 1013
25.2.9 syslog source ip address . . . 1014
25.2.10 syslog source ipv6 address . . . 1015

25.3 自動時刻設定情報 . . . 1016
25.3.1 time auto server . . . 1016
25.3.2 time auto interval . . . 1017
25.3.3 time zone . . . 1018

25.4 ProxyDNS 情報 . . . 1019
25.4.1 proxydns domain . . . 1019
25.4.2 proxydns domain move . . . 1023
25.4.3 proxydns address . . . 1024
25.4.4 proxydns address move . . . 1027
25.4.5 proxydns unicode . . . 1028
25.4.6 proxydns agetime . . . 1029
25.4.7 proxydns ttl . . . 1030
25.4.8 proxydns source-port . . . 1031

25.5 ホストデータベース情報 . . . 1032
25.5.1 host name . . . 1032
25.5.2 host ip address . . . 1033
25.5.3 host ipv6 address . . . 1034
25.5.4 host mac . . . 1035
25.5.5 host duid . . . 1036
25.5.6 host rpon . . . 1037

25.6 スケジュール情報 . . . 1038
25.6.1 schedule at . . . 1038
25.6.2 schedule in . . . 1040
25.6.3 schedule syslog . . . 1042

25.7 外部メディアスタート機能の情報 . . . 1043
25.7.1 storage setup mode . . . 1043
25.7.2 storage setup machine . . . 1044

25.8 電話番号変更予約情報 . . . 1045
25.8.1 dnconvinfo date . . . 1045
25.8.2 dnconvinfo dial . . . 1046

25.9 ソフトウェア更新情報 . . . 1047
25.9.1 updateinfo . . . 1047

25.10 ドメインリスト情報 . . . 1049
25.10.1 domainlistinfo . . . 1049

25.11 装置ランプ情報 . . . 1051
25.11.1 lamp mode . . . 1051
25.11.2 lamp delay . . . 1052

25.12 資源情報 . . . 1053
25.12.1 resource system vlan . . . 1053
25.12.2 resource authenticated vlan . . . 1054

25.13 その他 . . . 1055
25.13.1 addact . . . 1055
25.13.2 watchdog service . . . 1057
25.13.3 consoleinfo . . . 1058
25.13.4 telnetinfo . . . 1059
25.13.5 sysdown harderr thermal . . . 1060
25.13.6 sysdown harderr other . . . 1061

25.13.7 mflag 1062
25.13.8 sysname. 1063
25.13.9 loopback ip address. 1064
25.13.10 loopback ip ospf use 1065
25.13.11 loopback ipv6 address 1066
25.13.12 serverinfo ftp. 1067
25.13.13 serverinfo ftp ipv6. 1068
25.13.14 serverinfo ftp filter 1069
25.13.15 serverinfo ftp filter move. 1071
25.13.16 serverinfo ftp filter default 1072
25.13.17 serverinfo sftp. 1073
25.13.18 serverinfo sftp ipv6 1074
25.13.19 serverinfo telnet 1075
25.13.20 serverinfo telnet ipv6. 1076
25.13.21 serverinfo telnet filter 1077
25.13.22 serverinfo telnet filter move 1079
25.13.23 serverinfo telnet filter default 1080
25.13.24 serverinfo ssh. 1081
25.13.25 serverinfo ssh ipv6. 1082
25.13.26 serverinfo ssh filter 1083
25.13.27 serverinfo ssh filter move. 1085
25.13.28 serverinfo ssh filter default 1086
25.13.29 serverinfo http. 1087
25.13.30 serverinfo http filter. 1088
25.13.31 serverinfo http filter move. 1090
25.13.32 serverinfo http filter default. 1091
25.13.33 serverinfo dns. 1092
25.13.34 serverinfo dns ipv6. 1093
25.13.35 serverinfo dns filter 1094
25.13.36 serverinfo dns filter move. 1096
25.13.37 serverinfo dns filter default 1097
25.13.38 serverinfo sntp. 1098
25.13.39 serverinfo sntp ipv6 1099
25.13.40 serverinfo sntp filter. 1100
25.13.41 serverinfo sntp filter move. 1102
25.13.42 serverinfo sntp filter default. 1103
25.13.43 serverinfo time ip tcp. 1104
25.13.44 serverinfo time ipv6 tcp 1105
25.13.45 serverinfo time ip udp. 1106
25.13.46 serverinfo time ipv6 udp 1107
25.13.47 serverinfo time filter. 1108
25.13.48 serverinfo time filter move. 1110
25.13.49 serverinfo time filter default. 1111
25.13.50 loopintercept internal. 1112
25.13.51 loopintercept external. 1113

第 26 章　証明書関連情報の設定 1114

26.1 証明書関連情報 1115
26.1.1 certificate local name 1115
26.1.2 certificate local line 1116
26.1.3 certificate remote name 1117
26.1.4 certificate remote line 1118
26.1.5 certificate ca name 1119
26.1.6 certificate ca line 1120
26.1.7 certificate request line. 1121
26.1.8 certificate private line. 1122

第 27 章　構成定義情報表示、削除、および操作コマンド 1123

27.1 構成定義情報表示. 1124
27.1.1 show candidate-config. 1124

27.1.2 show running-config 1125
27.1.3 show startup-config 1126
27.1.4 diff. 1127

27.2 構成定義情報削除. 1129
27.2.1 delete 1129

27.3 構成定義情報操作. 1130
27.3.1 load. 1130
27.3.2 save. 1132
27.3.3 commit 1133
27.3.4 commit try time 1134
27.3.5 commit try cancel. 1135
27.3.6 discard 1136

27.4 ファイル操作コマンド. 1137
27.4.1 dir 1137
27.4.2 copy. 1139
27.4.3 remove 1141
27.4.4 rename 1142
27.4.5 format 1143

第 28 章 モード操作コマンド／ターミナル操作コマンド 1144

28.1 モード操作 1145
28.1.1 admin. 1145
28.1.2 su 1147
28.1.3 exit. 1149
28.1.4 configure. 1150
28.1.5 end 1151
28.1.6 quit. 1152
28.1.7 top 1153
28.1.8 up 1154
28.1.9 !. 1155

28.2 ターミナル操作 1156
28.2.1 terminal pager 1156
28.2.2 terminal window 1159
28.2.3 terminal charset. 1160
28.2.4 terminal prompt 1161
28.2.5 terminal timestamp 1163
28.2.6 terminal bell. 1164
28.2.7 terminal logging. 1165
28.2.8 show terminal. 1166

28.3 コマンド実行履歴. 1167
28.3.1 show logging command. 1167
28.3.2 clear logging command. 1168

28.4 コマンドエイリアス 1169
28.4.1 alias. 1169
28.4.2 show alias 1171
28.4.3 clear alias 1172

28.5 コマンド出力操作. 1173
28.5.1 more. 1173
28.5.2 tail. 1174
28.5.3 grep. 1175

第 29 章 システム操作および表示コマンド. 1177

29.1 システム操作および表示 1178
29.1.1 show system information 1178
29.1.2 show system status 1180
29.1.3 show system funcswitch 1182
29.1.4 show tech-support. 1183

29.1.5 show logging error 1184
29.1.6 clear logging error 1187
29.1.7 show logging syslog 1188
29.1.8 clear logging syslog. 1189
29.1.9 clear statistics. 1190
29.1.10 show date 1191
29.1.11 date. 1192
29.1.12 rdate 1193
29.1.13 reset 1194
29.1.14 update 1195
29.1.15 getdomainlist 1197

第 30 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. 1198

30.1 Ethernet のカウンタ・ログ・統計・状態などの表示. 1199
30.1.1 show ether 1199
30.1.2 show ether brief. 1202
30.1.3 show ether statistics. 1204
30.1.4 show ether utilization 1211
30.1.5 show ether queue. 1213
30.1.6 show ether media-info. 1215

30.2 Ethernet のカウンタ・ログ・統計などのクリア. 1217
30.2.1 clear ether statistics 1217

第 31 章 VLAN 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. 1218

31.1 VLAN のカウンタ・ログ・統計・状態などの表示. 1219
31.1.1 show vlan. 1219

第 32 章 データ通信モジュール接続のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド 1221

32.1 データ通信モジュール接続のカウンタ・ログ・統計・状態などの表示 1222
32.1.1 show modemmodule. 1222
32.1.2 show modemmodule account. 1225
32.1.3 show modemmodule condition status. 1227
32.1.4 show modemmodule condition history 1231
32.1.5 show modemmodule condition statistics. 1234
32.1.6 show modemmodule statistics 1236

32.2 データ通信モジュール接続のカウンタ・ログ・統計などのクリア 1238
32.2.1 clear modemmodule account. 1238
32.2.2 clear modemmodule condition history 1239
32.2.3 clear modemmodule condition statistics 1240
32.2.4 clear modemmodule statistics. 1241

第 33 章 USB 接続のカウンタ・ログ・統計・状態などの表示コマンド. 1242

33.1 USB 接続のカウンタ・ログ・統計・状態などの表示 1243
33.1.1 show usb hcd status 1243
33.1.2 show usb storage status 1244

第 34 章 pseudo ether 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 1248

34.1 pseudo ether インタフェースのカウンタ・ログ・統計・状態などの表示 1249
34.1.1 show pseudo-ether. 1249
34.1.2 show pseudo-ether statistics. 1251

第 35 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 1253

35.1 インタフェースのカウンタ・ログ・統計・状態などの表示. 1254
35.1.1 show interface 1254
35.1.2 show interface brief. 1257
35.1.3 show interface summary 1258
35.1.4 show interface detail. 1259
35.1.5 show interface statistics. 1263
35.1.6 show access-point. 1265

35.1.7 show template . . . 1270
35.1.8 show template statistics . . . 1272
35.2 インタフェースのカウンタ・ログ・統計などのクリア . . . 1273
35.2.1 clear interface statistics . . . 1273
35.2.2 clear template statistics . . . 1274
第36章 ARPエントリの表示、削除コマンド . . . 1275
36.1 ARPエントリの表示 . . . 1276
36.1.1 show arp . . . 1276
36.2 ARPエントリの削除 . . . 1278
36.2.1 clear arp . . . 1278
第37章 Neighbor Cacheテーブルエントリの表示、削除コマンド . . . 1279
37.1 Neighbor Cacheテーブルエントリの表示 . . . 1280
37.1.1 show ndp . . . 1280
37.2 Neighbor Cacheテーブルエントリの削除 . . . 1282
37.2.1 clear ndp . . . 1282
第38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 . . . 1283
38.1 IPv4ルーティングテーブル情報・統計などの表示、クリア . . . 1284
38.1.1 show ip route . . . 1284
38.1.2 show ip route summary . . . 1287
38.1.3 clear ip route . . . 1289
38.1.4 show ip route kernel . . . 1290
38.1.5 show ip route kernel ecmp statistics . . . 1292
38.1.6 clear ip route kernel ecmp statistics . . . 1293
38.2 IPv6ルーティングテーブル情報・統計などの表示、クリア . . . 1294
38.2.1 show ipv6 route . . . 1294
38.2.2 show ipv6 route summary . . . 1297
38.2.3 clear ipv6 route . . . 1299
38.2.4 show ipv6 route kernel . . . 1300
38.2.5 show ipv6 ra default-router-list . . . 1302
38.2.6 show ipv6 ra prefix-list . . . 1304
第39章 RIP情報の表示、クリア操作コマンド . . . 1306
39.1 RIP情報の表示、クリア . . . 1307
39.1.1 show ip rip route . . . 1307
39.1.2 show ip rip protocol . . . 1309
39.1.3 clear ip rip statistics . . . 1311
39.2 IPv6 RIP情報の表示 . . . 1312
39.2.1 show ipv6 rip route . . . 1312
39.2.2 show ipv6 rip protocol . . . 1314
第40章 BGP情報の表示、クリア操作コマンド . . . 1316
40.1 BGP情報の表示、クリア . . . 1317
40.1.1 show ip bgp route . . . 1317
40.1.2 show ip bgp route summary . . . 1321
40.1.3 show ip bgp status . . . 1323
40.1.4 show ip bgp neighbors . . . 1325
40.1.5 clear ip bgp neighbors . . . 1329
40.1.6 clear ip bgp statistics . . . 1331
40.2 BGP IPv6情報の表示、クリア . . . 1332
40.2.1 show ipv6 bgp route . . . 1332
40.2.2 show ipv6 bgp route summary . . . 1336
40.2.3 show ipv6 bgp status . . . 1338
40.2.4 show ipv6 bgp neighbors . . . 1340
40.2.5 clear ipv6 bgp neighbors . . . 1344

40.2.6 clear ipv6 bgp statistics 1346

第 41 章 OSPF 情報の表示、クリア操作コマンド 1347

41.1 OSPF 情報の表示、クリア 1348
41.1.1 show ip ospf route 1348
41.1.2 show ip ospf protocol 1351
41.1.3 show ip ospf database 1354
41.1.4 show ip ospf interface 1361
41.1.5 show ip ospf neighbor 1364
41.1.6 clear ip ospf statistics 1367

41.2 IPv6 OSPF 情報の表示、クリア 1368
41.2.1 show ipv6 ospf route 1368
41.2.2 show ipv6 ospf protocol 1371
41.2.3 show ipv6 ospf database 1374
41.2.4 show ipv6 ospf interface 1385
41.2.5 show ipv6 ospf neighbor 1389
41.2.6 clear ipv6 ospf statistics 1393

第 42 章 パケットの統計情報の表示、クリア操作コマンド 1394

42.1 IPv4 パケットの統計情報の表示、クリア 1395
42.1.1 show ip traffic 1395
42.1.2 clear ip traffic 1398

42.2 IPv6 パケットの統計情報の表示、クリア 1399
42.2.1 show ipv6 traffic 1399
42.2.2 clear ipv6 traffic 1402

第 43 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 1403

43.1 IPv4 フィルタのカウンタ・ログ・統計・状態などの表示、クリア 1404
43.1.1 show ip filter 1404
43.1.2 show ip filter statistics 1407
43.1.3 show ip filter summary 1408
43.1.4 clear ip filter statistics 1409

43.2 IPv6 フィルタのカウンタ・ログ・統計・状態などの表示、クリア 1410
43.2.1 show ipv6 filter 1410
43.2.2 show ipv6 filter statistics 1412
43.2.3 show ipv6 filter summary 1413
43.2.4 clear ipv6 filter statistics 1414

第 44 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 1415

44.1 IPv4 IDS のカウンタ・ログ・統計・状態などの表示、クリア 1416
44.1.1 show ip ids statistics 1416
44.1.2 clear ip ids statistics 1419

第 45 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 1420

45.1 NAT のカウンタ・ログ・統計・状態などの表示 1421
45.1.1 show ip nat 1421
45.1.2 show ip nat statistics 1423
45.1.3 show ip nat summary 1425

45.2 NAT のカウンタ・ログ・統計などのクリア 1426
45.2.1 clear ip nat statistics 1426

第 46 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 1427

46.1 マルチキャストのカウンタ・ログ・統計・状態などの表示 1428
46.1.1 show ip multicast group 1428
46.1.2 show ip multicast interface 1430
46.1.3 show ip multicast interface statistics 1432
46.1.4 show ip multicast pimsm rp 1433
46.1.5 show ip multicast protocol 1434

46.1.6 show ip multicast route 1435
46.1.7 show ip multicast route kernel 1437
46.1.8 show ip multicast route kernel statistics 1439
46.1.9 show ip multicast statistics 1440
46.2 マルチキャストのカウンタ・ログ・統計などのクリア 1441
46.2.1 clear ip multicast interface statistics 1441
46.2.2 clear ip multicast route kernel statistics 1442
46.2.3 clear ip multicast statistics 1443
第 47 章 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 1444
47.1 IPv4 DHCP のカウンタ・ログ・統計・状態などの表示 1445
47.1.1 show ip dhcp 1445
47.2 IPv6 DHCP のカウンタ・ログ・統計・状態などの表示、クリア 1448
47.2.1 show ipv6 dhcp 1448
47.2.2 clear ipv6 dhcp server 1452
第 48 章 動的 VPN の状態などの表示、情報の削除コマンド 1453
48.1 動的 VPN の情報交換クライアントの状態などの表示 1454
48.1.1 show dvpn client user 1454
48.1.2 show dvpn client session 1456
48.2 動的 VPN サーバの状態などの表示 1458
48.2.1 show dvpn server 1458
48.2.2 show dvpn server user 1459
48.2.3 show dvpn server session 1461
48.3 動的 VPN サーバの情報の削除 1463
48.3.1 clear dvpn server user 1463
48.3.2 clear dvpn server session 1464
第 49 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 1465
49.1 IPsec/IKE のカウンタ・ログ・統計・状態などの表示 1466
49.1.1 show ipsec sa 1466
49.1.2 show ike statistics 1476
49.2 IPsec/IKE のカウンタ・ログ・統計などのクリア 1481
49.2.1 clear ike statistics 1481
第 50 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 1482
50.1 VRRP のカウンタ・ログ・統計・状態などの表示 1483
50.1.1 show vrrp 1483
50.2 VRRP のカウンタ・ログ・統計などのクリア 1487
50.2.1 clear vrrp statistics 1487
第 51 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 1488
51.1 ブリッジのカウンタ・ログ・統計・状態などの表示 1489
51.1.1 show bridge 1489
51.2 ブリッジのカウンタ・ログ・統計・状態などのクリア 1491
51.2.1 clear bridge 1491
51.3 スパニングツリーのカウンタ・ログ・統計・状態などの表示 1492
51.3.1 show spanning-tree 1492
51.4 スパニングツリーのカウンタ・ログ・統計・状態などのクリア 1504
51.4.1 clear spanning-tree statistics 1504
第 52 章 ブリッジグループのカウンタ・ログ・統計・状態などの表示、クリア操作コマンド 1505
52.1 ブリッジグループのカウンタ・ログ・統計・状態などの表示、クリア 1506
52.1.1 show bridgegroup 1506
52.1.2 show bridgegroup status 1508
52.1.3 clear bridgegroup statistics 1510

第 53 章　認証機能のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド 1511
53.1　認証成功端末情報のカウンタ・ログ・統計・状態などの表示 1512
53.1.1　show auth port ether. 1512
53.2　IEEE802.1X 認証のカウンタ・ログ・統計・状態などの表示 1514
53.2.1　show dot1x port ether. 1514
53.2.2　show dot1x statistics port ether. 1516
53.3　IEEE802.1X 認証のカウンタ・ログ・統計などのクリア 1518
53.3.1　clear dot1x statistics 1518
53.4　MAC アドレス認証のカウンタ・ログ・統計・状態などの表示 1519
53.4.1　show macauth port ether 1519
53.4.2　show macauth statistics port ether 1521
53.5　MAC アドレス認証のカウンタ・ログ・統計などのクリア 1522
53.5.1　clear macauth statistics. 1522
53.6　ARP 認証のカウンタ・ログ・統計・状態などの表示 1523
53.6.1　show arpauth vlan. 1523
53.6.2　show arpauth statistics 1525
53.7　ARP 認証のカウンタ・ログ・統計などのクリア 1526
53.7.1　clear arpauth statistics. 1526
第 54 章　トラッキング情報の表示、クリア操作コマンド 1527
54.1　トラッキング情報の表示 1528
54.1.1　show tracking. 1528
54.1.2　show tracking brief 1531
54.2　トラッキング統計情報のクリア. 1532
54.2.1　clear tracking statistics. 1532
第 55 章　SNMP 統計情報の表示、クリア操作コマンド. 1533
55.1　SNMP 統計情報の表示. 1534
55.1.1　show snmp statistics. 1534
55.2　SNMP 統計などのクリア 1537
55.2.1　clear snmp statistics. 1537
第 56 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 1538
56.1　NETTIME(time/sntp)統計情報の表示. 1539
56.1.1　show nettime statistics 1539
56.2　NETTIME(time/sntp)統計などのクリア 1542
56.2.1　clear nettime statistics. 1542
第 57 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. 1543
57.1　UPnP のカウンタ・ログ・統計・状態などの表示. 1544
57.1.1　show upnp. 1544
57.1.2　show upnp statistics. 1546
57.1.3　show upnp portmapping. 1548
57.2　UPnP のカウンタ・ログ・統計などのクリア. 1549
57.2.1　clear upnp statistics. 1549
57.2.2　clear upnp portmapping 1550
第 58 章　ポリシーグループの状態の表示コマンド. 1551
58.1　ポリシーグループの状態の表示. 1552
58.1.1　show policy-group. 1552
第 59 章　ドメインリストの状態の表示コマンド 1554
59.1　ドメインリストの状態の表示 1555
59.1.1　show domainlist 1555
第 60 章　SSH ホスト認証用公開鍵の表示コマンド 1557

60.1 SSH ホスト認証用公開鍵の表示 1558
60.1.1 show ssh server key 1558

第 61 章 AAA の状態の表示、クリア操作コマンド 1560

61.1 AAA の状態の表示 1561
61.1.1 show aaa radius client server-info 1561
61.1.2 show aaa radius client statistics 1562

61.2 MAC アドレス収集情報の表示、クリア 1564
61.2.1 show aaa mac collect status 1564
61.2.2 show aaa mac collect list 1565
61.2.3 clear aaa mac collect list 1566

第 62 章 ソケット状態の表示コマンド 1567

62.1 ソケット状態の表示 1568
62.1.1 show socket 1568

第 63 章 トレースの表示、クリア操作コマンド 1571

63.1 トレースの表示 1572
63.1.1 show trace ppp 1572
63.1.2 show trace pppoe 1575
63.1.3 show trace ike 1577
63.1.4 show trace modemmodule 1581
63.1.5 show trace ssh 1583

63.2 トレースのクリア 1585
63.2.1 clear trace ssh 1585

第 64 章 証明書関連の表示コマンド 1586

64.1 証明書関連の表示 1587
64.1.1 show crypto certificate 1587

第 65 章 認証関連制御コマンド 1595

65.1 IEEE802.1X 認証制御 1596
65.1.1 dot1xctl initialize port ether 1596
65.1.2 dot1xctl reconfirm port ether 1597

65.2 MAC アドレス認証制御 1598
65.2.1 macauthctl initialize port ether 1598

65.3 ARP 認証制御 1599
65.3.1 arpauthctl initialize 1599

第 66 章 回線制御コマンド 1600

66.1 回線制御 1601
66.1.1 offline 1601
66.1.2 online 1604

第 67 章 VRRP 制御コマンド 1607

67.1 VRRP 制御 1608
67.1.1 vrrp action 1608
67.1.2 vrrp preempt-permit 1610

第 68 章 動的 VPN サーバ制御コマンド 1612

68.1 動的 VPN サーバ制御 1613
68.1.1 dvpnserver disable 1613
68.1.2 dvpnserver enable 1614

第 69 章 RADIUS 制御コマンド 1615

69.1 RADIUS 制御 1616
69.1.1 radius recovery 1616

第 70 章　AAA 制御コマンド 1617
70.1　端末 MAC アドレス収集. 1618
70.1.1　aaactl mac collect start. 1618
70.1.2　aaactl mac collect stop 1620
70.1.3　aaactl mac collect mark 1621
70.1.4　aaactl mac collect unmark. 1622
70.1.5　aaactl mac collect commit. 1623
第 71 章　USB ポート制御コマンド 1625
71.1　USB ポート制御 1626
71.1.1　usbctl 1626
第 72 章　証明書関連制御コマンド 1628
72.1　証明書関連の制御. 1629
72.1.1　crypto certificate generate 1629
72.1.2　crypto certificate local. 1635
72.1.3　crypto certificate remote. 1637
72.1.4　crypto certificate ca. 1639
第 73 章　I'm here コマンド 1641
73.1　I'm here コマンド 1642
73.1.1　iamhere 1642
第 74 章　その他のコマンド. 1643
74.1　その他 1644
74.1.1　ping. 1644
74.1.2　traceroute 1646
74.1.3　telnet 1649
74.1.4　pwconv 1651
74.1.5　dnconv 1652
74.1.6　rpon. 1653
第 75 章　commit コマンド実行時の影響について 1654
索引 1663

第１章　パスワード情報の設定

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 G110

[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。本装置が故障するなどして代替装置に交換した場合は、保存しておいた構成定義をそのまま復元できなくなります。装置に保存した構成定義を代替装置に復元する必要がある場合は、共通パスワード形式で作成した構成定義ファイルを別の場所に保管しておいてください。

unique に設定した状態では、平文、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 admin set

[機能]

管理者パスワードの設定

[適用機種]

Si-R G110

[入力形式]

```
password admin set [<password> [encrypted]]
```

[オプション]

<password>

- 省略

  対話形式でパスワードを入力します。

- パスワード

  パスワードの文字列を、0x21,0x23～0x7e の 64 文字以内の ASCII 文字列で指定します。

- 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。

パスワードが推測されにくいように、8 文字以上で英字、数字、記号を混ぜたパスワードを設定してください。

パスワードを省略した場合は、対話形式でパスワードを入力できます。入力したパスワードは画面に表示されず、システムログ情報にも保存されないため、コマンド実行履歴出力の設定が有効な際もセキュリティ的に安全です。

本コマンドは設定した直後に有効となります。

ログインユーザ名に 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を使用できます。

[注意]

管理者パスワードは必ず設定してください。管理者パスワードを設定していない場合、パスワードなしでログインできます。また、設定したパスワードは定期的に変更するようにしてください。

ログインユーザ情報に、装置内の AAA ユーザ情報(aaa user id コマンド)または RADIUS サーバのユーザ情報を利用する場合でも、管理者パスワードが設定されている必要があります。

7 文字以下、英字だけ、数字だけのパスワードを設定した場合、および設定を削除した場合、設定および削除は行われますが、脆弱である旨の警告メッセージが表示されます。

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。

[メッセージ]

```
Password:
```

<password>引数を省略した場合に表示されます。
パスワードを入力してください。
入力したパスワードは画面に表示されません。

```
Retype password:
```

<password>引数を省略した場合に表示されます。
再度、パスワードを入力してください。
入力したパスワードは画面に表示されません。

```
<ERROR> mismatched password
```

対話形式で 2 回入力したパスワードが一致しませんでした。
再度、パスワードの設定を行ってください。

```
<WARNING> weak admin's password: set the password
```

管理者パスワードが設定されていません。
管理者パスワードを設定してください。

```
<WARNING> weak admin's password: contain at least 8 characters
```

管理者パスワードが 7 文字以下です。
8 文字以上の管理者パスワードを設定してください。

```
<WARNING> weak admin's password: contain a different kind of character
```

管理者パスワードが英字のみ、または数字のみです。
英字、数字、記号を混ぜて管理者パスワードを設定してください。
本メッセージは、ログイン時、および admin、load、discard コマンド実行時にも表示されます。

[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 G110

[入力形式]

```
password user set [<password> [encrypted]]
```

[オプション]

<password>

- 省略
  対話形式でパスワードを入力します。
- パスワード
  パスワードの文字列を、0x21,0x23～0x7e の 64 文字以内の ASCII 文字列で指定します。
- 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。

パスワードが推測されにくいように、8 文字以上で英字、数字、記号を混ぜたパスワードを設定してください。

パスワードを省略した場合は、対話形式でパスワードを入力できます。入力したパスワードは画面に表示されず、システムログ情報にも保存されないため、コマンド実行履歴出力の設定が有効な際もセキュリティ的に安全です。

本コマンドは設定した直後に有効となります。

ログインユーザ名に 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を使用できます。

[注意]

設定したパスワードは定期的に変更するようにしてください。

一般ユーザパスワードを設定していない場合、一般ユーザクラスでログインすることはできません。

7 文字以下、英字だけ、数字だけのパスワードを設定した場合、設定は行われますが、脆弱である旨の警告メッセージが表示されます。

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。

[メッセージ]

```
Password:
```

<password>引数を省略した場合に表示されます。
パスワードを入力してください。
入力したパスワードは画面に表示されません。

```
Retype password:
```

<password>引数を省略した場合に表示されます。
再度、パスワードを入力してください。
入力したパスワードは画面に表示されません。

```
<ERROR> mismatched password
```

対話形式で 2 回入力したパスワードが一致しませんでした。
再度、パスワードの設定を行ってください。

```
<WARNING> weak user's password: contain at least 8 characters
```

一般ユーザパスワードが 7 文字以下です。
8 文字以上の一般ユーザパスワードを設定してください。

```
<WARNING> weak user's password: contain a different kind of character
```

一般ユーザパスワードが英字のみ、または数字のみです。
英字、数字、記号を混ぜて一般ユーザパスワードを設定してください。
本メッセージは、ログイン時、および admin、load、discard コマンド実行時にも表示されます。

[未設定時]

一般ユーザパスワードは設定されていません。

1.1.4 password aaa

[機能]

ログインユーザの AAA 情報の設定

[適用機種]

Si-R G110

[入力形式]

password 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 進数で指定します。

範囲	機種
0～9	Si-R G110

[動作モード]

構成定義モード(管理者クラス)

[説明]

本装置にログインするときに参照する、AAA のグループ ID を指定します。
ログインする際の権限クラスは、以下のとおり決定します。

・ RADIUS サーバを使用する場合
RADIUS サーバに登録された Filter-ID アトリビュートで決定します。
"administrator"であれば管理者クラス、"user"であれば一般ユーザクラスとなります。

・ 本装置内のユーザ情報を使用する場合
AAA 情報に登録されている権限クラス(aaa user user-role)で決定します。

[注意]

管理者の AAA 情報または一般ユーザの AAA 情報が設定されている場合、本コマンドは無効になります。
管理者クラスでログインする場合は、管理者パスワード(password admin set)を必ず設定してください。設定していない場合はログインできません。
RADIUS サーバまたは本装置内のユーザ情報に権限クラスの設定がない場合は、正しい ID とパスワードが入力された場合でもログインできません。

[未設定時]

AAA 情報を参照しないものとみなされます。

1.1.5 password authtype

[機能]

ログインユーザ認証の認証プロトコルの設定

[適用機種]

Si-R G110

[入力形式]

password authtype <authtype>

[オプション]

<authtype>

- chap_md5
  認証プロトコルにMD5-CHAPを使用します。
- pap
  認証プロトコルに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]

ログインユーザ認証の認証プロトコルを設定します。

[未設定時]

ログインユーザ認証の認証プロトコルとしてMD5-CHAPが指定されたものとみなされます。

```
password authtype chap_md5
```

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)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	Si-R G110

・ USB 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 usb 〈line〉(USB 番号)に指定する挿入されている USB の番号(10 進数)は、機種ごとに以下に示す範囲で指定してください。ただし、USB ポートが 1 つの機種は、USB 番号の指定はできません。

範囲	機種
指定不可	Si-R G110

2.1　回線共通情報

2.1.1　wan description

[機能]

wan 回線の説明文の設定

[適用機種]

Si-R G110

[入力形式]

wan <number> description <description>

[オプション]

<number>

・ wan 定義番号
wan 定義の通し番号を、10 進数で指定します。
wan 定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<description>

・ 説明文
この wan 回線の説明文を、0x21,0x23～0x7e の 50 文字以内の ASCII 文字列で記入します。
(入力可能な文字の一覧については、コマンドユーザーズガイドを参照してください。)

[動作モード]

構成定義モード(管理者クラス)

[説明]

この wan 回線についての説明文を記入します。

[未設定時]

説明文を記入しないものとみなされます。

2.1.2 wan use

[機能]

wan 回線の使用の設定

[適用機種]

Si-R G110

[入力形式]

wan <number> use <mode>

[オプション]

<number>

・ wan 定義番号
wan 定義の通し番号を、10 進数で指定します。
wan 定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

使用モードを指定します。

・ off
wan 回線を使用しません。

・ on
wan 回線を使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

wan 回線の使用の設定を行います。

[未設定時]

wan 回線を使用しないものとみなされます。

```
wan <number> use off
```

2.1.3 wan bind

[機能]

利用する物理回線の設定

[適用機種]

Si-R G110

[入力形式]

wan <number> bind usb <line>

[オプション]

<number>

・ wan 定義番号
wan 定義の通し番号を、10 進数で指定します。
wan 定義番号の指定方法の詳細については、本章の冒頭を参照してください。

usb <line>

利用する物理回線のモジュールが、USB に挿入されている場合に指定します。

・ USB 番号
挿入されている USB の番号を、10 進数で指定します。
USB 番号の指定方法の詳細については、本章の冒頭を参照してください。

[動作モード]

構成定義モード(管理者クラス)

[説明]

wan 定義で利用する物理回線を設定します。
複数の wan 定義で同一の物理回線を指定すると、一番小さい定義番号の wan 定義のみ有効となります。
wan 定義と pseudo-ether 定義で同一の bind 先を指定した場合、データ通信モジュールの種別に従った定義が有効になります。
双方の定義を利用できるデータ通信モジュールの場合、pseudo-ether 定義が優先されます。

[未設定時]

物理回線を指定しないものとみなされます。

2.1.4 wan line

[機能]

物理回線の種別の設定

[適用機種]

Si-R G110

[入力形式]

wan <number> line modemmodule (データ通信モジュール)

[オプション]

<number>

・ wan 定義番号
wan 定義の通し番号を、10 進数で指定します。
wan 定義番号の指定方法の詳細については、本章の冒頭を参照してください。

[動作モード]

構成定義モード(管理者クラス)

[説明]

wan 定義で利用する物理回線の種別を設定します。

回線種別	Si-R G110
データ通信モジュール	○

[未設定時]

物理回線の種別が設定されていないものとみなされます。

2.2　データ通信モジュール情報

2.2.1　wan modemmodule condition mode

[機能]

電波状態監視の動作モードの設定

[適用機種]

Si-R G110

[入力形式]

wan <number> modemmodule condition mode <mode>

[オプション]

<number>

・ wan 定義番号
wan 定義の通し番号を、10 進数で指定します。
wan 定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

動作モードを指定します。

・ disable
電波状態監視を行いません。
・ enable
電波状態監視を行います。

[動作モード]

構成定義モード(管理者クラス)

[説明]

電波状態監視の動作モードを設定します。

[未設定時]

電波状態監視を行わないものとみなされます。

```
wan <number> modemmodule condition mode disable
```

2.2.2 wan modemmodule condition level

[機能]

電波状態監視の電波状態判定レベルの設定

[適用機種]

Si-R G110

[入力形式]

wan <number> modemmodule condition level <level>

[オプション]

<number>

・ wan 定義番号
wan 定義の通し番号を、10 進数で指定します。
wan 定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<level>

・ 電波状態判定レベル
電波状態判定レベルを、0～127 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]

電波状態良好と判定する電波レベルを設定します。電波状態監視で取得した電波レベルが本コマンドの設定値以上の場合、電波状態は良好と判定されます。

[注意]

wan <number> modemmodule condition mode コマンドで enable を指定した場合は、本コマンドを必ず設定してください。

[未設定時]

電波状態監視の接続可能レベルが設定されていないものとみなされます。

2.2.3 wan modemmodule condition watch

[機能]

電波状態監視間隔の設定

[適用機種]

Si-R G110

[入力形式]

wan <number> modemmodule condition watch <interval>

[オプション]

<number>

・ wan 定義番号
wan 定義の通し番号を、10 進数で指定します。
wan 定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<interval>

・ 監視間隔
監視間隔を、30 秒～1 日の範囲で指定します。
単位は、d(日)、h(時)、m(分)、s(秒)のいずれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

電波状態監視を行う間隔を設定します。

[注意]

・ wan <number> modemmodule condition mode コマンドで enable を指定した場合は、本コマンドを必ず設定してください。
・ 監視間隔は 2 秒単位で繰り上げられます。たとえば監視間隔を 31 秒に設定したときには、実際の送信間隔は 32 秒になります。

[未設定時]

電波状態監視間隔が設定されていないものとみなされます。

2.2.4 wan modemmodule condition connect mode

[機能]

電波状態監視の接続指示の設定

[適用機種]

Si-R G110

[入力形式]

wan <number> modemmodule condition connect mode <mode>

[オプション]

<number>

・ wan 定義番号
wan 定義の通し番号を、10 進数で指定します。
wan 定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

接続指示モードを指定します。

・ force
電波状態監視の結果にかかわらず、回線は常に接続可能と判断します。

・ level
電波状態監視の結果に応じて、回線の接続可否を判断します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

電波状態監視の接続指示を設定します。

[注意]

wan <number> modemmodule condition mode コマンドで enable を指定した場合は、本コマンドを必ず設定してください。

[未設定時]

電波状態監視の接続指示が設定されていないものとみなされます。

2.2.5 wan modemmodule condition history dupcut

[機能]

電波状態監視の履歴情報の出力設定

[適用機種]

Si-R G110

[入力形式]

wan <number> modemmodule condition history dupcut <mode>

[オプション]

<mode>

- enable
  直前に出力した履歴情報と重複する場合に出力しません。
- disable
  重複チェックを行わず、すべての履歴情報を出力します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

電波状態監視の履歴情報を出力する際、直前に出力した履歴情報と重複する場合に出力するかどうかを指定します。

[未設定時]

直前に出力した履歴情報と重複する場合に出力しないものとみなされます。

```
wan <number> modemmodule condition history dupcut enable
```

2.3 SNMP 関連情報

2.3.1 wan snmp trap linkdown

[機能]

linkDown トラップの設定

[適用機種]

Si-R G110

[入力形式]

wan <number> snmp trap linkdown <mode>

[オプション]

<number>

・ wan 定義番号
wan 定義の通し番号を、10 進数で指定します。
wan 定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

[注意]

snmp trap linkdown コマンドで trap 動作が無効にされた場合は、本コマンド設定値は意味を持ちません。

[未設定時]

linkDown トラップが有効とみなされます。

```
wan <number> snmp trap linkdown enable
```

2.3.2 wan snmp trap linkup

[機能]

linkUp トラップの設定

[適用機種]

Si-R G110

[入力形式]

wan <number> snmp trap linkup <mode>

[オプション]

<number>

・ wan 定義番号
wan 定義の通し番号を、10 進数で指定します。
wan 定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

[注意]

snmp trap linkup コマンドで trap 動作が無効にされた場合は、本コマンド設定値は意味を持ちません。

[未設定時]

linkUp トラップが有効とみなされます。

```
wan <number> snmp trap linkup enable
```

第 3 章　ether グループ情報の設定

・ ether グループ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〈group〉(ether グループ定義番号)に指定するグループ番号の通し番号(10 進数)は、以下に示す範囲で指定してください。

範囲	機種
2	Si-R G110

3.1 ether グループ共通情報

3.1.1 ethergroup vlan mode

[機能]

ether グループの VLAN モードの設定

[適用機種]

Si-R G110

[入力形式]

ethergroup <group> vlan mode <mode>

[オプション]

<group>

・ ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

VLAN モードを指定します。

・ enable
VLAN モードを使用します。
・ disable
VLAN モードを使用しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ether グループの VLAN モードの設定を行います。VLAN モードを使用しない設定の場合、該当 ether グループは透過モードになります。

VLAN モードを使用しない場合、以下のことに注意してください。

・ ether vlan 定義は無効になります。
・ lan vlan 定義において、装置内に未設定の VLAN ID を指定した場合でも、その lan 定義が有効になります。

[未設定時]

VLAN モードを使用するものとみなされます。

```
ethergroup <group> vlan mode enable
```

3.2 ether グループポート間アクセス制御情報

3.2.1 ethergroup access-control mode

[機能]

ether グループのポート間アクセス制御の設定

[適用機種]

Si-R G110

[入力形式]

ethergroup <group> access-control mode <mode>

[オプション]

<group>

・ ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

ポート間アクセスモードを設定します。

・ disable
ポート間アクセス制御を無効にします。

・ enable
ポート間アクセス制御を有効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ether グループのポート間アクセスモードの設定を行います。本設定を有効にした場合、ether グループ内のポート間転送が抑止されます。

[注意]

本機能は、透過モード(ethergroup vlan mode disable)設定時は無効となります。

[未設定時]

ポート間アクセス制御を行わないものとみなされます。

```
ethergroup <group> access-control mode disable
```

3.3 ブリッジグループ関連情報

3.3.1 ethergroup bridgegroup use

[機能]

ブリッジグループ機能の設定

[適用機種]

Si-R G110

[入力形式]

ethergroup <group> bridgegroup use <mode>

[オプション]

<group>

・ ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

ブリッジグループを使用するかどうかを指定します。

・ off
ブリッジグループを使用しない場合に指定します。

・ on
ブリッジグループ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]

ブリッジグループを使用するかどうかを設定します。
ブリッジグループを使用する場合、IP および IPv6 のパケット以外をすべてブリッジします。
IP および IPv6 の転送ポリシーは、ブリッジグループの設定に依存します。

[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グループを使用する場合は、ブリッジグループ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。

[未設定時]

ブリッジグループを使用しないものとみなされます。

```
ethergroup <group> bridgegroup use off
```

3.3.2 ethergroup bridgegroup group

[機能]

ブリッジグループ識別子の設定

[適用機種]

Si-R G110

[入力形式]

ethergroup <group> bridgegroup group <group_id>

[オプション]

<group>

・ ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<group_id>

・ グループ識別子
グループ識別子を、10 進数で指定します。

範囲	機種
0～19	Si-R G110

[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。

```
ethergroup <group> bridgegroup group 0
```

3.3.3 ethergroup bridgegroup control

[機能]

転送対象 MAC コントロールフレームの設定

[適用機種]

Si-R G110

[入力形式]

ethergroup <group> bridgegroup control <protocol>

[オプション]

<group>

・ ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<protocol>

転送対象とするフレームを設定します。
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)を透過、フラッディングします。
・ lacp
LACP のフレームを透過、フラッディングします。
・ eapol
IEEE 802.1X のフレーム(EAPOL)を透過、フラッディングします。
・ other
以下の範囲のフレームを透過、フラッディングします。
01:80:C2:00:00:04 ～ 01:80:C2:00:00:10
01:80:C2:00:00:20 ～ 01:80:C2:00:00:2F

[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透過、フラッディング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、転送のみ行い、本装置では受信しません。
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。
本設定は、ethergroup 2 vlan mode disable、かつ、ethergroup 2 bridgegroup use on の場合のみ有効となります。
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]

転送対象として指定可能なフレームの透過、フラッディングは行いません。

第 4 章　ポート情報の設定

・ グループ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〈group〉(ether グループ定義番号)に指定するグループ番号の通し番号(10 進数)は、以下に示す範囲で指定してください。

範囲	機種
1～2	Si-R G110

・ ポ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〈port〉(ether ポート定義番号)に指定するポート番号の通し番号(10 進数)は、以下に示す範囲で指定してください。

範囲	機種
1	Si-R G110 (グループ 1)
1～4	Si-R G110 (グループ 2)

・ ポート種別構成について

ether ポート定義番号に対応する、ポート種別の構成を以下に示します。

機種	10/100BASE-TX/1000BASE-T
Si-R G110	ether 1 1 ether 2 1～4

・ ポート番号の範囲指定について

本章のコマンドの[オプション]に記載されている〈port〉(ether ポート定義番号)には、以下のように複数ポートを範囲指定することができます。

－ 複数ポート範囲指定例

```
1           = port1
1-8         = port1～port8
1,2         = port1,port2
-8          = port1～port8
```

・ バックアップグループ番号の指定範囲

本章のコマンドの[オプション]に記載されている〈backup_group〉(バックアップグループ番号)に指定するグループ番号の通し番号(10 進数)は、以下に示す範囲で指定してください。

範囲	機種
1～2	Si-R G110

・ STP インスタンス ID 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〈instance_id〉(STP インスタンス ID 番号)に指定する STP インスタンス ID の通し番号(10 進数)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-R G110

4.1 ether 共通情報

4.1.1 ether description

[機能]

ether ポートの説明文の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> description <description>

[オプション]

<group>

・ ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<description>

・ 説明文
この ether ポートの説明文を、0x21,0x23～0x7e の 50 文字以内の ASCII 文字列で記入します。
(入力可能な文字の一覧については、コマンドユーザーズガイドを参照してください。)

[動作モード]

構成定義モード(管理者クラス)

[説明]

この ether ポートについての説明文を記入します。

[未設定時]

説明文を記入しないものとみなされます。

4.1.2 ether use

[機能]

ether ポートの使用の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> use <mode>

[オプション]

<group>

・ ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ) で区切ります。
複数の番号が続く場合、"-" (ハイフン) で区切ります (例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

ポートの使用モードを指定します。

・ on
ether ポートを使用します。
・ off
ether ポ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]

ether ポートの使用の設定を行います。

[未設定時]

ether ポートを使用するものとみなされます。

```
ether <group> <port> use on
```

4.1.3 ether media

[機能]

ether ポートのメディア種別の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> media <type>

[オプション]

<group>

・ ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<type>

メディア種別

・ auto
メディア種別を自動で選択します。
※ただし、両方接続されている場合は、SFP ポートを使用します。
・ metal
10/100/1000BASE-T ポート(RJ45)を使用します。
・ fiber
SFP 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]

ether ポートで使用するメディア種別を設定します。

[注意]

・ auto 指定の場合で、10/100/1000BASE-T ポート、SFP ポート共にケーブル接続した場合は、SFP ポートが選択されます。
・ 同様に、auto 指定で 10/100/1000BASE-T ポートがリンクアップしている状態で SFP ポートにケーブルを接続して SFP ポートをリンクアップさせると、SFP ポートの動作となり、10/100/1000BASE-T ポートはリンクダウン状態となります。
・ fiber 指定の場合は、mdi/duplex 定義は無視されます。
・ auto または fiber 指定で SFP ポートがリンクアップの場合は、mode の 100/10 設定は無視されます。
・ 本設定は、ether グループ 1 ポート 1 のみ設定できます。

[未設定時]

メディア種別の自動選択モードが指定されたものとみなされます。

```
ether <group> <port> media auto
```

4.1.4 ether mode

[機能]

ether ポートの通信速度の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> mode <speed>

[オプション]

<group>

・ ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<speed>

通信速度

・ auto
オートネゴシエーションにより通信速度を決定します。
・ 1000
1Gbps 固定にします。
・ 100
100Mbps 固定にします。
・ 10
10Mbps 固定にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ether ポートの通信速度の設定を行います。

[未設定時]

オートネゴシエーションモードが設定されたものとみなされます。

```
ether <group> <port> mode auto
```

4.1.5 ether duplex

[機能]

ether ポートの全二重/半二重の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> duplex <duplex>

[オプション]

<group>

・ ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、ether 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]

ether ポートの全二重/半二重の設定を行います。

[注意]

・ ether mode コマンドで 1000 を指定した場合は、本コマンドの設定内容は無効となり、全二重モードで動作します。
・ ether 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]

全二重モードが設定されたものとみなされます。

```
ether <group> <port> duplex full
```

4.1.6 ether mdi

[機能]

ether ポートの MDI の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> mdi <mode>

[オプション]

<group>

・ ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ) で区切ります。
複数の番号が続く場合、"-" (ハイフン) で区切ります (例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

MDI のモードを指定します。

・ auto
MDI/MDI-X 自動検出モードにします。
・ mdi
MDI モード固定にします。
・ mdix
MDI-X モード固定にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ether ポートの MDI のモードを設定します。

[注意]

・ MDI/MDI-X 自動検出モードは、ether mode コマンドの設定が 1Gbps 固定またはオートネゴシエーションの場合のみ有効となります。(ether mode コマンドの設定が、100Mbps または 10Mbps 固定の場合は無効となり、MDI-X 固定で動作します。)
・ MDI 固定モードは、ether mode コマンドの設定が 100Mbps または 10Mbps 固定の場合と、10/100BASE-TX ポートのオートネゴシエーションの場合のみ有効となります。(ether mode コマンドの設定が、1Gbps 固定または 10/100/1000BASE-T ポートのオートネゴシエーションの場合は無効となり、MDI-X 固定で動作します。)
・ ether mode と ether mdi の設定に対する MDI 動作を以下に示します。

ether mdi 設定 ether mode 設定	auto	mdi	mdix
auto	auto	mdix	mdix
1000	auto	mdix	mdix
100, 10	mdix	mdi	mdix

[未設定時]

MDI/MDI-X 自動検出モードが設定されたものとみなされます。

```
ether <group> <port> mdi auto
```

4.1.7 ether flowctl

[機能]

ether ポートのフロー制御機能の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> flowctl <send> <receive>

[オプション]

<group>

・ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<send>

・off
フロー制御パケットの送信を行いません。
・on
フロー制御パケットの送信を行います。

<receive>

・on
フロー制御パケットを受信した場合、フロー制御を行います。
・off
フロー制御パケットを受信した場合でも、フロー制御を行いません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ether ポートのフロー制御機能の動作を、送信機能と受信機能で設定します。
バックプレッシャー機能は、半二重モードの場合に有効です。
フロー制御機能は、ether mode コマンドの通信速度によらず有効です。

[未設定時]

フロー制御パケットを受信した場合だけ、フロー制御を行うように設定されたものとみなされます。

```
ether <group> <port> flowctl off on
```

4.1.8 ether type

[機能]

ether ポートの種別の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> type normal
ether <group> <port> type backup <backup_group> <priority>
ether <group> <port> type mirror <count> <source_group> <source_port> <mode>

[オプション]

<group>

・ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

normal

通常ポート

backup

バックアップポート

mirror

ミラーターゲットポート

<backup_group>

・グループ番号
バックアップグループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<priority>

・ポートの優先度
backup を指定したときに、優先ポートまたは待機ポートのどちらかを指定します。

master

優先ポート

backup

待機ポート

<count>

・定義番号
ソースポートを定義する場合に、10 進数で指定します。

範囲	機種
0～3	Si-R G110

<source_group> <source_port>

・ソースポート番号
mirror を指定したときに、ソースポートを設定します。
グループ番号、ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

・ ミラー動作モード

mirror を設定した場合、以下の動作モードのいずれかを設定します。

rx

：ソースポートの受信フレームをミラーします。

tx

：ソースポートの送信フレームをミラーします。

both

：ソースポートの送受信フレームをミラーします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ether ポートのタイプを設定します。

以下から選択します。

・ 通常ポート
・ バックアップポート
・ ミラーターゲットポート

また、ether ポート定義は、ether グループ 2 のみ設定できます。

[注意]

backup 指定時の注意

バックアップグループに master または backup ポートが未定義の場合、該当グループのポートはリンクアップせず使用できません。

mirror 指定時の注意

・ ミラーターゲットポートは装置で 1 ポートしか設定できません。
・ ミラーターゲットポートは通常運用には使用できません。
・ ミラーターゲットポートに出力されるパケットは以下のようになります。
  － 受信パケットをミラーリングした場合
    受信したパケットがそのまま出力されます。
  － 送信パケットをミラーリングした場合
    VLAN タグが付与された形式となってターゲットポートから送信されます。VLAN ID は、ソースポートに設定されている VLAN ID が付与されます。

[未設定時]

通常ポートが設定されたものとみなされます。

```
ether <group> <port> type normal
```

4.2 STP 情報

4.2.1 ether stp use

[機能]

ether ポートの STP 使用可否の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> stp use <mode>

[オプション]

<group>

・ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<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]

ether ポートでの STP 使用可否を設定します。

[注意]

本モードを使用するに設定した場合でも、装置の STP 動作モードが OFF(stp mode disable)の場合は設定が無効となります。
装置の STP 動作モードが OFF(stp mode disable)以外の場合、トポロジの変更によって、ポートが一時的に通信が行えない状態になることがあります。
STP を使用しないポートには、本モードを使用しないに設定してください。
また、ether ポートの STP 機能は、ether グループ 2 のみ設定できます。

[未設定時]

ether ポートで STP を使用するものとみなされます。

```
ether <group> <port> stp use on
```

4.2.2 ether stp domain cost

[機能]

ether ポートのパスコストの設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> stp domain <instance_id> cost <path_cost>

[オプション]

<group>

・ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<instance_id>

・STP インスタンス ID 番号
使用する STP インスタンス ID 番号を、10 進数で設定します。
STP インスタンス ID 番号の指定方法の詳細については、本章の冒頭を参照してください。

<path_cost>

・auto
自動的にコストを決定します。
・パスコスト
パスコストを 1～200000000 の 10 進数で設定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

STP のポートのパスコストを設定します。
また、ether ポートの STP 機能は、ether グループ 2 のみ設定できます。

[未設定時]

ether ポートのパスコストに、自動設定を使用するものとみなされます。

```
ether <group> <port> stp domain <instance_id> cost auto
```

4.2.3 ether stp domain priority

[機能]

ether ポートの優先度の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> stp domain <instance_id> priority <priority>

[オプション]

<group>

・ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<instance_id>

・STP インスタンス ID 番号
使用する STP インスタンス ID 番号を、10 進数で設定します。
STP インスタンス ID 番号の指定方法の詳細については、本章の冒頭を参照してください。

<priority>

・優先度
ポートの優先度に 16 で割り切れる値(有効値)を、0～240 の 10 進数で設定します。
有効値:
0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240
有効値以外は設定できません。また、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]

ポートの優先度を設定します。
また、ether ポートの STP 機能は、ether グループ 2 のみ設定できます。

[未設定時]

ether ポートの STP ポート優先度に 128 を使用するものとみなされます。

```
ether <group> <port> stp domain <instance_id> priority 128
```

4.3 VLAN 関連情報

4.3.1 ether vlan tag

[機能]

ether ポートの Tag 付き VLAN 登録

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> vlan tag <vidlist>

[オプション]

<group>

・ ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<vidlist>

・ Tag 付き VLAN ID リスト
Tag 付き VLAN ID を、1～4094 の 10 進数で指定します。
複数の VLAN ID を指定する場合は、"," (カンマ)で区切ります。

[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]

・ 同一ポートに同じ VID を Tag 付き、Tag なしを設定した場合、Tag なしが優先されます。
・ VLAN を追加登録する際には、すでに登録されている VLAN も含めた VLAN ID リストを指定してください。
・ ether グループ 1 と ether グループ 2 と pseudo-ether では、同じ VLAN ID を指定することはできません。
ether グループ 1 と ether グループ 2 と pseudo-ether では、異なる VLAN ID を指定してください。
ether グループ 1 と ether グループ 2 で同じ VLAN ID を指定した場合、ether グループ 1 の指定が有効になります。
ether と pseudo-ether で同じ VLAN ID を指定した場合、ether の指定が有効になります。
・ ether グループ 2 では同一 VLAN ID を複数ポートに指定できます。
・ ether グループ 1 の各ポートには、必ず Tag 付き VLAN か Tag なし VLAN を指定してください。
・ resource system vlan で設定されている VLAN ID を指定した場合、この指定は無効になります。
・ ethergroup vlan mode disable を設定した場合、本設定は無効となります。

[未設定時]

なし

4.3.2 ether vlan untag

[機能]

ether ポートの Tag なし VLAN 登録

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> vlan untag <vid>

[オプション]

<group>

・ ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<vid>

・ Tag なし VLAN ID
Tag なし VLAN ID を、1～4094 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]

Untagged VLAN ID の設定を行います。

[注意]

・ 同一ポートに同じ VID を Tag 付き、Tag なしを設定した場合、Tag なしが優先されます。
・ ether グループ 1 と ether グループ 2 と pseudo-ether では、同じ VLAN ID を指定することはできません。
ether グループ 1 と ether グループ 2 と pseudo-ether では、異なる VLAN ID を指定してください。
ether グループ 1 と ether グループ 2 で同じ VLAN ID を指定した場合、ether グループ 1 の指定が有効になります。
ether と pseudo-ether で同じ VLAN ID を指定した場合、ether の指定が有効になります。
・ ether グループ 2 では同一 VLAN ID を複数ポートに指定できます。
・ ether グループ 1 の各ポートには、必ず Tag 付き VLAN か Tag なし VLAN を指定してください。
・ resource system vlan で設定されている VLAN ID を指定した場合、この指定は無効になります。
・ ethergroup vlan mode disable を設定した場合、本設定は無効となります。

[未設定時]

ether vlan tag コマンドが設定されていない場合

・ ether グループ 1
Tag なし VLAN ID として 1 が設定されたとみなされます。

```
ether 1 <port> vlan untag 1
```

・ ether グループ 2

Tag なし VLAN ID として 1 が設定されたとみなされます。

```
ether 2 <port> vlan untag 1
```

ether vlan tag コマンドが設定されている場合

- ether グループ 1
  VLAN ID が設定されていないものとみなされます。
- ether グループ 2
  VLAN ID を設定しないものとみなされます。

4.3.3 ether vlan primap mode

[機能]

ether ポートの VLAN プライオリティマッピング動作の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> vlan primap mode <mode>

[オプション]

<group>

・ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ) で区切ります。
複数の番号が続く場合、"-" (ハイフン) で区切ります (例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

VLAN プライオリティマッピングの動作モードを指定します。

・disable
VLAN プライオリティマッピングを行いません。

・enable
VLAN プライオリティマッピングの設定内容に従って VLAN のプライオリティ値を設定します。

・ip
IP の ToS 値または IPv6 の Traffic Class 値の上位 3 ビットで VLAN のプライオリティ値を設定します。
以下に、ToS 値または Traffic Class 値と、設定値との対応を示します。

ToS 値または Traffic Class 値	設定値
0x00 ～ 0x1F	0
0x20 ～ 0x3F	1
0x40 ～ 0x5F	2
0x60 ～ 0x7F	3
0x80 ～ 0x9F	4
0xA0 ～ 0xBF	5
0xC0 ～ 0xDF	6
0xE0 ～ 0xFF	7

[動作モード]

構成定義モード (管理者クラス)

[説明]

VLAN プライオリティマッピング動作の設定を行います。

［注意］

VLAN プライオリティマッピングを設定する場合、ほかのポートと同一 VLAN を構成しないようにしてください。

［未設定時］

VLAN プライオリティマッピングを行わないものとみなされます。

```
ether <group> <port> vlan primap mode disable
```

4.3.4 ether vlan primap rule

[機能]

ether ポートの VLAN プライオリティマッピングの設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> vlan primap rule <count> <vid> <protocol> <tos> <priority>

[オプション]

<group>

・ ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～999	Si-R G110

<vid>

マッピング対象とする VLAN ID を、1～4094 の 10 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。
範囲指定する場合は、「1-4094」のように"-"(ハイフン)を使用して指定します。
VLAN ID 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。

・ 1～4094 の 10 進数値 (例: 4094 = 4094 の VLAN ID)
・ 10 進数値-10 進数値 (例: 10-50 = 10 から 50 までの VLAN ID)
・ 10 進数値- (例: 100- = 100 から 4094 までの VLAN ID)
・ -10 進数値 (例: -500 = 1 から 500 までの VLAN ID)
・ 10 進数値,10 進数値,… (例: 10,20,30- = 10 と 20 と 30 以降の VLAN ID)

<protocol>

・ 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。
・ ipv6
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。
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]

VLAN ID、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
1000	Si-R G110

[注意]

本設定は、ether ポートの VLAN プライオリティマッピング動作の設定で動作モードが enable の場合に有効になります。

[未設定時]

VLAN プライオリティマッピングの設定が指定されていないものとみなします。

4.4 ポート閉塞関連情報

4.4.1 ether recovery

[機能]

自動復旧モードの設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> recovery <mode> <startup>

[オプション]

<group>

・ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-" (ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

・auto
ether ポート障害復旧時に自動復旧します。
・manual
ether ポート障害発生時に自動的に閉塞状態となり、ether ポート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]

ether ポート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 ether 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]

閉塞状態に入ると、リンクランプは消灯します。
ポートバックアップ機能の待機ポート閉塞設定と起動時閉塞設定を併用した際、起動時閉塞が優先となります。

[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、ether ポート障害発生時には障害復旧後に自動復旧します。

```
ether <group> <port> recovery auto up
```

4.5 シェーピング関連情報

4.5.1 ether shaping

[機能]

シェーピング機能の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> shaping <mode> [<rate>]

[オプション]

<group>

・ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

・off
シェーピングを使用しません。
・on
シェーピングを使用します。

<rate>

・最大送出レート
最大送出レートを、10 進数と単位文字で指定します。
10 進数の末尾に 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-R G110

[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する場合、ほかのポートと同一 VLAN を構成しないようにしてください。

［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。

```
ether <group> <port> shaping off
```

4.5.2 ether shaping-opt tc

[機能]

シェーピング機能の単位時間の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> shaping-opt tc <tc>

[オプション]

<group>

・ ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<tc>

・ 単位時間
単位時間の値(単位はミリ秒)を、1～100 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]

シェーピング機能の単位時間を設定します。

[未設定時]

単位時間の値として、10 ミリ秒を設定したものとみなされます。

```
ether <group> <port> shaping-opt tc 10
```

4.6 WFQ 関連情報

4.6.1 ether priority ip

[機能]

ether ポートの帯域制御の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> priority ip <count> acl <acl_count> <width>

[オプション]

<group>

・ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

・帯域制御定義番号
帯域制御定義番号を、10 進数で指定します。

範囲	機種
0～99	Si-R G110

<acl_count>

・ACL 定義番号
使用する ACL 定義の番号を、10 進数で指定します。
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
0～999	Si-R G110

<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～1000000kbps または 1mbps～1000mbps 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。

<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。

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
3000	Si-R G110

[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。
- 帯域制御を使用する場合、シェーピングと同様、ほかのポートと同一 VLAN を構成しないようにしてください。
- <dst_addr>/<mask>に"dynamic"を指定した ACL は使用しないでください。

[未設定時]

帯域制御を行わないものとみなされます。

4.6.2 ether priority ipv6

[機能]

ether ポートの IPv6 プロトコル帯域制御の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> priority ipv6 <count> acl <acl_count> <width>

[オプション]

<group>

・ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

・帯域制御定義番号
帯域制御定義番号を、10 進数で指定します。

範囲	機種
0～99	Si-R G110

<acl_count>

・ACL 定義番号
使用する ACL 定義の番号を、10 進数で指定します。
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。

ipv6

ipv6 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

ipv6 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、ipv6 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

ipv6 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、ipv6 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

ipv6 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、ipv6 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-R G110

<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～1000000kbps または 1mbps～1000mbps 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。

<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。

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
3000	Si-R G110

[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。

帯域制御を使用する場合、シェーピングと同様、ほかのポートと同一 VLAN を構成しないようにしてください。

[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。

4.7 MAC アドレス認証情報

4.7.1 ether macauth use

[機能]

ether ポートの MAC アドレス認証使用の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> macauth use <mode>

[オプション]

<group>

・ ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

MAC アドレス認証モードを指定します。

・ off
MAC アドレス認証機能を無効にします。
・ on
MAC アドレス認証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]

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転送を行い、認められていなければパケットを破棄します。

<mode>が off の場合、MAC アドレス認証機能は無効です。

また、ether ポートの MAC アドレス認証機能は、ether グループ 2 のみ設定できます。

[注意]

・ VLAN 透過モード(ethergroup vlan mode disable)設定時は、本設定は無効となり、該当ポートは利用できなくなります。
・ 本モードが有効と指定された場合、macauth use 定義でシステム側が無効となっている場合はポート認証は行われません。
・ MAC アドレス認証を有効にしたポートに VLAN 設定はできません。VLAN 設定がされている場合、該当ポートは利用できなくなります。
・ 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、ether 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。
・ 本コマンドを動的定義変更すると該当ポートは、いったん閉塞し MAC アドレス認証状態を初期化します。

・ 認証サーバの認証データベースまたはローカル認証データベースには必ずVLAN IDも登録してください。認証実行時にVLAN IDの通知がない場合は、ether macauth vidコマンドで設定されたデフォルトVLANにマッピングします。また、認証された端末が割り当てられたVLAN IDを持つポートがMACアドレス認証ポート以外に存在しない場合はエラーとなり、常に認証が失敗します。
・ 本認証使用時は、etherポートの種別を通常ポート(ether type normal)設定にしてください。
・ 同一ポートで併用できる認証機能は以下のとおりです。

機種	IEEE802.1X認証	MACアドレス認証
Si-R G110	○	○

[未設定時]

MACアドレス認証機能を無効にするものとみなされます。

```
ether <group> <port> macauth use off
```

4.7.2 ether macauth aaa

[機能]

ether ポートの MAC アドレス認証で参照する AAA グループ ID の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> macauth aaa <group_id>

[オプション]

<group>

・ ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<group_id>

・ グループ ID
使用する AAA グループを示す ID を 10 進数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 アドレス認証の認証時参照する AAA のグループ ID を設定します。
また、ether ポートの MAC アドレス認証機能は、ether グループ 2 のみ設定できます。

[注意]

AAA グループ ID は必須設定項目です。MAC アドレス認証が有効であるポートで AAA グループ ID が未設定の場合、そのポートは利用できなくなります。
本コマンドを動的定義変更すると該当ポートは、いったん閉塞し MAC アドレス認証状態を初期化します。

[未設定時]

AAA 情報を使用しないものとみなされます。

4.7.3 ether macauth authenticated-mac

[機能]

ether ポートの MAC アドレス認証不要端末アドレスの設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> macauth authenticated-mac <count> <macaddr> <vid>

[オプション]

<group>

・ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

・定義番号
定義番号を、10 進数で指定します。

範囲	機種
0～499	Si-R G110

<macaddr>

・認証不要端末 MAC アドレス
認証しないで通信を許可する MAC アドレスを指定します。
(XX:XX:XX:XX:XX:XX の形式で、XX は 2 桁の 16 進数です。)

<vid>

・VLAN ID
認証不要端末に割り当てる VLAN ID を、1～4094 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]

MAC アドレス認証ポートで認証しないで通信を許可する端末(プリンタなど)を設定します。
また、ether ポートの MAC アドレス認証機能は、ether グループ 2 のみ設定できます。

[注意]

・MAC アドレス認証が無効な場合に、設定は無効となります。
・<macaddr>に、00:00:00:00:00:00 およびブロードキャスト、マルチキャストは指定できません。
・<vid>で指定された VLAN が未登録の場合に、設定は無効となります。
・同一アドレスを複数のポートへ登録することはできません。
・本コマンドで指定された認証不要端末を、別のポートへ接続した場合は正常に通信できない場合があります。
・本コマンドを動的定義変更すると該当ポートはいったん閉塞し MAC アドレス認証状態を初期化します。

［未設定時］

設定されなかったものとして動作します。

4.7.4 ether macauth expire

[機能]

ether ポートの認証結果保持時間の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> macauth expire <success_time> <failure_time>

[オプション]

<group>

・ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、60～86400 秒の範囲で指定します。
単位は、s(秒)、m(分)、h(時)、d(日)のいずれかを指定します。

<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、60～86400 秒の範囲で指定します。
単位は、s(秒)、m(分)、h(時)、d(日)のいずれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

MAC アドレス認証結果の保持時間を設定します。
認証成功端末で、認証成功保持時間を経過した場合に再認証を実施します。
認証失敗端末で、認証失敗保持時間を経過するまでの間は、再認証を実施しません。
また、ether ポートの MAC アドレス認証機能は、ether グループ 2 のみ設定できます。

[注意]

認証成功および認証失敗保持時間の監視は 30 秒間隔で行っているため、最大 30 秒までの誤差が生じます。

[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 分が設定されたものとみなされます。

```
ether <group> <port> macauth expire 20m 5m
```

4.7.5 ether macauth vlan assign

[機能]

ether ポートの VLAN 割り当て方式の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> macauth vlan assign <mode>

[オプション]

<group>

・ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

AAA/RADIUS サーバから通知された VLAN ID を端末(Supplicant)に割り当てるかどうかを指定します。

・enable
VLAN ID を割り当てます。
・disable
VLAN ID を割り当てません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

MAC アドレス認証が成功したときに AAA/RADIUS サーバから通知された VLAN ID の端末(Supplicant)への割り当て方式を設定します。
また、ether ポートの MAC アドレス認証機能は、ether グループ 2 のみ設定できます。

[注意]

<mode> が enable の場合

AAA/RADIUS サーバから VLAN ID が通知された場合、その VLAN ID が割り当てられます。
AAA/RADIUS サーバから VLAN ID が通知されなかった場合、ether macauth vid コマンドで設定された VLAN ID が割り当てられます。
ether macauth vid コマンドが未設定の場合は VLAN1 が割り当てられます。

<mode> が disable の場合

AAA/RADIUS サーバからの VLAN ID 通知有無にかかわらず、ether macauth vid コマンドで設定された VLAN ID が割り当てられます。
ether macauth vid コマンドが未設定の場合は VLAN1 が割り当てられます。

[未設定時]

AAA/RADIUS サーバから通知された VLAN ID を端末(Supplicant)に割り当てるものとみなされます。

```
ether <group> <port> macauth vlan assign enable
```

4.7.6 ether macauth vid

[機能]

ether ポートの端末(Supplicant)に割り当てるデフォルト VLAN ID の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> macauth vid <vid>

[オプション]

<group>

・ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<vid>

端末(Supplicant)に割り当てるデフォルト VLAN ID を 1～4094 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]

MAC アドレス認証が成功したときに端末(Supplicant)に割り当てるデフォルト VLAN ID を指定します。

[注意]

AAA/RADIUS サーバから端末(Supplicant)に割り当てる VLAN ID の通知があった場合はここで定義された VLAN ID ではなく、AAA/RADIUS サーバから通知された VLAN ID が優先的に割り当てられます。

本設定で指定される VLAN ID と同じ VLAN ID を持つインタフェースを別のポートに対して必ず設定してください。同一 VLAN ID を持つインタフェースがない場合、認証結果にかかわらず認証が失敗します。

本コマンドを動的定義変更すると該当ポートはいったん閉塞し MAC アドレス認証状態を初期化します。

[未設定時]

デフォルト VLAN ID を設定しないものとみなされます。

なお、本コマンドの設定がなく AAA/RADIUS サーバからの VLAN ID がない場合は、システムログに VLAN ID の通知がない旨表示のうえ、認証に成功した端末(Supplicant)を VLAN1 にマッピングします。

4.8 IEEE802.1X 認証情報

4.8.1 ether dot1x use

[機能]

ether ポートの IEEE802.1X 認証の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> dot1x use <mode>

[オプション]

<group>

・ ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

IEEE802.1X 認証モードを指定します。

・ off
IEEE802.1X 認証機能を無効にします。
・ on
IEEE802.1X 認証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]

ポートアクセス制御として IEEE802.1X 認証モードを設定します。
IEEE802.1X 認証モードを有効にすると、認証により許容された端末(Supplicant)以外の通信は遮断されます。
また、ether ポートの IEEE802.1X 認証機能は、ether グループ 2 のみ設定できます。

[注意]

・ VLAN 透過モード(ethergroup vlan mode disable)設定時は、本設定は無効となり、該当ポートは利用できなくなります。
・ 本モードが有効と指定された場合、dot1x use 定義でシステム側が無効となっている場合はポート認証は行われません。
・ IEEE802.1X 認証を有効にしたポートに VLAN 設定はできません。VLAN 設定がされている場合、該当ポートは利用できなくなります。
・ IEEE802.1X 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、ether dot1x aaa <group_id>で認証先データベースの指定を行ってください。
・ 認証サーバの認証データベースまたはローカル認証データベースには必ず VLAN ID も登録してください。認証処理時に VLAN ID の通知がない場合は ether dot1x vid コマンドで設定されたデフォルト VLAN にマッピングします。また、認証された端末が割り当てられた VLAN ID を持つポートが IEEE802.1X 認証ポート以外に存在しない場合はエラーとなり、常に認証が失敗します。

・ 本認証使用時は、ether ポートの種別を通常ポート(ether type normal)設定にしてください。
・ 同一ポートで併用できる認証機能は以下のとおりです。

機種	IEEE802.1X 認証	MAC アドレス認証
Si-R G110	○	○

[未設定時]

IEEE802.1X 認証モードを無効にするものとみなされます。

```
ether <group> <port> dot1x use off
```

4.8.2 ether dot1x aaa

[機能]

ether ポートの IEEE802.1X 認証で参照する AAA 情報の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> dot1x aaa <group_id>

[オプション]

<group>

・ ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<group_id>

・ グループ ID
使用する AAA グループを示す ID を 10 進数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]

IEEE802.1X 認証の認証時参照する AAA のグループ ID を指定します。
また、ether ポートの IEEE802.1X 認証機能は、ether グループ 2 のみ設定できます。

[注意]

AAA グループ ID は必須設定項目です。IEEE802.1X 認証が有効であるポートで AAA グループ ID が未設定の場合、そのポートは利用できなくなります。

[未設定時]

AAA 情報を使用しないものとみなされます。

4.8.3 ether dot1x quietperiod

[機能]

ether ポートの認証失敗時再認証抑止時間の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> dot1x quietperiod <time>

[オプション]

<group>

・ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<time>

認証失敗後の再認証開始時間を 0～600 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。
0 秒を指定した場合は、認証失敗後の再認証抑止なしに即座に認証要求を受け付けます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

認証が拒否された端末(Supplicant)との再認証を開始するまでの時間を設定します。
また、ether ポートの IEEE802.1X 認証機能は、ether グループ 2 のみ設定できます。

[未設定時]

認証失敗後、再認証を開始するまでの時間として 60 秒(1 分)が設定されたものとみなされます。

```
ether <group> <port> dot1x quietperiod 1m
```

4.8.4 ether dot1x txperiod

[機能]

ether ポートの認証開始要求送信待ち時間の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> dot1x txperiod <time>

[オプション]

<group>

・ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<time>

認証開始要求の送信待ち時間を 1～600 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]

ユーザ ID 要求の送信間隔を設定します。

[未設定時]

ユーザ ID 要求の送信間隔として 30 秒が設定されたものとみなされます。

```
ether <group> <port> dot1x txperiod 30s
```

4.8.5 ether dot1x supptimeout

[機能]

ether ポートの EAP 応答待ち時間の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> dot1x supptimeout <time>

[オプション]

<group>

・ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<time>

EAP パケットの応答待ち時間を 1～600 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]

端末(Supplicant)に対する EAP 応答待ち時間を設定します。
また、ether ポートの IEEE802.1X 認証機能は、ether グループ 2 のみ設定できます。

[未設定時]

EAP 応答待ち時間として 30 秒が設定されたものとみなされます。

```
ether <group> <port> dot1x supptimeout 30s
```

4.8.6 ether dot1x maxreq

[機能]

ether ポートの EAP 再送回数の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> dot1x maxreq <count>

[オプション]

<group>

・ ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

EAP 再送回数を 1～10 回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]

EAP 応答が受信できない場合の EAP 再送回数を指定します。
また、ether ポートの IEEE802.1X 認証機能は、ether グループ 2 のみ設定できます。

[未設定時]

EAP 再送回数として 2 回が設定されたものとみなされます。

```
ether <group> <port> dot1x maxreq 2
```

4.8.7 ether dot1x reauthperiod

[機能]

ether ポートの再認証間隔の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> dot1x reauthperiod <time>

[オプション]

<group>

・ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<time>

・infinity
再認証を行いません。この場合は、端末(Supplicant)からのログオフメッセージを受信するか、ポートのリンクダウンを検出するまでは認証済みの状態が保持されます。

・上記以外
再認証間隔を 15～18000 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

端末(Supplicant)の再認証間隔を指定します。
また、ether ポートの IEEE802.1X 認証機能は、ether グループ 2 のみ設定できます。

[注意]

短い再認証間隔設定で同時に複数ポートに対する再認証を行った場合、認証処理が完了する前に再認証処理が起動され認証が失敗することがあります。

[未設定時]

再認証間隔として 3600 秒(1 時間)が設定されたものとみなされます。

```
ether <group> <port> dot1x reauthperiod 1h
```

4.8.8 ether dot1x vlan assign

[機能]

ether ポートの VLAN 割り当て方式の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> dot1x vlan assign <mode>

[オプション]

<group>

・ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

AAA/RADIUS サーバから通知された VLAN ID を端末(Supplicant)に割り当てるかどうかを指定します。

・enable
VLAN ID を割り当てます。

・disable
VLAN ID を割り当てません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IEEE802.1X 認証が成功したときに AAA/RADIUS サーバから通知された VLAN ID の端末(Supplicant)への割り当て方式を設定します。
また、ether ポートの IEEE802.1X 認証機能は、ether グループ 2 のみ設定できます。

[注意]

<mode> が enable の場合

AAA/RADIUS サーバから VLAN ID が通知されなかった場合、ether dot1x vid コマンドで設定された VLAN ID が割り当てられます。
ether dot1x vid コマンドが未設定の場合は VLAN1 が割り当てられます。

<mode> が disable の場合

AAA/RADIUS サーバからの VLAN ID 通知有無にかかわらず ether dot1x vid コマンドで設定された VLAN ID が割り当てられます。
ether dot1x vid コマンドが未設定の場合は VLAN1 が割り当てられます。

[未設定時]

AAA/RADIUS サーバから通知された VLAN ID を端末(Supplicant)に割り当てるものとみなされます。

```
ether <group> <port> dot1x vlan assign enable
```

4.8.9 ether dot1x vid

[機能]

端末(Supplicant)に割り当てるデフォルト VLAN ID の設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> dot1x vid <vid>

[オプション]

<group>

・ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<vid>

端末(Supplicant)に割り当てるデフォルト VLAN ID を 1～4094 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]

IEEE802.1X 認証が成功したときに端末(Supplicant)に割り当てるデフォルト VLAN ID を指定します。
また、ether ポートの IEEE802.1X 認証機能は、ether グループ 2 のみ設定できます。

[注意]

AAA/RADIUS サーバから端末(Supplicant)に割り当てる VLAN ID の通知があった場合はここで定義された VLAN ID ではなく、AAA/RADIUS サーバから通知された VLAN ID が割り当てられます。
本設定で指定される VLAN ID と同じ VLAN ID を持つインタフェースを別のポートに対して必ず設定してください。同一 VLAN ID を持つインタフェースがない場合、認証結果にかかわらず認証が失敗します。
認証前の状態で登録済みの VLAN ID は、認証成功した端末に割り当てることはできません。

[未設定時]

デフォルト VLAN ID を設定しないものとみなされます。なお、本コマンドの設定がなく AAA/RADIUS サーバからの VLAN ID がない場合は、システムログに VLAN ID の通知がない旨表示のうえ、認証に成功した端末(Supplicant)を VLAN1 にマッピングします。

4.9 SNMP 関連情報

4.9.1 ether snmp trap linkdown

[機能]

ether ポートの linkDown トラップの設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> snmp trap linkdown <mode>

[オプション]

<group>

・ ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-" (ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

[注意]

snmp trap linkdown コマンドで trap 動作が無効にされた場合は、本コマンド設定値は意味を持ちません。

[未設定時]

linkDown トラップが有効とみなされます。

```
ether <group> <port> snmp trap linkdown enable
```

4.9.2 ether snmp trap linkup

[機能]

ether ポートの linkUp トラップの設定

[適用機種]

Si-R G110

[入力形式]

ether <group> <port> snmp trap linkup <mode>

[オプション]

<group>

・ ether グループ番号
使用する ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

・ ether ポート番号
使用する ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ) で区切ります。
複数の番号が続く場合、"-" (ハイフン) で区切ります (例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

[注意]

snmp trap linkup コマンドで trap 動作が無効にされた場合は、本コマンド設定値は意味を持ちません。

[未設定時]

linkUp トラップが有効とみなされます。

```
ether <group> <port> snmp trap linkup enable
```

4.10 バックアップポート関連情報

4.10.1 backup mode

[機能]

バックアップポートの使用ポート選択方法の設定

[適用機種]

Si-R G110

[入力形式]

backup <backup_group> mode <mode>

[オプション]

<backup_group>

・ バックアップグループ番号
バックアップグループ番号を、10 進数で指定します。
バックアップグループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

master ポートと backup ポートの両方が使用可能な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]

バックアップグループごとに使用ポートの選択方法を設定します。

[未設定時]

バックアップの切り替えモードとして master ポートを優先的に使用するように設定されたものとみなされます。

```
backup <backup_group> mode master
```

4.10.2 backup standby

[機能]

バックアップポートの待機状態の設定

[適用機種]

Si-R G110

[入力形式]

backup <backup_group> standby <mode>

[オプション]

<backup_group>

・ バックアップグループ番号

バックアップグループ番号を、10 進数で指定します。

バックアップグループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

バックアップポートの待機状態を指定します。

online

待機状態であってもバックアップポートを閉塞しません。

offline

待機状態でバックアップポートを閉塞します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

バックアップポートの待機状態を設定します。

待機状態を offline と指定した場合に、待機状態のバックアップポートを閉塞します。

閉塞となったポートの状態は Ethernet ポート制御コマンドの offline を実行した状態と同じです。

また、稼動しているバックアップポートがダウンすると閉塞解除を実行します。

閉塞解除を実行したポートがほかの機能により閉塞されていたり、異常が発生していなければ切り替わります。

[注意]

・ バックアップポートの使用ポート選択方法が master と設定されている場合に、待機状態でバックアップポートを閉塞する設定としても、バックアップの優先ポートは閉塞しません。

バックアップの優先ポートを閉塞させたい場合は、バックアップポートの使用ポート選択方法を earlier に設定してください。

・ 待機状態でバックアップポートを閉塞する設定とした場合に、バックアップポート機能以外が閉塞したポートを自動で閉塞解除しません。offline コマンドで閉塞したポートである場合も同じです。

・ ポートバックアップ機能の待機ポート閉塞設定と起動時閉塞設定を併用した際、起動時閉塞が優先となります。そのため、バックアップポートの切り替えによる閉塞解除が不可となります。

この場合、online コマンドで閉塞解除すると、バックアップ機能による閉塞状態となり、自動的に切り替えが行えるようになります。

・ ポートバックアップ機能と自動復旧モード設定の手動復旧設定が併用された場合、ポートがダウンした際、自動復旧モードによる閉塞状態となり、バックアップポートの切り替えによる閉塞解除が不可となります。

[未設定時]

バックアップポートの待機状態として online が設定されたものとみなされます。

```
backup <backup_group> standby online
```

第 5 章　STP 情報の設定

・ STP インスタンス ID 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〈instance_id〉(STP インスタンス ID 番号)に指定する STP インスタンス ID の通し番号(10 進数)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-R G110

5.1 STP 情報

5.1.1 stp mode

[機能]

STP(Spanning Tree Protocol)動作モードの設定

[適用機種]

Si-R G110

[入力形式]

stp mode <mode>

[オプション]

<mode>

- disable
  STP を使用しない場合に指定します。
- stp
  STP(dot1d)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]

STP(Spanning Tree Protocol)動作モードを設定します。

[未設定時]

STP 動作モードに disable を設定したものとみなされます。

```
stp mode disable
```

5.1.2 stp age

[機能]

ブリッジ構成情報の最大有効時間の設定

[適用機種]

Si-R G110

[入力形式]

stp age <max_age>

[オプション]

<max_age>

・ 最大有効時間
ルートブリッジから送出される BPDU 情報の有効時間を、6～40 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]

ルートブリッジが送信する BPDU の有効時間を示します。
ルートブリッジから Max Age の時間内に BPDU フレームを受信しない場合、本装置は自身がルートブリッジとして BPDU を送信し始めます。

[注意]

<max_age> は、stp delay <delay_time>、stp hello <time> との間で以下の定義値関連チェックを行います。

・ forward delay time とのチェック
max age time <= 2 × (forward delay time - 1.0 seconds)

・ hello time とのチェック
max age time >= 2 × (hello time + 1.0 seconds)

上記チェック条件のどちらか 1 つでも満たさない場合は、無効な定義値となり、<max_age>、<delay_time>、<time> の設定が無効となります。
stp age コマンド、stp delay コマンド、stp hello コマンドの関連チェックで有効となる定義条件を以下に示します。

2 × (forward delay time - 1.0 seconds) >= max age time >= 2 × (hello time + 1.0 seconds)

[未設定時]

ルートブリッジが送信する BPDU の有効時間に、20 秒が設定されているものとみなされます。

```
stp age 20s
```

5.1.3 stp delay

[機能]

最大中継遅延時間の設定

[適用機種]

Si-R G110

[入力形式]

stp delay <delay_time>

[オプション]

<delay_time>

・ 最大中継遅延時間
最大中継遅延時間を、4～30 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]

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を指定します。

[注意]

<delay_time> は、stp age <max_age> との間で以下の定義値関連チェックを行います。

・ max age time とのチェック
max age time <= 2 × (forward delay time - 1.0 seconds)

上記チェック条件を満たさない場合は、無効な定義値となり、<max_age>、<delay_time>の設定が無効となります。
stp age コマンド、stp delay コマンド、stp hello コマンドの関連チェックで有効となる定義条件を以下に示します。

2 × (forward delay time - 1.0 seconds) >= max age time >= 2 × (hello time + 1.0 seconds)

[未設定時]

最大中継遅延時間に、15 秒が設定されているものとみなされます。

```
stp delay 15s
```

5.1.4 stp hello

[機能]

Helloメッセージ送信間隔の設定

[適用機種]

Si-R G110

[入力形式]

stp hello <time>

[オプション]

<time>

・ 送信間隔
ルートブリッジになったときに定期的に送信する構成情報BPDUの送信間隔を、1～10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]

本装置がルートブリッジとなったときに送信する構成情報BPDUの送信間隔を指定します。
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]

<time> は、stp age <max_age> との間で以下の定義値関連チェックを行います。

・ max age time とのチェック
max age time >= 2 × (hello time + 1.0 seconds)

上記チェック条件を満たさない場合は、無効な定義値となり、<max_age>、<time>の設定が無効となります。

stp ageコマンド、stp delayコマンド、stp helloコマンドの関連チェックで有効となる定義条件を以下に示します。

2 × (forward delay time - 1.0 seconds) >= max age time >= 2 × (hello time + 1.0 seconds)

[未設定時]

構成情報BPDU送信間隔に、2秒が設定されているものとみなされます。

```
stp hello 2s
```

5.1.5 stp domain priority

[機能]

ブリッジ優先度の設定

[適用機種]

Si-R G110

[入力形式]

stp domain <instance_id> priority <priority>

[オプション]

<instance_id>

・ STP インスタンス ID 番号
使用する STP インスタンス ID 番号を、10 進数で設定します。
STP インスタンス ID 番号の指定方法の詳細については、本章の冒頭を参照してください。

<priority>

・ 優先度
ブリッジネットワーク内での本装置の優先度に 4096 で割り切れる値(有効値)を、0～61440 の 10 進数で設定します。

有効値:

0, 4096, 8192, 12288, 16384, 20480, 24576, 28672,
32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440

有効値以外は設定できません。また、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]

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。
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。

[未設定時]

インスタンスの優先度に 32768 が設定されているものとみなされます。

```
stp domain <instance_id> priority 32768
```

第 6 章　VLAN 情報の設定

・ VLAN ID 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〈vid〉(VLAN VID)は、以下に示す範囲で指定してください。

範囲	機種
1～4094	Si-R G110

・ 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)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-R G110

6.1 VLAN 共通情報

6.1.1 vlan description

[機能]

VLAN の説明文の設定

[適用機種]

Si-R G110

[入力形式]

vlan <vid> description <description>

[オプション]

<vid>

・ VLAN ID
VLAN ID を、10 進数で指定します。

<description>

・ 説明文
この VLAN の説明文を、0x21,0x23～0x7e の 50 文字以内の ASCII 文字列で記入します。
(入力可能な文字の一覧については、コマンドユーザーズガイドを参照してください。)

[動作モード]

構成定義モード(管理者クラス)

[説明]

この VLAN についての説明文を記入します。

[未設定時]

説明文を記入しないものとみなされます。

6.1.2 vlan forward

[機能]

VLAN の転送設定

[適用機種]

Si-R G110

[入力形式]

vlan <vid> forward <count> <dst_addr> <kind> <group> <port>

[オプション]

<vid>

・ VLAN ID
VLAN ID を、10 進数で指定します。

<count>

・ 定義番号
0～399 の 10 進数で指定します。

<dst_addr>

・ 転送先 MAC アドレス
静的に学習テーブルに追加する MAC アドレスを指定します。
(XX:XX:XX:XX:XX:XX の形式で、XX は 2 桁の 16 進数です。)

<kind>

ポート種別を指定します。

・ ether
ether ポート

<group>

・ グループ番号
対象となるグループ番号を、10 進数で指定します。

<port>

・ ポート番号
対象となるポート番号を、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]

静的な転送ルールを設定します。

[注意]

・ <dst_addr>に、00:00:00:00:00:00 およびブロードキャスト、マルチキャストは指定できません。
・ <vid>で指定された VLAN が未登録の場合、設定は無効となります。
・ <port>で指定されたポートが<vid>で指定された VLAN に設定されていない場合、設定は無効になります。

[未設定時]

静的な転送ルールを設定しないものとみなされます。

6.2 ブリッジグループ関連情報

6.2.1 vlan bridgegroup use

[機能]

ブリッジグループ機能の設定

[適用機種]

Si-R G110

[入力形式]

vlan <vid> bridgegroup use <mode>

[オプション]

<vid>

・ VLAN ID
VLAN ID を、10 進数で指定します。

<mode>

ブリッジグループを使用するかどうかを指定します。

・ off
ブリッジグループを使用しない場合に指定します。

・ on
ブリッジグループ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]

ブリッジグループを使用するかどうかを設定します。
ブリッジグループを使用する場合、IP および IPv6 のパケット以外をすべてブリッジします。
IP および IPv6 の転送ポリシーは、ブリッジグループの設定に依存します。

[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グループを使用する場合は、ブリッジグループ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。

[未設定時]

ブリッジグループを使用しないものとみなされます。

```
vlan <vid> bridgegroup use off
```

6.2.2 vlan bridgegroup group

[機能]

ブリッジグループ識別子の設定

[適用機種]

Si-R G110

[入力形式]

vlan <vid> bridgegroup group <group_id>

[オプション]

<vid>

・ VLAN ID
VLAN ID を、10 進数で指定します。

<group_id>

・ グループ識別子
グループ識別子を、10 進数で指定します。

範囲	機種
0～19	Si-R G110

[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。

```
vlan <vid> bridgegroup group 0
```

6.2.3 vlan bridgegroup macfilter

[機能]

MAC フィルタの設定

[適用機種]

Si-R G110

[入力形式]

vlan <vid> bridgegroup macfilter <count> <action> acl <acl_count> [<direction>]

[オプション]

<vid>

・ VLAN ID
VLAN ID を、10 進数で指定します。

<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
0～255	Si-R G110

<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 進数で指定します。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。
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。

<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 MAC アドレスとあて先 MAC アドレス

[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。

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
3000	Si-R G110

[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グループを使用する場合は、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。
- 同一 VLAN に属する ether ポート間の通信では MAC フィルタは対象外のため、本設定でフィルタリングすることはできません。

[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。

6.2.4 vlan bridgegroup macfilter move

[機能]

MAC フィルタの優先順序の変更

[適用機種]

Si-R G110

[入力形式]

vlan <vid> bridgegroup macfilter move <count> <new_count>

[オプション]

<vid>

・ VLAN ID
VLAN ID を、10 進数で指定します。

<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-R G110

[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。

6.3 ARP 認証関連情報

6.3.1 vlan arpauth use

[機能]

ARP 認証機能の設定

[適用機種]

Si-R G110

[入力形式]

vlan <vid> arpauth use <mode>

[オプション]

<vid>

・ VLAN ID
VLAN ID を、1～4094 の 10 進数で指定します。

<mode>

・ off
ARP 認証機能を使用しません。
・ on
ARP 認証機能を使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ARP パケットに対して、MAC アドレスの認証を行うかどうかを設定します。

[未設定時]

ARP 認証を行わないものとみなされます。

```
vlan <vid> arpauth use off
```

6.3.2 vlan arpauth aaa

[機能]

ARP 認証機能で使用する AAA グループの設定

[適用機種]

Si-R G110

[入力形式]

vlan <vid> arpauth aaa <group_id>

[オプション]

<vid>

・ VLAN ID
VLAN ID を、1～4094 の 10 進数で指定します。

<group_id>

・ グループ ID
各グループを示す ID を 10 進数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]

ARP 認証機能で使用する 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。

6.3.3 vlan arpauth obstruction

[機能]

ARP 認証機能での通信妨害の設定

[適用機種]

Si-R G110

[入力形式]

vlan <vid> arpauth obstruction <mode> [<interval>]

[オプション]

<vid>

- VLAN ID
  VLAN ID を、1～4094 の 10 進数で指定します。

<mode>

- disable
  通信妨害を行いません。
- enable
  通信妨害を行います。

<interval>

- 通信妨害間隔
  通信妨害を行う場合、通信妨害を行う時間間隔を、0 秒または 10 秒～43200 秒の範囲で指定します。
  0 秒を指定した場合は、通信妨害は認証時のみに行い、定期的な通信妨害は行いません。
  単位は、s(秒)、m(分)、h(時)のいずれかを指定します。
  省略した場合は、0 秒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]

ARP 認証で MAC アドレスが登録されていなかった端末に対して、通信妨害を行うかどうかを設定します。

[未設定時]

通信妨害を行わないものとみなされます。

```
vlan <vid> arpauth obstruction disable
```

6.3.4 vlan arpauth dummymac

[機能]

ARP 認証機能の使用するダミー MAC アドレス

[適用機種]

Si-R G110

[入力形式]

vlan <vid> arpauth dummymac <mac>

[オプション]

<vid>

・ VLAN ID
VLAN ID を、1～4094 の 10 進数で指定します。

<mac>

・ MAC アドレス
通信妨害に使用するダミー 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 認証機能で通信妨害に使用する MAC アドレスを設定します。実際にネットワークには存在しない MAC アドレスを設定してください。

[注意]

<mac>に、00:00:00:00:00:00 およびブロードキャスト、マルチキャストは指定できません。

[未設定時]

デフォルトの MAC アドレス(02:ff:ff:ff:ff:ff)を使用するものとみなされます。

```
vlan <vid> arpauth dummymac 02:ff:ff:ff:ff:ff
```

6.3.5 vlan arpauth expire

[機能]

ARP 認証機能の認証結果保持時間の設定

[適用機種]

Si-R G110

[入力形式]

vlan <vid> arpauth expire <success_time> [<failure_time>]

[オプション]

<vid>

・ VLAN ID
VLAN ID を、1～4094 の 10 進数で指定します。

<success_time>

・ 認証成功保持時間
ARP 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)のいずれかを指定します。

<failure_time>

・ 認証失敗保持時間
ARP 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)のいずれかを指定します。
省略した場合は、認証成功保持時間と同じ時間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]

ARP 認証結果の保持時間を設定します。
保持時間を経過するまでの間は、再認証を実施しません。

[未設定時]

ARP 認証結果保持時間として認証成功保持時間、認証失敗保持時間ともに 20 分を指定したものとみなされます。

```
vlan <vid> arpauth expire 20m 20m
```

6.3.6 vlan arpauth overflow

[機能]

ARP 認証機能の端末数超過時の動作の設定

[適用機種]

Si-R G110

[入力形式]

vlan <vid> arpauth overflow <mode>

[オプション]

<vid>

- VLAN ID
  VLAN ID を、1～4094 の 10 進数で指定します。

<mode>

- failure
  認証が失敗したものとして動作します。
- success
  認証が成功し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]

ARP 認証結果を保持可能な端末数を超えた場合の動作を設定します。

[未設定時]

端末数超過時、認証が失敗したものとして動作します。

```
vlan <vid> arpauth overflow failure
```

6.3.7 vlan arpauth type

[機能]

ARP 認証の認証プロトコルの設定

[適用機種]

Si-R G110

[入力形式]

vlan <vid> arpauth type <authtype>

[オプション]

<vid>

- VLAN ID
  VLAN ID を、1～4094 の 10 進数で指定します。

<authtype>

- chap_md5
  認証プロトコルに MD5-CHAP を使用します。
- pap
  認証プロトコルに 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]

ARP 認証の認証プロトコルを設定します。

[未設定時]

ARP 認証の認証プロトコルとして MD5-CHAP が指定されたものとみなします。

```
vlan <vid> arpauth type chap_md5
```

6.3.8 vlan arpauth authenticated-ip

[機能]

ARP 認証の認証不要 IP アドレスの設定

[適用機種]

Si-R G110

[入力形式]

vlan <vid> arpauth authenticated-ip <count> <ip_address>

[オプション]

<vid>

・ VLAN ID
VLAN ID を、1～4094 の 10 進数で指定します。

<count>

・ 定義番号
認証不要 IP アドレスの定義番号を 10 進数で指定します。

範囲	機種
0～249	Si-R G110

<ip_address>

・ 認証不要 IP アドレス
認証不要 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]

ARP 認証の認証不要 IP アドレスを設定します。

[未設定時]

ARP 認証の認証不要 IP アドレスはないものとみなします。

第 7 章　MAC 情報の設定

7.1 MAC 情報

7.1.1 mac age

[機能]

MAC アドレス学習テーブルのエージングアウト時間の設定

[適用機種]

Si-R G110

[入力形式]

mac age <time>

[オプション]

<time>

・ エージングアウト時間
MAC アドレス学習テーブルのエージングアウト時間を、10～1,000,000 秒の範囲の秒単位で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

MAC アドレス学習テーブルのエージングアウト時間を設定します。

[未設定時]

エージングアウト時間に 300 秒が設定されたものとみなされます。

```
mac age 300
```

第 8 章　pseudo ether 情報の設定

・ pseudo ether 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>(pseudo ether 定義番号)に指定する pseudo ether 定義の通し番号(10 進数)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	Si-R G110

・ USB 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 usb <line>(USB 番号)に指定する挿入されている USB の番号(10 進数)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
指定不可	Si-R G110

8.1 pseudo ether インタフェース共通情報

8.1.1 pseudo-ether description

[機能]

pseudo ether インタフェースの説明文の設定

[適用機種]

Si-R G110

[入力形式]

pseudo-ether <number> description <description>

[オプション]

<number>

・ pseudo ether 定義番号

pseudo ether 定義の通し番号を、10 進数で指定します。

pseudo ether 定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<description>

・ 説明文

この pseudo ether インタフェースの説明文を、0x21,0x23～0x7e の 50 文字以内の ASCII 文字列で記入します。

(入力可能な文字の一覧については、コマンドユーザーズガイドを参照してください。)

[動作モード]

構成定義モード(管理者クラス)

[説明]

この pseudo ether インタフェースについての説明文を記入します。

[未設定時]

説明文を記入しないものとみなされます。

8.1.2 pseudo-ether use

[機能]

pseudo ether インタフェースの使用の設定

[適用機種]

Si-R G110

[入力形式]

pseudo-ether <number> use <mode>

[オプション]

<number>

- pseudo ether 定義番号
  pseudo ether 定義の通し番号を、10 進数で指定します。
  pseudo ether 定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

使用モードを指定します。

- off
  pseudo ether インタフェースを使用しません。
- on
  pseudo ether インタフェースを使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

pseudo ether インタフェースの使用の設定を行います。

[注意]

本設定を変更した場合は、装置の再起動が必要です。

[未設定時]

pseudo ether インタフェースを使用しないものとみなされます。

```
pseudo-ether <number> use off
```

8.1.3 pseudo-ether bind

[機能]

利用するUSBポートの設定

[適用機種]

Si-R G110

[入力形式]

pseudo-ether <number> bind usb <line>

[オプション]

<number>

・ pseudo ether 定義番号
pseudo ether 定義の通し番号を、10進数で指定します。
pseudo ether 定義番号の指定方法の詳細については、本章の冒頭を参照してください。

usb <line>

利用するUSBポートを指定します。

・ USB番号
挿入されているUSBの番号を、10進数で指定します。
USB番号の指定方法の詳細については、本章の冒頭を参照してください。

[動作モード]

構成定義モード(管理者クラス)

[説明]

pseudo ether 定義で利用するUSBポートを設定します。

wan 定義と pseudo-ether 定義で同一の bind 先を指定した場合、データ通信モジュールの種別に従った定義が有効になります。

双方の定義を利用できるデータ通信モジュールの場合、pseudo-ether 定義が優先されます。

[未設定時]

USBポートを指定しないものとみなされます。

8.1.4 pseudo-ether startup-delay

[機能]

pseudo ether インタフェースのリンクアップ遅延時間の設定

[適用機種]

Si-R G110

[入力形式]

pseudo-ether <number> startup-delay <delay>

[オプション]

<number>

・ pseudo ether 定義番号
pseudo ether 定義の通し番号を、10 進数で指定します。
pseudo ether 定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<delay>

・ リンクアップ遅延時間
リンクアップ遅延時間を、0s～2m 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]

装置の起動時、リセット時に<delay>秒間、リンクアップを遅延させます。

[未設定時]

0 秒が設定されているとみなされます。

8.2 VLAN 関連情報

8.2.1 pseudo-ether vlan untag

[機能]

pseudo ether の Tag なし VLAN 登録

[適用機種]

Si-R G110

[入力形式]

pseudo-ether <number> vlan untag <vid>

[オプション]

<number>

・ pseudo ether 定義番号
pseudo ether 定義の通し番号を、10 進数で指定します。
pseudo ether 定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<vid>

・ Tag なし VLAN ID
Tag なし VLAN ID を、1～4094 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]

Untagged VLAN ID の設定を行います。

[注意]

・ 本設定を変更した場合は、装置の再起動が必要です。
・ ether グループ 1 と ether グループ 2 と pseudo-ether では、同じ VLAN ID を指定することはできません。
ether グループ 1 と ether グループ 2 と pseudo-ether では、異なる VLAN ID を指定してください。
ether グループ 1 と ether グループ 2 で同じ VLAN ID を指定した場合、ether グループ 1 の指定が有効になります。
ether と pseudo-ether で同じ VLAN ID を指定した場合、ether の指定が有効になります。
・ resource system vlan で設定されている VLAN ID を指定した場合、この指定は無効になります。

[未設定時]

Tag なし VLAN ID として 1 が設定されたとみなされます。

```
pseudo-ether <number> vlan untag 1
```

8.3 SNMP 関連情報

8.3.1 pseudo-ether snmp trap linkdown

[機能]

pseudo ether インタフェースの linkDown トラップの設定

[適用機種]

Si-R G110

[入力形式]

pseudo-ether <number> snmp trap linkdown <mode>

[オプション]

<number>

・ pseudo ether 定義番号
pseudo ether 定義の通し番号を、10 進数で指定します。
pseudo ether 定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

[注意]

snmp trap linkdown コマンドで trap 動作が無効にされた場合は、本コマンド設定値は意味を持ちません。

[未設定時]

linkDown トラップが有効とみなされます。

```
pseudo-ether <number> snmp trap linkdown enable
```

8.3.2 pseudo-ether snmp trap linkup

[機能]

pseudo ether インタフェースの linkUp トラップの設定

[適用機種]

Si-R G110

[入力形式]

pseudo-ether <number> snmp trap linkup <mode>

[オプション]

<number>

- pseudo ether 定義番号
  pseudo ether 定義の通し番号を、10 進数で指定します。
  pseudo ether 定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

[注意]

snmp trap linkup コマンドで trap 動作が無効にされた場合は、本コマンド設定値は意味を持ちません。

[未設定時]

linkUp トラップが有効とみなされます。

```
pseudo-ether <number> snmp trap linkup enable
```

第 9 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)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-R G110

9.1　lan 共通情報

9.1.1　lan description

[機能]

lan ポートの説明文の設定

[適用機種]

Si-R G110

[入力形式]

lan <number> description <description>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<description>

・ 説明文
この lan インタフェースの説明文を、0x21,0x23～0x7e の 50 文字以内の ASCII 文字列で記入します。
(入力可能な文字の一覧については、コマンドユーザーズガイドを参照してください。)

[動作モード]

構成定義モード(管理者クラス)

[説明]

この lan インタフェースについての説明文を記入します。

[未設定時]

説明文を記入しないものとみなされます。

9.1.2 lan mtu

[機能]

送信パケット最大長(MTU 値)の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mtu>

・ MTU 値
MTU 値を、200～1500 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]

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
```

9.1.3 lan shaping

[機能]

シェーピング機能の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

・ off
シェーピングを使用しません。

・ on
シェーピングを使用します。

<rate>

・ 最大送出レート
最大送出レートを、10 進数と単位文字で指定します。
10 進数の末尾に 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-R G110

[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する場合、括り付く VLAN は単一ポートで構成するようにしてください。
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
```

9.1.4 lan shaping-opt tc

[機能]

シェーピング機能の単位時間の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] shaping-opt tc <tc>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<tc>

・ 単位時間
単位時間の値(単位はミリ秒)を、1～100 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]

シェーピング機能の単位時間を設定します。

[未設定時]

単位時間の値として、10 ミリ秒を設定したものとみなされます。

```
lan <number> shaping-opt tc 10
```

9.2 IP 関連情報

9.2.1 lan ip address

[機能]

IP アドレスの設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

9.2.2 lan ip alias

[機能]

セカンダリ IP アドレスの設定

[適用機種]

Si-R G110

[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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

9.2.3 lan ip dhcp service

[機能]

DHCP 機能の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

DHCP 機能のモードを指定します。

・ off
IPv4 DHCP 機能を使用しません。
・ client
IPv4 DHCP クライアント機能を使用します。
・ relay
IPv4 DHCP リレーエージェント機能を使用します。
・ server
IPv4 DHCP サーバ機能を使用します。

<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
```

9.2.4 lan ip dhcp info

[機能]

DHCP 配布情報の設定

[適用機種]

Si-R G110

[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>
lan [<number>] ip dhcp info wins server <winsserver1> [<winsserver2>]
lan [<number>] ip dhcp info sipserver <type> <sipserver1> [<sipserver2>]
```

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、割り当て先頭 IP アドレスと割り当てアドレス数によって規定される動的割り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)のいずれかを指定します。

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

<winsserver1>

・ WINS サーバ IP アドレス

DHCP クライアントに配布する、WINS 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

<winsserver2>

・ セカンダリ WINS 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 WINS 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

<type>

SIP サーバの記述形式

・ domain

ドメイン名指定

DHCP クライアントに配布する SIP サーバ情報としてドメイン名を配布する場合に指定します。

・ address

IPv4 アドレス指定

DHCP クライアントに配布する SIP サーバ情報として IP アドレスを配布する場合に指定します。

<sipserver1>

・ プライマリ SIP ドメイン名

<type>オプションに domain を指定した場合に設定します。

DHCP クライアントに配布する SIP ドメイン名は、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。

・ プライマリ SIP サーバ IP アドレス

<type>オプションに address を指定した場合に設定します。

DHCP クライアントに配布する、SIP 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

<sipserver2>

・ セカンダリ SIP ドメイン名

<type>オプションに domain を指定した場合に設定します。

DHCP クライアントに配布する SIP ドメイン名は、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。

・ セカンダリ SIP サーバ IP アドレス

<type>オプションに address を指定した場合に設定します。

DHCP クライアントに配布する、セカンダリ SIP 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]

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。

[注意]

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)は 60 秒単位で繰り上げられます。

たとえば、割り当て時間を 61 秒に設定したときには、実際の割り当て時間は 120 秒になります。

［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。

9.2.5 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 G110

[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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

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
```

9.2.6 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 G110

[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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

9.2.7 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<group_id>

・ グループ ID
各グループを示す ID を、10 進数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。

9.2.8 lan ip dhcp macauth type

[機能]

DHCP MAC アドレスチェック機能の認証プロトコルの設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ip dhcp macauth type <authtype>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<authtype>

- chap_md5
  認証プロトコルに MD5-CHAP を使用します。
- pap
  認証プロトコルに 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]

DHCP MAC アドレスチェック機能の認証プロトコルを設定します。

[未設定時]

DHCP MAC アドレスチェック機能の認証プロトコルとして MD5-CHAP が指定されたものとみなされます。

```
lan <number> ip dhcp macauth type chap_md5
```

9.2.9 lan ip proxyarp

[機能]

ProxyARP 機能の設定

[適用機種]

Si-R G110

[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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

9.2.10 lan ip localproxyarp

[機能]

ローカル ProxyARP 機能の設定

[適用機種]

Si-R G110

[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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

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

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
```

9.2.11 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。

範囲	機種
0～255	Si-R G110

<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、1～14 の 10 進数で指定します。
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、1～254 の 10 進数で指定します。
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、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。

<distance>で指定した優先度は、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。

また、IPv4 スタティック経路を以下のように使用できます。

- 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できます。

  RIP テーブルには、設定した RIP メトリック値+1 のメトリック値で登録されます。
- 複数のスタティック経路情報で ECMP 機能を使用できます。このとき、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 サーバの Router オプションで IPv4 スタティック経路を設定できます。

  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 1 のデフォルトルートが自動生成されます。

  ここで、優先度 1 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 1 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
256	Si-R G110

[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 1 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されます。

9.2.12 lan ip rip use

[機能]

RIP 基本情報の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<send>

RIP の送信について指定します。

・ off
RIP を送信しません。
・ 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。

<receive>

RIP の受信について指定します。

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

<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、0～14 の 10 進数で指定します。

<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。

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

<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。

たとえば、RIP テーブルのメトリック値が 3 の場合、<metric>に 0 を指定するとメトリックは 3 で広報され、1 を指定すると、4 で広報されます。

なお、受信側の装置では、通常、受信したメトリックに 1 を加算した値で RIP テーブルに登録します。

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
120	Si-R G110

[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 と併用できません。

[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
```

9.2.13 lan ip rip filter act

[機能]

RIP フィルタ動作の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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-R G110

<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
400	Si-R G110

［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で、遮断条件だけを設定した場合、すべての経路情報は遮断されます。
送受信する経路情報が存在する場合、透過条件に対象の経路情報を設定してください。

［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。

9.2.14 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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-R G110

[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。

9.2.15 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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-R G110

<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
<address>/<mask>で指定した経路情報を本装置が保有する経路情報と比較し、完全一致したものをフィルタリング対象とします。

・ inexact
指定した<address>の先頭から<mask>ビット部分だけを本装置が保有する経路情報と比較し、一致したものを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。

・<prefix_match>は以下のように動作します。

<address>/<mask>で"192.168.0.0/16"を指定し、本装置が以下の経路情報を保有している場合、exact を指定すると、"192.168.0.0/16"がフィルタリング対象となります。

inexact を指定すると、"192.168.0.0"と一致する"192.168.0.0/16、192.168.1.0/24、192.168.1.1/32"の 3 つがフィルタリング対象となります。

172.16.0.0/16
192.168.0.0/16
192.168.1.0/24
192.168.1.1/32

[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。

9.2.16 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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-R G110

<metric>

・ メトリック値
メトリック値を、0～15 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]

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 1～15 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。

9.2.17 lan ip ospf use

[機能]

OSPF 利用可否の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～2	Si-R G110

[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-R G110

[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
```

9.2.18 lan ip ospf cost

[機能]

OSPF 出力コストの設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 1 が設定されているものとみなされます。

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

9.2.19 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 G110

[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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<hello_interval>

・ Helloパケット送信間隔
Helloパケットの送信間隔時間を、1～65535秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
各単位での指定可能範囲は、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、隣接関係が構築できません。

[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
```

9.2.20 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、1～65535 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
各単位での指定可能範囲は、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
```

9.2.21 lan ip ospf retrans

[機能]

OSPF パケット再送間隔の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<retransmit_interval>

・ パケット再送間隔
パケットの再送間隔を、3～65535 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
各単位での指定可能範囲は、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
```

9.2.22 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、1～65535 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
各単位での指定可能範囲は、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
```

9.2.23 lan ip ospf priority

[機能]

OSPF 指定ルータ優先度の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

9.2.24 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

9.2.25 lan ip ospf auth textkey

[機能]

OSPF テキスト認証鍵の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

9.2.26 lan ip ospf auth md5key

[機能]

OSPF MD5 認証鍵情報の設定

[適用機種]

Si-R G110

[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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

9.2.27 lan ip ospf passive

[機能]

OSPF パケット送信抑止の設定

[適用機種]

Si-R G110

[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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<interface_type>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

OSPF 経路計算の対象に含めながら、OSPF パケットを送信しないインタフェースを設定します。

[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
```

9.2.28 lan ip nat mode

[機能]

アドレス変換の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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>

・ 割り当て時間
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)のいずれかを指定します。
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
```

9.2.29 lan ip nat static

[機能]

静的アドレス変換の設定

[適用機種]

Si-R G110

[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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。

範囲	機種
0～199	Si-R G110

<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
200	Si-R G110

[未設定時]

静的アドレス変換は設定されません。

9.2.30 lan ip nat static default

[機能]

静的アドレス変換に一致しないパケットの扱いの設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<action>

すべての静的アドレス変換に一致しなかったパケットをどう扱うかを指定します。

・ reject
該当するパケットを破棄します。

・ 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。

[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
```

9.2.31 lan ip nat rule

[機能]

アドレス変換ルールの設定

[適用機種]

Si-R G110

[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>
```

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 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。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

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

ftp, irc, dns, sip, mldt, ipbs

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。

9.2.32 lan ip nat wellknown

[機能]

ポート番号変換の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

ポート番号変換定義番号を、0～99 の 10 進数で指定します。

範囲	機種
0～99	Si-R G110

<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)
```

9.2.33 lan ip nat destination

[機能]

あて先変換の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～199	Si-R G110

<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
200	Si-R G110

[注意]

本設定によりパケットのあて先は変換されますが、データ内に含まれる IP アドレスは変換されません。
たとえば、ftp 接続パケットのあて先は変換されますが、ftp データ内の ftp データセッション用 IP アドレスは変換されないため、ftp データセッションが接続できない場合があります。
そのような通信がある場合は、以下に示す静的アドレス変換も設定してください。

```
lan <number> ip nat static <count> 0.0.0.1 any 0.0.0.1-255.255.255.254 any any
```

[未設定時]

あて先変換は設定されません。

9.2.34 lan ip nat appli

[機能]

アプリ対応の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。
・ 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。

<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]

アプリ対応を以下のように指定したものとみなされます。

```
lan [<number>] ip nat appli ftp on
lan [<number>] ip nat appli sip on
lan [<number>] ip nat appli dns on
lan [<number>] ip nat appli snmp on
```

9.2.35 lan ip filter

[機能]

IP フィルタの設定

[適用機種]

Si-R G110

[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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～199	Si-R G110

<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
0～999	Si-R G110

<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
200	Si-R G110

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
3000	Si-R G110

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。

・ <dst_addr>/<mask>に″dynamic″を指定した ACL は使用しないでください。

[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。

9.2.36 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～199	Si-R G110

[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。

9.2.37 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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>

・ 割り当て時間
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)のいずれかを指定します。
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
```

9.2.38 lan ip tos

[機能]

TOS 値書き換え条件の設定

[適用機種]

Si-R G110

[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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～99	Si-R G110

<acl_count>

・ ACL 定義番号

使用する ACL 定義の番号を、10 進数で指定します。

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
0～999	Si-R G110

<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
100	Si-R G110

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
3000	Si-R G110

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]

<dst_addr>/<mask>に"dynamic"を指定した ACL は使用しないでください。

[未設定時]

TOS 値書き換えを行わないものとみなされます。

9.2.39 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～99	Si-R G110

[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。

9.2.40 lan ip priority

[機能]

帯域制御の設定

[適用機種]

Si-R G110

[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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

・ 帯域制御定義番号

帯域制御定義番号を、10 進数で指定します。

範囲	機種
0～99	Si-R G110

<acl_count>

・ ACL 定義番号

使用する ACL 定義の番号を、10 進数で指定します。

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
0～999	Si-R G110

<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～1000000kbps または 1mbps～1000mbps 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。
<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。
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
100	Si-R G110

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
3000	Si-R G110

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。
・ <dst_addr>/<mask>に"dynamic"を指定した ACL は使用しないでください。

[未設定時]

帯域制御を行わないものとみなされます。

9.2.41 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<in-policy_number>

・ Ingress ポリシールーティング定義番号
このインタフェースでの Ingress ポリシールーティング定義の通し番号を、10 進数で指定します。
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
200	Si-R G110

<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
0～99	Si-R G110

[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。

9.2.42 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

9.2.43 lan ip msschange

[機能]

MSS 書き換えの設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ip msschange <mss>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mss>

・ MSS 値
MSS の書き換え値を、0 または 160～1460 の 10 進数で指定します。
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。

```
lan <number> ip msschange 0
```

9.2.44 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

9.2.45 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

9.2.46 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

9.2.47 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 G110

[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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

9.2.48 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 G110

[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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

9.2.49 lan ip arp cycle

[機能]

ARP 定期送信機能の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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]

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。

9.2.50 lan ip arp static

[機能]

スタティック ARP の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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～ 99	Si-R G110

<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)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。

9.2.51 lan ip ids use

[機能]

IDS の設定

[適用機種]

Si-R G110

[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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

9.3 IPv6 関連情報

9.3.1 lan ipv6 use

[機能]

IPv6 機能の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 use <mode>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

IPv6 パケットの送受信を行うかどうか指定します。

・ 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。

・ 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。

[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> ipv6 use off
```

9.3.2 lan ipv6 ifid

[機能]

IPv6 インタフェース ID の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 ifid <interfaceID>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 上で他装置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> ipv6 ifid auto
```

9.3.3 lan ipv6 address

[機能]

IPv6 アドレスの設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 address [<count>] <address>/<prefixlen>
lan [<number>] ipv6 address [<count>] <anycast_address>/<prefixlen>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
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。
プレフィックス長には 64 を指定してください。
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、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～rmt99	Si-R G110

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

dhcp@rmt0::/64
または、
dhcp@rmt0::1:2:3:4/64

・ auto
RA(Router Advertisement) メッセージで受信したプレフィックスを使用して自動的にアドレスを設定する場合に指定します。
lan ipv6 ra mode recv を設定する必要があります。

<anycast_address>/<prefixlen>

・ IPv6 エニキャストアドレス/プレフィックス長
エニキャストアドレスを指定します。プレフィックス長には 128 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]

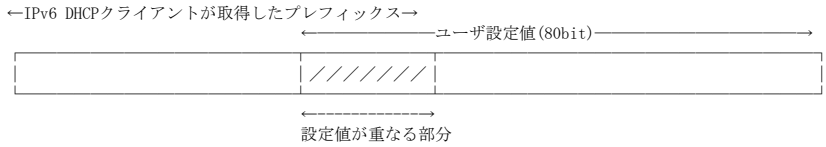
このインタフェースの IPv6 アドレスを設定します。

<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。

<anycast_address>の指定では、インタフェース ID によるアドレス生成は行われません。

[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。



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

エニキャストアドレスは、ほかのアドレスと重複設定できません。

[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。

9.3.4 lan ipv6 ra mode

[機能]

RA(Router Advertisement)メッセージの動作設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 ra mode <mode>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

・ off
RA メッセージの送受信機能を無効にします。
・ recv
RA メッセージの受信機能を有効にします。
・ send
RA メッセージの送信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]

RA メッセージの送受信機能を設定します。設定機能は以下のとおりです。

・ RA メッセージ受信機能
有効な場合、RA メッセージをもとに ND(Neighbor Discovery)のパラメタ、デフォルトルート、およびグローバルアドレスを自装置に自動設定することができます。
グローバルアドレスの自動設定を行う場合は、"lan ipv6 address auto"を設定します。
・ RA メッセージ送信機能
有効な場合、自装置に定義したプレフィックス情報などを広報することができます。

[未設定時]

RA メッセージの送受信機能が無効とみなされます。

```
lan <number> ipv6 ra mode off
```

9.3.5 lan ipv6 ra interval

[機能]

RA(Router Advertisement)メッセージ送信間隔の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<max>

・ 最大送信間隔
RA メッセージを定期送信する場合の最大送信間隔(秒)を、4～1800 の 10 進数で指定します。

<min>

・ 最小送信間隔
RA メッセージを定期送信する場合の最小送信間隔(秒)を、3～<max>×3/4 の 10 進数で指定します。

<lifetime>

・ Router Lifetime の値
送信する RA メッセージの Router Lifetime の値を、0 または<max>～9000 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]

RA の送信間隔、および RA の Router Lifetime 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> ipv6 ra interval 600 200 1800
```

9.3.6 lan ipv6 ra mtu

[機能]

RA(Router Advertisement)メッセージに含める MTU option の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 ra mtu <mtu>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mtu>

・ MTU option の内容
RA に含める MTU option の値を、0 または 1280～1500 の 10 進数で指定します。
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 メッセージに含める MTU option の値を設定します。

[未設定時]

送信する RA メッセージに MTU option を含めないものとみなされます。

```
lan <number> ipv6 ra mtu 0
```

9.3.7 lan ipv6 ra reachabletime

[機能]

RA(Router Advertisement)メッセージに含める Reachable Time の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 ra reachabletime <reachabletime>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<reachabletime>

・ Reachable Time の値
RA メッセージに含める Reachable Time の値(ミリ秒)を、0～3600000 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]

RA メッセージに含める Reachable Time の値(ミリ秒)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> ipv6 ra reachabletime 0
```

9.3.8 lan ipv6 ra retranstimer

[機能]

RA(Router Advertisement)メッセージに含める Retrans Timer の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 ra retranstimer <retranstimer>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<retranstimer>

・ Retrans Timer の値 RA メッセージに含める Retrans Timer の値(ミリ秒)を、0～4294967295 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]

RA メッセージに含める Retrans Timer の値(ミリ秒)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> ipv6 ra retranstimer 0
```

9.3.9 lan ipv6 ra curhoplimit

[機能]

RA(Router Advertisement)メッセージに含める Cur Hop Limit の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 ra curhoplimit <curhoplimit>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<curhoplimit>

・ Cur Hop Limit の値
RA メッセージに含める Cur Hop Limit の値を、0～255 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]

RA メッセージに含める 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> ipv6 ra curhoplimit 64
```

9.3.10 lan ipv6 ra flags

[機能]

RA(Router Advertisement)メッセージに含める flags field の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 ra flags <flags>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<flags>

・ flags field の値
RA メッセージに含める flags field の値を、00～ff の 16 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]

RA メッセージに含める 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> ipv6 ra flags 00
```

9.3.11 lan ipv6 ra prefix

[機能]

RA(Router Advertisement)メッセージに含める広報プレフィックス情報の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 ra prefix [<count>] <prefix>/<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

・ 広報プレフィックス定義番号
広報プレフィックスの定義番号を、0～3 の 10 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。

<prefix>/<prefixlen>

・ 広報プレフィックス/プレフィックス長
広報プレフィックスとプレフィックス長を指定します。
リンクローカルスコープのプレフィックスは指定できません。
プレフィックス長には 64 を指定してください。
IPv6 DHCP クライアントが取得したプレフィックスを指定する場合は上位を"dhcp@インタフェース名"の形式で指定し、下位 80 ビット分を IPv6 アドレス形式で指定します。インタフェース名には、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～rmt99	Si-R G110

例)

rmt0 の 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：

dhcp@rmt0::/64
または、
dhcp@rmt0::1:2:3:4/64

<valid>

・ valid lifetime の時間
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)のいずれかを指定します。

・ infinity
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。

<prefix>/<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。

<preferred>

・ preferred lifetime の時間
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)のいずれかを指定します。

・ infinity

このプレフィックスに対する preferred lifetime を無限とする場合に指定します。

<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。

<prefix>/<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。

<flags>

・ RA Prefix Information に付与されるフラグ

この prefix に対する flags フィールドの値を、0～ff の 16 進数で指定します。

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]

RA メッセージに含める広報プレフィックス情報を設定します。

lan ipv6 address で定義したアドレスプレフィックスから、広報したいプレフィックスと同じ情報を指定してください。アドレスプレフィックスに一致しないものは広報されません。

[注意]

VRRP 機能と RA 送信機能を併用する場合、マスタルータおよびバックアップルータに広報プレフィックス情報の設定を行う必要があります。RA 送信機能は、マスタルータのときだけ RA メッセージを送信します。

[未設定時]

送信する RA メッセージに広報プレフィックス情報を含めないものとみなされます。

9.3.12 lan ipv6 ra trigger ifdown

[機能]

RA(Router Advertisement)メッセージにおけるインタフェースダウントリガの設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 ra trigger ifdown [<count>] <interface>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

・ トリガ定義番号
インタフェースダウントリガの定義番号を、0～3 の 10 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。

<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～rmt99	Si-R G110

[動作モード]

構成定義モード(管理者クラス)

[説明]

デフォルトルータ広報に関するインタフェースダウントリガを設定します。

<interface>で指定したすべてのインタフェースがダウンした場合、Router Lifetime に 0 を設定した RA(Router Advertisement)メッセージを広報します。

<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。

<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場合に、ダウンしたとみなします。

[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。

9.3.13 lan ipv6 ra recv valid-lifetime

[機能]

RA(Router Advertisement)受信における valid-lifetime のモード設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 ra recv valid-lifetime <mode>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

valid-lifetime タイマのモードを指定します。

・ defense
防御モードで使用します。
・ normal
通常モードで使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RA を受信する装置は、不当に小さい lifetime 値を含んだ RA メッセージによるサービス否認攻撃を受ける可能性があります。本コマンドでは、このようなサービス否認攻撃に対し、防御モードで動作させるか、通常モードで動作させるかを設定します。

防御モード

valid-lifetime タイマの残り時間と、RA メッセージで受信した valid-lifetime 値をチェックし、攻撃の可能性がある場合は、安全に動作するように以下の処理を実施します。

・ タイマの残り時間が 2 時間を超過している状態で、受信した valid-lifetime 値が、タイマの残り時間以下で、かつ、0 秒から 2 時間以内の場合は、タイマを"2 時間"に再設定します。
・ タイマの残り時間が 2 時間を超過している状態で、受信した valid-lifetime 値が、タイマの残り時間以下で、かつ、2 時間を超過している場合は、タイマを valid-lifetime 値に再設定します。
・ タイマの残り時間が 2 時間以内の状態で、受信した valid-lifetime 値が、タイマの残り時間以下の場合は、タイマを再設定しません。
・ 受信した valid-lifetime 値が、タイマの残り時間を超過している場合は、タイマを valid-lifetime 値に再設定します。

通常モード

valid-lifetime タイマを、RA メッセージで受信した valid-lifetime 値に再設定します。

[注意]

RA の送信元の安全性が確認できない場合は、防御モードを使用してください。

[未設定時]

防御モードを使用するものとみなされます。

```
lan <number> ipv6 ra recv valid-lifetime defense
```

9.3.14 lan ipv6 route

[機能]

IPv6 スタティック経路情報の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。

範囲	機種
0～255	Si-R G110

<address>/<prefixlen>

・ IPv6 アドレス/プレフィックス長
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。
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、1～14 の 10 進数で指定します。
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、1～254 の 10 進数で指定します。
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、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]

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。

<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。

<distance>で指定した優先度は、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。

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 ipv6 distance コマンドを参照してください。

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
256	Si-R G110

[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]

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。

9.3.15 lan ipv6 rip use

[機能]

IPv6 RIP 基本情報の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<send>

RIP(IPv6)パケットを送信するかどうか指定します。

・ off
RIP(IPv6)パケットを送信しません。

・ on
RIP(IPv6)パケットを送信します。

<receive>

RIP(IPv6)パケットを受信するかどうか指定します。

・ off
RIP(IPv6)パケットを受信しません。

・ on
RIP(IPv6)パケットを受信します。

<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、0～14 の 10 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。

[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 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。
たとえば、RIP テーブルのメトリック値が 3 の場合、<metric>に 0 を指定するとメトリックは 3 で広報され、1 を指定すると、4 で広報されます。
なお、受信側の装置では、通常、受信したメトリックに 1 を加算した値で RIP テーブルに登録します。
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
120	Si-R G110

[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> ipv6 rip use off off 0
```

9.3.16 lan ipv6 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 G110

[入力形式]

lan [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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> ipv6 rip site-local on
```

9.3.17 lan ipv6 rip aggregate

[機能]

IPv6 RIP の集約経路の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 ipv6 rip use および lan ipv6 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。

9.3.18 lan ipv6 rip filter act

[機能]

IPv6 RIP フィルタ動作の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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-R G110

<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 ipv6 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-R G110

［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で、遮断条件だけを設定した場合、すべての経路情報は遮断されます。
送受信する経路情報が存在する場合、透過条件に対象の経路情報を設定してください。

［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。

9.3.19 lan ipv6 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 G110

[入力形式]

lan [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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-R G110

[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。

9.3.20 lan ipv6 rip filter route

[機能]

IPv6 RIP フィルタの経路情報設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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-R G110

<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
<address>/<prefixlen>で指定した経路情報を本装置が保有する経路情報と比較し、完全一致したものをフィルタリング対象とします。
・ inexact
指定した<address>の先頭から<prefixlen>ビット部分だけを本装置が保有する経路情報と比較し、一致したものを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。
・ <prefix_match>は以下のように動作します。
<address>/<prefixlen>で"2001:db8::/32"を指定し、本装置が以下の経路情報を保有している場合、exact を指定すると、"2001:db8::/32"がフィルタリング対象となります。

inexact を指定すると、"2001:db8::"と一致する"2001:db8::/32、2001:db8:ffff::/48、2001:db8:ffff:1000::/64"の 3 つがフィルタリング対象となります。

1000:db8::/32

2001:db8::/32

2001:db8:ffff::/48

2001:db8:ffff:1000::/64

[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。

9.3.21 lan ipv6 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 G110

[入力形式]

lan [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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-R G110

<metric>

・ メトリック値
メトリック値を、0～15 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]

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 1～15 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 ipv6 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。

9.3.22 lan ipv6 ospf use

[機能]

IPv6 OSPF 利用可否の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

OSPF を利用するかどうかを指定します。

・ 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
0～2	Si-R G110

[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
15	Si-R G110

[注意]

OSPF の利用は、"ospf ipv6 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> ipv6 ospf use off
```

9.3.23 lan ipv6 ospf cost

[機能]

IPv6 OSPF 出力コストの設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 ospf cost <cost>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 1 が設定されているものとみなされます。

```
lan <number> ipv6 ospf cost 1
```

9.3.24 lan ipv6 ospf hello

[機能]

IPv6 OSPF Helloパケット送信間隔の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<hello_interval>

・ Helloパケット送信間隔
Helloパケットの送信間隔時間を、1～65535秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
各単位での指定可能範囲は、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、隣接関係が構築できません。

[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> ipv6 ospf hello 10s
```

9.3.25 lan ipv6 ospf dead

[機能]

IPv6 OSPF 隣接ルータ停止確認間隔の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、1～65535 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
各単位での指定可能範囲は、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、隣接関係が構築できません。
隣接ルータ停止確認間隔の設定値は、装置起動時での指定ルータ/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> ipv6 ospf dead 40s
```

9.3.26 lan ipv6 ospf retrans

[機能]

IPv6 OSPF パケット再送間隔の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<retransmit_interval>

・ パケット再送間隔
パケットの再送間隔を、3～65535 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
各単位での指定可能範囲は、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(LSupdate、LSrequest、DD)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> ipv6 ospf retrans 5s
```

9.3.27 lan ipv6 ospf delay

[機能]

IPv6 OSPF LSU パケット送信遅延時間の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、1～65535 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
各単位での指定可能範囲は、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]

OSPF 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> ipv6 ospf delay 1s
```

9.3.28 lan ipv6 ospf priority

[機能]

IPv6 OSPF 指定ルータ優先度の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 ospf priority <priority>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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> ipv6 ospf priority 1
```

9.3.29 lan ipv6 ospf passive

[機能]

IPv6 OSPF パケット送信抑止の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<interface_type>

OSPF パケットの送信を抑止するかどうかを指定します。

・ off
パケットの送信を抑止しません。

・ on
パケットの送信を抑止します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

OSPF 経路計算の対象に含めながら、OSPF パケットを送信しないインタフェースを設定します。

[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> ipv6 ospf passive off
```

9.3.30 lan ipv6 filter

[機能]

IPv6 フィルタの設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 filter <count> <action> acl <acl_count> [<direction>]

lan [<number>] ipv6 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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～199	Si-R G110

<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。

－ ipv6

ipv6 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

ipv6 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、ipv6 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

ipv6 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、ipv6 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

ipv6 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、ipv6 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-R G110

<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、または、"-"を使用して表現される 16 進数の範囲を指定します。

Traffic Class 値の指定は、"," を区切りとして 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 を指定したものとみなされます。

<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 の 10 進数、または"-"を使用して表現される 10 進数の範囲を指定します。

icmptype 値の指定は、"," を区切りとして 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 を指定したものとみなされます。

<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 の 10 進数、または"-"を使用して表現される 10 進数の範囲を指定します。

icmptype 値の指定は、"," を区切りとして 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 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-layer protocol 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、本装置全体で以下の数まで定義できます。

最大定義数	機種
200	Si-R G110

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
3000	Si-R G110

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。

9.3.31 lan ipv6 filter move

[機能]

IPv6 フィルタの優先順序の変更

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～199	Si-R G110

[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。

9.3.32 lan ipv6 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 G110

[入力形式]

lan [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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>

・ 割り当て時間
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)のいずれかを指定します。
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> ipv6 filter default pass
```

9.3.33 lan ipv6 trafficclass

[機能]

Traffic Class 値書き換え条件の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 trafficclass <count> acl <acl_count> <new_trafficclass>

lan [<number>] ipv6 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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～99	Si-R G110

<acl_count>

・ ACL 定義番号

使用する ACL 定義の番号を、10 進数で指定します。

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。

－ ipv6

ipv6 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

ipv6 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、ipv6 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

ipv6 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、ipv6 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

ipv6 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、ipv6 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-R G110

<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、または、"-"を使用して表現される 16 進数の範囲を指定します。

Traffic Class 値の指定は、"," を区切りとして 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、本装置全体で以下の数まで定義できます。

最大定義数	機種
100	Si-R G110

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
3000	Si-R G110

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。

9.3.34 lan ipv6 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 G110

[入力形式]

lan [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～99	Si-R G110

[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。

9.3.35 lan ipv6 priority

[機能]

IPv6 プロトコル帯域制御の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 priority <count> acl <acl_count> <width>

lan [<number>] ipv6 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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

・ 帯域制御定義番号

帯域制御定義番号を、10 進数で指定します。

範囲	機種
0～99	Si-R G110

<acl_count>

・ ACL 定義番号

使用する ACL 定義の番号を、10 進数で指定します。

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。

－ ipv6

ipv6 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

ipv6 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、ipv6 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

ipv6 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、ipv6 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

ipv6 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、ipv6 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-R G110

<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、または、"-"を使用して表現される 16 進数の範囲を指定します。

Traffic Class 値の指定は、"," を区切りとして 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 を指定したものとみなされます。

<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～1000000kbps または 1mbps～1000mbps 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、本装置全体で以下の数まで定義できます。

最大定義数	機種
100	Si-R G110

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
3000	Si-R G110

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。

9.3.36 lan ipv6 in-policy

[機能]

Ingress ポリシールーティングの設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<in-policy_number>

・ Ingress ポリシールーティング定義番号
このインタフェースでの Ingress ポリシールーティング定義の通し番号を、10 進数で指定します。
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
200	Si-R G110

<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。
－ ipv6 ipv6 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 ipv6 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、ipv6 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 ipv6 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、ipv6 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 ipv6 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、ipv6 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
0～99	Si-R G110

[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。

9.3.37 lan ipv6 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 G110

[入力形式]

lan [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

9.3.38 lan ipv6 dhcp service

[機能]

IPv6 DHCP 機能の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 dhcp service <mode> [auto]

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。
・ relay
IPv6 DHCP リレーエージェント機能を使用します。
・ server
IPv6 DHCP サーバ機能を使用します。

以下のパラメタは、<mode>に client を指定した場合のみ有効です。

auto

M または O フラグが指定された RA を受信した場合に、動作を開始します。
省略時は、RA 連携を行わず、起動直後に動作を開始します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 DHCP 機能情報を設定します。
IPv6 DHCP クライアント機能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
4	Si-R G110

[注意]

リレーエージェント機能を使用する場合、使用するインタフェースにユニークローカルユニキャストアドレスのプレフィックス「fc00::/7」、またはグローバルユニキャストアドレスのプレフィックス「2000::/3」を持つ IPv6 アドレスを設定する必要があります。

[未設定時]

IPv6 DHCP 機能を使用しないものとみなされます。

```
lan <number> ipv6 dhcp service off
```

9.3.39 lan ipv6 dhcp duid

[機能]

IPv6 DHCP の DUID 設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 dhcp duid <duid>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<duid>

・ DUID
260 桁以内の 16 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]

IPv6 DHCP サーバ／クライアントの DUID を指定します。

例)

```
lan ipv6 dhcp duid 2105afffe66437d
```

[未設定時]

DUID を自動生成するものとみなされます。

9.3.40 lan ipv6 dhcp client option na

[機能]

IPv6 DHCP クライアントの IPv6 アドレス要求の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 dhcp client option na <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 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。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

- on
  IPv6 アドレスを要求します。
- off
  IPv6 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 IPv6 アドレスを要求するかどうかを設定します。

[注意]

RA 連携が有効な場合、本設定は M フラグが指定された RA を受信した場合に有効になります。
O フラグが指定された RA を受信した場合は、off で動作します。

[未設定時]

IPv6 アドレスを要求するものとみなされます。

```
lan <number> ipv6 dhcp client option na on
```

9.3.41 lan ipv6 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 G110

[入力形式]

lan [<number>] ipv6 dhcp client option pd <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 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。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

- off
  プレフィックスを要求しません。
- on
  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。

[注意]

RA 連携が有効な場合、本設定は M フラグが指定された RA を受信した場合に有効になります。
O フラグが指定された RA を受信した場合は、off で動作します。

[未設定時]

プレフィックスを要求しないものとみなされます。

```
lan <number> ipv6 dhcp client option pd off
```

9.3.42 lan ipv6 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 G110

[入力形式]

lan [<number>] ipv6 dhcp client option dns <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 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。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

```
lan <number> ipv6 dhcp client option dns on
```

9.3.43 lan ipv6 dhcp client option domain

[機能]

IPv6 DHCP クライアントの DNS ドメイン名要求の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 dhcp client option domain <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 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。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

- on
  DNS ドメイン名を要求します。
- off
  DNS ドメイン名を要求しません。

[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 ドメイン名を要求するかどうかを設定します。

[未設定時]

DNS ドメイン名を要求するものとみなされます。

```
lan <number> ipv6 dhcp client option domain on
```

9.3.44 lan ipv6 dhcp client option sipserver address

[機能]

IPv6 DHCP クライアントの SIP サーバアドレス要求の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 dhcp client option sipserver address <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 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。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

- on
  SIP サーバアドレスを要求します。
- off
  SIP 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 SIP 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]

SIP サーバアドレスを要求するものとみなされます。

```
lan <number> ipv6 dhcp client option sipserver address on
```

9.3.45 lan ipv6 dhcp client option sipserver domain

[機能]

IPv6 DHCP クライアントの SIP ドメイン名要求の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 dhcp client option sipserver domain <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 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。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

- on
  SIP ドメイン名を要求します。
- off
  SIP ドメイン名を要求しません。

[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 SIP ドメイン名を要求するかどうかを設定します。

[未設定時]

SIP ドメイン名を要求するものとみなされます。

```
lan <number> ipv6 dhcp client option sipserver domain on
```

9.3.46 lan ipv6 dhcp client option sntpserver

[機能]

IPv6 DHCP クライアントの SNTP サーバアドレス要求の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 dhcp client option sntpserver <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 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。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

- on
  SNTP サーバアドレスを要求します。
- off
  SNTP 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 SNTP 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]

SNTP サーバアドレスを要求するものとみなされます。

```
lan <number> ipv6 dhcp client option sntpserver on
```

9.3.47 lan ipv6 dhcp client option refreshtime

[機能]

IPv6 DHCP クライアントの情報リフレッシュ時間要求の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 dhcp client option refreshtime <mode> [<time>]

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

- on
  情報リフレッシュ時間を要求します。
- off
  情報リフレッシュ時間を要求しません。

<time>

情報リフレッシュ時間オプションを取得しなかった、またはできなかった場合のデフォルトリフレッシュ時間を、10 分～365 日の範囲で指定します。
単位は、d(日)、h(時)、m(分)、s(秒)のいずれかを指定します。
省略時は、1 日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 DHCP クライアント機能を使用する場合に、サーバに情報リフレッシュ時間を要求するかどうかを設定します。

[注意]

本設定は、Information-Request による要求をした場合のみ有効です。
Solicit/Request による要求をした場合は、off で動作します。

[未設定時]

情報リフレッシュ時間を要求するものとみなされます。

```
lan <number> ipv6 dhcp client option refreshtime on 1d
```

9.3.48 lan ipv6 dhcp client iaid

[機能]

IPv6 DHCP クライアントの IAID 設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 dhcp client iaid <iaid>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 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。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

```
lan <number> ipv6 dhcp client iaid auto
```

9.3.49 lan ipv6 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 G110

[入力形式]

lan [<number>] ipv6 dhcp client route <mode>

[オプション]

<number>

- lan 定義番号
  lan 定義の通し番号を、10 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。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

```
lan <number> ipv6 dhcp client route blackhole
```

9.3.50 lan ipv6 dhcp relay interface

[機能]

IPv6 DHCP リレーエージェントのリレー先インタフェース設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 dhcp relay interface <interface>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<interface>

リレー先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～rmt99	Si-R G110

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 DHCP リレーエージェント機能を使用する場合に、リレー先インタフェースの設定をします。

[未設定時]

リレー先インタフェースを指定しないものとみなされます。
IPv6 DHCP リレーエージェント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。

9.3.51 lan ipv6 dhcp relay server

[機能]

IPv6 DHCP リレーエージェントのリレー先サーバアドレス設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 dhcp relay server <address>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<address>

リレー先サーバアドレスを指定します。

・ リレー先サーバアドレス
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

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 DHCP リレーエージェント機能を使用する場合に、リレー先サーバアドレスの設定をします。

[未設定時]

規定のマルチキャストアドレス(ff05::1:3)あてにリレーします。

9.3.52 lan ipv6 dhcp relay source

[機能]

IPv6 DHCP リレーエージェントのリレーパケット送信元アドレス設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 dhcp relay source <address>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<address>

リレーパケットの送信元アドレスを指定します。

・ リレーパケットの送信元アドレス
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

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 DHCP リレーエージェント機能を使用する場合に、リレーパケットの送信元アドレスの設定をします。

[未設定時]

リレーパケットの送信元アドレスを設定しないものとみなされます。

9.3.53 lan ipv6 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 G110

[入力形式]

lan [<number>] ipv6 dhcp server preference <preference>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

```
lan <number> ipv6 dhcp server preference 0
```

9.3.54 lan ipv6 dhcp server info address

[機能]

IPv6 DHCP サーバの IPv6 アドレス配布情報設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 dhcp server info address <address> <num> <valid> <preferred>

[オプション]

<number>

・ lan 定義番号

lan 定義の通し番号を、10 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。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<address>

・ 割り当て開始 IPv6 アドレス

配布する IPv6 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。

::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配布する場合は上位を"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、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～rmt99	Si-R G110

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

dhcp@rmt0::1000

<num>

・ 割り当て IPv6 アドレス数

割り当て可能な IPv6 アドレスの総数を、0～300 の 10 進数で指定します。

ホストデータベース機能を使用すると、特定の IPv6 DHCP クライアントに対して固有の IPv6 アドレスを割り当てることができます。この場合の IPv6 アドレスは、割り当て先頭 IPv6 アドレスと割り当て IPv6 アドレス数によって規定される動的割り当て範囲である必要はありません。

<valid>

・ valid lifetime

このインタフェースから配布する IPv6 アドレスに対する 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)のいずれかを指定します。

・ infinity

このインタフェースから配布する IPv6 アドレスに対する 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 IPv6 アドレスに対する 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)のいずれかを指定します。

<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IPv6アドレスに対するpreferred lifetimeを無限とします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 DHCPサーバ機能を使用する場合に、IPv6アドレス配布情報を設定します。

9.3.55 lan ipv6 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 G110

[入力形式]

lan [<number>] ipv6 dhcp server info dns <dns1> [<dns2>]

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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

IPv6 DHCP クライアントが取得した DNS サーバアドレスを配布する場合は"dhcp@インタフェース名"の形式で指定します。インタフェース名には、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～rmt99	Si-R G110

<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

<dns1>に"dhcp@インタフェース名"を指定した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。

9.3.56 lan ipv6 dhcp server info domain

[機能]

IPv6 DHCP サーバの DNS ドメイン名配布情報設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 dhcp server info domain <domain>

[オプション]

<number>

・ lan 定義番号

lan 定義の通し番号を、10 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。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<domain>

・ DNS ドメイン名

IPv6 DHCP クライアントに配布する DNS ドメイン名を、英数字、"-"(ハイフン)、"."(ピリオド)の文字で構成される 80 文字以内の文字列で指定します。

ドメイン名は RFC1035 に準拠している必要があります。

IPv6 DHCP クライアントが取得した DNS ドメイン名を配布する場合は"dhcp@インタフェース名"の形式で指定します。インタフェース名には、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～rmt99	Si-R G110

[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 ドメイン名情報の設定をします。

9.3.57 lan ipv6 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 G110

[入力形式]

lan [<number>] ipv6 dhcp server info prefix <prefix>/<prefixlen> <valid><preferred> <routeset> <duid>

[オプション]

<number>

・ lan 定義番号

lan 定義の通し番号を、10 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。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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を、48～64 の 10 進数で指定します。

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、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～rmt99	Si-R G110

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

dhcp@rmt0:1234::/64

プレフィックス長には、取得したプレフィックス長より大きい値を指定してください。

<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)のいずれかを指定します。

・ 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)のいずれかを指定します。

<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。

<duid>

- DUID

  260 桁以内の 16 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]

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。

設定に一致する DUID のクライアント以外にはプレフィックスを配布しません。プレフィックス配布情報を設定していない場合は、プレフィックスを配布することはできません。

9.3.58 lan ipv6 dhcp server info sipserver address

[機能]

IPv6 DHCP サーバの SIP サーバアドレス配布情報設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 dhcp server info sipserver address <sip1> [<sip2>]

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<sip1>

・ SIP サーバ IPv6 アドレス
IPv6 DHCP クライアントに配布する SIP 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

IPv6 DHCP クライアントが取得した SIP サーバアドレスを配布する場合は、"dhcp@インタフェース名"の形式で指定します。インタフェース名には、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～rmt99	Si-R G110

<sip2>

・ セカンダリ SIP 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 SIP 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

<sip1>に"dhcp@インタフェース名"を指定した場合は、<sip2>を指定できません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 DHCP サーバ機能を使用する場合に、配布する SIP サーバアドレス情報の設定をします。

9.3.59 lan ipv6 dhcp server info sipserver domain

[機能]

IPv6 DHCP サーバの SIP ドメイン名配布情報設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 dhcp server info sipserver domain <sip1> [<sip2>]

[オプション]

<number>

・ lan 定義番号

lan 定義の通し番号を、10 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。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<sip1>

・ SIP ドメイン名

IPv6 DHCP クライアントに配布する SIP ドメイン名を、英数字、"-"(ハイフン)、"."(ピリオド)の文字で構成される 80 文字以内の文字列で指定します。

ドメイン名は RFC1035 に準拠している必要があります。

IPv6 DHCP クライアントが取得した SIP ドメイン名を配布する場合は、"dhcp@インタフェース名"の形式で指定します。インタフェース名には、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～rmt99	Si-R G110

<sip2>

・ セカンダリ SIP ドメイン名

IPv6 DHCP クライアントに配布するセカンダリ SIP ドメイン名を、英数字、"-"(ハイフン)、"."(ピリオド)の文字で構成される 80 文字以内の文字列で指定します。

ドメイン名は RFC1035 に準拠している必要があります。

<sip1>に"dhcp@インタフェース名"を指定した場合は、<sip2>を指定できません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 DHCP サーバ機能を使用する場合に、配布する SIP ドメイン名情報の設定をします。

9.3.60 lan ipv6 dhcp server info sntpserver

[機能]

IPv6 DHCP サーバの SNTP サーバアドレス配布情報設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] ipv6 dhcp server info sntpserver <sntp1> [<sntp2>]

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<sntp1>

・ SNTP サーバ IPv6 アドレス
IPv6 DHCP クライアントに配布する、SNTP 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

IPv6 DHCP クライアントが取得した SNTP サーバアドレスを配布する場合は"dhcp@インタフェース名"の形式で指定します。インタフェース名には、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～rmt99	Si-R G110

<sntp2>

・ セカンダリ SNTP 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 SNTP サーバの IPv6 アドレスを指定します。
<sntp1>に"dhcp@インタフェース名"を指定した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 サーバ機能を使用する場合に、配布する SNTP サーバアドレス情報の設定をします。

9.4 VRRP 関連情報

9.4.1 lan vrrp use

[機能]

VRRP 動作モードの設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

VRRP 機能を使用するかどうかを指定します。

・ 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。

・ 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。

[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
```

9.4.2 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

[注意]

VRRP-AD の認証は IPv6 では機能しません。

[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
```

9.4.3 lan vrrp group id

[機能]

VRRP グループの設定

[適用機種]

Si-R G110

[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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、1～254 の 10 進数で指定します。

VRRP グループは、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。

・ master [<protocol>]

VRRP ルータの優先度に"master"を指定します。

優先度に"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 IP アドレスは<number>で指定した lan インタフェースの実 IP アドレスになります。"master"を指定した場合のみ<protocol>を指定できます。

<protocol>に ip を指定。または<protocol>を省略の場合：

lan <number> ip address <address>/<mask> <broadcast>で設定された<address>が実 IP アドレスです。

<protocol>に ipv6 を指定した場合：

<number>で指定した lan インタフェースの IPv6 リンクローカルアドレスが実 IP アドレスです。

"master"を指定した場合は 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。

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 グループの設定された 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、指定することはできません。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。

・ 仮想ルータの IPv6 アドレス

VRRP グループで使用する仮想ルータの 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。

fe80::1 ～ fe80::ffff:ffff:ffff:ffff

<priority>に"master ipv6"を指定した場合は、仮想ルータの IPv6 アドレスは<number>で指定した lan インタフェースの実 IPv6 リンクローカルアドレスとなるため、指定することはできません。

それ以外の場合は、仮想ルータの IPv6 アドレスを指定しなければなりません。

また、仮想ルータの IPv6 アドレスに<number>で指定した lan インタフェースの実 IPv6 リンクローカル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 IP 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 IP 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。

IPv4 VRRP の場合

00:00:5e:00:01:{VRID}

IPv6 VRRP の場合

00:00:5e:00:02:{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。

[注意]

定義変更後の VRID が同一であっても、IPv4 VRRP から IPv6 VRRP に変更、または IPv6 VRRP から IPv4 VRRP に定義を変更し、動的定義反映した場合は、VRID を変更した場合と同じ動的定義反映動作となります。

[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。

9.4.4 lan vrrp group ad

[機能]

VRRP-AD の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。

<interval>

・ VRRP-AD 送出間隔
VRRP-AD の送出間隔を、1～255 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
```

9.4.5 lan vrrp group preempt

[機能]

プリエンプトモードの設定

[適用機種]

Si-R G110

[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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 0～900 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、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
```

9.4.6 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。

範囲	機種
0～127	Si-R G110

<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～rmt99	Si-R G110

・ 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。

9.4.7 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 G110

[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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。

範囲	機種
0～127	Si-R G110

<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）

・ default4

経路として IPv4 デフォルトルートを指定します。

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。

default と指定した場合は default4 に変換します。

・ IPv6 アドレス/プレフィックス長

あて先または中継先ネットワークの 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。マルチキャストアドレスやリンクローカルアドレスは指定できません。

また、::/0 以外の組み合わせでの::やプレフィックス長 0 も指定できません。

・ default6

経路として IPv6 デフォルトルートを指定します。

::/0 を指定するのと同じ意味になります。

<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～rmt99	Si-R G110

・ 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。

9.4.8 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 G110

[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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。

範囲	機種
0～127	Si-R G110

<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。

IPv4 の場合：

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 の場合：

::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff

fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

以下の範囲を指定した場合は IPv6 リンクローカルアドレスとなりますので以降の<interface>に IPv6 リンクローカルアドレスのインタフェースを指定してください。

fe80:: ～ fe80::ffff:ffff:ffff:ffff

<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。

<dst_addr>が IPv6 リンクローカルアドレスの場合は lan インタフェースも指定可能です。

それ以外では以下となります。

・ 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～rmt99	Si-R G110

・ 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、1～60 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、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>+1～240 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、<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>+1～255 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。

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、1～255 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。

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などのユニキャストアドレス以外の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。

あて先 IP アドレスが IPv4 アドレスである場合、ノードダウントリガで送信される ICMP ECHO パケット送信元 IP アドレスは、VRRP グループが設定された lan インタフェースの IPv4 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。あて先 IP アドレスが IPv6 アドレスである場合は、プロトコルが選択した本装置 IPv6 アドレスが送信元 IP アドレスとなります。

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。

9.4.9 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 G110

[入力形式]

lan [<number>] vrrp group <vrrp_number> action <action_no> <state> online ether [group <group> [port <port>]]

lan [<number>] vrrp group <vrrp_number> action <action_no> <state> online pseudo-ether [<interface_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 ether [group <group> [port <port>]]

lan [<number>] vrrp group <vrrp_number> action <action_no> <state> offline pseudo-ether [<interface_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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。

範囲	機種
0～19	Si-R G110

<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、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。

backup と設定されている場合は、マスタ状態からイニシャルまたはバックアップ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、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。

backup と設定されている場合は、マスタ状態からイニシャルまたはバックアップ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。

ether, pseudo-ether, access-point, template interface, template, remote

アクション適用対象の種別を指定します。

・ ether

適用対象を指定された ether とします。

・ pseudo-ether

適用対象を指定された pseudo-ether 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。

group <group> port <port>

ether グループ番号と ether ポート番号を指定します。

<group>

・ ether グループ番号

使用する ether グループ番号を、10 進数で指定します。

グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

省略時は、全ポートが指定されたものとみなされます。

範囲	機種
1～2	Si-R G110

<port>

・ ether ポート番号

使用する ether ポート番号を、10 進数で指定します。

複数のポート番号を設定する場合、"," (カンマ)で区切ります。

複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。

ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

省略時は、対象グループの全ポートが指定されたものとみなされます。

範囲	機種
1	Si-R G110（グループ 1）
1～4	Si-R G110（グループ 2）

<remote_number> ap <ap_number> id <id> <password>

相手定義番号と接続先定義番号で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
0～99	Si-R G110

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 進数で指定します。

範囲	機種
0～99	Si-R G110

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 128 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 128 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 進数で指定します。

範囲	機種
0～1	Si-R G110

<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>が示す状態の間自動発信または自動着信を抑止します。構成定義で自動発信または自動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 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。

9.4.10 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

・ 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。
・ 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。

<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
```

9.4.11 lan vrrp group vaddr etherip

[機能]

仮想 IP アドレスあて EtherIP パケット受信動作の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] vrrp group <vrrp_number> vaddr etherip <mode>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 進数で指定します。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。
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 進数で指定します。

<mode>

仮想 IP アドレスあて EtherIP パケットを受理するか破棄するかを指定します。

・ discard
仮想 IP アドレスあて EtherIP パケットを破棄する場合に指定します。
・ accept
仮想 IP アドレスあて EtherIP パケットを受理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]

VRRP の仮想 IP あて EtherIP パケット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 EtherIP パケットは受理しないものとみなされます。

```
lan <number> vrrp group <vrrp_number> vaddr etherip discard
```

9.4.12 lan vrrp trap

[機能]

IPv4 VRRP が送信する TRAP モードの設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] vrrp trap <mode>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

IPv4 VRRP が送信する TRAP モードとして旧仕様(RFC2787)か新仕様(draft-ietf-vrrp-unified-mib-06)を指定します。

・ old
IPv4 VRRP が送信する TRAP モードとして旧仕様(RFC2787)を使用します。

・ new
IPv4 VRRP が送信する TRAP モードとして新仕様(draft-ietf-vrrp-unified-mib-06)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]

この lan インタフェースで動作する IPv4 VRRP が送信する TRAP モードを設定します。

[未設定時]

IPv4 VRRP が送信する TRAP モードは旧仕様とみなされます。

```
lan <number> vrrp trap old
```

9.5 VLAN 関連情報

9.5.1 lan vlan

[機能]

VLAN ID の設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] vlan <vid>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<vid>

VLAN ID を、0～4094 の 10 進数で指定します。
VLAN ID 0 は ethergroup vlan mode disable 設定時にだけ有効です。

[動作モード]

構成定義モード(管理者クラス)

[説明]

VLAN ID と lan 定義番号の関連付けを行います。

[注意]

・ <vid>で指定された VLAN が未登録の場合、設定は無効となります。
・ <vid>で指定された VLAN が複数の lan に対して設定された場合は、もっとも小さい lan 定義のみが有効となります。
・ 0 を設定した場合、ethergroup vlan mode enable 設定時は、本設定は無効となります。

[未設定時]

なし

9.6 SNMP 関連情報

9.6.1 lan snmp trap linkdown

[機能]

linkDown トラップの設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] snmp trap linkdown <mode>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

[注意]

snmp trap linkdown コマンドで trap 動作が無効にされた場合は、本コマンド設定値は意味を持ちません。

[未設定時]

linkDown トラップが有効とみなされます。

```
lan <number> snmp trap linkdown enable
```

9.6.2 lan snmp trap linkup

[機能]

linkUp トラップの設定

[適用機種]

Si-R G110

[入力形式]

lan [<number>] snmp trap linkup <mode>

[オプション]

<number>

・ lan 定義番号
lan 定義の通し番号を、10 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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

[注意]

snmp trap linkup コマンドで trap 動作が無効にされた場合は、本コマンド設定値は意味を持ちません。

[未設定時]

linkUp トラップが有効とみなされます。

```
lan <number> snmp trap linkup enable
```

第 10 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)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
0～99	Si-R G110

・ 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)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
0～99	Si-R G110

10.1 相手共通情報

10.1.1 remote description

[機能]

相手ネットワークの説明文の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] description <description>

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<description>

・ 説明文
相手ネットワークの説明文を、0x21,0x23～0x7e の 50 文字以内の ASCII 文字列で記入します。
(入力可能な文字の一覧については、コマンドユーザーズガイドを参照してください。)

[動作モード]

構成定義モード(管理者クラス)

[説明]

この相手ネットワークについての説明文を記入します。

[未設定時]

説明文を記入しないものとみなされます。

10.1.2 remote name

[機能]

相手ネットワーク名称の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

10.1.3 remote autodial

[機能]

自動ダイヤル可否の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

[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
```

10.1.4 remote mtu

[機能]

送信パケット最大長(MTU 値)の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mtu>

・ MTU 値
MTU 値を、200～1500 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]

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
```

10.1.5 remote shaping

[機能]

シェーピング機能の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数と単位文字で指定します。
10 進数の末尾に 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-R G110

[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 Ethernet 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
```

10.1.6 remote shaping-opt tc

[機能]

シェーピング機能の単位時間の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] shaping-opt tc <tc>

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<tc>

・ 単位時間
単位時間の値(単位はミリ秒)を、1～100 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]

シェーピング機能の単位時間を設定します。

[未設定時]

単位時間の値として、10 ミリ秒を設定したものとみなされます。

```
remote <number> shaping-opt tc 10
```

10.2 接続先情報

10.2.1 remote ap description

[機能]

接続先の名称の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] description <ap_description>

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<ap_description>

・ 接続先名説明
接続先名の説明を、0x21,0x23～0x7e の 50 文字以内の ASCII 文字列で指定します。
(入力可能な文字の一覧については、コマンドユーザーズガイドを参照してください。)

[動作モード]

構成定義モード(管理者クラス)

[説明]

接続先名の説明を設定します。

[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。

10.2.2 remote ap name

[機能]

接続先の名称の設定

[適用機種]

Si-R G110

[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 進数で指定します。
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 進数で指定します。
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／切断コマンドで使用する予約語であるため、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。

10.2.3 remote ap move

[機能]

接続先の優先順序の変更

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

[動作モード]

構成定義モード(管理者クラス)

[説明]

接続先の順序を変更します。

10.2.4 remote ap datalink type

[機能]

パケット転送方法の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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-R G110
Ethernet	PPPoE 方式	○
データ通信モジュール(*1)	非同期 PPP	○

*1) USB に挿入したデータ通信モジュールを利用

・ 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。

・ 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
```

10.2.5 remote ap datalink bind

[機能]

パケット転送回線の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。
・ vlan
vlan 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>

wan 定義または vlan 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 進数で指定します。

範囲	機種
1	Si-R G110

・ vlan 定義の定義番号
利用する lan の定義番号を、10 進数で指定します。

範囲	機種
1～4094	Si-R G110

[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]

パケット転送回線を設定しないものとみなされます。

10.2.6 remote ap recovery

[機能]

接続自動復旧モードの設定

[適用機種]

Si-R G110

[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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

10.2.7 remote ap ip dns

[機能]

DNS サーバアドレスの設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] ip dns <primary_dns> [<secondary_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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<primary_dns>

・ プライマリ 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

<secondary_dns>

・ セカンダリ 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、<primary_dns>、<secondary_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、<primary_dns>、<secondary_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。

[注意]

<secondary_dns>のみが未設定の場合、および<secondary_dns>に 0.0.0.0 を設定した場合は、<primary_dns>の設定値に応じて以下のように判断されます。

<primary_dns>設定値	<secondary_dns>解釈値
0.0.0.0	0.0.0.0
255.255.255.255	255.255.255.255
上記以外	0.0.0.0

[未設定時]

プライマリ DNS サーバアドレス、セカンダリ DNS サーバ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
```

10.2.8 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 G110

[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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～99	Si-R G110

<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
100	Si-R G110

[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されます。

10.2.9 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～99	Si-R G110

[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。

10.2.10 remote ap limit time

[機能]

接続時間累計制限の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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)のいずれかを指定します。
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
```

10.2.11 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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)のいずれかを指定します。
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モジュール接続時に有効です。

[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
```

10.2.12 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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モジュール接続時に有効です。

[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
```

10.2.13 remote ap ppp auth type

[機能]

認証方法の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<authtype>

認証プロトコルのタイプを指定します。

・ 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。
・ 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。

[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
```

10.2.14 remote ap ppp auth send

[機能]

送信認証情報の設定

[適用機種]

Si-R G110

[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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<id>

・ 認証 ID

認証 ID を、0x21,0x23～0x7e の文字で構成される 128 文字以内の文字列で指定します。

<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 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 128 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。

10.2.15 remote ap ppp auth receive

[機能]

受諾認証情報の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<id>

・ 認証 ID
認証 ID を、0x21,0x23～0x7e の文字で構成される 128 文字以内の文字列で指定します。

<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 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]

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。

10.2.16 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

10.2.17 remote ap pppoe svname

[機能]

サービスネーム(Service-Name)の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

10.2.18 remote ap dial number

[機能]

接続先の電話番号の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] dial <count> number<dial_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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

ダイヤル定義番号として、以下のいずれかを指定します。

・ 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。

[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。

[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。

10.2.19 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

10.2.20 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

10.2.21 remote ap called number

[機能]

CLID の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

[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
```

10.2.22 remote ap connect priority

[機能]

接続優先制御の設定

[適用機種]

Si-R G110

[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 進数で指定します。
  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 進数で指定します。
  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]

互いの装置からの接続要求が競合した場合にどちらの接続を優先するかを設定します。

IPsec/IKE の場合は、自装置から送信する鍵交換要求と相手装置から受信する鍵交換要求が競合した場合に、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、接続優先制御を行いません。

[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。同じ優先制御を行った場合、IPsec/IKE では鍵交換に失敗する場合があります。

[未設定時]

接続優先制御を行いません。

```
remote <number> ap <ap_number> connect priority off
```

10.2.23 remote ap idle

[機能]

無通信監視タイマの設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<time>

・ 無通信監視時間
無通信監視時間を、0～3600 秒の範囲で指定します。
単位は、d(日)、h(時)、m(分)、s(秒)のいずれかを指定します。
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
```

10.2.24 remote ap keep

[機能]

回線接続保持機能の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。
本コマンドは、以下の場合だけ有効です。

・ remote ap datalink type の<type>で ipsec を指定している場合。
・ remote ap datalink type の<type>で physical 指定、かつ remote ap datalink bind の<kind>として vlan を指定している場合。

上記の場合、"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。

[注意]

IPsec および動的 VPN で常時接続機能を使用した場合は、以下の点に注意してください。

・ 手動鍵設定では、当機能は無効となります。
・ Aggressive Mode の Responder 設定で、初回の IKE ネゴシエーションは行えません。
・ 動的 VPN 設定を使用する場合は、「動的 VPN サーバに登録する自側ユーザ ID の設定」を設定してください。設定しない場合は、常時接続機能を行えません。

データ通信モジュールでは本コマンドは無効となります。

[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
```

10.2.25 remote ap ipsec type

[機能]

IPsec 情報のタイプの設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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(IPsec Version2)で使用します。
・ ike
IPsec 自動鍵交換(IKE Version1/IPsec Version2)を使用します。
・ ikev2
IPsec 自動鍵交換(IKE Version2/IPsec Version3)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。
また、IPsec プロトコル Version2 を使用します。
－ remote ap ipsec send
－ remote ap ipsec receive
・ IPsec 情報のタイプに ike または ikev2 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。
また、ike を指定した場合は、IKE Version1/IPsec プロトコル Version2 を使用し、ikev2 を指定した場合は IKE Version2/IPsec プロトコル Version3 を使用します。
－ 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。
また、IKE Version1/IPsec プロトコル Version2 を使用します。
－ 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とき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。

IKE Version1 と IKE Version2 で使用可能な IKE 定義一覧

・ IKE Version1 でのみ使用できるコマンド一覧
－ remote ap ike port
－ remote ap ike idtype
－ remote ap ike mode
－ remote ap dvpn
－ dvpn client
・ IKE Version2 でのみ使用できるコマンド一覧
－ remote ap ike proposal prf
－ remote ap ike local-idtype
－ remote ap ike remote-idtype
－ remote ap ike remote-id-send
－ remote ap ike eap auth send
－ remote ap ike ts multi
－ remote ap ipsec ike esn

[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
```

10.2.26 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

10.2.27 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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)	×

auth(認証)	encrypt(暗号)	セキュリティプロトコル	IPsec SA
−	○	−	×
○	○	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
```

10.2.28 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

10.2.29 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<enc_algo>

暗号アルゴリズムを指定します。

・ none
・ des-cbc
・ 3des-cbc
・ aes-cbc-128
・ aes-cbc-192
・ aes-cbc-256
・ null

<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

鍵種別 暗号アルゴリズム	hex 16 進数鍵	text 文字列鍵
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、いずれかの鍵が 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
```

10.2.30 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<auth_algo>

認証アルゴリズムを指定します。

・ none
・ hmac-md5
・ hmac-sha1
・ hmac-sha256
・ hmac-sha384
・ hmac-sha512

<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
hmac-sha256	1～64 桁	32 文字

鍵種別 認証アルゴリズム	hex 16 進数鍵	text 文字列鍵
hmac-sha384	1～96 桁	48 文字
hmac-sha512	1～128 桁	64 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
```

10.2.31 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

10.2.32 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

10.2.33 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

10.2.34 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<enc_algo>

暗号アルゴリズムを指定します。

・ none
・ des-cbc
・ 3des-cbc
・ aes-cbc-128
・ aes-cbc-192
・ aes-cbc-256
・ null

<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

鍵種別 暗号アルゴリズム	hex 16 進数鍵	text 文字列鍵
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、いずれかの鍵が 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
```

10.2.35 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<auth_algo>

認証アルゴリズムを指定します。

・ none
・ hmac-md5
・ hmac-sha1
・ hmac-sha256
・ hmac-sha384
・ hmac-sha512

<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
hmac-sha256	1～64 桁	32 文字
hmac-sha384	1～96 桁	48 文字

鍵種別 認証アルゴリズム	hex 16 進数鍵	text 文字列鍵
hmac-sha512	1～128 桁	64 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
```

10.2.36 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

10.2.37 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。複数定義するときは、アルゴリズムを空白なしでカンマ','で区切ります。

・ none
・ des-cbc
・ 3des-cbc
・ aes-cbc-128
・ aes-cbc-192
・ aes-cbc-256
・ null

[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
```

10.2.38 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。複数定義するときは、アルゴリズムを空白なしでカンマ','で区切ります。

・ none
・ hmac-md5
・ hmac-sha1
・ hmac-sha256
・ hmac-sha384
・ hmac-sha512

[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
・ hmac-sha256
・ hmac-sha384
・ hmac-sha512

[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
```

10.2.39 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<pfs_group>

Diffie-Hellman グループについて指定します。

・ off
Diffie-Hellman グループを使用しません。
・ 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)
・ modp2048
Diffie-Hellman グループの MODP2048(グループ 14)

[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
```

10.2.40 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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)のいずれかを指定します。

[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
```

10.2.41 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

10.2.42 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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)のどちらかを指定します。

<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]

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
```

10.2.43 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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)のどちらかを指定します。

・ 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]

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
```

10.2.44 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

10.2.45 remote ap ipsec ike anti-replay

[機能]

自動鍵交換用 IPsec 情報のリプレイ攻撃防御機能の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike anti-replay <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

・ リプレイ攻撃防御機能
AH または認証付き ESP を利用した IPsec 通信でリプレイ攻撃防御機能の使用有無を指定します。
－ on
リプレイ攻撃防御機能を使用します。
－ off
リプレイ攻撃防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]

AH または認証付き ESP を利用した IPsec 通信の受信(復号・認証)時でリプレイ攻撃防御機能を使用するかどうかの設定を行います

[注意]

リプレイ攻撃防御機能を使用しない場合は、重複攻撃(なりすまし)などによる検出が行えなくなるため、セキュリティが弱くなります。

[未設定時]

リプレイ攻撃防御機能を使用するものとみなされます。

```
remote <number> ap <ap_number> ipsec ike anti-replay on
```

10.2.46 remote ap ipsec ike esn

[機能]

IPsecV3 情報の ESN(拡張シーケンス番号)の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike esn <esn>

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<esn>

ESN(拡張シーケンス番号)の有無を指定します。

・ enable
ESN(拡張シーケンス番号)を IKE ネゴシエーションで要求します。

・ disable
ESN(拡張シーケンス番号)を IKE ネゴシエーションで拒否します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPsec Version3 では、ESN(拡張シーケンス番号)をサポートしています。相手装置との IKE ネゴシエーション確立時にその使用の有無を行います。

<esn>が enable の場合は、IKE ネゴシエーション確立時に ESN を要求します。disable の場合は、IKE ネゴシエーション確立時に ESN を要求せず、さらに相手装置からの要求に対して拒否します。

[注意]

本設定は IKE Version2(remote ap ipsec type ikev2)のみ有効となります。

[未設定時]

IKE Version2 セッション確立のネゴシエーションパケットの ESN を要求すると指定したものとみなされます。

```
remote <number> ap <ap_number> ipsec ike esn enable
```

10.2.47 remote ap ipsec ike exchange-sa initiator

[機能]

自動鍵交換用 IPsec 情報の Initiator SA 更新時の切り替え待ち時間の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike exchange-sa initiator <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<time>

・ Initiator SA 切り替え待ち時間
Initiator SA 切り替え待ち時間を、0 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]

自側が Initiator の場合に、IPsec SA の更新後、New SA に切り替える時間の設定を行います。
0 秒を設定した場合は、IPsec SA の更新後即時、New SA に切り替わります。

[注意]

本設定は、IKE Version1(remote ap ipsec type ike)の設定をした場合のみ有効です。
remote ap ipsec ike lifebyte に 0 以外を設定した場合は、本コマンドは未設定時と同様の動作となります。

[未設定時]

Initiator SA 切り替え待ち時間として 0s(0 秒)が設定されたものとして扱います。

```
remote <number> ap <ap_number> ipsec ike exchange-sa initiator 0s
```

10.2.48 remote ap ipsec ike exchange-sa responder

[機能]

自動鍵交換用 IPsec 情報の Responder SA 更新時の切り替え待ち時間の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike exchange-sa responder <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<time>

・ Responder SA 切り替え待ち時間
Responder SA 切り替え待ち時間を、0 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]

自側が Responder の場合に、IPsec SA の更新後、New SA に切り替える時間の設定を行います。
0 秒を設定した場合は、IPsec SA の更新後即時、New SA に切り替わります。

[注意]

本設定は、IKE Version1(remote ap ipsec type ike)の設定をした場合のみ有効です。
remote ap ipsec ike lifebyte に 0 以外を設定した場合は、本コマンドは未設定時と同様の動作となります。

[未設定時]

Responder SA 切り替え待ち時間として 0s(0 秒)が設定されたものとして扱います。

```
remote <number> ap <ap_number> ipsec ike exchange-sa responder 0s
```

10.2.49 remote ap ipsec extension-range

[機能]

拡張 IPsec 対象範囲の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～99	Si-R G110

<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
100	Si-R G110

[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。

10.2.50 remote ap ike port

[機能]

IKE Version1 情報の相手側 IKE ポート番号の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

[注意]

本設定は、IKE Version1(remote ap ipsec type ike)の設定をした場合のみ有効です。

[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
```

10.2.51 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。
IKE Version2 EAP 認証機能を使用している場合は、設定された共有鍵は使用されません。

[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。

10.2.52 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 で動作させるときに、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。

10.2.53 remote ap ike proposal auth-method

[機能]

IKE セッション用相手装置認証情報の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] ike proposal [<proposal_number>]auth-method <auth_method>

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<proposal_number>

・ Proposal 定義番号
Proposal 定義番号を、0～2 の 10 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。

<auth_method>

認証方式を指定します。

・ shared-key
認証方式として共有鍵を使用します。
・ rsa-signature
認証方式として RSA デジタル署名方式を使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

相手装置を認証するための、認証方式の設定を行います。

[注意]

認証方式として shared-key を指定した場合は必ず共有鍵の設定を行ってください。
認証方式として rsa-signature を指定した場合は必ず以下の設定を行ってください。
・ "IKE セッション用秘密鍵情報"の設定
・ "IKE セッション用自装置証明書情報"の設定
ただし、IKE Version2 EAP 認証機能を使用している場合は、EAP 認証が行われます。
IKE Version2(remote ap ipsec type ikev2)を指定した場合で、複数の Proposal を指定した場合は、同一の認証方式を選択してください。異なる認証方式を選択すると定義エラーとなります。

[未設定時]

相手装置認証のための認証方式に shared-key を指定したものとみなされます。

```
remote <number> ap <ap_number> ike proposal <proposal_number> auth-method shared-key
```

10.2.54 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<proposal_number>

・ Proposal 定義番号
Proposal 定義番号を、0～2 の 10 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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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あると 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。

10.2.55 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<proposal_number>

・ Proposal 定義番号
Proposal 定義番号を、0～2 の 10 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。

<hash_algo>

認証(ハッシュ)アルゴリズムを指定します。

・ hmac-md5
・ hmac-sha1
・ hmac-sha256
・ hmac-sha384
・ hmac-sha512

[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
```

10.2.56 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<proposal_number>

・ Proposal 定義番号
Proposal 定義番号を、0～2 の 10 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。

<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
・ modp2048
MODP2048(グループ 14)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。

[注意]

IKE Version2(remote ap ipsec type ikev2)を指定した場合で、複数の Proposal を指定した場合は、同一の DH グループを選択してください。異なる DH グループを選択すると定義エラーとなります。

[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
```

10.2.57 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<proposal_number>

・ Proposal 定義番号
Proposal 定義番号を、0～2 の 10 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。

<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)のいずれかを指定します。

[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
```

10.2.58 remote ap ike proposal prf

[機能]

IKE Version2セッション用prf(Pseudo Random Function)の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] ike proposal [<proposal_number>]prf <prf>

[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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<proposal_number>

・ Proposal定義番号
Proposal定義番号を、0～2の10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。

<prf>

Pseudo Random Functionについて指定します。

・ hmac-md5
・ hmac-sha1
・ hmac-sha256
・ hmac-sha384
・ hmac-sha512

[動作モード]

構成定義モード(管理者クラス)

[説明]

IKE Version2セッションの鍵生成で使用される疑似乱数関数のハッシュ関数の設定を行います。

[注意]

本設定は、IKE Version2(remote ap ipsec type ikev2)の設定をした場合のみ有効です。

[未設定時]

IKE Version2セッション用prf(Pseudo Random Function)に指定がされません。
IKE Version2を使用する場合は必ず設定してください。

10.2.59 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

10.2.60 remote ap ike idtype

[機能]

IKE Version1 情報の送信 ID タイプの設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
・ x501_sbj
X.501 証明書対象者名

[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。

[注意]

<id_type>に x501_sbj を設定する場合は、Aggressive モードで使用することはできません。
本設定は IKE Version1(remote ap ipsec type ike)のみ有効となります。

[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
```

10.2.61 remote ap ike eap auth send

[機能]

IKE Version2 情報の EAP 認証機能の送信認証情報の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] ike eap 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<id>

・ 認証 ID
認証 ID を、0x21,0x23～0x7e の文字で構成される 128 文字以内の文字列で指定します。

<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 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文字列を encrypted と共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 128 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

・ 暗号化された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]

IKE Version2 情報の EAP 認証機能で利用する送信認証情報(認証 ID およびパスワード)を設定します。

[注意]

EAP 認証機能を利用する場合、IKE Version2 情報で IKE ネゴシエーションを行う必要があります。
認証 ID およびパスワードが設定されていない場合、IKE ネゴシエーションが失敗します。
show 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]

IKE Version2 情報で送信する認証情報は定義しないものとみなされます。

10.2.62 remote ap ike ts multi

[機能]

IKE Version2 情報の Traffic Selector 複数設定の利用可否の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] ike ts multi <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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

- disable
  複数設定を利用しません。
- enable
  複数設定を利用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IKE Version2 情報の Traffic Selector 複数設定を使用するかどうか設定します。
複数設定を使用する場合、remote ap ipsec extension-range コマンドで設定した IPsec 対象範囲の Traffic Selector を生成します。

[注意]

- 本設定は IKE Version2(remote ap ipsec type ikev2)のみ有効となります。
- 複数設定を使用しない場合は、remote ap ipsec extension-range コマンドの設定にかかわらず、Traffic Selector は 1 つしか生成されません。
- 複数設定を使用しない場合でも、複数設定された Traffic Selector を受信することは可能です。ただし、remote ap ipsec extension-range コマンドの設定にかかわらず、IPsec 対象範囲は 1 つとなります。
- 本設定を有効にする場合は、remote ap ipsec extension-range コマンドの設定が必要です。
  remote ap ipsec extension-range コマンドを設定しない場合は、Traffic Selector は 1 つしか生成されません。
- Traffic Selector 数を複数送受信する場合は、拡張 IPsec 対象範囲(remote ap ipsec extension-range コマンド)は、0～45 の範囲内で定義してください。

[未設定時]

IKE Version2 情報の Traffic Selector 複数設定を使用しないものとみなされます。

```
remote <number> ap <ap_number> ike ts multi disable
```

10.2.63 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<name>

・ 自装置識別情報
自装置を識別する名前を、1～128 文字で指定します。
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 Version1(remote ap ipsec type ike)の場合
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。
・ IKE Version2(remote ap ipsec type ikev2)の場合
IKE Version2 用自装置 ID タイプ設定に address, x501_sbj 以外の設定をした場合に識別情報の設定を行います。
ただし、IKE Version2 用 EAP 認証機能を使用した場合は、EAP 認証 ID が識別情報として利用されます。

[注意]

・ IKE Version1 の場合で、Aggressive Mode(Initiator)により鍵交換を行う場合は必ず設定してください。
・ IKE Version2 の場合で、IKE Version2 用自装置 ID タイプ設定に address, x501_sbj 以外の設定をした場合は必ず設定してください。
ただし、IKE Version2 用 EAP 認証機能を使用した場合は、EAP 認証 ID が識別情報として利用されますので設定の必要はありません。

[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。
IKE Version1 の場合で、Aggressive Mode(Initiator)により鍵交換を行う場合は必ず設定してください。

IKE Version2 の場合で、IKE Version2 用自装置 ID タイプ設定に address, x501_sbj 以外の設定をした場合は必ず設定してください。

10.2.64 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<name>

・ 相手装置識別情報
相手装置を識別する名前を、1～128 文字で指定します。
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 Version1(remote ap ipsec type ike)の場合
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。
・ IKE Version2(remote ap ipsec type ikev2)の場合
IKE Version2 用相手装置 ID タイプ設定に address, x501_sbj 以外の設定をした場合に識別情報の設定を行います。

[注意]

・ IKE Version1 の場合で、Aggressive Mode(Responder)により鍵交換を行う場合は必ず設定してください。
・ IKE Version2 の場合で、IKE Version2 用相手装置 ID タイプ設定に address, x501_sbj 以外の設定をした場合は必ず設定してください。

[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。
IKE Version1 の場合で、Aggressive Mode(Responder)により鍵交換を行う場合は必ず設定してください。
IKE Version2 の場合で、IKE Version2 用相手装置 ID タイプ設定に address, x501_sbj 以外の設定をした場合は必ず設定してください。

10.2.65 remote ap ike release

[機能]

IPsec/IKE 情報の解放動作の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、相手側エンドポイントアドレスに対する経路情報が存在する場合で以下の回線切断動作時に有効です。

・ PPPoE を使用したときの切断時
・ データ通信モジュールを使用したときの切断時

[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
```

10.2.66 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、相手側エンドポイントアドレスに対する経路情報があらかじめ存在する場合で以下の回線接続時に有効です。

・ PPPoE を使用したとき
・ データ通信モジュールを使用したとき

[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
```

10.2.67 remote ap ike mode

[機能]

IKE Version1 情報の交換モードの設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 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)	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。

※mode が aggressive モードの場合は、idtype に x501_sbj を指定することはできません。

*1 初期動作として Initiator、Responder 両方の動作が可能です。

[注意]

本設定は IKE Version1(remote ap ipsec type ike)のみ有効となります。

[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。

```
remote <number> ap <ap_number> ike mode auto
```

10.2.68 remote ap ike bind

[機能]

利用 IKE 情報の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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を、0 以上の 10 進数で指定します。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。

・ IKE Version1 を使用した場合
- 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 certificate local
- remote ap ike certificate remote
- remote ap ike certificate key
- remote ap ike certificate expired
- remote ap ike certificate send
- remote ap ike certificate request
- remote ap ike dpd use
- remote ap ike dpd idle
- remote ap ike dpd retry
- remote ap ike dpd anti-replay
- remote ap tunnel local
- remote ap tunnel remote

・IKE Version2を使用した場合

- 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 local-idtype
- remote ap ike remote-idtype
- remote ap ike remote-id-send
- remote ap ike name local
- remote ap ike name remote
- remote ap ike release
- remote ap ike initial
- remote ap ike certificate local
- remote ap ike certificate remote
- remote ap ike certificate key
- remote ap ike certificate expired
- remote ap ike certificate send
- remote ap ike certificate request
- remote ap ike eap auth send
- remote ap ike ts multi
- remote ap ike dpd use
- remote ap ike dpd idle
- remote ap ike dpd retry
- remote ap ike dpd anti-replay
- 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
```

10.2.69 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 Version1 のみの注意事項

・ 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 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。

IKE Version1 および IKE Version2 共通の注意事項

- 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。
- 自側および相手側トンネルエンドポイントアドレスに IPv6 アドレスを設定した場合は動作しません。
- IKE モードが Aggressive Mode 設定で、自側および相手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
```

10.2.70 remote ap ike certificate remote

[機能]

IKE セッション用相手装置証明書情報

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] ike certificate remote <cert_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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<cert_number>

・ 相手装置証明書識別番号
相手装置証明書の識別番号を、10 進数で指定します。
crypto certificate remote コマンドで取り込んだ相手装置証明書の識別番号を指定してください。
機種ごとの相手装置証明書識別番号の範囲は以下のとおりです。

範囲	機種
0～49	Si-R G110

[動作モード]

構成定義モード(管理者クラス)

[説明]

相手装置証明書の設定を行います。

[未設定時]

・ IKE Version1 の場合
IKE の認証方式として RSA デジタル署名が設定されている場合、Main モードでは IKE ネゴシエーションで受信した ID(IP アドレスまたは FQDN)でサブジェクト代替名称(IP アドレスまたはドメイン名または証明書対象者名)と一致する相手装置証明書を使用します。
Aggressive モードでは IKE ネゴシエーション内の ID(IP アドレスまたは FQDN)でサブジェクト代替名称(IP アドレスまたはドメイン名)と一致する相手装置証明書を使用します。

・ IKE Version2 の場合
IKE の認証方式として RSA デジタル署名が設定されている場合、IKE ネゴシエーションで受信した ID でサブジェクト代替名称と一致する相手装置証明書を使用します。

10.2.71 remote ap ike certificate local

[機能]

IKE セッション用自装置証明書情報

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] ike certificate local <cert_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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<cert_number>

・ 自装置証明書識別番号
自装置証明書の識別番号を、0～4 の 10 進数で指定します。
crypto certificate generate コマンドで設定、または crypto certificate local コマンドで取り込んだ自装置証明書の識別番号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]

自装置証明書の設定を行います。

[注意]

必ず秘密鍵に合った鍵ペアの自装置証明書を設定してください。

[未設定時]

IKE セッション用自装置証明書情報に指定がされません。
認証方式として RSA デジタル署名方式を使用する場合は必ず設定してください。

10.2.72 remote ap ike certificate key

[機能]

IKE セッション用秘密鍵情報

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] ike certificate key <key_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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<key_number>

・ 秘密鍵識別番号
秘密鍵の識別番号を、0～4 の 10 進数で指定します。
crypto certificate generate コマンドで設定した秘密鍵の識別番号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]

秘密鍵の設定を行います。

[注意]

必ず自装置証明書に合った鍵ペアの秘密鍵を設定してください。

[未設定時]

IKE セッション用秘密鍵情報に設定がされません。
認証方式として RSA デジタル署名方式を使用する場合は必ず設定してください。

10.2.73 remote ap ike certificate expired

[機能]

IKE セッション用有効期限切れ証明書の使用の有無

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] ike certificate expired <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

・ use
有効期限が切れている証明書を使用します。
・ unuse
有効期限が切れている証明書を使用しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

有効期限が切れている証明書を使用するかどうかを設定します。
<mode>が use の場合、有効期限が切れている証明書をそのまま使用します。
<mode>が unuse の場合、有効期限が切れている証明書を使用しません。この場合 IKE ネゴシエーションが失敗します。

[注意]

認証局証明書の有効期限切れチェックは、自装置が証明書要求ペイロードを送信するときのみ行っています。

[未設定時]

有効期限が切れている証明書を使用するものとみなされます。

```
remote <number> ap <ap_number> ike certificate expired use
```

10.2.74 remote ap ike certificate send

[機能]

IKE セッション用自装置証明書情報の送信

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] ike certificate send <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<action>

・ reply
相手装置から証明書要求ペイロードを受信したときに、自装置証明書情報を送信する場合に指定します。
・ enable
相手装置から証明書要求ペイロードの受信にかかわらず、常に自装置証明書情報を送信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]

自装置証明書の送信設定を行います。

[未設定時]

IKE セッション用自装置証明書情報の送信設定に reply を指定したものとみなされます。

```
remote <number> ap <ap_number> ike certificate send reply
```

10.2.75 remote ap ike certificate request

[機能]

IKE セッション用証明書要求の送信

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] ike certificate request <action> [<ca_cert>]

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<action>

・ enable
証明書要求を送信する場合に指定します。
・ disable
証明書要求を送信しない場合に指定します。

<ca_cert>

・ 送信する認証局の識別番号
認証局の識別番号を、0～4 の 10 進数で指定します。
crypto certificate ca コマンドで設定した認証局の識別番号を指定してください。
(※certificate request が enable の場合のみ有効)
省略時は、送信する認証局情報がないものとみなします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

証明書要求の送信設定を行います。

[未設定時]

送信する認証局情報がない、証明書要求を送信するを指定したものとみなされます。

```
remote <number> ap <ap_number> ike certificate request enable
```

10.2.76 remote ap ike local-idtype

[機能]

IKE Version2 情報の自装置 ID タイプの設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] ike local-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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<id_type>

ネゴシエーションの自装置 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
・ x501_sbj
X.501 証明書対象者名
・ address
IPv4 アドレス、または、IPv6 アドレス

[動作モード]

構成定義モード(管理者クラス)

[説明]

IKE Version2 セッションを確立するネゴシエーションの自装置 ID タイプの設定を行います。

IKE Version2 セッション確立のネゴシエーションパケットの ID ペイロードに使用されます。

<id_type>に fqdn,user_fqdn または x501_sbj を設定した場合は、IKE 情報の自装置識別情報の設定(remote ap ike name local)が必須となります。また、address を設定した場合は、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(remote ap tunnel local)が必須となります。

[注意]

本設定は IKE Version2(remote ap ipsec type ikev2)のみ有効となります。

また、IKE Version2(remote ap ipsec type ikev2)の EAP 認証機能利用時に限り、<id_type>は fqdn,user_fqdn のみ有効となります。

[未設定時]

IKE Version2 セッション確立のネゴシエーションパケットの自装置 ID タイプを設定しないものとみなされます。

10.2.77 remote ap ike remote-idtype

[機能]

IKE Version2 情報の相手装置 ID タイプの設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] ike remote-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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<id_type>

ネゴシエーションの相手装置 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
・ x501_sbj
X.501 証明書対象者名
・ address
IPv4 アドレス、または、IPv6 アドレス

[動作モード]

構成定義モード(管理者クラス)

[説明]

IKE Version2 セッションを確立するネゴシエーションの相手装置 ID タイプの設定を行います。

IKE Version2 セッション確立のネゴシエーションパケットの ID ペイロードに使用されます。

<id_type>に fqdn,user_fqdn または x501_sbj を設定した場合は、IKE 情報の相手装置識別情報の設定(remote ap ike name remote)が必須となります。また、address を設定した場合は、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(remote ap tunnel remote)が必須となります。

[注意]

本設定は IKE Version2(remote ap ipsec type ikev2)のみ有効となります。

また、IKE Version2(remote ap ipsec type ikev2)の EAP 認証機能利用時に限り、<id_type>は fqdn,user_fqdn のみ有効となります。

[未設定時]

IKE Version2 セッション確立のネゴシエーションパケットの相手装置 ID タイプを設定しないものとみなされます。

10.2.78 remote ap ike remote-id-send

[機能]

IKE Version2 情報の相手装置 ID 送信の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] ike remote-id-send <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<id_type>

ネゴシエーションの相手装置 ID を送信するかどうか指定します。

・ disable
相手装置 ID を送信しません。

・ enable
相手装置 ID 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]

IKE Version2 セッションを確立するネゴシエーションの Initiator 装置が相手装置 ID を送信するかどうかの設定を行います。

<mode>に enable を設定した場合に Initiator 装置が IKE ネゴシエーション内に相手装置 ID を含めて送信します。受信した Responder 側装置は、Initiator/Responder 装置の ID と一致するものが装置内部に存在するかを検索して相手装置との整合性を確認します。

<mode>に disable を設定した場合は相手装置 ID を送信しません。

[注意]

本設定は IKE Version2(remote ap ipsec type ikev2)のみ有効となります。

[未設定時]

IKE Version2 情報の相手装置 ID 送信の設定に off を指定したものとみなされます。

```
remote <number> ap <ap_number> ike remote-id-send disable
```

10.2.79 remote ap ike dpd use

[機能]

IKE 情報の Dead Peer Detection(DPD)利用可否の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] ike dpd 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

・ off
DPD を利用しません。
・ on
DPD 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]

IKE で DPD を利用する設定を行います。

[注意]

IKEv1 で DPD 機能を使用する場合は、相手装置の DPD 機能設定も有効にしてください。

[未設定時]

IKE 情報の DPD 利用に off を指定したものとみなされます。

```
remote <number> ap <ap_number> ike dpd use off
```

10.2.80 remote ap ike dpd idle

[機能]

IKE 情報の Dead Peer Detection(DPD)パケット送信を開始する無通信監視時間の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] ike dpd idle <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<time>

・ 無通信監視時間
無通信監視時間を、5～600 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。

[動作モード]

構成定義モード(管理者クラス)

[説明]

DPD パケット送信を開始する IPsec 受信パケット無通信監視時間の設定を行います。

[未設定時]

無通信監視時間に 10 秒を設定したものとみなされます。

```
remote <number> ap <ap_number> ike dpd idle 10s
```

10.2.81 remote ap ike dpd retry

[機能]

IKE 情報の Dead Peer Detection(DPD)再送時間／回数の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] ike dpd 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<time>

・ 再送時間
再送時間を、1～60 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]

DPD パケットに対する再送時間および再送回数の設定を行います。

[注意]

DPD パケットの再送時間と再送回数は、「DPD パケット送信を開始する IPsec 受信パケット無通信監視時間」より短い時間を設定してください。

再送時間×(再送回数＋ 1)＜無通信監視時間

その範囲を超えた場合は、定義反映時に設定エラーとなります。

[未設定時]

再送時間に 1 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 dpd retry 1s 3
```

10.2.82 remote ap ike dpd anti-replay

[機能]

IKE 情報の Dead Peer Detection(DPD)リプレイ攻撃防御機能の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] ike dpd anti-replay <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

・ リプレイ攻撃防御機能
DPD メッセージリプレイ攻撃防御機能の使用有無を指定します。
－ enable
リプレイ攻撃防御機能を使用します。
－ disable
リプレイ攻撃防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]

DPD メッセージ機能の利用時、DPD メッセージパケット受信時でリプレイ攻撃防御機能を使用するかどうかの設定を行います。

[注意]

リプレイ攻撃防御機能を使用しない場合は、重複攻撃(なりすまし)などによる検出が行えなくなるため、セキュリティが弱くなります。

[未設定時]

リプレイ攻撃防御機能を使用するものとみなされます。

```
remote <number> ap <ap_number> ike dpd anti-replay enable
```

10.2.83 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 G110

[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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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進数で指定します。

範囲	機種
0～1	Si-R G110

[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。

10.2.84 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 G110

[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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、0～19の10進数で指定します。
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 接続をするときは、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。

10.2.85 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 G110

[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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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とき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ときの相手側ユーザ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。

10.2.86 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 G110

[入力形式]

```
remote [<number>] ap [<ap_number>] tunnel local <address>
remote [<number>] ap [<ap_number>] tunnel local <fqdn>
```

[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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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～rmt99	Si-R G110

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

```
dhcp@rmt0::
dhcp@rmt0::1:2:3:4
```

RA で取得した IP アドレスを自動設定する場合は"ra@インタフェース名"の形式で指定します。

インタフェース名（lan インタフェース）の指定方法の詳細については、本章の冒頭を参照してください。

例)

lan0 で動作する RA が取得した IP アドレスを使用する場合

```
ra@lan0
```

<fqdn>

・ 自側のトンネルエンドポイントのFQDN

自側のトンネルエンドポイントの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。

[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。

FQDNを指定する場合、以下のことに注意してください。

・ remote ap datalink typeの<type>でipsecを指定してください。

・ remote ap ipsec typeの<type>でikeまたは、ikev2または、dvpnを指定してください。

・ 名前解決したネットワークアドレスがIPv6アドレスの時のみ利用できます。

以下の場合、IEKv1かつAggressive Modeを設定することを推奨します。

・ FQDNを指定する場合。

・ raを指定する場合。

[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。

10.2.87 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 G110

[入力形式]

remote [<number>] ap [<ap_number>] tunnel remote <address>
remote [<number>] ap [<ap_number>] tunnel remote <fqdn>

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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

<fqdn>

・ 相手側のトンネルエンドポイントの FQDN
相手側のトンネルエンドポイントの 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。

[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。

[注意]

FQDN を指定する場合、以下のことに注意してください。

・ remote ap datalink type の<type>で ipsec を指定してください。
・ remote ap ipsec type の<type>で ike または、ikev2 または、dvpn を指定してください。

・ 名前解決したネットワークアドレスが IPv6 アドレスの時のみ利用できます。

以下の場合、IEKv1 かつ Aggressive Mode を設定することを推奨します。

・ FQDN を指定する場合。

・ ra を指定する場合。

[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。

10.2.88 remote ap tunnel mtu

[機能]

トンネル利用時の送信パケット最大長(MTU 値)の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] tunnel 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mtu>

・ MTU 値
MTU 値を、1280～1560 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]

トンネル利用時の送信パケット最大長(MTU 値)を設定します。
本設定は、IPv6 トンネル設定時のみ有効です。

[未設定時]

MTU 値に 1280 を指定したものとみなされます。

```
remote <number> ap <ap_number> tunnel mtu 1280
```

10.2.89 remote ap overlap to

[機能]

overlap ap の実際の送出先の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。

範囲	機種
0～19	Si-R G110

・ remote 定義の定義番号
利用する remote の定義番号を、10 進数で指定します。
ただし、<number>と同じ値は指定できません。

範囲	機種
0～99	Si-R G110

[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。

10.2.90 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 G110

[入力形式]

remote [<number>] ap [<ap_number>] overlap nexthop <address>
remote [<number>] ap [<ap_number>] overlap nexthop dhcp

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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

dhcp

転送先として、DHCP クライアントで取得したルータオプションのルータ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]

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。

10.2.91 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

10.2.92 remote ap sessionwatch address

[機能]

接続先監視のアドレス設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 アドレスのいず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］

指定した送信元 IP アドレスを持つインタフェースが利用不可能な状態の場合は、通信に利用できません。

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。

IPsec 情報のタイプ設定で dvpn を指定(remote ap ipsec type dvpn)した場合は、動的 VPN 情報交換では本設定の ICMP ECHO パケットの送信元 IP アドレスを通知します。また、動的 VPN 接続で接続相手から監視先アドレスを通知されても使用しないで、本設定の ICMP ECHO パケットのあて先 IP アドレスに対して監視を行います。

以下の場合では、監視を行いません。

・ 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。

10.2.93 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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～3600 秒(1 時間)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、1 秒～3600 秒(1 時間)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ときの 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ときを復旧とみなし、正常時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。

・ 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]

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
```

10.2.94 remote ap sessionwatch ttl

[機能]

接続先監視の TTL/HopLimit 値設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<send_ttl>

・ 送信 TTL / HopLimit 値
ICMP ECHO パケットを送信するときの 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。
・ 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]

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
```

10.2.95 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

・ 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]

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
```

10.2.96 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 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]

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。

・ 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]

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
```

10.2.97 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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)のいずれかを指定します。

[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。
・ 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]

```
remote <number> ap <ap_number> sessionwatch error-wait 0s
```

10.2.98 remote ap snmp trap linkdown

[機能]

linkDown トラップの設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] snmp trap linkdown <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

トラップの動作を指定します。

・ disable
トラップを無効にします。

・ enable
トラップを有効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

linkDown トラップを有効または無効にするかを設定します。

[注意]

snmp trap linkdown コマンドで trap 動作が無効にされた場合は、本コマンド設定値は意味を持ちません。

[未設定時]

linkDown トラップが無効とみなされます。

```
remote <number> snmp trap linkdown disable
```

10.2.99 remote ap snmp trap linkup

[機能]

linkUp トラップの設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ap [<ap_number>] snmp trap linkup <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

トラップの動作を指定します。

・ disable
トラップを無効にします。

・ enable
トラップを有効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

linkUp トラップを有効または無効にするかを設定します。

[注意]

snmp trap linkup コマンドで trap 動作が無効にされた場合は、本コマンド設定値は意味を持ちません。

[未設定時]

linkUp トラップが無効とみなされます。

```
remote <number> snmp trap linkup disable
```

10.3 PPP 関連情報

10.3.1 remote ppp ipcp vjcomp

[機能]

VJ-Compression の利用の有無の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

```
remote <number> ppp ipcp vjcomp enable
```

10.3.2 remote ppp ipcp iphc

[機能]

IPv4 の IP ヘッダ圧縮(IPHC)の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

・ disable
IP ヘッダ圧縮を使用しない場合に指定します。
・ enable
IP ヘッダ圧縮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]

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。

```
remote <number> ppp ipcp iphc disable
```

10.3.3 remote ppp ipv6cp iphc

[機能]

IPv6 の IP ヘッダ圧縮(IPHC)の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

・ disable
IP ヘッダ圧縮を使用しない場合に指定します。
・ enable
IP ヘッダ圧縮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]

IPv6 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]

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
```

10.4 IP関連情報

10.4.1 remote ip address local

[機能]

自側IPアドレスの設定

[適用機種]

Si-R G110

[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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

10.4.2 remote ip address remote

[機能]

相手側 IP アドレスの設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

10.4.3 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。

範囲	機種
0～255	Si-R G110

<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、1～14 の 10 進数で指定します。
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、1～254 の 10 進数で指定します。
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、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。

<distance>で指定した優先度は、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。

IPv4 スタティック経路を以下のように使用できます。

・ 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できます。

  RIP テーブルには、設定した RIP メトリック値+1 のメトリック値で登録されます。

・ 複数のスタティック経路情報で ECMP 機能を使用できます。このとき、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
256	Si-R G110

[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使用しないものとみなされます。

10.4.4 remote ip rip use

[機能]

RIP 基本情報の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、0～14 の 10 進数で指定します。

<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。

たとえば、RIP テーブルのメトリック値が 3 の場合、<metric>に 0 を指定するとメトリックは 3 で広報され、1 を指定すると、4 で広報されます。

なお、受信側の装置では、通常、受信したメトリックに 1 を加算した値で RIP テーブルに登録します。

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
120	Si-R G110

[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 と併用できません。

[未設定時]

RIP 機能を使用しないものとみなされます。

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

10.4.5 remote ip rip filter act

[機能]

RIP フィルタ動作の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

範囲	機種
0～399	Si-R G110

<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
400	Si-R G110

［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で、遮断条件だけを設定した場合、すべての経路情報は遮断されます。
送受信する経路情報が存在する場合、透過条件に対象の経路情報を設定してください。

［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。

10.4.6 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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-R G110

[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。

10.4.7 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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-R G110

<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
<address>/<mask>で指定した経路情報を本装置が保有する経路情報と比較し、完全一致したものをフィルタリング対象とします。

・ inexact
指定した<address>の先頭から<mask>ビット部分だけを本装置が保有する経路情報と比較し、一致したものを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。

・<prefix_match>は以下のように動作します。

<address>/<mask>で"192.168.0.0/16"を指定し、本装置が以下の経路情報を保有している場合、exact を指定すると、"192.168.0.0/16"がフィルタリング対象となります。

inexact を指定すると、"192.168.0.0"と一致する"192.168.0.0/16、192.168.1.0/24、192.168.1.1/32"の 3 つがフィルタリング対象となります。

172.16.0.0/16
192.168.0.0/16
192.168.1.0/24
192.168.1.1/32

[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。

10.4.8 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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-R G110

<metric>

・ メトリック値
メトリック値を、0～15 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]

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 1～15 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。

10.4.9 remote ip ospf use

[機能]

OSPF 利用可否の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～2	Si-R G110

[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-R G110

[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
```

10.4.10 remote ip ospf cost

[機能]

OSPF 出力コストの設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 1 が設定されているものとみなされます。

```
remote <number> ip ospf cost 1
```

10.4.11 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 G110

[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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<hello_interval>

・ Helloパケット送信間隔
Helloパケットの送信間隔時間を、1～65535秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
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
```

10.4.12 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、1～65535 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
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
```

10.4.13 remote ip ospf retrans

[機能]

OSPF パケット再送間隔の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<retransmit_interval>

・ パケット再送間隔
パケットの再送間隔を、3～65535 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
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
```

10.4.14 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、1～65535 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
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
```

10.4.15 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

10.4.16 remote ip ospf auth textkey

[機能]

OSPF テキスト認証鍵の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

10.4.17 remote ip ospf auth md5key

[機能]

OSPF MD5 認証鍵情報の設定

[適用機種]

Si-R G110

[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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

10.4.18 remote ip ospf passive

[機能]

OSPF パケット送信抑止の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<interface_type>

・ off
パケットの送信を抑止しません。

・ on
パケットの送信を抑止します。

[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
```

10.4.19 remote ip ospf multicast

[機能]

OSPF 送信方法の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

10.4.20 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

10.4.21 remote ip nat mode

[機能]

アドレス変換の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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>

・ 割り当て時間
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)のいずれかを指定します。
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
```

10.4.22 remote ip nat static

[機能]

静的アドレス変換の設定

[適用機種]

Si-R G110

[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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。

範囲	機種
0～199	Si-R G110

<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
200	Si-R G110

[未設定時]

静的アドレス変換は設定されません。

10.4.23 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

・ reject
該当するパケットを破棄します。

・ 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。

[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
```

10.4.24 remote ip nat rule

[機能]

アドレス変換ルールの設定

[適用機種]

Si-R G110

[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>
```

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

・変換ルール番号
変換ルール番号を、0～31 の 10 進数で指定します。

ftp, irc, dns, sip, mldt, ipbs

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。

10.4.25 remote ip nat wellknown

[機能]

ポート番号変換の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

ポート番号変換定義番号を、0～99 の 10 進数で指定します。

<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)
```

10.4.26 remote ip nat destination

[機能]

あて先変換の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～199	Si-R G110

<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
200	Si-R G110

[未設定時]

あて先変換は設定されません。

10.4.27 remote ip nat appli

[機能]

アプリ対応の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。
・ 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。

<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]

アプリ対応を以下のように指定したものとみなされます。

```
remote <number> ip nat appli ftp on
remote <number> ip nat appli sip on
remote <number> ip nat appli dns on
remote <number> ip nat appli snmp on
```

10.4.28 remote ip filter

[機能]

IP フィルタの設定

[適用機種]

Si-R G110

[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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～199	Si-R G110

<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
0～999	Si-R G110

<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
200	Si-R G110

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
3000	Si-R G110

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。

・ <dst_addr>/<mask>に"dynamic"を指定した ACL は使用しないでください。

[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。

10.4.29 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～199	Si-R G110

[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。

10.4.30 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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>

・ 割り当て時間
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)のいずれかを指定します。
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
```

10.4.31 remote ip tos

[機能]

TOS 値書き換え条件の設定

[適用機種]

Si-R G110

[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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～99	Si-R G110

<acl_count>

・ ACL 定義番号

使用する ACL 定義の番号を、10 進数で指定します。

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
0～999	Si-R G110

<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
100	Si-R G110

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
3000	Si-R G110

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]

<dst_addr>/<mask>に"dynamic"を指定した ACL は使用しないでください。

[未設定時]

TOS 値書き換えを行わないものとみなされます。

10.4.32 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～99	Si-R G110

[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。

10.4.33 remote ip priority

[機能]

帯域制御の設定

[適用機種]

Si-R G110

[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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

・ 帯域制御定義番号

帯域制御定義番号を、10 進数で指定します。

範囲	機種
0～99	Si-R G110

<acl_count>

・ ACL 定義番号

使用する ACL 定義の番号を、10 進数で指定します。

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、ipv6 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-R G110

<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～1000000kbps または 1mbps～1000mbps 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。
<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。
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
100	Si-R G110

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
3000	Si-R G110

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 Ethernet 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。
・ <dst_addr>/<mask>に"dynamic"を指定した ACL は使用しないでください。

[未設定時]

帯域制御を行わないものとみなされます。

10.4.34 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<in-policy_number>

・ Ingress ポリシールーティング定義番号
このインタフェースでの Ingress ポリシールーティング定義の通し番号を、10 進数で指定します。
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
200	Si-R G110

<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
0～99	Si-R G110

[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。

10.4.35 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

10.4.36 remote ip msschange

[機能]

MSS 書き換えの設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mss>

・ MSS 値
MSS の書き換え値を、0 または 160～1460 の 10 進数で指定します。
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
```

10.4.37 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

10.4.38 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

10.4.39 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 G110

[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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

```
remote <number> ip multicast pim preference 1024
```

10.4.40 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 G110

[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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

10.4.41 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 G110

[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>
remote [<number>] ip dvpn <count> autoignore

[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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～2999	Si-R G110

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。

autoignore

接続先情報の動的VPN接続後に相手装置から通知されたネットワークの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
0～999	Si-R G110

<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進数で指定します。

<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。

範囲	機種
0～1	Si-R G110

[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。

autoignore を指定した場合は、相手装置から通知されたネットワークをテンプレート情報の動的 VPN 接続対象外とし、INVITE 要求を発行しません。

また、対象の相手情報を通過するセッション監視についても、動的 VPN 接続対象外とし、INVITE 要求を発行しません。

[注意]

- 本コマンドの autoignore を指定した場合に相手装置から通知されたネットワーク情報内の all-0(0.0.0.0/0)は autoignore 対象外とします。
- <dst_addr>/<mask>に"dynamic"を指定した ACL は使用しないでください。

[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。

10.4.42 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～2999	Si-R G110

[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を変更します。

10.4.43 remote ip ids use

[機能]

IDS の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

```
remote <number> ip ids use off
```

10.5 IPv6 関連情報

10.5.1 remote ipv6 use

[機能]

IPv6 機能の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

IPv6 パケットの送受信を行うかどうかを指定します。

・ 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。

・ 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。

[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> ipv6 use off
```

10.5.2 remote ipv6 ifid

[機能]

IPv6 インタフェース ID の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 上で他装置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> ipv6 ifid auto
```

10.5.3 remote ipv6 address

[機能]

IPv6 アドレスの設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 address [<count>] <address>/<prefixlen>
remote [<number>] ipv6 address [<count>] <anycast_address>/<prefixlen>

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
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。
プレフィックス長には 64 を指定してください。
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、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～rmt99	Si-R G110

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
dhcp@rmt0::/64
または、
dhcp@rmt0::1:2:3:4/64

・ auto
RA(Router Advertisement) メッセージで受信したプレフィックスを使用して自動的にアドレスを設定する場合に指定します。
remote ipv6 ra mode recv を設定する必要があります。

<anycast_address>/<prefixlen>

・ IPv6 エニキャストアドレス/プレフィックス長
エニキャストアドレスを指定します。プレフィックス長には 128 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]

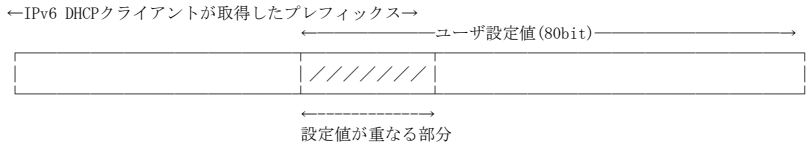
このインタフェースの IPv6 アドレスを設定します。

<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。

<anycast_address>の指定では、インタフェース ID によるアドレス生成は行われません。

[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。



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

エニキャストアドレスはほかのアドレスと重複設定できません。

[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。

10.5.4 remote ipv6 ra mode

[機能]

RA(Router Advertisement) メッセージの動作設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

・ off
RA メッセージの送受信機能を無効にします。
・ recv
RA メッセージの受信機能を有効にします。
・ send
RA メッセージの送信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]

RA メッセージの送受信機能を設定します。設定機能は以下のとおりです。

・ RA メッセージ受信機能
有効な場合、RA メッセージをもとに ND(Neighbor Discovery)のパラメタ、デフォルトルート、およびグローバルアドレスを自装置に自動設定することができます。
グローバルアドレスの自動設定を行う場合は、"remote ipv6 address auto"を設定します。
・ RA メッセージ送信機能
有効な場合、自装置に定義したプレフィックス情報などを広報することができます。

[未設定時]

RA メッセージの送受信機能が無効とみなされます。

```
remote <number> ipv6 ra mode off
```

10.5.5 remote ipv6 ra interval

[機能]

RA(Router Advertisement)メッセージ送信間隔の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<max>

・ 最大送信間隔
RA メッセージを定期送信する場合の最大送信間隔(秒)を、4～1800 の 10 進数で指定します。

<min>

・ 最小送信間隔
RA メッセージを定期送信する場合の最小送信間隔(秒)を、3～<max>×3/4 の 10 進数で指定します。

<lifetime>

・ Router Lifetime の値
送信する RA メッセージの Router Lifetime の値を、0 または<max>～9000 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]

RA メッセージの送信間隔、および RA メッセージの Router Lifetime の値の設定を行います。RA メッセージは<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> ipv6 ra interval 600 200 1800
```

10.5.6 remote ipv6 ra mtu

[機能]

RA(Router Advertisement)メッセージに含める MTU option の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mtu>

・ MTU option の内容
RA メッセージに含める MTU option の値を、0 または 1280～1500 の 10 進数で設定します。
0 を指定した場合は、RA メッセージに 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 メッセージに含める MTU option の値を設定します。

[未設定時]

送信する RA メッセージに MTU option を含めないものとみなされます。

```
remote <number> ipv6 ra mtu 0
```

10.5.7 remote ipv6 ra reachabletime

[機能]

RA(Router Advertisement)メッセージに含める Reachable Time の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<time>

・ Reachable Time の値
RA メッセージに含める Reachable Time の値(ミリ秒)を、0～3600000 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]

RA メッセージに含める Reachable Time の値(ミリ秒)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> ipv6 ra reachabletime 0
```

10.5.8 remote ipv6 ra retranstimer

[機能]

RA(Router Advertisement)メッセージに含める Retrans Timer の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<time>

・ Retrans Timer の値
RA メッセージに含める Retrans Timer の値(ミリ秒)を、0～4294967295 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]

RA メッセージに含める Retrans Timer の値(ミリ秒)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> ipv6 ra retranstimer 0
```

10.5.9 remote ipv6 ra curhoplimit

[機能]

RA(Router Advertisement)メッセージに含める Cur Hop Limit の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<CurHopLimit>

・ Cur Hop Limit の値
RA メッセージに含める Cur Hop Limit の値を、0～255 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]

RA メッセージに含める 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> ipv6 ra curhoplimit 64
```

10.5.10 remote ipv6 ra flags

[機能]

RA(Router Advertisement)メッセージに含める flags field の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<flags>

・ flags field の値
RA メッセージに含める flags field の値を、00～ff の 16 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]

RA メッセージに含める 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> ipv6 ra flags 00
```

10.5.11 remote ipv6 ra prefix

[機能]

RA(Router Advertisement)メッセージに含める広報プレフィックス情報の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 ra prefix [<count>] <prefix>/<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

・ 広報プレフィックス定義番号
広報プレフィックスの定義番号を、0～3 の 10 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。

<prefix>/<prefixlen>

・ 広報プレフィックス/プレフィックス長
広報プレフィックスとプレフィックス長を指定します。
リンクローカルスコープのプレフィックスは指定できません。
プレフィックス長には 64 を指定してください。
IPv6 DHCP クライアントが取得したプレフィックスを指定する場合は上位を"dhcp@インタフェース名"の形式で指定し、下位 80 ビット分を IPv6 アドレス形式で指定します。インタフェース名には、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～rmt99	Si-R G110

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:

dhcp@rmt0::/64
または、
dhcp@rmt0::1:2:3:4/64

<valid>

・ valid lifetime の時間
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)のいずれかを指定します。

・ infinity
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。

<prefix>/<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。

<preferred>

・ preferred lifetime の時間
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)のいずれかを指定します。

・ infinity

このプレフィックスに対するpreferred lifetimeを無限とする場合に指定します。

<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。

<prefix>/<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。

<flags>

・ RA Prefix Informationに付与されるフラグ

このprefixに対するflagsフィールドの値を、0～ffの16進数で指定します。

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]

RAメッセージに含める広報プレフィックス情報を設定します。

remote ipv6 addressで定義したアドレスプレフィックスから、広報したいプレフィックスと同じ情報を指定してください。アドレスプレフィックスに一致しないものは広報されません。

[未設定時]

送信するRAメッセージに広報プレフィックス情報を含めないものとみなされます。

10.5.12 remote ipv6 ra trigger ifdown

[機能]

RA(Router Advertisement)メッセージでのインタフェースダウントリガの設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 ra trigger ifdown [<count>] <interface>

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

・ トリガ定義番号
インタフェースダウントリガの定義番号を、0～3 の 10 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。

<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～rmt99	Si-R G110

[動作モード]

構成定義モード(管理者クラス)

[説明]

デフォルトルータ広報に関するインタフェースダウントリガを設定します。

<interface>で指定したすべてのインタフェースがダウンした場合、Router Lifetime に 0 を設定した RA(Router Advertisement)メッセージを広報します。

<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。

<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場合に、ダウンしたとみなします。

[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。

10.5.13 remote ipv6 ra recv valid-lifetime

[機能]

RA(Router Advertisement)受信での valid-lifetime のモード設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 ra recv valid-lifetime <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

valid-lifetime タイマのモードを指定します。

・ defense
防御モードで使用します。

・ normal
通常モードで使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RA を受信する装置は、不当に小さい lifetime 値を含んだ RA メッセージによるサービス否認攻撃を受ける可能性があります。本コマンドでは、このようなサービス否認攻撃に対し、防御モードで動作させるか、通常モードで動作させるかを設定します。

防御モード

valid-lifetime タイマの残り時間と、RA メッセージで受信した valid-lifetime 値をチェックし、攻撃の可能性がある場合は、安全に動作するように以下の処理を実施します。

・ タイマの残り時間が 2 時間を超過している状態で、受信した valid-lifetime 値が、タイマの残り時間以下で、かつ、0 秒から 2 時間以内の場合は、タイマを"2 時間"に再設定します。

・ タイマの残り時間が 2 時間を超過している状態で、受信した valid-lifetime 値が、タイマの残り時間以下で、かつ、2 時間を超過している場合は、タイマを valid-lifetime 値に再設定します。

・ タイマの残り時間が 2 時間以内の状態で、受信した valid-lifetime 値が、タイマの残り時間以下の場合は、タイマを再設定しません。

・ 受信した valid-lifetime 値が、タイマの残り時間を超過している場合は、タイマを valid-lifetime 値に再設定します。

通常モード

valid-lifetime タイマを、RA メッセージで受信した valid-lifetime 値に再設定します。

[注意]

RA の送信元の安全性が確認できない場合は、防御モードを使用してください。

[未設定時]

防御モードを使用するものとみなされます。

```
remote <number> ipv6 ra recv valid-lifetime defense
```

10.5.14 remote ipv6 route

[機能]

IPv6 スタティック経路情報の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。

範囲	機種
0～255	Si-R G110

<address>/<prefixlen>

・ IPv6 アドレス/プレフィックス長
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。
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、1～14 の 10 進数で指定します。
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、1～254 の 10 進数で指定します。
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、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]

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。

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。

<distance>で指定した優先度は、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。

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 ipv6 distance コマンドを参照してください。

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
256	Si-R G110

[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]

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。

10.5.15 remote ipv6 rip use

[機能]

IPv6 RIP 基本情報の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<send>

RIP(IPv6)パケットを送信するかどうか指定します。

・ off
RIP(IPv6)パケットを送信しません。

・ on
RIP(IPv6)パケットを送信します。

<receive>

RIP(IPv6)パケットを受信するかどうか指定します。

・ off
RIP(IPv6)パケットを受信しません。

・ on
RIP(IPv6)パケットを受信します。

<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、0～14 の 10 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。

[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 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。
たとえば、RIP テーブルのメトリック値が 3 の場合、<metric>に 0 を指定するとメトリックは 3 で広報され、1 を指定すると、4 で広報されます。
なお、受信側の装置では、通常、受信したメトリックに 1 を加算した値で RIP テーブルに登録します。
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
120	Si-R G110

[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> ipv6 rip use off off 0
```

10.5.16 remote ipv6 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 G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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> ipv6 rip site-local on
```

10.5.17 remote ipv6 rip aggregate

[機能]

IPv6 RIP の集約経路の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 ipv6 rip use および remote ipv6 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。

10.5.18 remote ipv6 rip filter act

[機能]

IPv6 RIP フィルタ動作の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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-R G110

<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 ipv6 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-R G110

［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で、遮断条件だけを設定した場合、すべての経路情報は遮断されます。
送受信する経路情報が存在する場合、透過条件に対象の経路情報を設定してください。

［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。

10.5.19 remote ipv6 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 G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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-R G110

[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。

10.5.20 remote ipv6 rip filter route

[機能]

IPv6 RIP フィルタの経路情報設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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-R G110

<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
<address>/<prefixlen>で指定した経路情報を本装置が保有する経路情報と比較し、完全一致したものをフィルタリング対象とします。
・ inexact
指定した<address>の先頭から<prefixlen>ビット部分だけを本装置が保有する経路情報と比較し、一致したものを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。
・ <prefix_match>は以下のように動作します。
<address>/<prefixlen>で"2001:db8::/32"を指定し、本装置が以下の経路情報を保有している場合、exact を指定すると、"2001:db8::/32"がフィルタリング対象となります。

inexact を指定すると、"2001:db8::"と一致する"2001:db8::/32、2001:db8:ffff::/48、2001:db8:ffff:1000::/64"の 3 つがフィルタリング対象となります。

1000:db8::/32

2001:db8::/32

2001:db8:ffff::/48

2001:db8:ffff:1000::/64

[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。

10.5.21 remote ipv6 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 G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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-R G110

<metric>

・メトリック値
メトリック値を、0～15 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]

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 1～15 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 ipv6 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。

10.5.22 remote ipv6 ospf use

[機能]

IPv6 OSPF 利用可否の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

OSPF を利用するかどうかを指定します。

・ 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
0～2	Si-R G110

[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
15	Si-R G110

[注意]

OSPF の利用は、"ospf ipv6 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。

```
remote <number> ipv6 ospf use off
```

10.5.23 remote ipv6 ospf cost

[機能]

IPv6 OSPF 出力コストの設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 1 が設定されているものとみなされます。

```
remote <number> ipv6 ospf cost 1
```

10.5.24 remote ipv6 ospf hello

[機能]

IPv6 OSPF Helloパケット送信間隔の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<hello_interval>

・ Helloパケット送信間隔
Helloパケットの送信間隔時間を、1～65535秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
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、隣接関係が構築できません。

[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> ipv6 ospf hello 10s
```

10.5.25 remote ipv6 ospf dead

[機能]

IPv6 OSPF 隣接ルータ停止確認間隔の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、1～65535 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
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、隣接関係が構築できません。

[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> ipv6 ospf dead 40s
```

10.5.26 remote ipv6 ospf retrans

[機能]

IPv6 OSPF パケット再送間隔の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<retransmit_interval>

・ パケット再送間隔
パケットの再送間隔を、3～65535 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
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(LSupdate、LSrequest、DD)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> ipv6 ospf retrans 5s
```

10.5.27 remote ipv6 ospf delay

[機能]

IPv6 OSPF LSU パケット送信遅延時間の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、1～65535 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
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]

OSPF 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> ipv6 ospf delay 1s
```

10.5.28 remote ipv6 ospf passive

[機能]

IPv6 OSPF パケット送信抑止の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<interface_type>

OSPF パケットの送信を抑止するかどうかを指定します。

・ off
パケットの送信を抑止しません。

・ on
パケットの送信を抑止します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

OSPF 経路計算の対象に含めながら、OSPF パケットを送信しないインタフェースを設定します。

[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> ipv6 ospf passive off
```

10.5.29 remote ipv6 ospf checkmtu

[機能]

IPv6 OSPF パケットの MTU 値確認抑止の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 は、DD 交換時に MTU 値が自装置と相手装置で同一値であることを確認します。
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> ipv6 ospf checkmtu on
```

10.5.30 remote ipv6 filter

[機能]

IPv6 フィルタの設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 filter <count> <action> acl <acl_count> [<direction>]

remote [<number>] ipv6 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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～199	Si-R G110

<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。

－ ipv6

ipv6 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

ipv6 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、ipv6 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

ipv6 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、ipv6 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

ipv6 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、ipv6 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-R G110

<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、または、"-"を使用して表現される 16 進数の範囲を指定します。

Traffic Class 値の指定は、"," を区切りとして 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 を指定したものとみなされます。

<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 の 10 進数、または"-"を使用して表現される 10 進数の範囲を指定します。

icmptype 値の指定は、"," を区切りとして 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 を指定したものとみなされます。

<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 の 10 進数、または"-"を使用して表現される 10 進数の範囲を指定します。

icmptype 値の指定は、"," を区切りとして 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 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 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-layer protocol 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、本装置全体で以下の数まで定義できます。

最大定義数	機種
200	Si-R G110

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
3000	Si-R G110

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。

10.5.31 remote ipv6 filter move

[機能]

IPv6 フィルタの優先順序の変更

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～199	Si-R G110

[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。

10.5.32 remote ipv6 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 G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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>

・ 割り当て時間
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)のいずれかを指定します。
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> ipv6 filter default pass
```

10.5.33 remote ipv6 trafficclass

[機能]

Traffic Class 値書き換え条件の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 trafficclass <count> acl <acl_count> <new_trafficclass>

remote [<number>] ipv6 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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～99	Si-R G110

<acl_count>

・ ACL 定義番号

使用する ACL 定義の番号を、10 進数で指定します。

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。

－ ipv6

ipv6 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

ipv6 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、ipv6 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

ipv6 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、ipv6 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

ipv6 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、ipv6 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-R G110

<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、または、"-"を使用して表現される 16 進数の範囲を指定します。

Traffic Class 値の指定は、"," を区切りとして 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、本装置全体で以下の数まで定義できます。

最大定義数	機種
100	Si-R G110

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
3000	Si-R G110

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。

10.5.34 remote ipv6 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 G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～99	Si-R G110

[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。

10.5.35 remote ipv6 priority

[機能]

IPv6 プロトコル帯域制御の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 priority <count> acl <acl_count> <width>

remote [<number>] ipv6 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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

・ 帯域制御定義番号

帯域制御定義番号を、10 進数で指定します。

範囲	機種
0～99	Si-R G110

<acl_count>

・ ACL 定義番号

使用する ACL 定義の番号を、10 進数で指定します。

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。

－ ipv6

ipv6 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

ipv6 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、ipv6 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

ipv6 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、ipv6 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

ipv6 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、ipv6 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-R G110

<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、または、"-"を使用して表現される 16 進数の範囲を指定します。

Traffic Class 値の指定は、"," を区切りとして 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 を指定したものとみなされます。

<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～1000000kbps または 1mbps～1000mbps 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。

<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。

IPv6 プロトコル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
100	Si-R G110

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
3000	Si-R G110

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 Ethernet 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]

IPv6 プロトコル帯域制御を行わないものとみなされます。

10.5.36 remote ipv6 in-policy

[機能]

Ingress ポリシールーティングの設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<in-policy_number>

・ Ingress ポリシールーティング定義番号
このインタフェースでの Ingress ポリシールーティング定義の通し番号を、10 進数で指定します。
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
200	Si-R G110

<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。

－ ipv6
ipv6 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
ipv6 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、ipv6 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
ipv6 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、ipv6 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
ipv6 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、ipv6 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
0～99	Si-R G110

[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。

10.5.37 remote ipv6 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 G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

10.5.38 remote ipv6 dhcp service

[機能]

IPv6 DHCP 機能の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 dhcp service <mode> [auto]

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。
・ relay
IPv6 DHCP リレーエージェント機能を使用します。
・ server
IPv6 DHCP サーバ機能を使用します。

以下のパラメタは、<mode>に client を指定した場合のみ有効です。

auto

M または O フラグが指定された RA を受信した場合に、動作を開始します。
省略時は、RA 連携を行わず、起動直後に動作を開始します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 DHCP 機能情報を設定します。
IPv6 DHCP クライアント機能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
4	Si-R G110

[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> ipv6 dhcp service off
```

10.5.39 remote ipv6 dhcp duid

[機能]

IPv6 DHCP の DUID 設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 dhcp duid <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<duid>

・ DUID
260 桁以内の 16 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]

IPv6 DHCP サーバ／クライアントの DUID を指定します。

例)

```
remote ipv6 dhcp duid 2105afffe66437d
```

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。

10.5.40 remote ipv6 dhcp client option na

[機能]

IPv6 DHCP クライアントの IPv6 アドレス要求の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 dhcp client option na <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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

- on
  IPv6 アドレスを要求します。
- off
  IPv6 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 IPv6 アドレスを要求するかどうかを設定します。

[注意]

RA 連携が有効な場合、本設定は M フラグが指定された RA を受信した場合に有効になります。
O フラグが指定された RA を受信した場合は、off で動作します。

[未設定時]

IPv6 アドレスを要求するものとみなされます。

```
remote <number> ipv6 dhcp client option na on
```

10.5.41 remote ipv6 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 G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

- off
  プレフィックスを要求しません。
- on
  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。

[注意]

RA 連携が有効な場合、本設定は M フラグが指定された RA を受信した場合に有効になります。
O フラグが指定された RA を受信した場合は、off で動作します。

[未設定時]

プレフィックスを要求しないものとみなされます。

```
remote <number> ipv6 dhcp client option pd off
```

10.5.42 remote ipv6 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 G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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> ipv6 dhcp client option dns on
```

10.5.43 remote ipv6 dhcp client option domain

[機能]

IPv6 DHCP クライアントの DNS ドメイン名要求の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 dhcp client option domain <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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

- on
  DNS ドメイン名を要求します。
- off
  DNS ドメイン名を要求しません。

[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 ドメイン名を要求するかどうかを設定します。

[未設定時]

DNS ドメイン名を要求するものとみなされます。

```
remote <number> ipv6 dhcp client option domain on
```

10.5.44 remote ipv6 dhcp client option sipserver address

[機能]

IPv6 DHCP クライアントの SIP サーバアドレス要求の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 dhcp client option sipserver address <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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

- on
  SIP サーバアドレスを要求します。
- off
  SIP 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 SIP 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]

SIP サーバアドレスを要求するものとみなされます。

```
remote <number> ipv6 dhcp client option sipserver address on
```

10.5.45 remote ipv6 dhcp client option sipserver domain

[機能]

IPv6 DHCP クライアントの SIP ドメイン名要求の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 dhcp client option sipserver domain <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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

- on
  SIP ドメイン名を要求します。
- off
  SIP ドメイン名を要求しません。

[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 SIP ドメイン名を要求するかどうかを設定します。

[未設定時]

SIP ドメイン名を要求するものとみなされます。

```
remote <number> ipv6 dhcp client option sipserver domain on
```

10.5.46 remote ipv6 dhcp client option sntpserver

[機能]

IPv6 DHCP クライアントの SNTP サーバアドレス要求の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 dhcp client option sntpserver <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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

- on
  SNTP サーバアドレスを要求します。
- off
  SNTP 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 SNTP 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]

SNTP サーバアドレスを要求するものとみなされます。

```
remote <number> ipv6 dhcp client option sntpserver on
```

10.5.47 remote ipv6 dhcp client option refreshtime

[機能]

IPv6 DHCP クライアントの情報リフレッシュ時間要求の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 dhcp client option refreshtime <mode> [<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

・ on
情報リフレッシュ時間を要求します。
・ off
情報リフレッシュ時間を要求しません。

<time>

情報リフレッシュ時間オプションを取得しなかった、またはできなかった場合のデフォルトリフレッシュ時間を、10 分～365 日の範囲で指定します。
単位は、d(日)、h(時)、m(分)、s(秒)のいずれかを指定します。
省略時は、1 日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 DHCP クライアント機能を使用する場合に、サーバに情報リフレッシュ時間を要求するかどうかを設定します。

[注意]

本設定は、Information-Request による要求をした場合のみ有効です。
Solicit/Request による要求をした場合は、off で動作します。

[未設定時]

情報リフレッシュ時間を要求するものとみなされます。

```
remote <number> ipv6 dhcp client option refreshtime on 1d
```

10.5.48 remote ipv6 dhcp client iaid

[機能]

IPv6 DHCP クライアントの IAID 設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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> ipv6 dhcp client iaid auto
```

10.5.49 remote ipv6 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 G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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> ipv6 dhcp client route blackhole
```

10.5.50 remote ipv6 dhcp relay interface

[機能]

IPv6 DHCP リレーエージェントのリレー先インタフェース設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 dhcp relay interface <interface>

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<interface>

リレー先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～rmt99	Si-R G110

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 DHCP リレーエージェント機能を使用する場合に、リレー先インタフェースの設定をします。

[未設定時]

リレー先インタフェースを指定しないものとみなされます。
IPv6 DHCP リレーエージェント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。

10.5.51 remote ipv6 dhcp relay server

[機能]

IPv6 DHCP リレーエージェントのリレー先サーバアドレス設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 dhcp relay server <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<address>

リレー先サーバアドレスを指定します。

・ リレー先サーバアドレス
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

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 DHCP リレーエージェント機能を使用する場合に、リレー先サーバアドレスの設定をします。

[未設定時]

規定のマルチキャストアドレス(ff05::1:3)あてにリレーします。

10.5.52 remote ipv6 dhcp relay source

[機能]

IPv6 DHCP リレーエージェントのリレーパケット送信元アドレス設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 dhcp relay source <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<address>

リレーパケットの送信元アドレスを指定します。

・ リレーパケットの送信元アドレス
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

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 DHCP リレーエージェント機能を使用する場合に、リレーパケットの送信元アドレスの設定をします。

[未設定時]

リレーパケットの送信元アドレスを設定しないものとみなされます。

10.5.53 remote ipv6 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 G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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> ipv6 dhcp server preference 0
```

10.5.54 remote ipv6 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 G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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

IPv6 DHCP クライアントが取得した DNS サーバアドレスを配布する場合は"dhcp@インタフェース名"の形式で指定します。インタフェース名には、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～rmt99	Si-R G110

<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

<dns1>に"dhcp@インタフェース名"を指定した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。

10.5.55 remote ipv6 dhcp server info domain

[機能]

IPv6 DHCP サーバの DNS ドメイン名配布情報設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 dhcp server info domain <domain>

[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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<domain>

・ DNS ドメイン名

IPv6 DHCP クライアントに配布する DNS ドメイン名を、英数字、"-"(ハイフン)、"."(ピリオド)の文字で構成される 80 文字以内の文字列で指定します。

ドメイン名は RFC1035 に準拠している必要があります。

IPv6 DHCP クライアントが取得した DNS ドメイン名を配布する場合は"dhcp@インタフェース名"の形式で指定します。インタフェース名には、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～rmt99	Si-R G110

[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 ドメイン名情報の設定をします。

10.5.56 remote ipv6 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 G110

[入力形式]

remote [<number>] ipv6 dhcp server info prefix <prefix>/<prefixlen> <valid><preferred> <routeset> [<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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。

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、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～rmt99	Si-R G110

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

dhcp@rmt0:1234::/64

プレフィックス長には、取得したプレフィックス長より大きい値を指定してください。

<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)のいずれかを指定します。

・ 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)のいずれかを指定します。

<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。

<duid>

- DUID

  260 桁以内の 16 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]

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。

DUID を設定した場合は、設定に一致する DUID のクライアント以外にはプレフィックスを配布しません。プレフィックス配布情報を設定していない場合は、プレフィックスを配布することはできません。

10.5.57 remote ipv6 dhcp server info sipserver address

[機能]

IPv6 DHCP サーバの SIP サーバアドレス配布情報設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 dhcp server info sipserver address <sip1> [<sip2>]

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<sip1>

・ SIP サーバ IPv6 アドレス
IPv6 DHCP クライアントに配布する SIP 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

IPv6 DHCP クライアントが取得した SIP サーバアドレスを配布する場合は、"dhcp@インタフェース名"の形式で指定します。インタフェース名には、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～rmt99	Si-R G110

<sip2>

・ セカンダリ SIP 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 SIP 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

<sip1>に"dhcp@インタフェース名"を指定した場合は、<sip2>を指定できません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 DHCP サーバ機能を使用する場合に、配布する SIP サーバアドレス情報の設定をします。

10.5.58 remote ipv6 dhcp server info sipserver domain

[機能]

IPv6 DHCP サーバの SIP ドメイン名配布情報設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 dhcp server info sipserver domain <sip1> [<sip2>]

[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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<sip1>

・ SIP ドメイン名

IPv6 DHCP クライアントに配布する SIP ドメイン名を、英数字、"-"(ハイフン)、"."(ピリオド)の文字で構成される 80 文字以内の文字列で指定します。

ドメイン名は RFC1035 に準拠している必要があります。

IPv6 DHCP クライアントが取得した SIP ドメイン名を配布する場合は、"dhcp@インタフェース名"の形式で指定します。インタフェース名には、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～rmt99	Si-R G110

<sip2>

・ セカンダリ SIP ドメイン名

IPv6 DHCP クライアントに配布するセカンダリ SIP ドメイン名を、英数字、"-"(ハイフン)、"."(ピリオド)の文字で構成される 80 文字以内の文字列で指定します。

ドメイン名は RFC1035 に準拠している必要があります。

<sip1>に"dhcp@インタフェース名"を指定した場合は、<sip2>を指定できません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 DHCP サーバ機能を使用する場合に、配布する SIP ドメイン名情報の設定をします。

10.5.59 remote ipv6 dhcp server info sntpserver

[機能]

IPv6 DHCP サーバの SNTP サーバアドレス配布情報設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] ipv6 dhcp server info sntpserver <sntp1> [<sntp2>]

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<sntp1>

・ SNTP サーバ IPv6 アドレス
IPv6 DHCP クライアントに配布する、SNTP 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

IPv6 DHCP クライアントが取得した SNTP サーバアドレスを配布する場合は"dhcp@インタフェース名"の形式で指定します。インタフェース名には、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～rmt99	Si-R G110

<sntp2>

・ セカンダリ SNTP 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 SNTP サーバの IPv6 アドレスを指定します。
<sntp1>に"dhcp@インタフェース名"を指定した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 サーバ機能を使用する場合に、配布する SNTP サーバアドレス情報の設定をします。

10.5.60 remote ipv6 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 G110

[入力形式]

remote [<number>] ipv6 dvpn <count> invite acl <acl_count> <invite_mask> <template_number>
remote [<number>] ipv6 dvpn <count> ignore acl <acl_count>
remote [<number>] ipv6 dvpn <count> autoignore

[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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～2999	Si-R G110

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。

autoignore

接続先情報の動的VPN接続後に相手装置から通知されたネットワークの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
0～999	Si-R G110

<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進数で指定します。

<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。

範囲	機種
0～1	Si-R G110

[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。

autoignore を指定した場合は、相手装置から通知されたネットワークをテンプレート情報の動的 VPN 接続対象外とし、INVITE 要求を発行しません。

また、対象の相手情報を通過するセッション監視についても、動的 VPN 接続対象外とし、INVITE 要求を発行しません。

[注意]

本コマンドの autoignore を指定した場合に相手装置から通知されたネットワーク情報内の all-0(::/0)は autoignore 対象外とします。

[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。

10.5.61 remote ipv6 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 G110

[入力形式]

remote [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～2999	Si-R G110

[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を変更します。

10.6 ブリッジグループ関連情報

10.6.1 remote bridgegroup use

[機能]

ブリッジグループ機能の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] bridgegroup 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

ブリッジグループを使用するかどうかを指定します。

・ off
ブリッジグループを使用しない場合に指定します。

・ on
ブリッジグループ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]

ブリッジグループを使用するかどうかを設定します。
ブリッジグループを使用する場合、IP および IPv6 のパケット以外をすべてブリッジします。
IP および IPv6 の転送ポリシーは、ブリッジグループの設定に依存します。
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グループを使用する場合は、ブリッジグループ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。

[未設定時]

ブリッジグループを使用しないものとみなされます。

```
remote <number> bridgegroup use off
```

10.6.2 remote bridgegroup group

[機能]

ブリッジグループ識別子の設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] bridgegroup 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<group_id>

・ グループ識別子
グループ識別子を、10 進数で指定します。

範囲	機種
0～19	Si-R G110

[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> bridgegroup group 0
```

10.6.3 remote bridgegroup macfilter

[機能]

MAC フィルタの設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] bridgegroup macfilter <count> <action> acl <acl_count> [<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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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-R G110

<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
0～999	Si-R G110

<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 MAC アドレスとあて先 MAC アドレス

[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。
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
3000	Si-R G110

[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。ルーティングと併せて使用する場合は、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。

10.6.4 remote bridgegroup macfilter move

[機能]

MAC フィルタの優先順序の変更

[適用機種]

Si-R G110

[入力形式]

remote [<number>] bridgegroup macfilter 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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-R G110

[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。

10.7 SNMP 関連情報

10.7.1 remote snmp trap linkdown

[機能]

linkDown トラップの設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] snmp trap linkdown <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

[注意]

snmp trap linkdown コマンドで trap 動作が無効にされた場合は、本コマンド設定値は意味を持ちません。

[未設定時]

linkDown トラップが有効とみなされます。

```
remote <number> snmp trap linkdown enable
```

10.7.2 remote snmp trap linkup

[機能]

linkUp トラップの設定

[適用機種]

Si-R G110

[入力形式]

remote [<number>] snmp trap linkup <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

[注意]

snmp trap linkup コマンドで trap 動作が無効にされた場合は、本コマンド設定値は意味を持ちません。

[未設定時]

linkUp トラップが有効とみなされます。

```
remote <number> snmp trap linkup enable
```

第 11 章 着信デフォルト情報の設定

11.1　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

11.1.1　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 G110

[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
```

11.1.2 answer ppp auth type

[機能]

着信認証方式の設定

[適用機種]

Si-R G110

[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
```

11.1.3 answer ppp auth receive add

[機能]

受諾認証情報の設定

[適用機種]

Si-R G110

[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 128 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 128 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。
設定可能な定義の最大数は以下のとおりです。

定義可能数	機種
64	Si-R G110

[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。

第 12 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)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
0～1	Si-R G110

12.1 テンプレート共通情報

12.1.1 template description

[機能]

テンプレート説明文の設定

[適用機種]

Si-R G110

[入力形式]

template [<number>] description <description>

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<description>

・説明文
テンプレートの説明文を、0x21,0x23～0x7e の 50 文字以内の ASCII 文字列で記入します。
(入力可能な文字の一覧については、コマンドユーザーズガイドを参照してください。)

[動作モード]

構成定義モード(管理者クラス)

[説明]

テンプレートについての説明文を設定します。

[未設定時]

説明文を設定しないものとみなされます。

12.1.2 template name

[機能]

テンプレート名称の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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用する予約語であるため、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。

12.1.3 template mtu

[機能]

送信パケット最大長(MTU 値)の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mtu>

・ MTU 値
MTU 値を、200～1500 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]

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
```

12.1.4 template idle

[機能]

無通信監視タイマの設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<time>

・無通信監視時間
無通信監視時間を、0～14400 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
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ときに 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
```

12.1.5 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。

範囲	機種
0～99	Si-R G110

<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 進数で指定します。

最大インタフェース数	機種
100	Si-R G110

[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。)

12.1.6 template aaa

[機能]

参照する AAA 情報の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。

範囲	機種
0～9	Si-R G110

[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。

12.1.7 template datalink type

[機能]

パケット転送方法の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<type>

パケットの転送方式を指定します。

・ 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]

パケット転送方式を設定しないものとみなされます。

12.1.8 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<function>

テンプレートが利用する機能を指定します。

・ aaa
不特定相手着信機能を利用する場合に指定します。
・ dvpn
動的 VPN 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
```

12.2 IP関連情報

12.2.1 template ip dns

[機能]

DNSサーバアドレスの設定

[適用機種]

Si-R G110

[入力形式]

template [<number>] ip dns <primary_dns> [<secondary_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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<primary_dns>

・プライマリ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

<secondary_dns>

・セカンダリ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。

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、<primary_dns>、<secondary_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。

[注意]

<secondary_dns>のみが未設定の場合は、0.0.0.0が設定されたものとみなされます。

[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
```

12.2.2 template ip nat mode

[機能]

アドレス変換の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、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>

・ 割り当て時間
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)のいずれかを指定します。
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
```

12.2.3 template ip nat static

[機能]

静的アドレス変換の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。

範囲	機種
0～199	Si-R G110

<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
200	Si-R G110

[未設定時]

静的アドレス変換は設定されません。

12.2.4 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 G110

[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し番号を、10 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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

12.2.5 template ip nat rule

[機能]

アドレス変換ルールの設定

[適用機種]

Si-R G110

[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>
```

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

・変換ルール番号
変換ルール番号を、0～31 の 10 進数で指定します。

ftp, irc, dns, sip, mldt, ipbs

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。

12.2.6 template ip nat wellknown

[機能]

ポート番号変換の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

ポート番号変換定義番号を、0～99 の 10 進数で指定します。

<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)
```

12.2.7 template ip nat destination

[機能]

あて先変換の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～199	Si-R G110

<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
200	Si-R G110

[未設定時]

あて先変換は設定されません。

12.2.8 template ip nat appli

[機能]

アプリ対応の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。
・ 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。

<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]

アプリ対応を以下のように指定したものとみなされます。

```
template [<number>] ip nat appli ftp on
template [<number>] ip nat appli sip on
template [<number>] ip nat appli dns on
template [<number>] ip nat appli snmp on
```

12.2.9 template ip filter

[機能]

IP フィルタの設定

[適用機種]

Si-R G110

[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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～199	Si-R G110

<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
0～999	Si-R G110

<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
200	Si-R G110

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
3000	Si-R G110

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。

<dst_addr>/<mask>に″dynamic″を指定した ACL は使用しないでください。

[未設定時]

IP フィルタを設定しないものとみなされます。

12.2.10 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～199	Si-R G110

[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。

12.2.11 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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>

・ 割り当て時間
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)のいずれかを指定します。
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
```

12.2.12 template ip tos

[機能]

TOS 値書き換え条件の設定

[適用機種]

Si-R G110

[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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～99	Si-R G110

<acl_count>

・ACL 定義番号

使用する ACL 定義の番号を、10 進数で指定します。

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
0～999	Si-R G110

<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
100	Si-R G110

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
3000	Si-R G110

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。
・ <dst_addr>/<mask>に″dynamic″を指定した ACL は使用しないでください。

[未設定時]

TOS 値書き換えを行わないものとみなされます。

12.2.13 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～99	Si-R G110

[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。

12.2.14 template ip msschange

[機能]

MSS 書き換えの設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mss>

・ MSS 値
MSS の書き換え値を、0 または 160～1460 の 10 進数で指定します。
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
```

12.2.15 template ip ids use

[機能]

IDS の設定

[適用機種]

Si-R G110

[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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

[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
```

12.2.16 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<in-policy_number>

・Ingress ポリシールーティング定義番号
このインタフェースでの Ingress ポリシールーティング定義の通し番号を、10 進数で指定します。
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
200	Si-R G110

<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
0～99	Si-R G110

[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。

12.2.17 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

12.3 IPv6 関連情報

12.3.1 template ipv6 use

[機能]

IPv6 機能の設定

[適用機種]

Si-R G110

[入力形式]

template [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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> ipv6 use off
```

12.3.2 template ipv6 ifid

[機能]

IPv6 インタフェース ID の設定

[適用機種]

Si-R G110

[入力形式]

template [<number>] ipv6 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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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> ipv6 ifid auto
```

12.3.3 template ipv6 filter

[機能]

IPv6 フィルタの設定

[適用機種]

Si-R G110

[入力形式]

template [<number>] ipv6 filter <count> <action> acl <acl_count> [<direction>]

template [<number>] ipv6 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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～199	Si-R G110

<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。

－ ipv6

ipv6 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

ipv6 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、ipv6 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

ipv6 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、ipv6 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

ipv6 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、ipv6 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-R G110

<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、または、"-"を使用して表現される 16 進数の範囲を指定します。

Traffic Class 値の指定は、"," を区切りとして 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 を指定したものとみなされます。

<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 の 10 進数、または"-"を使用して表現される 10 進数の範囲を指定します。

icmptype 値の指定は、"," を区切りとして 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 を指定したものとみなされます。

<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 の 10 進数、または"-"を使用して表現される 10 進数の範囲を指定します。

icmptype 値の指定は、"," を区切りとして 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 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 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-layer protocol 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、本装置全体で以下の数まで定義できます。

最大定義数	機種
200	Si-R G110

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
3000	Si-R G110

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。

12.3.4 template ipv6 filter move

[機能]

IPv6 フィルタの優先順序の変更

[適用機種]

Si-R G110

[入力形式]

template [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～199	Si-R G110

[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。

12.3.5 template ipv6 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 G110

[入力形式]

template [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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>

・割り当て時間
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)のいずれかを指定します。
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> ipv6 filter default pass
```

12.3.6 template ipv6 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 G110

[入力形式]

template [<number>] ipv6 trafficclass <count> acl <acl_count> <new_trafficclass>

template [<number>] ipv6 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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～99	Si-R G110

<acl_count>

・ACL 定義番号

使用する ACL 定義の番号を、10 進数で指定します。

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。

－ ipv6

ipv6 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

ipv6 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、ipv6 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

ipv6 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、ipv6 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

ipv6 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、ipv6 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-R G110

<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、または、"-"を使用して表現される 16 進数の範囲を指定します。

Traffic Class 値の指定は、"," を区切りとして 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、本装置全体で以下の数まで定義できます。

最大定義数	機種
100	Si-R G110

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
3000	Si-R G110

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。

12.3.7 template ipv6 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 G110

[入力形式]

template [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
0～99	Si-R G110

[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。

12.3.8 template ipv6 priority

[機能]

IPv6 プロトコル帯域制御の設定

[適用機種]

Si-R G110

[入力形式]

template [<number>] ipv6 priority <count> acl <acl_count> <width>

template [<number>] ipv6 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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

・ 帯域制御定義番号

帯域制御定義番号を、10 進数で指定します。

範囲	機種
0～99	Si-R G110

<acl_count>

・ ACL 定義番号

使用する ACL 定義の番号を、10 進数で指定します。

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。

－ ipv6

ipv6 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

ipv6 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、ipv6 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

ipv6 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、ipv6 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

ipv6 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、ipv6 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-R G110

<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、または、"-"を使用して表現される 16 進数の範囲を指定します。

Traffic Class 値の指定は、"," を区切りとして 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 を指定したものとみなされます。

<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～1000000kbps または 1mbps～1000mbps 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。
<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。
IPv6 プロトコル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
100	Si-R G110

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
3000	Si-R G110

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]

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。

12.3.9 template ipv6 in-policy

[機能]

Ingress ポリシールーティングの設定

[適用機種]

Si-R G110

[入力形式]

template [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<in-policy_number>

・Ingress ポリシールーティング定義番号
このインタフェースでの Ingress ポリシールーティング定義の通し番号を、10 進数で指定します。
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
200	Si-R G110

<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。

－ ipv6
ipv6 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
ipv6 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、ipv6 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
ipv6 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、ipv6 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
ipv6 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、ipv6 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
0～99	Si-R G110

[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。

12.3.10 template ipv6 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 G110

[入力形式]

template [<number>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

12.4 動的VPN関連情報

12.4.1 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 G110

[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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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進数で指定します。

範囲	機種
0～1	Si-R G110

[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。

12.4.2 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 G110

[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進数で指定します。

省略時は、0を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

・動的VPNサーバ定義番号

動的VPNサーバの定義番号を、0～1の10進数で指定します。

<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。

動的VPNクライアントアドレス設定(template dvpn ua)と同一のアドレスファミリである必要があります。

［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。

12.4.3 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 G110

[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進数で指定します。

省略時は、0を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

・動的VPNサーバ定義番号

動的VPNサーバの定義番号を、0～1の10進数で指定します。

<id>

・認証ID

認証IDを、0x21,0x23～0x7eの文字で構成される50文字以内の文字列で指定します。

<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とき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。

12.4.4 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、90～86400 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
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
```

12.4.5 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 G110

[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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、90～3600秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
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
```

12.4.6 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 G110

[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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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～rmt99	Si-R G110

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

```
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。

動的VPNサーバアドレス設定(template dvpn server address)と同一のアドレスファミリである必要があります。

[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。

12.4.7 template dvpn domain

[機能]

動的VPNドメイン名の設定

[適用機種]

Si-R G110

[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進数で指定します。

省略時は、0を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

12.4.8 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 G110

[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進数で指定します。

省略時は、0を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、0～19の10進数で指定します。

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～rmt99	Si-R G110

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

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な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。

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。

Si-Rシリーズ(V30ソフトウェア)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なるアドレスファミリの設定を行わないでください。

[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。

12.4.9 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 G110

[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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

12.4.10 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。

範囲	機種
0～19	Si-R G110

・rmt 定義の定義番号
利用する rmt の定義番号を、10 進数で指定します。

範囲	機種
0～99	Si-R G110

<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。

12.4.11 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

12.5 IPsec 関連情報

12.5.1 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

12.5.2 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。複数定義するときは、アルゴリズムを空白なしでカンマ','で区切ります。

・ none
・ des-cbc
・ 3des-cbc
・ aes-cbc-128
・ aes-cbc-192
・ aes-cbc-256
・ null

[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
```

12.5.3 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。複数定義するときは、アルゴリズムを空白なしでカンマ','で区切ります。

・ none
・ hmac-md5
・ hmac-sha1
・ hmac-sha256
・ hmac-sha384
・ hmac-sha512

[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
・ hmac-sha256
・ hmac-sha384
・ hmac-sha512

[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
```

12.5.4 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<pfs_group>

Diffie-Hellman グループについて指定します。

・ off
Diffie-Hellman グループを使用しません。
・ 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)
・ modp2048
Diffie-Hellman グループの MODP2048(グループ 14)

[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
```

12.5.5 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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)のいずれかを指定します。

[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
```

12.5.6 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 G110

[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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

12.5.7 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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)のどちらかを指定します。

<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]

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
```

12.5.8 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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)のどちらかを指定します。

・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]

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
```

12.5.9 template ipsec ike anti-replay

[機能]

自動鍵交換用 IPsec 情報のリプレイ攻撃防御機能の設定

[適用機種]

Si-R G110

[入力形式]

template [<number>] ipsec ike anti-replay <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

・リプレイ攻撃防御機能
AH または認証付き ESP を利用した IPsec 通信でリプレイ攻撃防御機能の使用有無を指定します。
－ on
リプレイ攻撃防御機能を使用します。
－ off
リプレイ攻撃防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]

AH または認証付き ESP を利用した IPsec 通信の受信(復号・認証)時でリプレイ攻撃防御機能を使用するかどうかの設定を行います

[注意]

リプレイ攻撃防御機能を使用しない場合は、重複攻撃(なりすまし)などによる検出が行えなくなるため、セキュリティが弱くなります。

[未設定時]

リプレイ攻撃防御機能を使用するものとみなされます。

```
template <number> ipsec ike anti-replay on
```

12.5.10 template ipsec ike exchange-sa initiator

[機能]

自動鍵交換用 IPsec 情報の Initiator SA 更新時の切り替え待ち時間の設定

[適用機種]

Si-R G110

[入力形式]

template [<number>] ipsec ike exchange-sa initiator <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<time>

・ Initiator SA 切り替え待ち時間
Initiator SA 切り替え待ち時間を、0 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]

自側が Initiator の場合に、IPsec SA の更新後、New SA に切り替える時間の設定を行います。
0 秒を設定した場合は、IPsec SA の更新後即時、New SA に切り替わります。

[注意]

template ipsec ike lifebyte に 0 以外を設定した場合は、本コマンドは未設定時と同様の動作となります。

[未設定時]

Initiator SA 切り替え待ち時間として 0s(0 秒)が設定されたものとして扱います。

```
template <number> ipsec ike exchange-sa initiator 0s
```

12.5.11 template ipsec ike exchange-sa responder

[機能]

自動鍵交換用 IPsec 情報の Responder SA 更新時の切り替え待ち時間の設定

[適用機種]

Si-R G110

[入力形式]

template [<number>] ipsec ike exchange-sa responder <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<time>

・ Responder SA 切り替え待ち時間
Responder SA 切り替え待ち時間を、0 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]

自側が Responder の場合に、IPsec SA の更新後、New SA に切り替える時間の設定を行います。
0 秒を設定した場合は、IPsec SA の更新後即時、New SA に切り替わります。

[注意]

template ipsec ike lifebyte に 0 以外を設定した場合は、本コマンドは未設定時と同様の動作となります。

[未設定時]

Responder SA 切り替え待ち時間として 0s(0 秒)が設定されたものとして扱います。

```
template <number> ipsec ike exchange-sa responder 0s
```

12.6 IKE 関連情報

12.6.1 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

12.6.2 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 で動作させるときに、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。

12.6.3 template ike proposal auth-method

[機能]

IKE セッション用相手装置認証情報の設定

[適用機種]

Si-R G110

[入力形式]

template [<number>] ike proposal [<proposal_number>]
auth-method <auth_method>

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<proposal_number>

・ Proposal 定義番号
Proposal 定義番号を、0～2 の 10 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。

<auth_method>

認証方式を指定します。

・ shared-key
認証方式として共有鍵を使用します。
・ rsa-signature
認証方式として RSA デジタル署名方式を使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

相手装置を認証するための、認証方式の設定を行います。
認証方式を rsa-signature に指定した場合、動的 VPN 機能が設定されたときのみ動作します。

[注意]

・ 認証方式として shared-key を指定した場合は必ず共有鍵の設定を行ってください。
・ 認証方式として rsa-signature を指定した場合は必ず以下の設定を行ってください。
－ "IKE セッション用秘密鍵情報"の設定
－ "IKE セッション用自装置証明書情報"の設定

[未設定時]

相手装置認証のための認証方式に shared-key を指定したものとみなされます。

```
template <number> ike proposal <proposal_number> auth-method shared-key
```

12.6.4 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<proposal_number>

・ Proposal 定義番号
Proposal 定義番号を、0～2 の 10 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。

<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あると 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。

12.6.5 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<proposal_number>

・ Proposal 定義番号
Proposal 定義番号を、0～2 の 10 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。

<hash_algo>

認証(ハッシュ)アルゴリズムを指定します。

・ hmac-md5
・ hmac-sha1
・ hmac-sha256
・ hmac-sha384
・ hmac-sha512

[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
```

12.6.6 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<proposal_number>

・ Proposal 定義番号
Proposal 定義番号を、0～2 の 10 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。

<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
・ modp2048
MODP2048(グループ 14)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
```

12.6.7 template ike proposal lifetime

[機能]

IKE 情報の SA 有効時間の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<proposal_number>

・Proposal 定義番号
Proposal 定義番号を、0～2 の 10 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。

<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)のいずれかを指定します。

[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
```

12.6.8 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

12.6.9 template ike idtype

[機能]

IKE 情報の送信 ID タイプの設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
・ x501_sbj
X.501 証明書対象者名

[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。

[注意]

<id_type>に x501_sbj を設定する場合は、Aggressive モードで使用することはできません。

[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
```

12.6.10 template 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 G110

[入力形式]

template [<number>] ike name local <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<name>

・ 自装置識別情報
自装置を識別する名前を、1～128 文字で指定します。
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、自装置の識別情報の設定を行います。

[注意]

・ テンプレートが利用する機能に動的 VPN 機能が設定された場合に動作します。
・ 相手装置認証方式の設定に RSA デジタル署名認証方式が設定されていた場合に動作します。

[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。

12.6.11 template ike release

[機能]

IPsec/IKE 情報の解放動作の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

・ PPPoE を使用したときの切断時
・ データ通信モジュールを使用したときの切断時

[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
```

12.6.12 template ike mode

[機能]

IKE 情報の交換モードの設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

12.6.13 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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せて使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。
・ 自側および相手側トンネルエンドポイントアドレスに IPv6 アドレスを設定した場合は動作しません。
・ IKE モードが Aggressive Mode 設定で、自側および相手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
```

12.6.14 template ike certificate local

[機能]

IKE セッション用自装置証明書情報

[適用機種]

Si-R G110

[入力形式]

template [<number>] ike certificate local <cert_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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<cert_number>

・ 自装置証明書識別番号

自装置証明書の識別番号を、0～4 の 10 進数で指定します。

crypto certificate generate コマンドで設定、または crypto certificate local コマンドで取り込んだ自装置証明書の識別番号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]

自装置証明書の設定を行います。

[注意]

・ 必ず秘密鍵に合った鍵ペアの自装置証明書を設定してください。
・ テンプレートが利用する機能に動的 VPN 機能が設定された場合に動作します。
・ 相手装置認証方式の設定に RSA デジタル署名認証方式が設定されていた場合に動作します。

[未設定時]

IKE セッション用自装置証明書情報に指定がされません。

認証方式として RSA デジタル署名方式を使用する場合は必ず設定してください。

12.6.15 template ike certificate key

[機能]

IKE セッション用秘密鍵情報

[適用機種]

Si-R G110

[入力形式]

template [<number>] ike certificate key <key_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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<key_number>

・ 秘密鍵識別番号
秘密鍵の識別番号を、0～4 の 10 進数で指定します。
crypto certificate generate コマンドで設定した秘密鍵の識別番号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]

秘密鍵の設定を行います。

[注意]

・ 必ず自装置証明書に合った鍵ペアの秘密鍵を設定してください。
・ テンプレートが利用する機能に動的 VPN 機能が設定された場合に動作します。
・ 相手装置認証方式の設定に RSA デジタル署名認証方式が設定されていた場合に動作します。

[未設定時]

IKE セッション用秘密鍵情報に設定がされません。
認証方式として RSA デジタル署名方式を使用する場合は必ず設定してください。

12.6.16 template ike certificate expired

[機能]

IKE セッション用有効期限切れ証明書の使用の有無

[適用機種]

Si-R G110

[入力形式]

template [<number>] ike certificate expired <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

・ use
有効期限が切れている証明書を使用します。
・ unuse
有効期限が切れている証明書を使用しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

有効期限が切れている証明書を使用するかどうかを設定します。
<mode>が use の場合、有効期限が切れている証明書をそのまま使用します。
<mode>が unuse の場合、有効期限が切れている証明書を使用しません。この場合 IKE ネゴシエーションに失敗します。

[注意]

・ テンプレートが利用する機能に動的 VPN 機能が設定された場合に動作します。
・ 相手装置認証方式の設定に RSA デジタル署名認証方式が設定されていた場合に動作します。
・ 認証局証明書の有効期限切れチェックは、自装置が証明書要求ペイロードを送信するときのみ行っています。

[未設定時]

有効期限が切れている証明書を使用するものとみなされます。

```
template <number> ike certificate expired use
```

12.6.17 template ike certificate send

[機能]

IKE セッション用自装置証明書情報の送信

[適用機種]

Si-R G110

[入力形式]

template [<number>] ike certificate send <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し番号を、10 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。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<action>

・ reply
相手装置から証明書要求ペイロードを受信したときに、自装置証明書情報を送信する場合に指定します。

・ enable
相手装置から証明書要求ペイロードの受信にかかわらず、常に自装置証明書情報を送信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]

自装置証明書の送信設定を行います。

[注意]

・ テンプレートが利用する機能に動的 VPN 機能が設定された場合に動作します。
・ 相手装置認証方式の設定に RSA デジタル署名認証方式が設定されていた場合に動作します。

[未設定時]

IKE セッション用自装置証明書情報の送信設定に reply を指定したものとみなされます。

```
template <number> ike certificate send reply
```

12.6.18 template ike certificate request

[機能]

IKE セッション用証明書要求の送信

[適用機種]

Si-R G110

[入力形式]

template [<number>] ike certificate request <action> [<ca_cert>]

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<action>

・ enable
証明書要求を送信する場合に指定します。
・ disable
証明書要求を送信しない場合に指定します。

<ca_cert>

・ 送信する認証局の識別番号
認証局の識別番号を、0～4 の 10 進数で指定します。
crypto certificate ca コマンドで設定した認証局の識別番号を指定してください。
(※certificate request が enable の場合のみ有効)
省略時は、送信する認証局情報がないものとみなします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

証明書要求の送信設定を行います。

[注意]

・ テンプレートが利用する機能に動的 VPN 機能が設定された場合に動作します。
・ 相手装置認証方式の設定に RSA デジタル署名認証方式が設定されていた場合に動作します。

[未設定時]

送信する認証局情報がない、証明書要求を送信するを指定したものとみなされます。

```
template <number> ike certificate-request send enable
```

12.6.19 template ike dpd use

[機能]

IKE 情報の Dead Peer Detection(DPD)利用可否の設定

[適用機種]

Si-R G110

[入力形式]

template [<number>] ike dpd 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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

- off
  DPD を利用しません。
- on
  DPD 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]

IKE で DPD を利用する設定を行います。

[注意]

DPD 機能を使用する場合は、相手装置の DPD 機能設定も有効にしてください。

[未設定時]

IKE 情報の DPD 利用に off を指定したものとみなされます。

```
template <number> ike dpd use off
```

12.6.20 template ike dpd idle

[機能]

IKE 情報の Dead Peer Detection(DPD)パケット送信を開始する無通信監視時間の設定

[適用機種]

Si-R G110

[入力形式]

template [<number>] ike dpd idle <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<time>

・ 無通信監視時間
無通信監視時間を、5～600 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。

[動作モード]

構成定義モード(管理者クラス)

[説明]

DPD パケット送信を開始する IPsec 受信パケット無通信監視時間の設定を行います。

[未設定時]

無通信監視時間に 10 秒を設定したものとみなされます。

```
template <number> ike dpd idle 10s
```

12.6.21 template ike dpd retry

[機能]

IKE 情報の Dead Peer Detection(DPD)再送時間／回数の設定

[適用機種]

Si-R G110

[入力形式]

template [<number>] ike dpd 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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<time>

・ 再送時間
再送時間を、1～60 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]

DPD パケットに対する再送時間および再送回数の設定を行います。

[注意]

DPD パケットの再送時間と再送回数は、「DPD パケット送信を開始する IPsec 受信パケット無通信監視時間」より短い時間を設定してください。

再送時間×(再送回数＋ 1)＜無通信監視時間

その範囲を超えた場合は、定義反映時に設定エラーとなります。

[未設定時]

再送時間に 1 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 dpd retry 1s 3
```

12.6.22 template ike dpd anti-replay

[機能]

IKE 情報の Dead Peer Detection(DPD)リプレイ攻撃防御機能の設定

[適用機種]

Si-R G110

[入力形式]

template [<number>] ike dpd anti-replay <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。
省略時は、0 を指定したものとみなされます。

<mode>

・ リプレイ攻撃防御機能
DPD メッセージリプレイ攻撃防御機能の使用有無を指定します。
－ enable
リプレイ攻撃防御機能を使用します。
－ disable
リプレイ攻撃防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]

DPD メッセージ機能の利用時、DPD メッセージパケット受信時でリプレイ攻撃防御機能を使用するかどうかの設定を行います。

[注意]

リプレイ攻撃防御機能を使用しない場合は、重複攻撃(なりすまし)などによる検出が行えなくなるため、セキュリティが弱くなります。

[未設定時]

リプレイ攻撃防御機能を使用するものとみなされます。

```
template <number> ike dpd anti-replay enable
```

12.7 トンネル関連情報

12.7.1 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 G110

[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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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～rmt99	Si-R G110

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

```
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。

12.8 セッション監視関連情報

12.8.1 template sessionwatch address

[機能]

接続先監視アドレスの設定

[適用機種]

Si-R G110

[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 進数で指定します。

省略時は、0 を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 アドレスのいず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～rmt99	Si-R G110

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

```
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。

12.8.2 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、1～60 秒の 10 進数で指定します。
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><th rowspan="2"></th><th rowspan="2">利用機能</th><th colspan="2">接続先監視あり</th><th rowspan="2">接続先監視なし</th></tr>
<tr><th>正常時送信間隔あり</th><th>正常時送信間隔なし</th></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>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</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>
</table>

	利用機能	接続先監視あり		接続先監視なし
		正常時送信間隔あり	正常時送信間隔なし	
		動作する		
	RADIUS または AAA	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	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	動作しない

［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。

12.9 SNMP 関連情報

12.9.1 template snmp trap linkdown

[機能]

linkDown トラップの設定

[適用機種]

Si-R G110

[入力形式]

template [<number>] snmp trap linkdown <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

[注意]

snmp trap linkdown コマンドで trap 動作が無効にされた場合は、本コマンド設定値は意味を持ちません。

[未設定時]

linkDown トラップが有効とみなされます。

```
template <number> snmp trap linkdown enable
```

12.9.2 template snmp trap linkup

[機能]

linkUp トラップの設定

[適用機種]

Si-R G110

[入力形式]

template [<number>] snmp trap linkup <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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

[注意]

snmp trap linkup コマンドで trap 動作が無効にされた場合は、本コマンド設定値は意味を持ちません。

[未設定時]

linkUp トラップが有効とみなされます。

```
template <number> snmp trap linkup enable
```

第 13 章 IP 関連情報の設定

13.1 IP 関連情報

13.1.1 ip arp age

[機能]

ARP エントリ有効時間の設定

[適用機種]

Si-R G110

[入力形式]

ip arp age <time>

[オプション]

<time>

ARP エントリの有効時間(分)を、1～240 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]

ARP エントリの有効時間を設定します。

[未設定時]

20 分が設定されたものとみなされます。

```
ip arp age 20
```

13.1.2 ip arp verify mode

[機能]

ARP 確認動作モードの設定

[適用機種]

Si-R G110

[入力形式]

ip arp verify mode <mode>

[オプション]

<mode>

- enable
  ARP 確認を行います。
- disable
  ARP 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]

ARP エントリ有効時間経過による ARP エントリ削除前に、ARP リクエスト発行による ARP 確認を行うかどうかを設定します。

[未設定時]

ARP 確認を行うものとみなされます。

```
ip arp verify mode enable
```

第 14 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)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
0～1	Si-R G110

14.1 動的VPNサーバ情報

14.1.1 dvpn server use

[機能]

動的VPNサーバ利用可否の設定

[適用機種]

Si-R G110

[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
```

14.1.2 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 G110

[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。

14.1.3 dvpn server auth use

[機能]

動的VPNサーバの認証の設定

[適用機種]

Si-R G110

[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
```

14.1.4 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 G110

[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進数で指定します。
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-R G110

[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
```

14.2 動的VPNクライアント情報

14.2.1 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 G110

[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]

Si-Rシリーズ(V30ソフトウェア)の装置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
```

14.2.2 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 G110

[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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

・動的VPNサーバ定義番号
動的VPNサーバの定義番号を、0～1の10進数で指定します。

<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。

動的VPNクライアントアドレス設定(dvpn client ua)と同一のアドレスファミリである必要があります。

［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。

14.2.3 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 G110

[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進数で指定します。

省略時は、0を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

・動的VPNサーバ定義番号

動的VPNサーバの定義番号を、0～1の10進数で指定します。

<id>

・認証ID

認証IDを、0x21,0x23～0x7eの文字で構成される50文字以内の文字列で指定します。

<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とき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。

14.2.4 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 G110

[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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、90～86400秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
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
```

14.2.5 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 G110

[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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、90～3600秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
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
```

14.2.6 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 G110

[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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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～rmt99	Si-R G110

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
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。
動的VPNサーバアドレス設定(dvpn client server address)と同一のアドレスファミリである必要があります。

［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。

14.2.7 dvpn client domain

[機能]

動的VPNドメイン名の設定

[適用機種]

Si-R G110

[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進数で指定します。

省略時は、0を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

14.2.8 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 G110

[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進数で指定します。

省略時は、0を指定したものとみなされます。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、0～19の10進数で指定します。

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～rmt99	Si-R G110

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

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な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。

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。

Si-Rシリーズ(V30ソフトウェア)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なるアドレスファミリの設定を行わないでください。

[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。

14.2.9 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 G110

[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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

14.2.10 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 進数で指定します。

範囲	機種
0～19	Si-R G110

・rmt 定義の定義番号
利用する rmt の定義番号を、10 進数で指定します。

範囲	機種
0～99	Si-R G110

<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。

14.2.11 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 G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

14.2.12 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 G110

[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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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ときに優先度を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サーバへ登録するとき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
```

14.2.13 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 G110

[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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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
```

14.2.14 dvpn client ipv6 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 G110

[入力形式]

dvpn client [<number>] ipv6 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進数で指定します。
省略時は、0を指定したものとみなされます。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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> ipv6 route distance 1
```

第 15 章 ルーティングプロトコル情報の設定

15.1 ルーティングマネージャ情報

15.1.1 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 G110

[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 進数で指定します。

<external_distance>

・ EBGP 優先度
EBGP の優先度を、1～254 の 10 進数で指定します。

<internal_distance>

・ IBGP 優先度
IBGP の優先度を、1～254 の 10 進数で指定します。
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 進数で指定します。

<dns_distance>

・ DNS 優先度
DNS の優先度を、1～254 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]

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。登録済み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
```

15.1.2 routemanage ip redist rip

[機能]

RIP 再配布経路の設定

[適用機種]

Si-R G110

[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、0～14 の 10 進数で指定します。
  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。
  省略時は、現在設定されているメトリック値を指定したものとみなされます。
  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。

[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
```

15.1.3 routemanage ip redist bgp

[機能]

BGP 再配布経路の設定

[適用機種]

Si-R G110

[入力形式]

routemanage ip redist bgp <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。
- ospf
  OSPF 経路情報を示します。
- dns
  DNS 経路情報を示します。

<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。

[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
```

15.1.4 routemanage ip redist ospf

[機能]

OSPF 再配布経路の設定

[適用機種]

Si-R G110

[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。

[注意]

デフォルトルートの再配布については、 OSPF AS 境界ルータでのデフォルトルート広報の設定(ospf ip definfo)も参照してください。

[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
```

15.1.5 routemanage ip ecmp mode

[機能]

IPv4 ルーティングの ECMP の設定

[適用機種]

Si-R G110

[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 アドレスをもと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
```

15.1.6 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 G110

[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 の 10 進数で指定します。
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
```

15.1.7 routemanage ipv6 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 G110

[入力形式]

```
routemanage ipv6 distance rip <rip_distance>
routemanage ipv6 distance bgp <external_distance> [<internal_distance>]
routemanage ipv6 distance ospf <ospf_distance>
routemanage ipv6 distance dns <dns_distance>
routemanage ipv6 distance dhcp <dhcp_distance>
routemanage ipv6 distance ra <ra_distance>
```

[オプション]

<rip_distance>

・ RIP 優先度
RIP の優先度を、1～254 の 10 進数で指定します。

<external_distance>

・ EBGP 優先度
EBGP の優先度を、1～254 の 10 進数で指定します。

<internal_distance>

・ IBGP 優先度
IBGP の優先度を、1～254 の 10 進数で指定します。
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 進数で指定します。

<dns_distance>

・ DNS 優先度
DNS の優先度を、1～254 の 10 進数で指定します。

<dhcp_distance>

・ DHCP 優先度
DHCP の優先度を、1～254 の 10 進数で指定します。

<ra_distance>

・ RA 優先度
RA の優先度を、1～254 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]

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。

[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。登録済み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、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、DHCP の優先度を 10、RA 経路の優先度を 12 として優先経路選択を行うものとみなされます。

```
routemanage ipv6 distance rip 120
routemanage ipv6 distance bgp 20 200
routemanage ipv6 distance ospf 110
routemanage ipv6 distance dns 15
routemanage ipv6 distance dhcp 10
routemanage ipv6 distance ra 12
```

15.1.8 routemanage ipv6 redist rip

[機能]

IPv6 RIP 再配布経路の設定

[適用機種]

Si-R G110

[入力形式]

routemanage ipv6 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。
- 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、0～14 の 10 進数で指定します。
  BGP、OSPF、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。
  省略時は、現在設定されているメトリック値を指定したものとみなされます。
  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。

[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 ipv6 redist rip static on
routemanage ipv6 redist rip connected on
routemanage ipv6 redist rip bgp off 0
routemanage ipv6 redist rip ospf off 0
routemanage ipv6 redist rip dns off 0
routemanage ipv6 redist rip dhcp off 0
```

15.1.9 routemanage ipv6 redist bgp

[機能]

BGP IPv6 再配布経路の設定

[適用機種]

Si-R G110

[入力形式]

routemanage ipv6 redist bgp <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。
- ospf
  OSPF 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>

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。
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。

[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 ipv6 redist bgp static off
routemanage ipv6 redist bgp connected off
routemanage ipv6 redist bgp rip off
routemanage ipv6 redist bgp ospf off
routemanage ipv6 redist bgp dns off
routemanage ipv6 redist bgp dhcp off
```

15.1.10 routemanage ipv6 redist ospf

[機能]

IPv6 OSPF 再配布経路の設定

[適用機種]

Si-R G110

[入力形式]

routemanage ipv6 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。
- dhcp
  DHCP 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。
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。

[注意]

デフォルトルートの再配布については、 IPv6 OSPF AS 境界ルータでのデフォルトルート広報の設定(ospf ipv6 definfo)も参照してください。

[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 ipv6 redist ospf static off 20 type2
routemanage ipv6 redist ospf connected off 20 type2
routemanage ipv6 redist ospf rip off 20 type2
routemanage ipv6 redist ospf bgp off 20 type2
routemanage ipv6 redist ospf dns off 20 type2
routemanage ipv6 redist ospf dhcp off 20 type2
```

15.2 RIP情報

15.2.1 rip ip timers basic

[機能]

RIPタイマの設定

[適用機種]

Si-R G110

[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、10～3600秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
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、10～3600秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
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、10～3600秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
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
```

15.2.2 rip ip timers jitter

[機能]

RIP 定期広報ゆらぎ幅の設定

[適用機種]

Si-R G110

[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
```

15.2.3 rip ip multipath

[機能]

RIP マルチパスの設定

[適用機種]

Si-R G110

[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 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]

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、経路切り替わ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、追加済みの 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
```

15.2.4 rip ip redist

[機能]

RIP 再配布フィルタの設定

[適用機種]

Si-R G110

[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-R G110

<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
<address>/<mask>で指定した経路情報を本装置が保有する経路情報と比較し、完全一致したものをフィルタリング対象とします。

・ inexact
指定した<address>の先頭から<mask>ビット部分だけを本装置が保有する経路情報と比較し、一致したものを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。
- <prefix_match>は以下のように動作します。

  <address>/<mask>で"192.168.0.0/16"を指定し、本装置が以下の経路情報を保有している場合、exact を指定すると、"192.168.0.0/16"がフィルタリング対象となります。

  inexact を指定すると、"192.168.0.0"と一致する"192.168.0.0/16、192.168.1.0/24、192.168.1.1/32"の 3 つがフィルタリング対象となります。

  172.16.0.0/16

  192.168.0.0/16

  192.168.1.0/24

  192.168.1.1/32
- 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
50	Si-R G110

[注意]

フィルタリング条件で、遮断条件だけを設定した場合、すべての経路情報は RIP に再配布されません。RIP に再配布する IPv4 経路情報が存在する場合、透過条件に対象の経路情報を設定してください。

[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。

15.2.5 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 G110

[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-R G110

[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。

15.2.6 rip ip neighbor

[機能]

RIP ユニキャスト送信の設定

[適用機種]

Si-R G110

[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 進数で指定します。
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、ユニキャストで RIP パケットを送信します。
<neighbor_address>が属する LAN インタフェースに lan ip rip コマンドを設定することで、加算メトリックの設定、認証機能の使用が可能となります。
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。
この設定は RIP パケット送信に関してのみ利用されます。RIP パケットの受信は lan ip rip コマンドで設定してください。

[未設定時]

RIP ユニキャスト送信を設定しないものとみなされます。

15.2.7 rip ip gwfilter

[機能]

RIP 相手フィルタの設定

[適用機種]

Si-R G110

[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されます。

15.2.8 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 G110

[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。

15.2.9 rip ipv6 timers basic

[機能]

IPv6 RIP タイマの設定

[適用機種]

Si-R G110

[入力形式]

rip ipv6 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、10～3600 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
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、10～3600 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
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、10～3600 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
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 ipv6 timers basic 30s 3m 2m
```

15.2.10 rip ipv6 multipath

[機能]

IPv6 RIP マルチパスの設定

[適用機種]

Si-R G110

[入力形式]

rip ipv6 multipath <path_num>

[オプション]

<path_num>

・同一パス数
同一パス数を、1～2 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]

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、経路切り替わ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、追加済みの 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 ipv6 multipath 1
```

15.2.11 rip ipv6 redist

[機能]

IPv6 RIP 再配布フィルタの設定

[適用機種]

Si-R G110

[入力形式]

rip ipv6 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-R G110

<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
<address>/<prefixlen>で指定した経路情報を本装置が保有する経路情報と比較し、完全一致したものをフィルタリング対象とします。

・ inexact
指定した<address>の先頭から<prefixlen>ビット部分だけを本装置が保有する経路情報と比較し、一致したものを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。
- <prefix_match>は以下のように動作します。

  <address>/<prefixlen>で"2001:db8::/32"を指定し、本装置が以下の経路情報を保有している場合、exactを指定すると、"2001:db8::/32"がフィルタリング対象となります。

  inexactを指定すると、"2001:db8::"と一致する"2001:db8::/32、2001:db8:ffff::/48、2001:db8:ffff:1000::/64"の3つがフィルタリング対象となります。

  1000:db8::/32

  2001:db8::/32

  2001:db8:ffff::/48

  2001:db8:ffff:1000::/64
- 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
50	Si-R G110

[注意]

フィルタリング条件で、遮断条件だけを設定した場合、すべての経路情報はRIPに再配布されません。RIPに再配布するIPv6経路情報が存在する場合、透過条件に対象の経路情報を設定してください。

[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。

15.2.12 rip ipv6 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 G110

[入力形式]

rip ipv6 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-R G110

[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。

15.3 BGP 情報

15.3.1 bgp as

[機能]

BGP AS 番号の設定

[適用機種]

Si-R G110

[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 番号を以下に示す 4 オクテット AS 番号の形式で指定します。

0.0～65535.65535

0.0 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。

[注意]

BGP を利用する場合は、必ず設定してください。

[未設定時]

BGP を動作させないものとみなされます。

```
bgp as 0.0
```

15.3.2 bgp id

[機能]

BGP IDの設定

[適用機種]

Si-R G110

[入力形式]

bgp id <identifier>

[オプション]

<identifier>

・ BGPのID
0.0.0.0～255.255.255.255のIPv4アドレス形式で指定します。

[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。
本設定を省略時は、以下の基準に従いBGP IDが自動選択されます。

・ loopbackインタフェースに追加IPv4アドレスが設定されている場合は、そのIPv4アドレスを採用します。
・ loopbackインタフェースに追加IPv4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IPv4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。

なお、IPv4アドレスがひとつも設定されていないIPv6環境の場合、本IDを必ず設定してください。

[未設定時]

BGPのIDが指定されていないものとみなされます。

```
bgp id 0.0.0.0
```

15.3.3 bgp ip network route

[機能]

BGP IPv4 ネットワークの設定

[適用機種]

Si-R G110

[入力形式]

bgp ip network route [<count>] <address>/<mask>

[オプション]

<count>

・ BGP IPv4 ネットワークの定義番号
BGP IPv4 ネットワークの定義番号を、10 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。

範囲	機種
0～15	Si-R G110

<address>/<mask>

・ BGP 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)
BGP IPv4 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 IPv4 ネットワークアドレス/マスクビット数（例: 192.168.1.0/24）
－ BGP IPv4 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 IPv4 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 IPv4 経路情報を広報する場合に設定します。

bgp ip 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 IPv4 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 ip 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。

[未設定時]

BGP IPv4 ネットワークが設定されていないものとみなされます。

15.3.4 bgp ip network igp

[機能]

BGP IPv4 ネットワークの IGP との同期設定

[適用機種]

Si-R G110

[入力形式]

bgp ip 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 IPv4 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 IPv4 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 ip network igp on
```

15.3.5 bgp ip aggregate

[機能]

BGP IPv4 集約経路の設定

[適用機種]

Si-R G110

[入力形式]

bgp ip aggregate [<count>] <address>/<mask> [<action>]

[オプション]

<count>

・ BGP IPv4 集約経路の定義番号
集約経路の定義番号を、10 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。

範囲	機種
0～15	Si-R G110

<address>/<mask>

・ BGP IPv4 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 IPv4 集約経路アドレス/マスクビット数（例: 192.168.1.0/24）
－ BGP IPv4 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>

経路集約時の動作を指定します。

・ summary-only
BGP IPv4 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 IPv4 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 IPv4 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。

[未設定時]

BGP IPv4 集約経路が設定されていないものとみなされます。

15.3.6 bgp ip redist

[機能]

BGP IPv4 再配布フィルタの設定

[適用機種]

Si-R G110

[入力形式]

bgp 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-R G110

<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 IPv4 経路情報を透過します。

・ reject
該当する IPv4 経路情報を遮断します。

<address>/<mask>

フィルタリング対象とする IPv4 経路情報のネットワークアドレスを指定します。

・ 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 IPv4 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 IPv4 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>

IPv4 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>/<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
<address>/<mask>で指定した経路情報を本装置が保有する経路情報と比較し、完全一致したものをフィルタリング対象とします。

・ inexact
指定した<address>の先頭から<mask>ビット部分だけを本装置が保有する経路情報と比較し、一致したものを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 IPv4 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 IPv4 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。
- <prefix_match>は以下のように動作します。

  <address>/<mask>で"192.168.0.0/16"を指定し、本装置が以下の経路情報を保有している場合、exact を指定すると、"192.168.0.0/16"がフィルタリング対象となります。

  inexact を指定すると、"192.168.0.0"と一致する"192.168.0.0/16、192.168.1.0/24、192.168.1.1/32"の 3 つがフィルタリング対象となります。

  172.16.0.0/16
  192.168.0.0/16
  192.168.1.0/24
  192.168.1.1/32
- BGP IPv4 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
50	Si-R G110

[注意]

フィルタリング条件で、遮断条件だけを設定した場合、すべての経路情報は BGP に再配布されません。BGP に再配布する IPv4 経路情報が存在する場合、透過条件に対象の経路情報を設定してください。

[未設定時]

BGP IPv4 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。

15.3.7 bgp ip redist move

[機能]

BGP IPv4 再配布フィルタの優先順序の変更

[適用機種]

Si-R G110

[入力形式]

bgp 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-R G110

[動作モード]

構成定義モード(管理者クラス)

[説明]

BGP IPv4 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。

15.3.8 bgp ipv6 network route

[機能]

BGP IPv6 ネットワークの設定

[適用機種]

Si-R G110

[入力形式]

bgp ipv6 network route [<count>] <address>/<prefixlen>

[オプション]

<count>

・ BGP IPv6 ネットワークの定義番号
BGP IPv6 ネットワークの定義番号を、10 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。

範囲	機種
0～15	Si-R G110

<address>/<prefixlen>

・ BGP IPv6 ネットワークアドレス/プレフィックス長
BGP IPv6 ネットワークを IPv6 グローバル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。
以下に、有効な記述形式を示します。
－ BGP IPv6 ネットワークアドレス/プレフィックス長(例：3000::/64)

[動作モード]

構成定義モード(管理者クラス)

[説明]

BGP IPv6 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 IPv6 経路情報を広報する場合に設定します。

bgp ipv6 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 IPv6 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 ipv6 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。

[未設定時]

BGP IPv6 ネットワークが設定されていないものとみなされます。

15.3.9 bgp ipv6 network igp

[機能]

BGP IPv6 ネットワークの IGP との同期設定

[適用機種]

Si-R G110

[入力形式]

bgp ipv6 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 IPv6 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 IPv6 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 ipv6 network igp on
```

15.3.10 bgp ipv6 aggregate

[機能]

BGP IPv6 集約経路の設定

[適用機種]

Si-R G110

[入力形式]

bgp ipv6 aggregate [<count>] <address>/<prefixlen> [<action>]

[オプション]

<count>

・ BGP IPv6 集約経路の定義番号
集約経路の定義番号を、10 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。

範囲	機種
0～15	Si-R G110

<address>/<prefixlen>

・ BGP IPv6 集約経路アドレス/プレフィックス長
集約経路を IPv6 グローバル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。
以下に、有効な記述形式を示します。
－ BGP IPv6 集約経路アドレス/プレフィックス長(例：3000::/64)
::/0 は指定できません。

<action>

経路集約時の動作を指定します。

・ summary-only
BGP IPv6 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 IPv6 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 IPv6 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。

[未設定時]

BGP IPv6 集約経路が設定されていないものとみなされます。

15.3.11 bgp ipv6 redist

[機能]

BGP IPv6 再配布フィルタの設定

[適用機種]

Si-R G110

[入力形式]

bgp ipv6 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-R G110

<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 IPv6 経路情報を透過します。

・ reject
該当する IPv6 経路情報を遮断します。

<address>/<prefixlen>

フィルタリング対象とする IPv6 経路情報のネットワークアドレスを指定します。

・ IPv6 グローバルアドレス/プレフィックス長
フィルタリング対象とする IPv6 経路情報を、IPv6 グローバル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。
以下に、有効な記述形式を示します。
－ IPv6 グローバルアドレス/プレフィックス長(例：3000::/64)

・ any
すべての IPv6 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>

IPv6 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
<address>/<prefixlen>で指定した経路情報を本装置が保有する経路情報と比較し、完全一致したものをフィルタリング対象とします。

・ inexact
指定した<address>の先頭から<prefixlen>ビット部分だけを本装置が保有する経路情報と比較し、一致したものを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 IPv6 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 IPv6 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。
- <prefix_match>は以下のように動作します。

  <address>/<prefixlen>で"2001:db8::/32"を指定し、本装置が以下の経路情報を保有している場合、exact を指定すると、"2001:db8::/32"がフィルタリング対象となります。

  inexact を指定すると、"2001:db8::"と一致する"2001:db8::/32、2001:db8:ffff::/48、2001:db8:ffff:1000::/64"の 3 つがフィルタリング対象となります。

  1000:db8::/32

  2001:db8::/32

  2001:db8:ffff::/48

  2001:db8:ffff:1000::/64
- BGP 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
50	Si-R G110

[注意]

フィルタリング条件で、遮断条件だけを設定した場合、すべての経路情報は BGP に再配布されません。BGP に再配布する IPv6 経路情報が存在する場合、透過条件に対象の経路情報を設定してください。

[未設定時]

BGP 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。

15.3.12 bgp ipv6 redist move

[機能]

BGP IPv6 再配布フィルタの優先順序の変更

[適用機種]

Si-R G110

[入力形式]

bgp ipv6 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-R G110

[動作モード]

構成定義モード(管理者クラス)

[説明]

BGP 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。

15.4 BGP 相手側情報

15.4.1 bgp neighbor address

[機能]

BGP 相手側アドレスの設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<address>

相手装置のアドレスを指定します。

・ IPv4 アドレス
IPv4 経路情報を交換する場合に指定します。
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
IPv6 経路情報を交換する場合に指定します。
リンクローカルアドレスは指定できません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

相手装置のアドレスを設定します。

[注意]

BGP を利用する場合は、必ず設定してください。
IPv4、IPv6 相手装置はそれぞれ 4 つまで設定できます。

[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。

15.4.2 bgp neighbor as

[機能]

BGP 相手側 AS 番号の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<as_number>

・ 相手側 AS 番号
BGP 相手側 AS 番号を、0.1～65535.65535 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]

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。

[注意]

BGP を利用する場合は、必ず設定してください。

[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。

15.4.3 bgp neighbor timers

[機能]

BGP 無通信監視タイマの設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<keepalive>

・ keepalive タイマ値
keepalive タイマ値を、1～65535 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
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
HoldTime のタイマ値を、3～65535 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。
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
```

15.4.4 bgp neighbor ebgp-multihop

[機能]

EBGP マルチホップの設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<ttl>

・ ホップ数
ホップ数を、1～255 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]

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(IPv4 パケットの TTL 値、IPv6 パケットの hoplimit 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
```

15.4.5 bgp neighbor family

[機能]

BGP アドレスファミリの設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<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。

・ ipv6
アドレスファミリとして IPv6 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 で送受信する経路情報のアドレスファミリを設定します。

[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
```

15.4.6 bgp neighbor source

[機能]

BGP 自側アドレスの設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<address>

相手装置との接続に使用する自側アドレスを設定します。

・ 自インタフェース IPv4 アドレス
相手装置と IPv4 で接続する場合に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

・ 自インタフェース IPv6 アドレス
相手装置と IPv6 で接続する場合に自装置のインタフェースのアドレスを指定します。
リンクローカルアドレスは指定できません。

この値は、bgp neighbor address コマンドで指定したアドレスの形式に合わせる必要があります。

[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アドレスを設定します。

[未設定時]

BGP セッションの自側アドレスを自動的に選択するものとみなされます。

15.4.7 bgp neighbor authentication

[機能]

BGP TCP-MD5 認証鍵の設定

[適用機種]

Si-R G110

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<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。

[注意]

BGP 相手側アドレスで<address>に IPv6 アドレスを設定した場合は無効となります。

[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。

15.4.8 bgp neighbor graceful-restart family

[機能]

BGP グレースフルリスタートを使用するアドレスファミリの設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] graceful-restart family <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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<family>

相手装置との間でグレースフルリスタート機能を使用するアドレスファミリを指定します。

・ ipv4
IPv4 ユニキャストの経路に対してグレースフルリスタート処理を行います。

[動作モード]

構成定義モード(管理者クラス)

[説明]

相手装置との BGP セッションでグレースフルリスタート機能を使用するアドレスファミリを指定します。
相手装置との間で、ここで指定したアドレスファミリに対してのみ、グレースフルリスタートの処理が実施されます。
本装置ではレシーブルータの機能のみが有効になります。

[未設定時]

相手装置との間でグレースフルリスタート機能を使用しないものとみなされます。

15.4.9 bgp neighbor graceful-restart stale-timer

[機能]

BGP グレースフルリスタート機能の stale タイマの設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] graceful-restart stale-timer <time>

[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 進数で指定します。

省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<time>

・ stale タイマ値

グレースフルリスタート処理の開始により一時的に削除を保留している経路の最大保持時間を、1～65535 秒の範囲で指定します。

単位は、h(時)、m(分)、s(秒)のいずれかを指定します。

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]

相手装置とのグレースフルリスタート処理による BGP セッションの切断が発生した場合に、その相手装置から受信した経路を削除するまでの最大待ち時間を指定します。指定した時間の間、経路をルーティングテーブルに保持することにより、パケットの転送能力を保持したまま、グレースフルリスタート処理の完了を待ち合わせます。

このタイマ値は、相手装置から OPEN メッセージで通知されるグレースフルリスタートの Restart タイマより大きくしておく必要があります。小さい値を設定すると、自動的に Restart タイマの値に変更されます。

bgp neighbor graceful-restart family で指定されていないアドレスファミリに対しては、このタイマは有効になりません。その場合、このタイマの設定にかかわらず、そのアドレスファミリの経路はグレースフルリスタート開始時に即時に削除されます。

[未設定時]

stale タイマに 360 秒が設定されているものとして扱います。

```
bgp neighbor <count> graceful-restart stale-timer 360s
```

15.4.10 bgp neighbor community

[機能]

BGP コミュニティ属性の設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] community <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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<mode>

コミュニティ属性を送信するかしないかを指定します。

・ on
コミュニティ属性を送信します。

・ off
コミュニティ属性を送信しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

BGP コミュニティ属性を送信するかしないかを設定します。

<mode>に on を設定した場合は、本装置や他装置で設定したコミュニティ属性を送信します。

本装置で設定する場合は、経路情報は bgp neighbor filter コマンドで指定します。

なお、経路情報にコミュニティ属性が設定されていた場合は上書きされます。

<mode>に off を設定した場合は、コミュニティ属性を送信しません。他装置が設定したコミュニティ属性も取り外して送信します。

[注意]

本設定を変更し commit コマンドを実行後、相手装置とのセッションが切断されなかった場合、相手装置にすでに送信済みの経路に対しては、変更内容が反映されません。経路変動などにより相手装置に経路を送信するタイミングで、設定変更が反映されます。すぐに変更を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

clear ip bgp neighbors address 相手装置アドレス soft out
clear ipv6 bgp neighbors address 相手装置アドレス soft out

[未設定時]

BGP コミュニティ属性を送信するものとみなされます。

```
bgp neighbor community on
```

15.4.11 bgp neighbor ip medmetric

[機能]

BGP IPv4 MED メトリックの設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ip 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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<medmetric>

・ 相手装置に広報する IPv4 経路情報の MED メトリック値
相手装置に広報する IPv4 経路情報の MED メトリック値を、0～4294967295 の 10 進数で指定します。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 IPv4 経路情報の 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 IPv4 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 IPv4 送信用フィルタを設定している場合は、本設定が無効になります。BGP 相手側アドレスで<address>に IPv6 アドレスを設定した場合は無効となります。

本設定を行い commit コマンドを実行後に相手装置とのセッションが切断されなかった場合、相手装置に設定内容が反映されません。すぐに設定を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

```
clear ip bgp neighbors address 相手装置アドレス soft out
```

[未設定時]

IPv4 経路情報の 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> ip medmetric 0
```

15.4.12 bgp neighbor ip asprepend

[機能]

BGP IPv4 AS パスプリペンドの設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ip 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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<asprepend>

・ AS 番号の追加数
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 EBGP で広報する IPv4 経路情報の AS 番号の個数を追加します。
<asprepend>で 0 を指定した場合は、追加される IPv4 経路情報の AS 番号は、自 AS 番号だけの 1 個として扱われます。

[注意]

BGP IPv4 送信用フィルタを設定している場合は、本設定が無効になります。
BGP 相手側アドレスで<address>に IPv6 アドレスを設定した場合は無効となります。
本設定を行い commit コマンドを実行後に相手装置とのセッションが切断されなかった場合、相手装置に設定内容が反映されません。すぐに設定を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

```
clear ip bgp neighbors address 相手装置アドレス soft out
```

[未設定時]

広報する IPv4 経路情報の AS 番号の個数を追加しないとみなされます。

```
bgp neighbor <count> ip asprepend 0
```

15.4.13 bgp neighbor ip localpref

[機能]

BGP IPv4 ローカル優先度の設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ip 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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<localpref>

・ ローカル優先度
ローカル優先度を、0～4294967295 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]

EBGP で受信する IPv4 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 IPv4 受信用フィルタを設定している場合は、本設定が無効になります。
BGP 相手側アドレスで<address>に IPv6 アドレスを設定した場合は無効となります。
本設定を行い commit コマンドを実行後に相手装置とのセッションが切断されなかった場合、相手装置に設定内容が反映されません。すぐに設定を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

```
clear ip bgp neighbors address 相手装置アドレス soft in
```

[未設定時]

EBGP で受信する IPv4 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> ip localpref 100
```

15.4.14 bgp neighbor ip nexthopself

[機能]

BGP IPv4 ネクストホップセルフの設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ip 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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<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 IPv4 経路情報のネクストホップを、自装置の IPv4 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 IPv4 経路情報のネクストホップを自装置の IPv4 アドレスに上書きして広報します。

<mode>に off を設定した場合は、IBGP で広報する IPv4 経路情報のネクストホップに BGP プロトコルの規定に従った値を設定して広報します。

[注意]

BGP 相手側アドレスで<address>に IPv6 アドレスを設定した場合は無効となります。

本設定を行い commit コマンドを実行後に相手装置とのセッションが切断されなかった場合、相手装置に設定内容が反映されません。すぐに設定を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

```
clear ip bgp neighbors address 相手装置アドレス soft out
```

[未設定時]

IBGP で広報する IPv4 経路情報のネクストホップを自装置の IPv4 アドレスに上書きしないものとみなされます。

```
bgp neighbor <count> ip nexthopself off
```

15.4.15 bgp neighbor ip default-originate

[機能]

BGP IPv4デフォルトルート広報可否の設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ip 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進数で指定します。
省略時は、0を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<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]

IPv4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IPv4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IPv4経路情報にデフォルトルートがあっても広報しません。

[注意]

BGP相手側アドレスで<address>にIPv6アドレスを設定した場合は無効となります。
本設定を行いcommitコマンドを実行後に相手装置とのセッションが切断されなかった場合、相手装置に設定内容が反映されません。すぐに設定を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

```
clear ip bgp neighbors address 相手装置アドレス soft out
```

[未設定時]

IPv4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> ip default-originate off
```

15.4.16 bgp neighbor ip filter act

[機能]

BGP IPv4 フィルタの動作設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ip 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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<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
0～199	Si-R G110

<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 IPv4 経路情報を透過します。

・ reject
該当する IPv4 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 IPv4 経路情報送受信時に、フィルタリング条件に一致した IPv4 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 IPv4 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 IPv4 経路情報は遮断されます。

フィルタリング条件は、bgp neighbor ip filter as コマンドを使用し AS 番号を、または、bgp neighbor ip filter route コマンドを使用し IPv4 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 IPv4 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
200	Si-R G110

[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 相手側アドレスで<address>に IPv6 アドレスを設定した場合は無効となります。

相手情報設定で MED メトリックを設定している場合は、以下に注意してください。

・ BGP IPv4 送信用フィルタで MED メトリック変更の設定を行った場合、フィルタ設定が有効となります。

・ BGP IPv4 送信用フィルタで MED メトリック変更の設定を行っていない場合、0 が広報されます。

相手情報設定で AS パスプリペンドを設定している場合は、以下に注意してください。

・ BGP IPv4 送信用フィルタで AS パスプリペンド変更の設定を行った場合、フィルタ設定が有効となります。

・ BGP IPv4 送信用フィルタで AS パスプリペンド変更の設定を行っていない場合、AS 番号を追加しません。

相手情報設定でローカル優先度を設定している場合は、以下に注意してください。

・ BGP IPv4 受信用フィルタでローカル優先度変更の設定を行った場合、フィルタ設定が有効となります。

・ BGP IPv4 受信用フィルタでローカル優先度変更の設定を行っていない場合、100 が設定されます。

本設定を行い commit コマンドを実行後に相手装置とのセッションが切断されなかった場合、相手装置に設定内容が反映されません。すぐに設定を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

```
clear ip bgp neighbors address 相手装置アドレス soft both
```

[未設定時]

BGP IPv4 フィルタを使用しないものとみなされ、すべての BGP の IPv4 経路情報を透過します。

15.4.17 bgp neighbor ip filter move

[機能]

BGP IPv4 フィルタの優先順序の変更

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ip 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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<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
0～199	Si-R G110

[動作モード]

構成定義モード(管理者クラス)

[説明]

BGP IPv4 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。

[注意]

本設定を行い commit コマンドを実行後に相手装置とのセッションが切断されなかった場合、相手装置に設定内容が反映されません。すぐに設定を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

clear ip bgp neighbors address 相手装置アドレス soft both

15.4.18 bgp neighbor ip filter as

[機能]

BGP IPv4フィルタのAS番号設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ip 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進数で指定します。
省略時は、0を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<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進数で指定します。

範囲	機種
0～199	Si-R G110

<as_number>

・AS番号
AS番号を、以下に示す4オクテットAS番号の形式で指定します。

0.1～65535.65535

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv4経路情報のAS番号をフィルタ条件として設定します。

[注意]

BGP相手側アドレスで<address>にIPv6アドレスを設定した場合は無効となります。

本設定を行いcommitコマンドを実行後に相手装置とのセッションが切断されなかった場合、相手装置に設定内容が反映されません。すぐに設定を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

clear ip bgp neighbors address 相手装置アドレス soft both

[未設定時]

IPv4経路情報のAS番号をフィルタ条件としないものとみなされます。

15.4.19 bgp neighbor ip filter route

[機能]

BGP IPv4 フィルタの経路情報設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ip 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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<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 進数で指定します。

範囲	機種
0～199	Si-R G110

<address>/<mask>

フィルタリング対象とする IPv4 経路情報のネットワークアドレスを指定します。

・ 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
<address>/<mask>で指定した経路情報を本装置が保有する経路情報と比較し、完全一致したものをフィルタリング対象とします。

・ inexact
指定した<address>の先頭から<mask>ビット部分だけを本装置が保有する経路情報と比較し、一致したものを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]

IPv4 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 番号のみがフィルタ条件となります。

  BGP 相手側アドレスで<address>に IPv6 アドレスを設定した場合は無効となります。
- <prefix_match>は以下のように動作します。

  <address>/<mask>で"192.168.0.0/16"を指定し、本装置が以下の経路情報を保有している場合、exact を指定すると、"192.168.0.0/16"がフィルタリング対象となります。

  inexact を指定すると、"192.168.0.0"と一致する"192.168.0.0/16、192.168.1.0/24、192.168.1.1/32"の 3 つがフィルタリング対象となります。

  172.16.0.0/16

  192.168.0.0/16

  192.168.1.0/24

  192.168.1.1/32
- 本設定を行い commit コマンドを実行後に相手装置とのセッションが切断されなかった場合、相手装置に設定内容が反映されません。すぐに設定を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

  clear ip bgp neighbors address 相手装置アドレス soft both

[未設定時]

IPv4 経路情報をフィルタ条件としないものとみなされます。

15.4.20 bgp neighbor ip filter set medmetric

[機能]

BGP IPv4 フィルタの MED メトリック設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ip 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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<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 進数で指定します。

範囲	機種
0～199	Si-R G110

<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 IPv4 経路情報の 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。
BGP 相手側アドレスで<address>に IPv6 アドレスを設定した場合は無効となります。

相手情報設定で MED メトリックを設定している場合は、以下に注意してください。
・ BGP IPv4 送信用フィルタで MED メトリック変更の設定を行った場合、フィルタ設定が有効となります。
・ BGP IPv4 送信用フィルタで MED メトリック変更の設定を行っていない場合、0 が広報されます。
本設定を行い commit コマンドを実行後に相手装置とのセッションが切断されなかった場合、相手装置に設定内容が反映されません。すぐに設定を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

```
clear ip bgp neighbors address 相手装置アドレス soft out
```

［未設定時］

MED メトリック値を 0 として広報します。

15.4.21 bgp neighbor ip filter set asprepend

[機能]

BGP IPv4 フィルタの AS パスプリペンド設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ip 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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<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 進数で指定します。

範囲	機種
0～199	Si-R G110

<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 IPv4 経路情報の 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。
BGP 相手側アドレスで<address>に IPv6 アドレスを設定した場合は無効となります。

相手情報設定で AS パスプリペンドを設定している場合は、以下に注意してください。
・ BGP IPv4 送信用フィルタで AS パスプリペンド変更の設定を行った場合、フィルタ設定が有効となります。
・ BGP IPv4 送信用フィルタで AS パスプリペンド変更の設定を行っていない場合、AS 番号を追加しません。
本設定を行い commit コマンドを実行後に相手装置とのセッションが切断されなかった場合、相手装置に設定内容が反映されません。すぐに設定を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

```
clear ip bgp neighbors address 相手装置アドレス soft out
```

［未設定時］

AS 番号の追加を行わないものとみなされます。

15.4.22 bgp neighbor ip filter set localpref

[機能]

BGP IPv4 フィルタのローカル優先度設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ip 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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<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 進数で指定します。

範囲	機種
0～199	Si-R G110

<localpref>

・ ローカル優先度
ローカル優先度を、0～4294967295 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]

EBGP で受信する IPv4 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。
BGP 相手側アドレスで<address>に IPv6 アドレスを設定した場合は無効となります。

相手情報設定でローカル優先度を設定している場合は、以下に注意してください。
・ BGP IPv4 受信用フィルタでローカル優先度変更の設定を行った場合、フィルタ設定が有効となります。
・ BGP IPv4 受信用フィルタでローカル優先度変更の設定を行っていない場合、100 が設定されます。
本設定を行い commit コマンドを実行後に相手装置とのセッションが切断されなかった場合、相手装置に設定内容が反映されません。すぐに設定を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

```
clear ip bgp neighbors address 相手装置アドレス soft in
```

［未設定時］

EBGP で受信する IPv4 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。

15.4.23 bgp neighbor ip filter set community

[機能]

BGP IPv4 フィルタのコミュニティ属性の設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ip filter <number> set community <value>

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<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 進数で指定します。

範囲	機種
0～199	Si-R G110

<value>

・ コミュニティ属性
相手装置に広報するコミュニティ属性値を、16 進数で 0x0～0xffffffff 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]

相手装置に広報するコミュニティ属性の値を設定します。
送信時のフィルタ条件に一致した場合、コミュニティ属性に<value>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、コミュニティ属性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。
BGP 相手側アドレスで<address>に IPv6 アドレスを設定した場合は無効となります。
bgp neighbor community コマンドが on になっていない場合、本コマンドの設定は無効となります。
本設定を変更し commit コマンドを実行後、相手装置とのセッションが切断されなかった場合、相手装置にすでに送信済みの経路に対しては、変更内容が反映されません。経路変動などにより相手装置に経路を送信するタイミングで、設定変更が反映されます。すぐに変更を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

```
clear ip bgp neighbors address 相手装置アドレス soft out
```

[未設定時]

本装置で community 属性を設定しないものとみなされます。

15.4.24 bgp neighbor ipv6 medmetric

[機能]

BGP IPv6 MED メトリックの設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<medmetric>

・ 相手装置に広報する IPv6 経路情報の MED メトリック値
相手装置に広報する IPv6 経路情報の MED メトリック値を、0～4294967295 の 10 進数で指定します。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 IPv6 経路情報の 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 IPv6 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 IPv6 送信用フィルタを設定している場合は、本設定が無効になります。

BGP 相手側アドレスで<address>に IPv4 アドレスを設定した場合は無効となります。

本設定を行い commit コマンドを実行後に相手装置とのセッションが切断されなかった場合、相手装置に設定内容が反映されません。すぐに設定を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

```
clear ipv6 bgp neighbors address 相手装置アドレス soft out
```

[未設定時]

IPv6 経路情報の 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> ipv6 medmetric 0
```

15.4.25 bgp neighbor ipv6 asprepend

[機能]

BGP IPv6 AS パスプリペンドの設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<asprepend>

・ AS 番号の追加数
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 EBGP で広報する IPv6 経路情報の AS 番号の個数を追加します。
<asprepend>で 0 を指定した場合は、追加される IPv6 経路情報の AS 番号は、自 AS 番号だけの 1 個として扱われます。

[注意]

BGP IPv6 送信用フィルタを設定している場合は、本設定が無効になります。
BGP 相手側アドレスで<address>に IPv4 アドレスを設定した場合は無効となります。
本設定を行い commit コマンドを実行後に相手装置とのセッションが切断されなかった場合、相手装置に設定内容が反映されません。すぐに設定を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

```
clear ipv6 bgp neighbors address 相手装置アドレス soft out
```

[未設定時]

広報する IPv6 経路情報の AS 番号の個数を追加しないとみなされます。

```
bgp neighbor <count> ipv6 asprepend 0
```

15.4.26 bgp neighbor ipv6 localpref

[機能]

BGP IPv6 ローカル優先度の設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<localpref>

・ ローカル優先度
ローカル優先度を、0～4294967295 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]

EBGP で受信する IPv6 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 IPv6 受信用フィルタを設定している場合は、本設定が無効になります。
BGP 相手側アドレスで<address>に IPv4 アドレスを設定した場合は無効となります。
本設定を行い commit コマンドを実行後に相手装置とのセッションが切断されなかった場合、相手装置に設定内容が反映されません。すぐに設定を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

```
clear ipv6 bgp neighbors address 相手装置アドレス soft in
```

[未設定時]

EBGP で受信する IPv6 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> ipv6 localpref 100
```

15.4.27 bgp neighbor ipv6 nexthopself

[機能]

BGP IPv6 ネクストホップセルフの設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<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 IPv6 経路情報のネクストホップを、自装置の IPv6 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 IPv6 経路情報のネクストホップを自装置の IPv6 アドレスに上書きして広報します。

<mode>に off を設定した場合は、IBGP で広報する IPv6 経路情報のネクストホップに BGP プロトコルの規定に従った値を設定して広報します。

[注意]

BGP 相手側アドレスで<address>に IPv4 アドレスを設定した場合は無効となります。

本設定を行い commit コマンドを実行後に相手装置とのセッションが切断されなかった場合、相手装置に設定内容が反映されません。すぐに設定を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

```
clear ipv6 bgp neighbors address 相手装置アドレス soft out
```

[未設定時]

IBGP で広報する IPv6 経路情報のネクストホップを自装置の IPv6 アドレスに上書きしないものとみなされます。

```
bgp neighbor <count> ipv6 nexthopself off
```

15.4.28 bgp neighbor ipv6 default-originate

[機能]

BGP IPv6デフォルトルート広報可否の設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ipv6 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進数で指定します。
省略時は、0を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<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]

IPv6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IPv6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IPv6経路情報にデフォルトルートがあっても広報しません。

[注意]

BGP相手側アドレスで<address>にIPv4アドレスを設定した場合は無効となります。
本設定を行いcommitコマンドを実行後に相手装置とのセッションが切断されなかった場合、相手装置に設定内容が反映されません。すぐに設定を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

```
clear ipv6 bgp neighbors address 相手装置アドレス soft out
```

[未設定時]

IPv6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> ipv6 default-originate off
```

15.4.29 bgp neighbor ipv6 filter act

[機能]

BGP IPv6 フィルタの動作設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<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
0～199	Si-R G110

<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 IPv6 経路情報を透過します。

・ reject
該当する IPv6 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 IPv6 経路情報送受信時に、フィルタリング条件に一致した IPv6 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 IPv6 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 IPv6 経路情報は遮断されます。

フィルタリング条件は、bgp neighbor ipv6 filter as コマンドを使用し AS 番号を、または、bgp neighbor ipv6 filter route コマンドを使用し IPv6 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 IPv6 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
200	Si-R G110

[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 相手側アドレスで<address>に IPv4 アドレスを設定した場合は無効となります。

相手情報設定で MED メトリックを設定している場合は、以下に注意してください。
・ BGP IPv6 送信用フィルタで MED メトリック変更の設定を行った場合、フィルタ設定が有効となります。
・ BGP IPv6 送信用フィルタで MED メトリック変更の設定を行っていない場合、0 が広報されます。
相手情報設定で AS パスプリペンドを設定している場合は、以下に注意してください。
・ BGP IPv6 送信用フィルタで AS パスプリペンド変更の設定を行った場合、フィルタ設定が有効となります。
・ BGP IPv6 送信用フィルタで AS パスプリペンド変更の設定を行っていない場合、AS 番号を追加しません。
相手情報設定でローカル優先度を設定している場合は、以下に注意してください。
・ BGP IPv6 受信用フィルタでローカル優先度変更の設定を行った場合、フィルタ設定が有効となります。
・ BGP IPv6 受信用フィルタでローカル優先度変更の設定を行っていない場合、100 が設定されます。
本設定を行い commit コマンドを実行後に相手装置とのセッションが切断されなかった場合、相手装置に設定内容が反映されません。すぐに設定を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

```
clear ipv6 bgp neighbors address 相手装置アドレス soft both
```

[未設定時]

BGP IPv6 フィルタを使用しないものとみなされ、すべての BGP の IPv6 経路情報が透過します。

15.4.30 bgp neighbor ipv6 filter move

[機能]

BGP IPv6 フィルタの優先順序の変更

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<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
0～199	Si-R G110

[動作モード]

構成定義モード(管理者クラス)

[説明]

BGP IPv6 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。

[注意]

本設定を行い commit コマンドを実行後に相手装置とのセッションが切断されなかった場合、相手装置に設定内容が反映されません。すぐに設定を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

clear ipv6 bgp neighbors address 相手装置アドレス soft both

15.4.31 bgp neighbor ipv6 filter as

[機能]

BGP IPv6フィルタのAS番号設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ipv6 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進数で指定します。
省略時は、0を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<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進数で指定します。

範囲	機種
0～199	Si-R G110

<as_number>

・ AS番号
AS番号を、以下に示す4オクテットAS番号の形式で指定します。

0.1～65535.65535

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6経路情報のAS番号をフィルタ条件として設定します。

[注意]

BGP相手側アドレスで<address>にIPv4アドレスを設定した場合は無効となります。

本設定を行いcommitコマンドを実行後に相手装置とのセッションが切断されなかった場合、相手装置に設定内容が反映されません。すぐに設定を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

clear ipv6 bgp neighbors address 相手装置アドレス soft both

[未設定時]

IPv6経路情報のAS番号をフィルタ条件としないものとみなされます。

15.4.32 bgp neighbor ipv6 filter route

[機能]

BGP IPv6 フィルタの経路情報設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ipv6 filter <number> route <address>/<prefixlen> [<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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<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 進数で指定します。

範囲	機種
0～199	Si-R G110

<address>/<prefixlen>

フィルタリング対象とする IPv6 経路情報のネットワークアドレスを指定します。

・ 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ルーティング情報を、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。
リンクローカルアドレスは指定できません。
以下に、有効な記述形式を示します。
－ IPv6 アドレス/プレフィックス長(例：3000::/64)

・ 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 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
<address>/<prefixlen>で指定した経路情報を本装置が保有する経路情報と比較し、完全一致したものをフィルタリング対象とします。

・ inexact
指定した<address>の先頭から<prefixlen>ビット部分だけを本装置が保有する経路情報と比較し、一致したものを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]

IPv6 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。

  BGP 相手側アドレスで<address>に IPv4 アドレスを設定した場合は無効となります。

- <prefix_match>は以下のように動作します。

  <address>/<prefixlen>で"2001:db8::/32"を指定し、本装置が以下の経路情報を保有している場合、exact を指定すると、"2001:db8::/32"がフィルタリング対象となります。

  inexact を指定すると、"2001:db8::"と一致する"2001:db8::/32、2001:db8:ffff::/48、2001:db8:ffff:1000::/64"の 3 つがフィルタリング対象となります。

  1000:db8::/32

  2001:db8::/32

  2001:db8:ffff::/48

  2001:db8:ffff:1000::/64

- 本設定を行い commit コマンドを実行後に相手装置とのセッションが切断されなかった場合、相手装置に設定内容が反映されません。すぐに設定を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

  clear ipv6 bgp neighbors address 相手装置アドレス soft both

[未設定時]

IPv6 経路情報をフィルタ条件としないものとみなされます。

15.4.33 bgp neighbor ipv6 filter set medmetric

[機能]

BGP IPv6フィルタのMEDメトリック設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ipv6 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進数で指定します。
省略時は、0を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<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進数で指定します。

範囲	機種
0～199	Si-R G110

<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IPv6経路情報の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。
BGP相手側アドレスで<address>にIPv4アドレスを設定した場合は無効となります。
相手情報設定でMEDメトリックを設定している場合は、以下に注意してください。

・ BGP IPv6送信用フィルタで MEDメトリック変更の設定を行った場合、フィルタ設定が有効となります。
・ BGP IPv6送信用フィルタで MEDメトリック変更の設定を行っていない場合、0が広報されます。

本設定を行いcommitコマンドを実行後に相手装置とのセッションが切断されなかった場合、相手装置に設定内容が反映されません。すぐに設定を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

```
clear ipv6 bgp neighbors address 相手装置アドレス soft out
```

[未設定時]

IPv6経路情報のMEDメトリック値を0として広報します。

15.4.34 bgp neighbor ipv6 filter set asprepend

[機能]

BGP IPv6 フィルタの AS パスプリペンド設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<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 進数で指定します。

範囲	機種
0～199	Si-R G110

<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 IPv6 経路情報の 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。
BGP 相手側アドレスで<address>に IPv4 アドレスを設定した場合は無効となります。

相手情報設定で AS パスプリペンドを設定している場合は、以下に注意してください。

・ BGP IPv6 送信用フィルタで AS パスプリペンド変更の設定を行った場合、フィルタ設定が有効となります。
・ BGP IPv6 送信用フィルタで AS パスプリペンド変更の設定を行っていない場合、AS 番号を追加しません。

本設定を行い commit コマンドを実行後に相手装置とのセッションが切断されなかった場合、相手装置に設定内容が反映されません。すぐに設定を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

```
clear ipv6 bgp neighbors address 相手装置アドレス soft out
```

［未設定時］

IPv6 経路情報の AS 番号の追加を行わないものとみなされます。

15.4.35 bgp neighbor ipv6 filter set localpref

[機能]

BGP IPv6 フィルタのローカル優先度設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ipv6 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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<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 進数で指定します。

範囲	機種
0～199	Si-R G110

<localpref>

・ ローカル優先度
ローカル優先度を、0～4294967295 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]

EBGP で受信する IPv6 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。
BGP 相手側アドレスで<address>に IPv4 アドレスを設定した場合は無効となります。

相手情報設定でローカル優先度を設定している場合は、以下に注意してください。
・ BGP IPv6 受信用フィルタでローカル優先度変更の設定を行った場合、フィルタ設定が有効となります。
・ BGP IPv6 受信用フィルタでローカル優先度変更の設定を行っていない場合、100 が設定されます。
本設定を行い commit コマンドを実行後に相手装置とのセッションが切断されなかった場合、相手装置に設定内容が反映されません。すぐに設定を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

```
clear ipv6 bgp neighbors address 相手装置アドレス soft in
```

［未設定時］

EBGP で受信する IPv6 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。

15.4.36 bgp neighbor ipv6 filter set community

[機能]

BGP IPv6 フィルタのコミュニティ属性の設定

[適用機種]

Si-R G110

[入力形式]

bgp neighbor [<count>] ipv6 filter <number> set community <value>

[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 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～7	Si-R G110

<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 進数で指定します。

範囲	機種
0～199	Si-R G110

<value>

・ コミュニティ属性
相手装置に広報するコミュニティ属性値を、16 進数で 0x0～0xffffffff 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]

相手装置に広報するコミュニティ属性の値を設定します。
送信時のフィルタ条件に一致した場合、コミュニティ属性に<value>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、コミュニティ属性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。
BGP 相手側アドレスで<address>に IPv4 アドレスを設定した場合は無効となります。
bgp neighbor community コマンドが on になっていない場合、本コマンドの設定は無効となります。

本設定を変更し commit コマンドを実行後、相手装置とのセッションが切断されなかった場合、相手装置にすでに送信済みの経路に対しては、変更内容が反映されません。経路変動などにより相手装置に経路を送信するタイミングで、設定変更が反映されます。すぐに変更を反映したい場合は、以下のコマンドを実行して、相手装置との経路情報の再交換を実施してください。

clear ipv6 bgp neighbors address 相手装置アドレス soft out

[未設定時]

本装置で community 属性を設定しないものとみなされます。

15.5 OSPF 情報

15.5.1 ospf ip id

[機能]

OSPF ID の設定

[適用機種]

Si-R G110

[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
```

15.5.2 ospf ipv6 id

[機能]

IPv6 OSPF IDの設定

[適用機種]

Si-R G110

[入力形式]

ospf ipv6 id <identifier>

[オプション]

<identifier>

・ OSPFのID
OSPF IDを0.0.0.1～255.255.255.255のIPv4アドレス表記(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]

IPv6 OSPF接続での自装置を一意に示すルータ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てください。

[注意]

IPv6 OSPFを利用する場合は、OSPF IDを必ず設定してください。
未設定時の自動設定機能はありません。

[未設定時]

IPv6 OSPFを利用しないものとみなされます。

15.6 OSPF エリア情報

15.6.1 ospf ip area id

[機能]

OSPF エリア ID の設定

[適用機種]

Si-R G110

[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
0～2	Si-R G110

<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。

15.6.2 ospf ip area type

[機能]

OSPF エリアタイプの設定

[適用機種]

Si-R G110

[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
0～2	Si-R G110

<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
```

15.6.3 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 G110

[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
0～2	Si-R G110

<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
```

15.6.4 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 G110

[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
0～2	Si-R G110

<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
0～3	Si-R G110

<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。

［注意］

装置内に同一あて先、または、包含関係にある集約経路の定義を設定できません。

［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。

15.6.5 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 G110

[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
0～2	Si-R G110

<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
0～29	Si-R G110

<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

  <address>/<mask>で指定した経路情報を本装置が保有する経路情報と比較し、完全一致したものをサマリLSA入出力可否の対象とします。

- inexact

  指定した<address>の先頭から<mask>ビット部分だけを本装置が保有する経路情報と比較し、一致したものをサマリ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。
- <prefix_match>は以下のように動作します。

  <address>/<mask>で"192.168.0.0/16"を指定し、本装置が以下の経路情報を保有している場合、exactを指定すると、"192.168.0.0/16"がサマリLSA入出力可否の対象となります。

  inexactを指定すると、"192.168.0.0"と一致する"192.168.0.0/16、192.168.1.0/24、192.168.1.1/32"の3つがサマリLSA入出力可否の対象となります。

  172.16.0.0/16

  192.168.0.0/16

  192.168.1.0/24

  192.168.1.1/32
- 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
30	Si-R G110

[注意]

本機能の出力方向の設定と、OSPFエリア内部集約経路機能を併用する場合は、以下の点に注意してください。

- エリア内部集約経路機能の動作は、本機能の出力方向の条件検索、および条件に一致した場合の動作実行後となります。このため、本機能により、集約対象となる経路がすべて遮断された場合、集約経路は生成されません。

以下の経路情報は、本機能で制御できません。

- 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。

15.6.6 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 G110

[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
0～2	Si-R G110

<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
0～29	Si-R G110

[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。

15.6.7 ospf ipv6 area id

[機能]

IPv6 OSPF エリア ID の設定

[適用機種]

Si-R G110

[入力形式]

ospf ipv6 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
0～2	Si-R G110

<area_id>

・エリア ID

エリア ID を 0.0.0.0～255.255.255.255 の IPv4 アドレス表記(ドット形式)または 0～4294967295 の 10 進数表記で指定します。

バックボーンエリアの場合は 0.0.0.0 または 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]

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。

15.6.8 ospf ipv6 area type

[機能]

IPv6 OSPF エリアタイプの設定

[適用機種]

Si-R G110

[入力形式]

ospf ipv6 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
0～2	Si-R G110

<area_type>

エリアタイプを指定します。

・ normal
通常エリア。

・ stub
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 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 ipv6 area <area_number> type normal
```

15.6.9 ospf ipv6 area defcost

[機能]

IPv6 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 G110

[入力形式]

ospf ipv6 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
0～2	Si-R G110

<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、1～16777215 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 ipv6 area <area_number> defcost 1
```

15.6.10 ospf ipv6 area range

[機能]

IPv6 OSPF エリア内部集約経路の設定

[適用機種]

Si-R G110

[入力形式]

ospf ipv6 area [<area_number>] range <range_number> <address>/<prefixlen> [<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
0～2	Si-R G110

<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
0～3	Si-R G110

<address>/<prefixlen>

・ IPv6 アドレス/プレフィックス長
集約経路を 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。
::/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。

同一<address>で<prefixlen>が大きいものと小さいものを指定した場合、<prefixlen>の大きい指定が有効となります。

<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。

[注意]

装置内に同一あて先、または、包含関係にある集約経路の定義を設定できません。

［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。

15.6.11 ospf ipv6 area inter-area-prefix

[機能]

IPv6 OSPF エリア間プレフィックス LSA 入出力可否の設定

[適用機種]

Si-R G110

[入力形式]

ospf ipv6 area [<area_number>] inter-area-prefix <count> <action> <address>/<prefixlen><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
0～2	Si-R G110

<count>

・ エリア間プレフィックス LSA 入出力可否定義番号
エリア間プレフィックス LSA 入出力可否の優先度を表す定義番号を、10 進数で指定します。
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
0～29	Si-R G110

<action>

エリア間プレフィックス 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
該当するエリア間プレフィックス LSA を透過します。
・ reject
該当するエリア間プレフィックス LSA を遮断します。

<address>/<prefixlen>

・ IPv6 アドレス/プレフィックス長
エリア間プレフィックス LSA 入出力可否の条件とする経路情報を、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。
::/0 は指定できません。
・ any
すべての経路情報をエリア間プレフィックス LSA 入出力可否の条件とする場合に指定します。

<direction>

エリア間プレフィックス LSA 入出力の方向を示します。

・ in
ほかのエリアからのエリア間プレフィックス LSA の入力を示します。
・ out
ほかのエリアへのエリア間プレフィックス LSA の出力を示します。

<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"を指定した場合は、<prefix_match>は指定できません。

・ exact

<address>/<prefixlen>で指定した経路情報を本装置が保有する経路情報と比較し、完全一致したものをエリア間プレフィックスLSA入出力可否の対象とします。

- inexact

  指定した<address>の先頭から<prefixlen>ビット部分だけを本装置が保有する経路情報と比較し、一致したものをエリア間プレフィックス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エリア間プレフィックスLSAを透過(pass)するか、または遮断(reject)するかを設定します。
- ほかのエリアからエリア間プレフィックスLSAの入力があった場合は、優先度順に<direction>にinが設定されているエリア間プレフィックス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。
- ほかのエリアへエリア間プレフィックスLSAを出力する場合は、優先度順に<direction>にoutが設定されているエリア間プレフィックス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。
- <prefix_match>は以下のように動作します。

  <address>/<prefixlen>で"2001:db8::/32"を指定し、本装置が以下の経路情報を保有している場合、exactを指定すると、"2001:db8::/32"がエリア間プレフィックスLSA入出力可否の対象となります。

  inexactを指定すると、"2001:db8::"と一致する"2001:db8::/32、2001:db8:ffff::/48、2001:db8:ffff:1000::/64"の3つがエリア間プレフィックスLSA入出力可否の対象となります。

  1000:db8::/32

  2001:db8::/32

  2001:db8:ffff::/48

  2001:db8:ffff:1000::/64
- エリア間プレフィックス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。

最大定義数	機種
30	Si-R G110

[注意]

本機能の出力方向の設定と、IPv6 OSPFエリア内部集約経路機能を併用する場合は、以下の点に注意してください。

- エリア内部集約経路機能の動作は、本機能の出力方向の条件検索、および条件に一致した場合の動作実行後となります。このため、本機能により、集約対象となる経路がすべて遮断された場合、集約経路は生成されません。

以下の経路情報は、本機能で制御できません。

- 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]

エリア間でエリア間プレフィックスLSAをすべて透過するものとみなされます。

15.6.12 ospf ipv6 area inter-area-prefix move

[機能]

IPv6 OSPF エリア間プレフィックス LSA 入出力可否の優先順序の変更

[適用機種]

Si-R G110

[入力形式]

ospf ipv6 area [<area_number>] inter-area-prefix 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
0～2	Si-R G110

<count>

・ エリア間プレフィックス LSA 入出力可否定義番号
優先順序を変更するエリア間プレフィックス LSA 入出力可否定義番号を指定します。

<new_count>

・ 移動先エリア間プレフィックス LSA 入出力可否定義番号
<count>に対する新しい順序を、10 進数で指定します。
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
0～29	Si-R G110

[動作モード]

構成定義モード(管理者クラス)

[説明]

エリア間プレフィックス 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。

15.7 ASBR 情報

15.7.1 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 G110

[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 境界ルータでのデフォルトルートの広報を設定します。

<mode>が off の場合は、OSPF にデフォルトルートが再配布されていても、デフォルトルートを広報しません。always は、本装置のデフォルトルートの有無にかかわらず、常にデフォルトルートを広報します。exist は、OSPF への再配布にかかわらず、本装置でデフォルトルートが有効な場合にのみ、デフォルトルートを広報します。

[注意]

<mode>に exist を設定する場合は、以下の点に注意してください。

- 再配布フィルタでデフォルトルートが破棄される設定がされている場合、デフォルトルートは広報されません。

[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
```

15.7.2 ospf ip summary

[機能]

OSPF AS 外部経路集約の設定

[適用機種]

Si-R G110

[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
0～3	Si-R G110

<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。

15.7.3 ospf ip redist

[機能]

OSPF 再配布フィルタの設定

[適用機種]

Si-R G110

[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-R G110

<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
<address>/<mask>で指定した経路情報を本装置が保有する経路情報と比較し、完全一致したものをフィルタリング対象とします。

・ inexact
指定した<address>の先頭から<mask>ビット部分だけを本装置が保有する経路情報と比較し、一致したものを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。

・ <prefix_match>は以下のように動作します。
<address>/<mask>で"192.168.0.0/16"を指定し、本装置が以下の経路情報を保有している場合、exact を指定すると、"192.168.0.0/16"がフィルタリング対象となります。
inexact を指定すると、"192.168.0.0"と一致する"192.168.0.0/16、192.168.1.0/24、192.168.1.1/32"の 3 つがフィルタリング対象となります。

172.16.0.0/16
192.168.0.0/16
192.168.1.0/24
192.168.1.1/32

・ 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
50	Si-R G110

[注意]

フィルタリング条件で、遮断条件だけを設定した場合、すべての経路情報は OSPF に再配布されません。OSPF に再配布する IPv4 経路情報が存在する場合、透過条件に対象の経路情報を設定してください。

デフォルトルートの再配布については、 OSPF AS 境界ルータでのデフォルトルート広報の設定(ospf ip definfo)も参照してください。

[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。

15.7.4 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 G110

[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-R G110

[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。

15.7.5 ospf ipv6 definfo

[機能]

IPv6 OSPF AS 境界ルータでのデフォルトルート広報の設定

[適用機種]

Si-R G110

[入力形式]

ospf ipv6 definfo <mode> [<metric> [<metric_type>]]

[オプション]

<mode>

デフォルトルートを広報するかどうかを指定します。

- 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常に広報します。
- exist
  デフォルトルートの有無により広報します。

<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>

デフォルトルートのメトリックタイプを指定します。

- 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 境界ルータでのデフォルトルートの広報を設定します。

<mode>が off の場合は、OSPF にデフォルトルートが再配布されていても、デフォルトルートを広報しません。always は、本装置のデフォルトルートの有無にかかわらず、常にデフォルトルートを広報します。exist は、OSPF への再配布にかかわらず、本装置でデフォルトルートが有効な場合にのみ、デフォルトルートを広報します。

[注意]

<mode>に exist を設定する場合は、以下の点に注意してください。

- 再配布フィルタでデフォルトルートが破棄される設定がされている場合、デフォルトルートは広報されません。

[未設定時]

AS 境界ルータでのデフォルトルートを広報しないものとみなされます。

```
ospf ipv6 definfo off
```

15.7.6 ospf ipv6 redist

[機能]

IPv6 OSPF 再配布フィルタの設定

[適用機種]

Si-R G110

[入力形式]

ospf ipv6 redist <number> <action> <address>/<prefixlen> [<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-R G110

<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
<address>/<prefixlen>で指定した経路情報を本装置が保有する経路情報と比較し、完全一致したものをフィルタリング対象とします。

・ inexact
指定した<address>の先頭から<prefixlen>ビット部分だけを本装置が保有する経路情報と比較し、一致したものを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、IPv6 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、IPv6 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>/<prefixlen>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、IPv6 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 ipv6 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。
- <prefix_match>は以下のように動作します。
  <address>/<prefixlen>で"2001:db8::/32"を指定し、本装置が以下の経路情報を保有している場合、exact を指定すると、"2001:db8::/32"がフィルタリング対象となります。
  inexact を指定すると、"2001:db8::"と一致する"2001:db8::/32、2001:db8:ffff::/48、2001:db8:ffff:1000::/64"の 3 つがフィルタリング対象となります。

  1000:db8::/32
  2001:db8::/32
  2001:db8:ffff::/48
  2001:db8:ffff:1000::/64
- 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。

最大定義数	機種
50	Si-R G110

[注意]

フィルタリング条件で、遮断条件だけを設定した場合、すべての経路情報は OSPF に再配布されません。OSPF に再配布する IPv6 経路情報が存在する場合、透過条件に対象の経路情報を設定してください。

デフォルトルートの再配布については、 IPv6 OSPF AS 境界ルータでのデフォルトルート広報の設定(ospf ipv6 definfo)も参照してください。

[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。

15.7.7 ospf ipv6 redist move

[機能]

IPv6 OSPF 再配布フィルタの優先順序の変更

[適用機種]

Si-R G110

[入力形式]

ospf ipv6 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-R G110

[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 16 章 ブリッジグループ情報の設定

・ ブリッジグループ識別子の指定範囲

本章のコマンドの[オプション]に記載されている〈group_id〉(ブリッジグループ識別子)の通し番号(10 進数)は、以下に示す範囲で指定してください。

範囲	機種
0～19	Si-R G110

16.1 ブリッジグループ情報

16.1.1 bridgegroup ip routing

[機能]

IPv4 ルーティングの設定

[適用機種]

Si-R G110

[入力形式]

bridgegroup [<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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  指定方法の詳細については、本章の冒頭を参照してください。

<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をします。
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。

```
bridgegroup <group_id> ip routing on
```

16.1.2 bridgegroup ip policy

[機能]

IPv4 転送ポリシーの設定

[適用機種]

Si-R G110

[入力形式]

bridgegroup [<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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  指定方法の詳細については、本章の冒頭を参照してください。

<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。

```
bridgegroup <group_id> ip policy strict
```

16.1.3 bridgegroup ipv6 routing

[機能]

IPv6 ルーティングの設定

[適用機種]

Si-R G110

[入力形式]

bridgegroup [<group_id>] ipv6 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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  指定方法の詳細については、本章の冒頭を参照してください。

<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をします。
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。

```
bridgegroup <group_id> ipv6 routing on
```

16.1.4 bridgegroup ipv6 policy

[機能]

IPv6 転送ポリシーの設定

[適用機種]

Si-R G110

[入力形式]

bridgegroup [<group_id>] ipv6 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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  指定方法の詳細については、本章の冒頭を参照してください。

<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。

```
bridgegroup <group_id> ipv6 policy strict
```

16.1.5 bridgegroup vlan tag transmit

[機能]

VLAN タグの転送方式の設定

[適用機種]

Si-R G110

[入力形式]

bridgegroup [<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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  指定方法の詳細については、本章の冒頭を参照してください。

<mode>

- off
  VLAN タグを挿抜してブリッジします。
- on
  VLAN タグをつけたまま透過ブリッジします。

[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。

```
bridgegroup <group_id> vlan tag transmit off
```

16.1.6 bridgegroup 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 G110

[入力形式]

bridgegroup [<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 進数で指定します。
  省略時は、0 を指定したものとみなされます。
  指定方法の詳細については、本章の冒頭を参照してください。

<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。

```
bridgegroup <group_id> inter-remote on
```

第 17 章 マルチキャスト情報の設定

17.1 マルチキャスト情報

17.1.1 multicast ip igmp report

[機能]

IGMP Membership Report パケットの送出の設定

[適用機種]

Si-R G110

[入力形式]

multicast ip igmp report <mode>

[オプション]

<mode>

・ IGMP Membership Report パケットの送出動作

IGMP Query 受信時の、IGMP Membership Report 送出による応答動作を指定します。

normal

IGMPv2(RFC2236)に準拠した動作となり、他ホストからの IGMP Membership Report が観測された場合は応答しません。

force

他ホストの存在にかかわらず IGMP Membership Report により応答します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IGMP Query 受信時の、IGMP Membership Report 送出による応答動作を指定します。

IGMPv2(RFC2236)では、他ホストからの IGMP Membership Report が観測された場合は、重複によるトラフィック増加の防止のため、IGMP Membership Report を送出しません。

[注意]

本コマンドは本装置が IGMP グループ参加する機能(RIP、OSPF、IPv4 マルチキャスト・スタティックルーティングによるグループ参加など)に対して有効です。

[未設定時]

IGMPv2(RFC2236)準拠となり、他ホストからの IGMP Membership Report が観測された場合は IGMP Membership Report を送出しません。

17.1.2 multicast ip pimsm candrp mode

[機能]

PIM-SM(IPv4)の RP の動作の設定

[適用機種]

Si-R G110

[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 として動作しません。
- on
  RP 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]

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
```

17.1.3 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 G110

[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
```

17.1.4 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 G110

[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]

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
```

17.1.5 multicast ip pimsm candbsr mode

[機能]

PIM-SM(IPv4)の BSR の動作の設定

[適用機種]

Si-R G110

[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 として動作しません。
- on
  BSR 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]

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
```

17.1.6 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 G110

[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
```

17.1.7 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 G110

[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]

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
```

17.1.8 multicast ip pimsm staticrp address

[機能]

PIM-SM(IPv4)のスタティック RP のアドレスの設定

[適用機種]

Si-R G110

[入力形式]

multicast ip pimsm staticrp address <count> <address> [<priority>]

[オプション]

<count>

・ スタティック RP 定義番号
スタティック RP 定義番号を、0～9 の 10 進数で指定します。

<address>

・ スタティック RP アドレス
スタティック RP 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>

・ プライオリティ
スタティック RP のプライオリティを、0～255 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]

PIM-SM(IPv4) のスタティック RP のアドレスを指定します。
スタティック RP 設定時には、PIM-SM バージョン 2 の RP 決定機能(Candidate-RP)は動作しません。

[未設定時]

PIM-SM バージョン 2 の RP 決定機能(Candidate-RP)により RP を決定します。

17.1.9 multicast ip pimsm spt mode

[機能]

PIM-SM(IPv4)の SPT への経路変更の動作の設定

[適用機種]

Si-R G110

[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
  経路変更を行います。
- off
  経路変更を行いません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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
```

17.1.10 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 G110

[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 進数と単位文字で指定します。
10 進数の末尾に 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-R G110

[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
```

17.1.11 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 G110

[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します。
- full
  パケット全体で計算しません。

[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
```

17.1.12 multicast ip route static

[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 G110

[入力形式]

multicast ip route <count> static <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。
any が指定された場合は、配送元ホストのチェックを行いません。
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

<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-R G110

<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は以下の範囲で指定します。

範囲	機種
lan0～lan19 rmt0～rmt99	Si-R G110

［注意］

以下の設定は重複定義となるため設定不可能です。

・ 2 つの経路(配送元ホストアドレスに両方とも any を指定)で、マルチキャスト・グループアドレスと入力インタフェースが一致している場合。
  (マルチキャスト・グループアドレスと入力インタフェースのどちらかが異なれば設定可能です)
・ 2 つの経路(配送元ホストアドレスに両方とも IPv4 アドレスを指定)で、配送元ホストアドレスとマルチキャスト・グループが一致している場合。
  (配送元ホストアドレスとマルチキャスト・グループアドレスのどちらかが異なれば設定可能です)
  (入力インタフェースが異なっていても設定不可能です)
・ 2 つの経路(配送元ホストアドレスに any と IPv4 アドレスを指定)で、マルチキャスト・グループアドレスが一致している場合。
  (入力インタフェースが異なっていても設定不可能です)

スタティックルーティング情報の削除時には、スタティックルーティング定義番号はリナンバリングされます。

［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 18 章 UPnP 情報の設定

18.1 UPnP 情報

18.1.1 upnp use

[機能]

VoIP NAT トラバーサル機能の設定

[適用機種]

Si-R G110

[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 アダプターを通信できるようにします。ただし、VoIP アダプターが 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 アダプター(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 アダプター(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 アダプター(UPnP クライアント)は通信できません。

[注意]

VoIP アダプター(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	1900
TCP	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 の割り当て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り当て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
```

18.1.2 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 G110

[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)のいずれかを指定します。

[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 19 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)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-R G110

19.1 ACL 情報

19.1.1 acl description

[機能]

ACL description 定義

[適用機種]

Si-R G110

[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 進数で指定します。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<description>

・ 設定の説明
この ACL 定義番号で設定の説明を、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。

19.1.2 acl mac

[機能]

ACL MAC 定義

[適用機種]

Si-R G110

[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 進数で指定します。
  定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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)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)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 進数で指定します。

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 進数で指定します。

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 進数で指定します。

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。

19.1.3 acl ip

[機能]

ACL IPv4 定義

[適用機種]

Si-R G110

[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>]]
acl <acl_count> ip <src_addr>/<mask> dynamic [<protocol> [any]]
acl <acl_count> ip <src_addr>/<mask> dynamic [<protocol> [tos <value>]]
acl <acl_count> ip <src_addr>/<mask> dynamic [<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 進数で指定します。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、0～255 の 10 進数で指定します(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。
0 を指定するのと同じ意味になります。

・ dynamic
クラウドサービスゲートウェイ機能で、あて先 IP アドレスが動的に決定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 値には、0～ff の 16 進数で指定します。
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。
・ <dst_addr>/<mask>に"dynamic"を指定した場合、その ACL は Ingress ポリシールーティング設定以外には使用しないでください。

[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)

19.1.4 acl ipv6

[機能]

ACL IPv6 定義

[適用機種]

Si-R G110

[入力形式]

```
acl <acl_count> ipv6 <src_addr>/<prefixlen> <dst_addr>/<prefixlen> [<protocol> [any]]
acl <acl_count> ipv6 <src_addr>/<prefixlen> <dst_addr>/<prefixlen> [<protocol> [tc <value>]]
acl <acl_count> ipv6 <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 進数で指定します。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。
255 を指定するのと同じ意味になります。

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、または、"-"を使用して表現される 16 進数の範囲を指定します。

Traffic Class 値の指定は、"," を区切りとして 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 ipv6 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)

19.1.5 acl tcp

[機能]

ACL TCP 定義

[適用機種]

Si-R G110

[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 進数で指定します。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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/ipv6で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。

19.1.6 acl udp

[機能]

ACL UDP 定義

[適用機種]

Si-R G110

[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 進数で指定します。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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/ipv6 で 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。

19.1.7 acl icmp

[機能]

ACL ICMP 定義

[適用機種]

Si-R G110

[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 進数で指定します。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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/ipv6 で<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。

第 20 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)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
0～99	Si-R G110

20.1 ポリシーグループ定義情報

20.1.1 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 G110

[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
3000	Si-R G110

<action>

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
0～999	Si-R G110

[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。
・参照する ACL 定義の IP あて先アドレスが"dynamic"指定の場合、そのポリシーグループは Ingress ポリシールーティング設定以外に使用しないでください。

［未設定時］

ポリシーグループ定義は無効とみなされます。

20.1.2 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 G110

[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。

20.1.3 policy-group interface

[機能]

送出先インタフェースの設定

[適用機種]

Si-R G110

[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。

20.1.4 policy-group nexthop

[機能]

送出先 IPv4 ルータの設定

[適用機種]

Si-R G110

[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。

20.1.5 policy-group nexthop6

[機能]

送出先 IPv6 ルータの設定

[適用機種]

Si-R G110

[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。

20.1.6 policy-group sessionwatch address

[機能]

接続先監視のアドレス設定

[適用機種]

Si-R G110

[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 アドレスのいず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とき、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とき、policy-group nexthop6 定義がない場合。
- 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。

20.1.7 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 G110

[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ときの 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ときを復旧とみなし、正常時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とき、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とき、policy-group nexthop6 定義がない場合。
- 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
```

20.1.8 policy-group sessionwatch ttl

[機能]

接続先監視の TTL/HopLimit 値設定

[適用機種]

Si-R G110

[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 進数で指定します。

<send_ttl>

・ 送信 TTL / HopLimit 値
ICMP ECHO パケットを送信するときの 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とき、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とき、policy-group nexthop6 定義がない場合。
・ 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
```

20.1.9 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 G110

[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 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]

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とき、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とき、policy-group nexthop6 定義がない場合。
・ 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
```

20.1.10 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 G110

[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)のいずれかを指定します。

[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とき、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とき、policy-group nexthop6 定義がない場合。
・ 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 21 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)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-R G110

・ 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)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-R G110

21.1 グループ ID 情報

21.1.1 aaa name

[機能]

グループ名称の設定

[適用機種]

Si-R G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<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。

21.2 AAA ユーザ情報

21.2.1 aaa user id

[機能]

認証情報の設定(ユーザ ID)

[適用機種]

Si-R G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・ AAA ユーザ情報定義番号
グループ内での通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
AAA ユーザ情報定義番号の指定範囲については、本章の冒頭を参照してください。

<id>

・ ユーザ ID
ユーザ ID を、0x21,0x23～0x7e の文字で構成される 128 文字以内の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]

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。

21.2.2 aaa user password

[機能]

認証情報の設定(パスワード)

[適用機種]

Si-R G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・ AAA ユーザ情報定義番号
グループ内での通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
AAA ユーザ情報定義番号の指定範囲については、本章の冒頭を参照してください。

<password>

・ 省略
対話形式で認証パスワードを入力します。
・ 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 文字以内の文字列で指定します。
・ 暗号化されたパスワード
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]

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。

認証パスワードを省略した場合は、対話形式でパスワードを入力できます。入力した認証パスワードの文字列は画面に表示されず、システムログ情報にも保存されないため、コマンド実行履歴出力の設定が有効な際もセキュリティ的に安全です。

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。
- password aaa コマンドで指定するログインユーザのパスワード情報の場合は、64 文字以内の文字列で指定してください。

[メッセージ]

```
Password:
```

<password>引数を省略した場合に表示されます。
認証パスワードを入力してください。
入力した認証パスワードは画面に表示されません。

```
Retype password:
```

<password>引数を省略した場合に表示されます。
再度、認証パスワードを入力してください。
入力した認証パスワードは画面に表示されません。

```
<ERROR> mismatched password
```

対話形式で 2 回入力した認証パスワードが一致しませんでした。
再度、認証情報の設定を行ってください。

[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。

21.2.3 aaa user called number

[機能]

CLID の設定

[適用機種]

Si-R G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・ AAA ユーザ情報定義番号
グループ内での通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
AAA ユーザ情報定義番号の指定範囲については、本章の冒頭を参照してください。

<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。

[未設定時]

CLID 相手判定を行わないものとみなされます。

21.2.4 aaa user ip address local

[機能]

自側 IP アドレスの設定

[適用機種]

Si-R G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・ AAA ユーザ情報定義番号
グループ内での通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
AAA ユーザ情報定義番号の指定範囲については、本章の冒頭を参照してください。

<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。

21.2.5 aaa user ip address remote

[機能]

相手側 IP アドレスの設定

[適用機種]

Si-R G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・ AAA ユーザ情報定義番号
グループ内での通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
AAA ユーザ情報定義番号の指定範囲については、本章の冒頭を参照してください。

<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。

21.2.6 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 G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・ AAA ユーザ情報定義番号
グループ内での通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
AAA ユーザ情報定義番号の指定範囲については、本章の冒頭を参照してください。

<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 進数で指定します。

範囲	機種
0～255	Si-R G110

<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、1～14 の 10 進数で指定します。

<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。

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、本装置全体で以下の数まで定義できます。

最大定義数	機種
256	Si-R G110

[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。

21.2.7 aaa user ipv6 ifid

[機能]

IPv6 インタフェース ID の設定

[適用機種]

Si-R G110

[入力形式]

aaa [<group_id>] user [<number>] ipv6 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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・ AAA ユーザ情報定義番号
グループ内での通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
AAA ユーザ情報定義番号の指定範囲については、本章の冒頭を参照してください。

<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。

21.2.8 aaa user ipv6 route

[機能]

IPv6 スタティック経路情報の設定

[適用機種]

Si-R G110

[入力形式]

aaa [<group_id>] user [<number>] ipv6 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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・ AAA ユーザ情報定義番号
グループ内での通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
AAA ユーザ情報定義番号の指定範囲については、本章の冒頭を参照してください。

<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 進数で指定します。

範囲	機種
0～255	Si-R G110

<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、 1～14 の 10 進数で指定します。
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 ipv6 distance コマンドを参照してください。

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、本装置全体で以下の数まで定義できます。

最大定義数	機種
256	Si-R G110

[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。

21.2.9 aaa user sessionwatch

[機能]

接続先監視アドレスの設定

[適用機種]

Si-R G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・AAA ユーザ情報定義番号
グループ内での通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
AAA ユーザ情報定義番号の指定範囲については、本章の冒頭を参照してください。

<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。

21.2.10 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 G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・ AAA ユーザ情報定義番号
グループ内での通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
AAA ユーザ情報定義番号の指定範囲については、本章の冒頭を参照してください。

<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 ipsec ike range any4 any4
```

21.2.11 aaa user ipsec extension-range

[機能]

拡張 IPsec 対象範囲の設定

[適用機種]

Si-R G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・ AAA ユーザ情報定義番号
グループ内での通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
AAA ユーザ情報定義番号の指定範囲については、本章の冒頭を参照してください。

<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
0～99	Si-R G110

<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
100	Si-R G110

[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。

21.2.12 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 G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・ AAA ユーザ情報定義番号
グループ内での通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
AAA ユーザ情報定義番号の指定範囲については、本章の冒頭を参照してください。

<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。

21.2.13 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 G110

[入力形式]

aaa [<group_id>] user [<number>] supplicant vid <vid>

[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。
グループIDの指定範囲については、本章の冒頭を参照してください。

<number>

・ AAAユーザ情報定義番号
グループ内での通し番号を、10進数で指定します。
省略時は、0を指定したものとみなされます。
AAAユーザ情報定義番号の指定範囲については、本章の冒頭を参照してください。

<vid>

Supplicantに割り当てるVLAN IDを、1～4094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]

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。

21.2.14 aaa user supplicant mac

[機能]

Supplicant MAC アドレスの設定

[適用機種]

Si-R G110

[入力形式]

aaa [<group_id>] user [<number>] supplicant mac <mac>

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・ AAA ユーザ情報定義番号
グループ内での通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
AAA ユーザ情報定義番号の指定範囲については、本章の冒頭を参照してください。

<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)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。

21.2.15 aaa user user-role

[機能]

権限クラスの設定

[適用機種]

Si-R G110

[入力形式]

aaa [<group_id>] user [<number>] user-role <class>

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・ AAA ユーザ情報定義番号
グループ内での通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。
AAA ユーザ情報定義番号の指定範囲については、本章の冒頭を参照してください。

<class>

権限クラスを指定します。

・ administrator
権限クラスを管理者クラスとします。
・ user
権限クラスを一般ユーザクラスとします。
・ none
権限クラスを指定しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ユーザの権限クラスを指定します。

[未設定時]

権限クラスを指定しないものとみなされます。

21.3 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)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-R G110

・ 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)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
0～1	Si-R G110

21.3.1 aaa radius service

[機能]

RADIUS サービスの設定

[適用機種]

Si-R G110

[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。

グループ ID の指定範囲については、本章の冒頭を参照してください。

<service>

・ server

RADIUS サーバ機能として使用します。

・ client

RADIUS クライア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 クライアント機能は、併用できません。
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
```

21.3.2 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 G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<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。

21.3.3 aaa radius auth message-authenticator

[機能]

Message-Authenticator の設定

[適用機種]

Si-R G110

[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。
  グループ ID の指定範囲については、本章の冒頭を参照してください。

<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
```

21.3.4 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 G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<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。

21.3.5 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 G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<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 進数で指定します。
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 文字列で指定します。
・ 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されます。

21.3.6 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 G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<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 進数で指定します。
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。

21.3.7 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 G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・ サーバ定義番号
相手装置の定義番号を、10 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。

<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 文字列で指定します。
・ 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されます。

21.3.8 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 G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・ サーバ定義番号
相手装置の定義番号を、10 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。

<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。

21.3.9 aaa radius client server-info auth port

[機能]

認証サーバ UDP ポートの設定(旧 RFC 仕様対応)

[適用機種]

Si-R G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・ サーバ定義番号
相手装置の定義番号を、10 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。

<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されます。

```
aaa <group_id> radius client server-info auth port 1812
```

21.3.10 aaa radius client server-info auth deadtime

[機能]

復旧待機時間の設定

[適用機種]

Si-R G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・ サーバ定義番号
相手装置の定義番号を、10 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。

<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)のいずれかを指定します。
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、以下のいず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 状態となったあと、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されます。

```
aaa <group_id> radius client server-info auth deadtime 0s
```

21.3.11 aaa radius client server-info auth priority

[機能]

優先度の設定

[適用機種]

Si-R G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・サーバ定義番号
相手装置の定義番号を、10 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。

<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。
指定可能な範囲は以下のとおりです。

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されます。

```
aaa <group_id> radius client server-info auth priority 0
```

21.3.12 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 G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・ サーバ定義番号
相手装置の定義番号を、10 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。

<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 auth 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 auth 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。

21.3.13 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 G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・ サーバ定義番号
相手装置の定義番号を、10 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。

<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 文字列で指定します。
・ 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されます。

21.3.14 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 G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・ サーバ定義番号
相手装置の定義番号を、10 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。

<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。

21.3.15 aaa radius client server-info accounting port

[機能]

アカウンティングサーバ UDP ポートの設定(旧 RFC 仕様対応)

[適用機種]

Si-R G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・ サーバ定義番号
相手装置の定義番号を、10 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。

<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されます。

```
aaa <group_id> radius client server-info accounting port 1813
```

21.3.16 aaa radius client server-info accounting deadtime

[機能]

復旧待機時間の設定

[適用機種]

Si-R G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・ サーバ定義番号
相手装置の定義番号を、10 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。

<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)のいずれかを指定します。
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、以下のいず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 状態となったあと、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されます。

```
aaa <group_id> radius client server-info accounting deadtime 0s
```

21.3.17 aaa radius client server-info accounting priority

[機能]

優先度の設定

[適用機種]

Si-R G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・ サーバ定義番号
相手装置の定義番号を、10 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。

<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。
指定可能な範囲は以下のとおりです。

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されます。

```
aaa <group_id> radius client server-info accounting priority 0
```

21.3.18 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 G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<number>

・ サーバ定義番号
相手装置の定義番号を、10 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。

<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 accounting 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 accounting 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。

21.3.19 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 G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<interval>

・ 送信間隔
RADIUS サーバ未応答時のパケットの送信間隔を、1～10(秒)で指定します。

<retry>

・ 再送回数
RADIUS サーバ未応答時のパケット再送回数を、1～10(回)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]

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 5 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、15 秒となります。

```
aaa <group_id> radius client retry 5 2
```

21.3.20 aaa radius client nas-identifier

[機能]

NAS 識別子の設定

[適用機種]

Si-R G110

[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。
グループ ID の指定範囲については、本章の冒頭を参照してください。

<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。

21.3.21 aaa radius client security

[機能]

RADIUS サーバ無応答時のセキュリティレベルの設定

[適用機種]

Si-R G110

[入力形式]

aaa [<group_id>] radius client security <level>

[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。
  グループ ID の指定範囲については、本章の冒頭を参照してください。

<level>

- high
  RADIUS サーバ無応答時のセキュリティレベルを高くします。
- normal
  RADIUS サーバ無応答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]

RADIUS サーバ無応答時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、認証に失敗したものとして動作します。<level>が normal の場合は、認証に成功したものとして動作します。

[注意]

- ログインユーザ認証では、本設定にかかわらず RADIUS サーバ無応答時は認証失敗とします。
- RADIUS サーバ無応答時のセキュリティレベルを normal とした場合、IEEE802.1X 認証ではサプリカントの仕様によって正常に動作しない場合があります。

[未設定時]

RADIUS サーバ無応答時のセキュリティレベルとして high を定義したものとみなされます。

```
aaa <group_id> radius client security high
```

第 22 章 認証情報の設定

22.1 IEEE802.1X 情報

22.1.1 dot1x use

[機能]

IEEE802.1X 認証モードの設定

[適用機種]

Si-R G110

[入力形式]

dot1x use <mode>

[オプション]

<mode>

IEEE802.1X 認証のモードを指定します。

- off
  IEEE802.1X 認証を無効にします。
- on
  IEEE802.1X 認証を有効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IEEE802.1X 認証の利用有無を指定します。

[注意]

本モードが有効と指定された場合でも、ether dot1x use 定義でポート側が無効となっている場合は IEEE802.1X 認証は行われません。
本コマンドを動的定義変更すると該当ポートはいったん閉塞し、IEEE802.1X 認証状態を初期化します。

[未設定時]

IEEE802.1X 認証を使用しないものとみなされます。

```
dot1x use off
```

22.2 MAC アドレス認証情報

22.2.1 macauth use

[機能]

MAC アドレス認証基本情報の設定

[適用機種]

Si-R G110

[入力形式]

macauth use <mode>

[オプション]

<mode>

MAC アドレス認証を装置として使用するかどうかを指定します。

- off
  MAC アドレス認証を使用しません。
- on
  MAC アドレス認証を使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

MAC アドレス認証を装置として使用するかどうかを指定します。

[注意]

本モードが有効と指定された場合でも、ether macauth use 定義でポート側が無効となっている場合は MAC アドレス認証は行われません。

本コマンドを動的定義変更すると該当ポートはいったん閉塞し、MAC アドレス認証状態を初期化します。

[未設定時]

MAC アドレス認証を装置として使用しないものとみなされます。

```
macauth use off
```

22.2.2 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 G110

[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 文字以内の文字列で指定します。
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 アドレス認証で使用する、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。
本コマンドを動的定義変更すると該当ポートはいったん閉塞し、MAC アドレス認証状態を初期化します。

[未設定時]

MAC アドレス認証情報に認証端末の MAC アドレスを使用するものとみなされます。

22.2.3 macauth type

[機能]

MAC アドレス認証の認証プロトコルの設定

[適用機種]

Si-R G110

[入力形式]

macauth type <authtype>

[オプション]

<authtype>

- chap_md5
  認証プロトコルに MD5-CHAP を使用します。
- pap
  認証プロトコルに 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]

MAC アドレス認証の認証プロトコルを設定します。

[未設定時]

MAC アドレス認証の認証プロトコルとして MD5-CHAP が設定されたものとみなされます。

```
macauth type chap_md5
```

22.3 ARP 認証情報

22.3.1 arpauth use

[機能]

ARP 認証基本情報の設定

[適用機種]

Si-R G110

[入力形式]

arpauth use <mode>

[オプション]

<mode>

ARP 認証を装置として使用するかどうかを指定します。

- off
  ARP 認証を使用しません。
- on
  ARP 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]

ARP 認証を装置として使用するかどうかを指定します。

[注意]

本モードが有効と指定された場合でも、vlan arpauth use 定義で VLAN 側が無効となっている場合は ARP 認証は行われません。

[未設定時]

ARP 認証を装置として使用しないものとみなされます。

```
arpauth use off
```

22.3.2 arpauth password

[機能]

ARP 認証情報(パスワード)の設定

[適用機種]

Si-R G110

[入力形式]

arpauth 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 文字以内の文字列で指定します。
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]

ARP 認証で使用する、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]

ARP 認証情報に認証端末の MAC アドレスを使用するものとみなされます。

第 23 章 トラッキング定義情報の設定

・ トラッキング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>(トラッキング定義番号)に指定するトラッキング定義の通し番号(10 進数)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-R G110

・ トリガ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<trigger_number>(トリガ定義番号)に指定するトリガ定義の通し番号(10 進数)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-R G110

・ ノードトリガ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<node_count>(ノードトリガ定義番号)に指定するノードトリガ定義の通し番号(10 進数)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-R G110

・ アクション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<action_number>(アクション定義番号)に指定するアクション定義の通し番号(10 進数)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-R G110

23.1 トラッキング定義情報

23.1.1 tracking trigger node

[機能]

ノードトリガの設定

[適用機種]

Si-R G110

[入力形式]

tracking <number> trigger <trigger_number> node <node_count>

[オプション]

<number>

・ トラッキング定義番号
トラッキングの通し番号を、10 進数で指定します。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<trigger_number>

・ トリガ定義番号
トリガの通し番号を、10 進数で指定します。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<node_count>

・ ノードトリガ定義番号
ノードトリガの通し番号を、10 進数で指定します。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

[動作モード]

構成定義モード(管理者クラス)

[説明]

このトラッキングに使用するトリガを設定します。
トラッキング機能を使用する場合は必ず設定してください。

[注意]

・ 指定したノードトリガ定義番号のノードトリガ情報に定義不足がある場合はそのトラッキング定義は無効となります。
・ 同一のノードトリガ定義番号を複数登録することはできません。
・ 同一のノードトリガ定義番号を複数設定した場合は、トリガ定義番号で若番定義の設定が有効となります。

[未設定時]

ノードトリガは設定されないものとみなされます。

23.1.2 tracking action

[機能]

アクションの設定

[適用機種]

Si-R G110

[入力形式]

tracking <number> action <action_number> <state> <command>

[オプション]

<number>

・ トラッキング定義番号
トラッキングの通し番号を、10 進数で指定します。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<action_number>

・ アクション定義番号
アクション定義通し番号を 10 進数で指定します。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<state>

適用する状態を指定します。

・ down
down 状態に遷移した場合に適用します。

・ up
up 状態に遷移した場合に適用します。

<command>

適用するコマンド文字列を 128 文字以内でダブルクォーテーションで囲んで指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

<state>が示す状態へ遷移した場合に<command>を適用します。
トラッキング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]

適用するコマンドとして、カウンタ・ログ・統計・状態などの表示コマンド、およびトラッキング機能自身の設定・削除や統計情報表示・クリア操作コマンドを指定した場合、コマンドは実行されません。

[未設定時]

アクションは設定されないものとみなされます。

23.2 ノードトリガ定義情報

23.2.1 node-trigger address

[機能]

監視先のアドレス設定

[適用機種]

Si-R G110

[入力形式]

node-trigger <node_count> address <source> <destination>

[オプション]

<node_count>

・ノードトリガ定義番号
ノードトリガの通し番号を、10 進数で指定します。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<source>

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 IP アドレスのいずれかを指定してください。

・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

<destination>

監視対象 IP アドレスを指定します。

・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

[動作モード]

構成定義モード(管理者クラス)

[説明]

指定した監視対象アドレスに対して ICMP ECHO パケットの送受信で生存確認を行います。
トラッキング機能でノードトリガを使用する場合は必ず設定してください。

［注意］

- 監視対象 IP アドレスには送信元 IP アドレスと違うプロトコルアドレスは指定できません。
- 同一の監視対象 IP アドレスを複数登録することはできません。
- 同一の監視対象 IP アドレスを複数設定した場合は、ノードトリガ定義番号で若番定義の設定が有効となります。

［未設定時］

監視先のアドレスを設定しないものとみなされます。

23.2.2 node-trigger interval

[機能]

監視先の各種インターバル設定

[適用機種]

Si-R G110

[入力形式]

node-trigger <node_count> interval <normal> <error> <timeout> [<retry>]

[オプション]

<node_count>

・ノードトリガ定義番号
ノードトリガの通し番号を、10 進数で指定します。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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～3600 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。

<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、1 秒～3600 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のいずれかを指定します。

<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ときの ICMP ECHO パケットの再送間隔を、1 秒～監視タイムアウト-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、2s 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]

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ときを復旧とみなし、正常時送信間隔での監視に戻ります。

[未設定時]

監視先の正常時送信間隔に 30 秒、異常時送信間隔に 2 分、監視タイムアウトに 10 秒、再送間隔に 2 秒を指定したものとみなされます。

```
node-trigger <node_count> interval 30s 2m 10s 2s
```

23.2.3 node-trigger ttl

[機能]

監視先の TTL/HopLimit 値設定

[適用機種]

Si-R G110

[入力形式]

node-trigger <node_count> ttl <send_ttl>

[オプション]

<node_count>

・ ノードトリガ定義番号
ノードトリガの通し番号を、10 進数で指定します。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<send_ttl>

・ 送信 TTL / HopLimit 値
ICMP ECHO パケットを送信するときの 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]

ICMP ECHO パケットの TTL/HopLimit 値を指定された値で送信します。

[未設定時]

監視先の TTL/HopLimit 値に 255 を指定したものとみなされます。

```
node-trigger <node_count> ttl 255
```

23.2.4 node-trigger recovery

[機能]

監視先の復旧タイミング設定

[適用機種]

Si-R G110

[入力形式]

node-trigger <node_count> recovery <count>

[オプション]

<node_count>

・ノードトリガ定義番号
ノードトリガの通し番号を、10 進数で指定します。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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]

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。

[注意]

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正常状態へ復旧したと判断されません。

[未設定時]

監視先の応答受信回数に 1 を指定したものとみなされます。

```
node-trigger <node_count> recovery 1
```

23.2.5 node-trigger error-wait

[機能]

監視先の異常時送信開始待ち時間設定

[適用機種]

Si-R G110

[入力形式]

node-trigger <node_count> error-wait <time>

[オプション]

<node_count>

・ノードトリガ定義番号
ノードトリガの通し番号を、10 進数で指定します。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<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)のいずれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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。

[未設定時]

監視先の異常時送信開始待ちをしないものとみなされます。

```
node-trigger <node_count> error-wait 0s
```

23.2.6 node-trigger tos

[機能]

監視先の TOS/Traffic Class 値設定

[適用機種]

Si-R G110

[入力形式]

node-trigger <node_count> tos <send_tos>

[オプション]

<node_count>

・ ノードトリガ定義番号
ノードトリガの通し番号を、10 進数で指定します。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<send_tos>

・ 送信 TOS / Traffic Class 値
ICMP ECHO パケットを送信するときの IPv4 TOS/IPv6 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]

ICMP ECHO パケットの TOS/Traffic Class 値を指定された値で送信します。

[未設定時]

監視先の TOS/Traffic Class 値に 0 を指定したものとみなされます。

```
node-trigger <node_count> tos 0
```

23.2.7 node-trigger error-mode

[機能]

監視先が down 状態継続時の異常時通知動作の設定

[適用機種]

Si-R G110

[入力形式]

node-trigger <node_count> error-mode <mode>

[オプション]

<node_count>

・ ノードトリガ定義番号
ノードトリガの通し番号を、10 進数で指定します。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

監視先が down 状態継続時の異常時通知動作を指定します。

・ enable
down 状態継続時に定期的な異常時通知を行います。

・ disable
down 状態継続時に定期的な異常時通知を行いません。
※異常時通知は初回 down 状態検出時のみとなります。

[動作モード]

構成定義モード(管理者クラス)

[説明]

監視先が down 状態継続時の異常時通知動作を指定します。

[未設定時]

down 状態継続時に定期的な異常時通知を行うものとみなされます。

```
node-trigger <node_count> error-mode enable
```

23.2.8 node-trigger error-retry

[機能]

監視先が down 状態継続時、異常時通知を行うまでの異常時送信回数

[適用機種]

Si-R G110

[入力形式]

node-trigger <node_count> error-retry <count>

[オプション]

<node_count>

・ ノードトリガ定義番号
ノードトリガの通し番号を、10 進数で指定します。
定義番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

・ 異常時送信回数
監視先が down 状態継続時、異常時通知を行うまでの異常時送信回数を 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]

監視先が down 状態継続時、異常時通知を行うまでの異常時送信回数を指定します。
※ノードトリガの down 状態でのアクションは、本コマンドでの定義回数だけ異常時送信を行った後に実行されることになります。

[注意]

本設定は、node-trigger error-mode コマンドで動作モードが enable の場合に有効になります。

[未設定時]

監視先が down 状態継続時、異常時通知を行うまでの異常時送信回数に 3 を指定したものとみなされます。

```
node-trigger <node_count> error-retry 3
```

第 24 章 メモリ予兆監視情報の設定

24.1 メモリ予兆監視情報

24.1.1 sysmemwatch mode

[機能]

メモリ予兆監視機能の動作設定

[適用機種]

Si-R G110

[入力形式]

sysmemwatch mode <mode>

[オプション]

<mode>

- log-restart
  メモリ予兆監視機能を有効にし、メモリ枯渇状態と判断したときにシステムログの出力と本装置を再起動します。
- log
  メモリ予兆監視機能を有効にし、メモリ枯渇状態と判断したときにシステムログを出力します。
- disable
  メモリ予兆監視機能を無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

メモリ予兆監視機能の動作を設定します。

[注意]

メモリ予兆監視機能を有効にした場合は、以下の点に注意してください。
本コマンドを変更して定義反映を行った場合、監視周期が再設定されます。

[未設定時]

メモリ予兆監視機能の動作に log-restart を指定したものとみなされます。

```
sysmemwatch mode log-restart
```

24.1.2 sysmemwatch threshold

[機能]

メモリ予兆監視機能のしきい値の設定

[適用機種]

Si-R G110

[入力形式]

sysmemwatch threshold <threshold>

[オプション]

<threshold>

・ しきい値
メモリ予兆監視機能のしきい値(%)を、70～99 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]

メモリ予兆監視機能でメモリ枯渇状態を判断するためのしきい値を指定します。

[注意]

メモリ予兆監視機能が無効の場合、本コマンドの設定は無効となります。
メモリ予兆監視機能が有効の場合、本コマンドを変更して定義反映を行った場合、監視周期が再設定されます。

[未設定時]

メモリ予兆監視機能のしきい値に 92%を指定したものとみなされます。

```
sysmemwatch threshold 92
```

24.1.3 sysmemwatch interval

[機能]

メモリ予兆監視機能の監視周期の設定

[適用機種]

Si-R G110

[入力形式]

sysmemwatch interval <interval>

[オプション]

<interval>

・監視周期
メモリ予兆監視機能の監視周期を、1秒～60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]

メモリ予兆監視機能でメモリ使用量を監視する周期を設定します。

[注意]

メモリ予兆監視機能が無効の場合、本コマンドの設定は無効となります。

[未設定時]

メモリ予兆監視機能の監視周期に2秒を指定したものとみなされます。

```
sysmemwatch interval 2s
```

第 25 章 装置情報の設定

25.1 SNMP 情報

25.1.1 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 G110

[入力形式]

snmp service <mode>

[オプション]

<mode>

- enable
  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。
- disable
  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 disable
```

25.1.2 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 G110

[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。

25.1.3 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 G110

[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。

25.1.4 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 G110

[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。

25.1.5 snmp agent ip address

[機能]

SNMP エージェント IPv4 アドレスの設定

[適用機種]

Si-R G110

[入力形式]

snmp agent ip address <address>

[オプション]

<address>

・ IPv4 アドレス
本装置のエージェント IPv4 アドレスを設定します。
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]

SNMP エージェントのアドレスを設定します。本設定はトラップ送信時の自局アドレスにも使用されます。

[注意]

自装置に存在しないアドレスを指定した場合は、未設定時と同様の動作となります。

[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、トラップパケットの自局 IP アドレスは送出されるインタフェースに割り当てられたアドレスとなります。

25.1.6 snmp agent ipv6 address

[機能]

SNMP エージェント IPv6 アドレスの設定

[適用機種]

Si-R G110

[入力形式]

snmp agent ipv6 address <address>

[オプション]

<address>

・ IPv6 アドレス

本装置のエージェント IPv6 アドレスを設定します。

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

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。

[動作モード]

構成定義モード(管理者クラス)

[注意]

自装置に存在しないアドレスを指定した場合は、未設定時と同様の動作となります。

SNMPv1 トラップパケットのエージェントアドレスパラメタは、0.0.0.0 固定となります。

[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、トラップパケットの自局 IPv6 アドレスは送出されるインタフェースに割り当てられたアドレスとなります。

25.1.7 snmp agent engineid

[機能]

SNMP エンジン ID の設定

[適用機種]

Si-R G110

[入力形式]

snmp agent engineid <engineID>

[オプション]

<engineID>

・ SNMP エンジン ID
SNMP エンジン ID を、1～27 文字で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNMPv3 での SNMP エンジン ID を設定します。トラップ通知ホストなどで SNMP エンジン ID をあらかじめ取り決めておく必要がある場合は、設定を行ってください。
装置に設定される SNMP エンジン ID の値は以下のようになります。

・ 本コマンドを設定した場合
第 1～5 オクテット ： 0x800000d304 固定。
第 6 オクテット以降 ： 本コマンドで設定したエンジン ID
・ 本コマンドを設定しない場合
第 1～5 オクテット ： 0x800000d380 固定。
第 6 オクテット以降 ： ランダム値

[未設定時]

SNMP エンジン ID を自動生成します。

25.1.8 snmp manager

[機能]

SNMP ホスト情報の設定

[適用機種]

Si-R G110

[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 進数で指定します。

<address>

アクセス許可およびトラップを送信するあて先アドレスを、以下の形式で指定します。

・ IPv4 アドレス
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、トラップ送信は行いません。
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

・ IPv6 アドレス
::(コロン 2 つ)を指定すると、すべての IPv6 ホストからのアクセスを許可し、トラップ送信は行いません。
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。

<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。

・ off
トラップ送信しない場合に指定します。

・ v1
SNMPv1 トラップ送信する場合に指定します。

・ v2c
SNMPv2 トラップ送信する場合に指定します。

<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。

25.1.9 snmp trap coldstart

[機能]

coldStart トラップの設定

[適用機種]

Si-R G110

[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
```

25.1.10 snmp trap linkdown

[機能]

linkDown トラップの設定

[適用機種]

Si-R G110

[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
```

25.1.11 snmp trap linkup

[機能]

linkUp トラップの設定

[適用機種]

Si-R G110

[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
```

25.1.12 snmp trap authfail

[機能]

authenticationFailure トラップの設定

[適用機種]

Si-R G110

[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
```

25.1.13 snmp trap vrrpnewmaster

[機能]

vrrpTrapNewMaster トラップの設定

[適用機種]

Si-R G110

[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
```

25.1.14 snmp trap vrrpauthfail

[機能]

vrrpTrapAuthFailure トラップの設定

[適用機種]

Si-R G110

[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
```

25.1.15 snmp trap vrrpprotoerror

[機能]

vrrpTrapProtoError トラップの設定

[適用機種]

Si-R G110

[入力形式]

snmp trap vrrpprotoerror <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]

vrrpTrapProtoError 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]

vrrpTrapProtoError トラップが有効とみなされます。

```
snmp trap vrrpprotoerror enable
```

25.1.16 snmp trap noserror

[機能]

nosError トラップの設定

[適用機種]

Si-R G110

[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
```

25.1.17 snmp user name

[機能]

SNMP ユーザ名の設定

[適用機種]

Si-R G110

[入力形式]

snmp user [<number>] name <user_name>

[オプション]

<number>

・ ユーザ定義番号
ユーザ定義番号を、0～7 の 10 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。

<user_name>

・ SNMP ユーザ名
SNMP ユーザ名を、1～32 文字で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNMPv3 での SNMP ユーザ名を設定します。SNMPv3 機能を使用する場合は必ず設定してください。

[未設定時]

SNMP ユーザ名を設定しないものとみなされます。

25.1.18 snmp user address

[機能]

SNMP ホストアドレスの設定

[適用機種]

Si-R G110

[入力形式]

snmp user [<number>] address [<addr_number>] <address>

[オプション]

<number>

・ ユーザ定義番号
ユーザ定義番号を、0～7 の 10 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。

<addr_number>

・ SNMP ホスト定義番号
SNMP ホスト定義番号を、0～7 の 10 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。

<address>

SNMPv3 アクセスを許可するホストのアドレスを以下の形式で指定します。

・ 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。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNMPv3 での SNMP ホストアドレスを設定します。定義可能数は"snmp user notification"コマンドと合わせて本装置全体で 8 個まで定義できます。

[未設定時]

SNMP ホストアドレスを設定しないものとみなされます。

25.1.19 snmp user notification

[機能]

トラップ通知ホストアドレスの設定

[適用機種]

Si-R G110

[入力形式]

snmp user [<number>] notification [<addr_number>] <address>

[オプション]

<number>

・ユーザ定義番号
ユーザ定義番号を、0～7 の 10 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。

<addr_number>

・トラップ通知ホスト定義番号
トラップ通知ホスト定義番号を、0～7 の 10 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。

<address>

トラップを通知するホストのアドレスを以下の形式で指定します。

・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。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNMPv3 でのトラップ通知ホストアドレスを設定します。定義可能数は"snmp user address"コマンドと合わせて本装置全体で 8 個まで定義できます。

[未設定時]

トラップ通知ホストアドレスを設定しないものとみなされます。

25.1.20 snmp user auth

[機能]

認証プロトコルの設定

[適用機種]

Si-R G110

[入力形式]

snmp user [<number>] auth <protocol> [<password> [encrypted]]

[オプション]

<number>

・ ユーザ定義番号
ユーザ定義番号を、0～7 の 10 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。

<protocol>

認証プロトコルを指定します。

・ none
認証プロトコルを使用しません。
・ md5
認証プロトコルとして MD5(HMAC-MD5-96)を使用します。
・ sha
認証プロトコルとして SHA(HMAC-SHA-96)を使用します。

<password>

認証パスワードを指定します。

・ 暗号化されていない認証パスワード
以下に、入力範囲を示します。

認証プロトコル	パスワード長
md5	8 文字～16 文字
sha	8 文字～20 文字

・ 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]

SNMPv3 での認証プロトコルを設定します。

[未設定時]

認証プロトコルを使用しないものとみなされます。

```
snmp user <number> auth none
```

25.1.21 snmp user priv

[機能]

暗号プロトコルの設定

[適用機種]

Si-R G110

[入力形式]

snmp user [<number>] priv <protocol> [<password> [encrypted]]

[オプション]

<number>

・ ユーザ定義番号
ユーザ定義番号を、0～7 の 10 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。

<protocol>

暗号プロトコルを指定します。

・ none
暗号プロトコルを使用しません。

・ des
暗号プロトコルとして DES(CBC-DES)を使用します。

<password>

暗号パスワードを指定します。

・ 暗号化されていない暗号パスワード
以下に、入力範囲を示します。

暗号プロトコル	パスワード長
des	8 文字～16 文字

・ 暗号化された暗号パスワード
show コマンドで表示される暗号化された暗号パスワードを 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

・ 暗号化暗号パスワード指定
<password>に暗号化された暗号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]

SNMPv3 での暗号プロトコルを設定します。

[注意]

暗号プロトコルを使用する場合は必ず認証プロトコルを設定してください。
認証プロトコルの設定がない場合、暗号プロトコルの設定は使用されません。

[未設定時]

暗号プロトコルを使用しないものとみなされます。

```
snmp user <number> priv none
```

25.1.22 snmp user write

[機能]

MIB 書き込み許可ビューの設定

[適用機種]

Si-R G110

[入力形式]

snmp user [<number>] write <access>

[オプション]

<number>

・ ユーザ定義番号
ユーザ定義番号を、0～7 の 10 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。

<access>

書き込み可能な MIB に対しての書き込み許可ビューを指定します。

・ none
MIB 書き込みを許可しない場合に指定します。

・ all
MIB 書き込みを許可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]

SNMPv3 での MIB 書き込み許可ビューを設定します。

[未設定時]

MIB 書き込みを許可しないものとみなされます。

```
snmp user <number> write none
```

25.1.23 snmp user read

[機能]

MIB 読み出し許可ビューの設定

[適用機種]

Si-R G110

[入力形式]

snmp user [<number>] read <access> [<view_number>]

[オプション]

<number>

・ ユーザ定義番号
ユーザ定義番号を、0～7 の 10 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。

<access>

MIB 読み出し許可ビューを指定します。

・ all
サポートしているすべての MIB 読み出しを許可する場合に指定します。

・ none
MIB 読み出しを許可しない場合に指定します。

・ view
"snmp view subtree"コマンドで設定した MIB ビュー情報を使用する場合に指定します。

<view_number>

使用する"snmp view subtree"コマンドのビュー定義番号を、0～7 の 10 進数で指定します。ビュー定義番号は、<access>に view を指定した場合にのみ設定可能です。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNMPv3 での MIB 読み出し許可ビューを設定します。

設定したビュー定義番号に対応する"snmp view subtree"コマンド定義が存在しない場合、MIB 読み出しを許可しないものとみなされます。

[未設定時]

サポートしているすべての MIB 読み出しを許可するものとみなされます。

```
snmp user <number> read all
```

25.1.24 snmp user notify

[機能]

トラップ通知許可ビューの設定

[適用機種]

Si-R G110

[入力形式]

snmp user [<number>] notify <access> [<view_number>]

[オプション]

<number>

・ユーザ定義番号
ユーザ定義番号を、0～7 の 10 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。

<access>

トラップ通知許可ビューを指定します。

・all
サポートしているすべてのトラップ通知を許可する場合に指定します。

・none
トラップ通知を許可しない場合に指定します。

・view
"snmp view subtree"コマンドで設定した MIB ビュー情報を使用する場合に指定します。

<view_number>

使用する"snmp view subtree"コマンドのビュー定義番号を、0～7 の 10 進数で指定します。ビュー定義番号は、<access>に view を指定した場合にのみ設定可能です。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNMPv3 でのトラップ通知許可ビューを設定します。

設定したビュー定義番号に対応する"snmp view subtree"コマンド定義が存在しない場合、トラップ通知を許可しないものとみなされます。

[未設定時]

サポートしているすべてのトラップ通知を許可するものとみなされます。

```
snmp user <number> notify all
```

25.1.25 snmp view subtree

[機能]

SNMP MIB ビュー情報の設定

[適用機種]

Si-R G110

[入力形式]

snmp view [<view_number>] subtree [<subtree_number>] <view_type> <subtree_name>

[オプション]

<view_number>

・ ビュー定義番号
ビュー定義番号を、0～7 の 10 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。

<subtree_number>

・ サブツリー定義番号
サブツリー定義番号を、0～15 の 10 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。

<view_type>

<subtree_name>を MIB ビューに含むか、それとも除くかを指定します。

・ include
<subtree_name>を MIB ビューに含む場合に指定します。

・ exclude
<subtree_name>を MIB ビューから除く場合に指定します。

<subtree_name>

・ サブツリー名
MIB ビュー対象とするサブツリー名を指定します。指定可能なサブツリー名は以下のとおりです。

サブツリー名		オブジェクト ID	備考
MIB グループ名	iso	1	
	internet	1.3.6.1	
	mib2	1.3.6.1.2.1	
	system	1.3.6.1.2.1.1	
	interfaces	1.3.6.1.2.1.2	
	at	1.3.6.1.2.1.3	
	ip	1.3.6.1.2.1.4	
	icmp	1.3.6.1.2.1.5	
	tcp	1.3.6.1.2.1.6	
	udp	1.3.6.1.2.1.7	
	transmission	1.3.6.1.2.1.10	
	snmp	1.3.6.1.2.1.11	
	ospf	1.3.6.1.2.1.14	
	bgp	1.3.6.1.2.1.15	
	rip2	1.3.6.1.2.1.23	
	ifMIB	1.3.6.1.2.1.31	
	radiusMIB	1.3.6.1.2.1.67	
	vrrpMIB	1.3.6.1.2.1.68	
	enterprises	1.3.6.1.4.1	
	coldstart	1.3.6.1.6.3.1.1.5.1	

サブツリー名		オブジェクト ID	備考
トラップ名	linkdown	1.3.6.1.6.3.1.1.5.3	
	linkup	1.3.6.1.6.3.1.1.5.4	
	authfail	1.3.6.1.6.3.1.1.5.5	
	vrrpnewmaster	1.3.6.1.2.1.68.0.1	
	vrrpauthfail	1.3.6.1.2.1.68.0.2	
	vrrpprotoerror	1.3.6.1.2.1.68.0.3	
	noserror	1.3.6.1.4.1.211.1.127.1.0.1	

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNMPv3 での MIB ビュー情報を設定します。

同じビュー定義番号を持つ MIB ビュー情報の設定で、同一サブツリー名が複数指定された場合、最小のサブツリー定義番号を持つサブツリー情報が有効となります。

[未設定時]

MIB ビュー情報を設定しないものとみなされます。

25.2 システムログ情報

25.2.1 syslog server address

[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 G110

[入力形式]

syslog server <number> address <address>

[オプション]

<number>

・ 定義番号
サーバ情報の定義番号を、0～2 の 10 進数で指定します。

<address>

syslog サーバのアドレスを以下の形式で指定します。

・ IPv4 アドレス
syslog 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

・ IPv6 アドレス
syslog 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]

syslog サーバの IP アドレスを設定します。

[未設定時]

syslog サーバを指定しないものとみなされます。

25.2.2 syslog server pri

[機能]

受信サーバごとの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 G110

[入力形式]

syslog server <number> pri <mode>

[オプション]

<number>

・ 定義番号
サーバ情報の定義番号を、0～2 の 10 進数で指定します。

<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]

syslog pri コマンドで指定したプライオリティの中から、syslog サーバごとに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]

syslog pri コマンドで指定したものと同じ内容とします。

25.2.3 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 G110

[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]

error,warn,info が指定されたものとみなされます。

```
syslog pri error,warn,info
```

25.2.4 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 G110

[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]

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
```

25.2.5 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 G110

[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。

csg
CSG 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]

以下を指定したものとみなされます。

```
syslog security ipfilter,nat,ids,ppp,dhcp,proxydns
```

25.2.6 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 G110

[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
```

25.2.7 syslog command-logging

[機能]

システムログ情報のコマンド実行履歴出力の設定

[適用機種]

Si-R G110

[入力形式]

syslog command-logging <mode>

[オプション]

<mode>

- enable
  コマンド実行履歴をシステムログに出力します。
- disable
  コマンド実行履歴をシステムログに出力しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

コマンド実行履歴をシステムログに出力するかどうかを指定します。

[注意]

セキュリティ確保のため、暗号化対象のパラメタについては、暗号化して出力します。

[未設定時]

コマンド実行履歴をシステムログに出力しないものとみなされます。

```
syslog command-logging disable
```

25.2.8 syslog header

[機能]

システムログ情報のHEADER部追加の設定

[適用機種]

Si-R G110

[入力形式]

syslog header <mode>

[オプション]

<mode>

- enable
  送信メッセージにHEADER部を追加します。
- disable
  送信メッセージにHEADER部を追加しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

送信メッセージにHEADER部を追加するかどうかを設定します。

[未設定時]

送信メッセージにHEADER部を追加しないものとみなされます。

```
syslog header disable
```

25.2.9 syslog source ip address

[機能]

システムログ情報の送信元 IPv4 アドレスの設定

[適用機種]

Si-R G110

[入力形式]

syslog source ip address <address>

[オプション]

<address>

・ IPv4 アドレス
送信メッセージの送信元 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

[動作モード]

構成定義モード(管理者クラス)

[説明]

送信メッセージの送信元 IPv4 アドレスを設定します。

[注意]

自装置に存在しないアドレスを指定した場合は、未設定時と同様の動作となります。

[未設定時]

送信メッセージの送信元 IPv4 アドレスを指定しないものとみなされます。その場合、送信メッセージの自局 IPv4 アドレスは不定となります。

25.2.10 syslog source ipv6 address

[機能]

システムログ情報の送信元 IPv6 アドレスの設定

[適用機種]

Si-R G110

[入力形式]

syslog source ipv6 address <address>

[オプション]

<address>

・ IPv6 アドレス

送信メッセージの送信元 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:ff

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。

[動作モード]

構成定義モード(管理者クラス)

[説明]

送信メッセージの送信元 IPv6 アドレスを設定します。

[注意]

自装置に存在しないアドレスを指定した場合は、未設定時と同様の動作となります。

[未設定時]

送信メッセージの送信元 IPv6 アドレスを指定しないものとみなされます。その場合、送信メッセージの自局 IPv6 アドレスは不定となります。

25.3 自動時刻設定情報

25.3.1 time auto server

[機能]

時刻情報の提供サーバの設定

[適用機種]

Si-R G110

[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。

25.3.2 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 G110

[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)のいずれかを指定します。
  0s を指定した場合は、未設定時を設定するものとします。

[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
```

25.3.3 time zone

[機能]

時刻情報のタイムゾーンの設定

[適用機種]

Si-R G110

[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
```

25.4 ProxyDNS 情報

25.4.1 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 G110

[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> [<ipaddress2>]
(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)
proxydns domain <count> domainlist <domain_id> acl <acl_count>
(ドメインリスト使用)

[オプション]

<count>

・ 転送先定義番号
転送先定義番号を、0～31 の 10 進数で指定します。
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 進数で指定します。
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にする場合に指定します。

domainlist

ドメインリストを使用する場合に指定します。

<domain_id>

・ ドメイン ID 定義番号
ドメイン定義番号を 10 進数で指定します。

指定した値とドメインリストに含まれる ID が一致したドメイン名が格納されます。

範囲	機種
0	Si-R G110

<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(プライマリ)

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

<ipaddress2>

・ DNS サーバ IP アドレス(セカンダリ)

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 進数で指定します。

範囲	機種
0～99	Si-R G110

<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～rmt99	Si-R G110

acl

ACL を使用する場合に指定します。

<acl_count>

・ ACL 定義番号

使用する ACL 定義番号を、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]

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> [<ipaddress2>]

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。

・ 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。

ドメインリスト使用

proxydns domain <count> domainlist <domain_id> acl <acl_count>

プロキシ DNS にドメインリストを使用する場合に設定します。

[注意]

・ ドメインリストを使用する場合、同じ<count>で転送要求破棄以外の設定を必ず行ってください。その際に、入力した<qname>は何を入力しても無視されます。
・ ドメインリストを使用する場合に指定した ACL 定義番号の IP あて先アドレスに必ず"dynamic"指定を行ってください。また、"dynamic"指定を行った ACL は Ingress ポリシールーティング以外には使用しないでください。

[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。

25.4.2 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 G110

[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。

25.4.3 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 G110

[入力形式]

proxydns address <count> <address>/<mask> reject
(転送要求の破棄)
proxydns address <count> <address>/<mask> static <ipaddress> [<ipaddress2>]
(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
転送先定義番号を、0～31 の 10 進数で指定します。
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(プライマリ)
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

<ipaddress2>

・ DNS サーバ IP アドレス(セカンダリ)

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 進数で指定します。

範囲	機種
0～99	Si-R G110

<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～rmt99	Si-R G110

[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> [<ipaddress2>]

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。

・ 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。

25.4.4 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 G110

[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。

25.4.5 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 G110

[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
```

25.4.6 proxydns agetime

[機能]

DNS 順引き動的経路の保持時間の設定

[適用機種]

Si-R G110

[入力形式]

proxydns agetime <agetime>

[オプション]

<agetime>

・ 動的経路の保持時間
動的経路を保持する時間を、1 秒～1 日の範囲で指定します。
単位は、d(日)、h(時)、m(分)、s(秒)のいずれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

クラウドサービスゲートウェイ機能で使用する経路の保持時間を指定します。

[注意]

クラウドサービスゲートウェイ機能を使用しない場合、 本設定は無効となります。

[未設定時]

保持時間を DNS 回答パケットの TTL(Time To Live)と同じ値にします。

25.4.7 proxydns ttl

[機能]

DNS パケットの TTL の最大時間の変更

[適用機種]

Si-R G110

[入力形式]

proxydns ttl <time>

[オプション]

<time>

・DNS パケットの TTL の最大時間
変更する DNS パケットの TTL(Time To Live)の時間を、1 秒～1 日の範囲で指定します。
単位は、d(日)、h(時)、m(分)、s(秒)のいずれかを指定します。
DNS パケットに含まれる TTL がここで設定した値よりも大きかった場合、パケットの TTL は書き換えられます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

DNS パケットに含まれる TTL(Time To Live)の最大時間を変更します。
DNS パケットに含まれる TTL がここで設定した値よりも大きかった場合のみ、パケットの TTL は書き換えられます。

[未設定時]

DNS パケットに含まれる TTL の時間を変更しません。

25.4.8 proxydns source-port

[機能]

DNS パケットの送信元ポート番号割り当て方式の設定

[適用機種]

Si-R G110

[入力形式]

proxydns source-port <mode>

[オプション]

<mode>

DNS パケットの送信元ポート番号割り当て方式を指定します。

- any
  送信元ポート番号に本装置で未使用のポート番号を割り当てます。
- fix
  送信元ポート番号に固定値(53)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]

プロキシ DNS が DNS サーバに送信するパケットの送信元ポート番号の割り当て方式を設定します。

[未設定時]

送信元ポート番号に本装置で未使用のポート番号を割り当てるものとみなされます。

```
proxydns source-port any
```

25.5 ホストデータベース情報

各機能とパラメタの関係は以下のようになります。

パラメタ 機能	name	ip_address	ipv6_address	mac_address	duid	rpon
簡易 DNS サーバ	○	○	○	−	−	−
IPv4 DHCP スタティック	−	○	−	○	−	−
IPv6 DHCP スタティック	−	−	○	−	○	−
リモートパワーオン (手動/schedule)	−	−	−	○	−	○

○:有効、−:無効

25.5.1 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 G110

[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 サーバ機能から利用されます。

[未設定時]

ホストデータベース情報のホスト名を設定しないものとみなされます。

25.5.2 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 G110

[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、IPv4 DHCP スタティック機能から利用されます。

[未設定時]

ホストデータベース情報の IP アドレスを設定しないものとみなされます。

25.5.3 host ipv6 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 G110

[入力形式]

host <number> ipv6 address <ipv6_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 進数で指定します。

<ipv6_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、IPv6 DHCP スタティック機能から利用されます。

[未設定時]

ホストデータベース情報の IPv6 アドレスを設定しないものとみなされます。

25.5.4 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 G110

[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)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、IPv4 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。

[未設定時]

ホストデータベース情報のMACアドレスを設定しないものとみなされます。

25.5.5 host duid

[機能]

ホストデータベース情報の DUID の設定

[適用機種]

Si-R G110

[入力形式]

host <number> duid <duid>

[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 進数で指定します。

<duid>

・ DUID
ホストの DUID を 260 桁以内の 16 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]

本装置配下に接続されたホストの DUID をホストデータベースに設定します。
本コマンドは、IPv6 DHCP スタティック機能から利用されます。

[未設定時]

ホストデータベース情報の DUID を設定しないものとみなされます。

25.5.6 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 G110

[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。
本コマンドはリモートパワーオン機能から利用されます。

[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。

25.6 スケジュール情報

25.6.1 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 G110

[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、0～19 の 10 進数で指定します。
- any
  スケジュール定義番号を省略する場合に指定します。
  delete コマンドで定義を削除する際に指定するとエラーになります。

<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 modemmodule account
  データ通信モジュール課金情報をクリアする場合に指定します。
- offline remote
  強制切断する場合に指定します。
- rpon all
  リモートパワーオンを実行する場合に指定します。
- getdomainlist
  ドメインリストを取得します。

[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。

25.6.2 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 G110

[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、0～19 の 10 進数で指定します。
- any
  スケジュール定義番号を省略する場合に指定します。
  delete コマンドで定義を削除する際に指定するとエラーになります。

<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。

[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。

25.6.3 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 G110

[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、0～19 の 10 進数で指定します。
- 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、対応するスケジュール番号にスケジュール定義が行われていない場合は、構成定義内容も表示されません。

対応するスケジュール定義番号にスケジュール定義が行われると有効になり、構成定義内容も表示されるようになります。

[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
```

25.7 外部メディアスタート機能の情報

25.7.1 storage setup mode

[機能]

外部メディアスタート機能の設定

[適用機種]

Si-R G110

[入力形式]

storage setup mode <mode>

[オプション]

<mode>

- enable
  外部メディアスタート機能を有効にします。
- disable
  外部メディアスタート機能を停止します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

外部メディアスタート機能を有効にするかどうかを設定します。
外部メディアスタート機能は外部メディアが挿入された状態での電源投入時のみ動作します。

[未設定時]

外部メディアスタート機能を有効にするとみなされます。

```
storage setup mode enable
```

25.7.2 storage setup machine

[機能]

外部メディアスタート機能有効時の装置名の設定

[適用機種]

Si-R G110

[入力形式]

storage setup machine <name>

[オプション]

<name>

装置名を 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]

外部メディアスタート機能の有効時の、ソフトウェアおよび構成定義の退避／復旧の際のファイル名に付加する装置名を指定します。

[未設定時]

装置名からハイフンを削除し小文字をすべて大文字に変換した名前を利用します。

25.8 電話番号変更予約情報

25.8.1 dnconvinfo date

[機能]

電話番号変更予約の日時の設定

[適用機種]

Si-R G110

[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 進数で指定します。

dd
日付を、1～31 の 10 進数で指定します。

HH
時間を、0～23 の 10 進数で指定します。

MM
分を、0～59 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]

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。

[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。

25.8.2 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 G110

[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。

[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。

25.9 ソフトウェア更新情報

25.9.1 updateinfo

[機能]

ソフトウェア更新情報の設定

[適用機種]

Si-R G110

[入力形式]

updateinfo <host> <user> <password> <pathname>

[オプション]

<host>

更新するソフト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 32 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

更新するソフトウェアの 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]

ソフト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 サーバ上のソフト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］

ソフトウェア更新情報を設定しないものとみなされます。

25.10 ドメインリスト情報

25.10.1 domainlistinfo

[機能]

ドメインリスト情報の設定

[適用機種]

Si-R G110

[入力形式]

domainlistinfo <host> <user> <password> <pathname>

[オプション]

<host>

ドメインリストの転送元ホスト(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 32 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

更新するドメインリストの 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]

ドメインリストの情報を設定します。

getdomainlist コマンドで ftp サーバ上のドメインリストを取得する場合は、必ず本コマンドを実行してください。

［未設定時］

ドメインリスト情報を設定しないものとみなされます。

25.11 装置ランプ情報

25.11.1 lamp mode

[機能]

運用中ランプ動作の設定

[適用機種]

Si-R G110

[入力形式]

lamp mode <mode>

[オプション]

<mode>

- enable
  運用中にランプを点灯します。
- disable
  運用中にランプを消灯します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

装置のランプを点灯するか消灯するかどうかを設定します。
disable を設定した場合、電源投入またはリセット操作により装置を起動してから lamp delay で設定されている時間経過後に装置のランプが消灯します。

[未設定時]

運用中にランプを点灯するものとみなされます。

```
lamp mode enable
```

25.11.2 lamp delay

[機能]

運用開始時のランプ消灯までの遅延時間の設定

[適用機種]

Si-R G110

[入力形式]

lamp delay <time>

[オプション]

<time>

・ 消灯までの遅延時間
lamp mode disable 設定時の消灯までの遅延時間を、1～20 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]

lamp mode disable 設定時の、装置起動時に消灯するまでの遅延時間を設定します。

[未設定時]

装置起動後、ランプ消灯までの遅延時間として 1 分を指定したものとみなされます。
本設定は、装置電源投入時および装置リセット時に適用されます。

```
lamp delay 1m
```

25.12 資源情報

25.12.1 resource system vlan

[機能]

予約 VLAN の設定

[適用機種]

Si-R G110

[入力形式]

resource system vlan <vidlist>

[オプション]

<vidlist>

・ VLAN ID リスト
VLAN ID を、1～4094 の 10 進数で指定します。
","または"-"で区切ることで複数の VLAN ID を指定できます。
VLAN ID は必ず以下の数を指定してください。

個数	機種
6	Si-R G110

[動作モード]

構成定義モード(管理者クラス)

[説明]

装置内部資源として予約する VLAN ID を設定します。

[注意]

本設定を変更した場合は、装置の再起動が必要です。
また、本設定で指定した VLAN は、ether vlan 定義では指定できません。

[未設定時]

以下のように VLAN が予約されているとみなされます。

Si-R G110 の場合

```
resource system vlan 4089-4094
```

25.12.2 resource authenticated vlan

[機能]

認証VLAN用予約VLANの設定

[適用機種]

Si-R G110

[入力形式]

resource authenticated vlan <vidlist>

[オプション]

<vidlist>

・ VLAN IDリスト
VLAN IDを、1～4094の10進数で指定します。
","または"-"で区切ることで複数のVLAN IDを指定できます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

認証VLAN用として予約するVLAN IDを設定します。

[注意]

・ ethernetグループ1と同じVLAN IDを指定することはできません。
ethernetグループ1とは、異なるVLAN IDを指定してください。
ethernetグループ1と同じVLAN IDを指定した場合、ethernetグループ1の指定が有効になります。
・ resource system vlanで設定されているVLAN IDを指定した場合、この指定は無効になります。
・ ethergroup vlan mode disableを設定した場合、本設定は無効となります。

[未設定時]

なし

25.13 その他

25.13.1 addact

[機能]

コマンド実行予約の設定

[適用機種]

Si-R G110

[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 進数で指定します。

dd
日付を、1～31 の 10 進数で指定します。

HH
時間を、0～23 の 10 進数で指定します。

MM
分を、0～59 の 10 進数で指定します。

<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。

［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。

25.13.2 watchdog service

[機能]

ウォッチドッグリセットの設定

[適用機種]

Si-R G110

[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
```

25.13.3 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 G110

[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)のいずれかを指定します。

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
```

25.13.4 telnetinfo

[機能]

TELNET 接続サービスの設定

[適用機種]

Si-R G110

[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)のいずれかを指定します。

[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。

[注意]

ご使用の telnet クライアントに Keep Alive 機能がある場合、利用者がキー入力しなくても telnet クライアントが定期的に telnet 制御パケットを送信するため、本装置に対して入力があったものとしてコネクション切断までの時間を延長してしまい、本設定時間を経過してもコネクションが切断されなくなる場合があります。

telnet クライアントの Keep Alive 機能を無効にするか、Keep Alive 設定時間より短い時間を本装置に設定してご利用ください。

[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
```

25.13.5 sysdown harderr thermal

[機能]

温度異常時の動作の設定

[適用機種]

Si-R G110

[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。(縮退モードへ遷移)
- 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。

[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
```

25.13.6 sysdown harderr other

[機能]

ハードエラー発生時の動作の設定

[適用機種]

Si-R G110

[入力形式]

sysdown harderr other <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。(縮退モードへ遷移)
- 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、温度異常および、リセットスイッチ、SELECT/ENTER ボタン、USB デバイス、I2C、PHY 以外のハードエラー発生時の動作を設定します。

[未設定時]

ハードエラー発生時に運用を継続するものとみなされます。

```
sysdown harderr other no
```

25.13.7 mflag

[機能]

CE 保守ログインの可否の設定

[適用機種]

Si-R G110

[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
```

25.13.8 sysname

[機能]

本装置の名称の設定

[適用機種]

Si-R G110

[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。

[注意]

本設定を変更した場合は、装置の再起動が必要です。

[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。

25.13.9 loopback ip address

[機能]

loopback インタフェース追加 IPv4 アドレスの設定

[適用機種]

Si-R G110

[入力形式]

loopback ip address [<number>] <address>

[オプション]

<number>

・ 追加 IPv4 アドレス定義番号

追加 IPv4 アドレス定義番号として 0 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。

<address>

・ IPv4 アドレス

loopback インタフェースに割り当てる IPv4 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 IPv4 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 IPv4 アドレスを通信に使用する場合は、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 IPv4 アドレスを設定します。

なお、loopback インタフェースの IPv4 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。

[未設定時]

追加 IPv4 アドレスなしとしてみなされます。

```
loopback ip address <number> 0.0.0.0
```

25.13.10 loopback ip ospf use

[機能]

OSPF 利用可否の設定

[適用機種]

Si-R G110

[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
0～2	Si-R G110

[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-R G110

[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
```

25.13.11 loopback ipv6 address

[機能]

loopback インタフェース追加 IPv6 アドレスの設定

[適用機種]

Si-R G110

[入力形式]

loopback ipv6 address [<number>] <address>

[オプション]

<number>

・ 追加 IPv6 アドレス定義番号
追加 IPv6 アドレス定義番号として 0 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。

<address>

・ IPv6 アドレス
loopback インタフェースに割り当てる IPv6 アドレスを指定します。
128 ビットすべてを指定します。
リンクローカルアドレスは指定できません。

[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 IPv6 アドレスを設定します。
なお、loopback インタフェースの IPv6 アドレスとしてはすでに::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、プレフィックス長は 128 固定です。
ほかのインタフェースと違うネットワークの IPv6 アドレスを設定する必要があります。

[未設定時]

追加 IPv6 アドレスなしとして動作します。

25.13.12 serverinfo ftp

[機能]

FTP サーバ機能の設定

[適用機種]

Si-R G110

[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
```

25.13.13 serverinfo ftp ipv6

[機能]

FTP サーバ機能の IPv6 の設定

[適用機種]

Si-R G110

[入力形式]

serverinfo ftp ipv6 <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 ipv6 on
```

25.13.14 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 G110

[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。

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-R G110

<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。

－ ipv6

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。

ipv6 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
0～999	Si-R G110

[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。

[注意]

<dst_addr>/<mask>に"dynamic"を指定した ACL は使用しないでください。

［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。

25.13.15 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 G110

[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-R G110

[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。

25.13.16 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 G110

[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
```

25.13.17 serverinfo sftp

[機能]

SSH FTP サーバ機能の設定

[適用機種]

Si-R G110

[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
```

25.13.18 serverinfo sftp ipv6

[機能]

SSH FTP サーバ機能の IPv6 の設定

[適用機種]

Si-R G110

[入力形式]

serverinfo sftp ipv6 <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 ipv6 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 ipv6 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 ipv6 on
```

25.13.19 serverinfo telnet

[機能]

TELNET サーバ機能の設定

[適用機種]

Si-R G110

[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
```

25.13.20 serverinfo telnet ipv6

[機能]

TELNET サーバ機能の IPv6 の設定

[適用機種]

Si-R G110

[入力形式]

serverinfo telnet ipv6 <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 ipv6 on
```

25.13.21 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 G110

[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。

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-R G110

<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。

－ ipv6

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。

ipv6 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
0～999	Si-R G110

[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。

[注意]

<dst_addr>/<mask>に"dynamic"を指定した ACL は使用しないでください。

［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。

25.13.22 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 G110

[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-R G110

[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。

25.13.23 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 G110

[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
```

25.13.24 serverinfo ssh

[機能]

SSH ログインサーバ機能の設定

[適用機種]

Si-R G110

[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
```

25.13.25 serverinfo ssh ipv6

[機能]

SSH ログインサーバ機能の IPv6 の設定

[適用機種]

Si-R G110

[入力形式]

serverinfo ssh ipv6 <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 ipv6 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 ipv6 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 ipv6 on
```

25.13.26 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 G110

[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。

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-R G110

<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。

－ ipv6

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。

ipv6 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
0～999	Si-R G110

[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。

[注意]

<dst_addr>/<mask>に"dynamic"を指定したACLは使用しないでください。

[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。

25.13.27 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 G110

[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-R G110

[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。

25.13.28 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 G110

[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
```

25.13.29 serverinfo http

[機能]

HTTP サーバ機能の設定

[適用機種]

Si-R G110

[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
```

25.13.30 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 G110

[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。

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-R G110

<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。

－ ipv6

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。

ipv6 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
0～999	Si-R G110

[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。

[注意]

<dst_addr>/<mask>に"dynamic"を指定した ACL は使用しないでください。

［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。

25.13.31 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 G110

[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-R G110

[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。

25.13.32 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 G110

[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
```

25.13.33 serverinfo dns

[機能]

DNS サーバ機能の設定

[適用機種]

Si-R G110

[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
```

25.13.34 serverinfo dns ipv6

[機能]

DNS サーバ機能の IPv6 の設定

[適用機種]

Si-R G110

[入力形式]

serverinfo dns ipv6 <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 ipv6 on
```

25.13.35 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 G110

[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。

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-R G110

<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。

－ ipv6

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。

ipv6 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
0～999	Si-R G110

[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。

[注意]

<dst_addr>/<mask>に"dynamic"を指定した ACL は使用しないでください。

［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。

25.13.36 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 G110

[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-R G110

[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。

25.13.37 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 G110

[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
```

25.13.38 serverinfo sntp

[機能]

SNTP サーバ機能の設定

[適用機種]

Si-R G110

[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
```

25.13.39 serverinfo sntp ipv6

[機能]

SNTP サーバ機能の IPv6 の設定

[適用機種]

Si-R G110

[入力形式]

serverinfo sntp ipv6 <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 ipv6 on
```

25.13.40 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 G110

[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。

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-R G110

<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。

－ ipv6

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。

ipv6 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
0～999	Si-R G110

[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。

[注意]

<dst_addr>/<mask>に"dynamic"を指定した ACL は使用しないでください。

［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。

25.13.41 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 G110

[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-R G110

[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。

25.13.42 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 G110

[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
```

25.13.43 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 G110

[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
```

25.13.44 serverinfo time ipv6 tcp

[機能]

TCP による TIME サーバ機能の IPv6 の設定

[適用機種]

Si-R G110

[入力形式]

serverinfo time ipv6 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 ipv6 tcp on
```

25.13.45 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 G110

[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
```

25.13.46 serverinfo time ipv6 udp

[機能]

UDP による TIME サーバ機能の IPv6 の設定

[適用機種]

Si-R G110

[入力形式]

serverinfo time ipv6 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 ipv6 udp on
```

25.13.47 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 G110

[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。

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-R G110

<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。

－ ipv6

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。

ipv6 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
0～999	Si-R G110

[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。

[注意]

<dst_addr>/<mask>に"dynamic"を指定した ACL は使用しないでください。

［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。

25.13.48 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 G110

[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-R G110

[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。

25.13.49 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 G110

[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
```

25.13.50 loopintercept internal

[機能]

装置内回り込みパケット検出機能の設定

[適用機種]

Si-R G110

[入力形式]

loopintercept internal <mode>

[オプション]

<mode>

- enable
  装置内回り込みパケット検出機能を使用します。
- disable
  装置内回り込みパケット検出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]

多重カプセル化による装置内での回り込みパケット検出機能を有効にするかどうかを設定します。

[未設定時]

装置内回り込みパケット検出機能を使用するとみなされます。

```
loopintercept internal enable
```

25.13.51 loopintercept external

[機能]

外部ネットワーク回り込みパケット検出機能の設定

[適用機種]

Si-R G110

[入力形式]

loopintercept external <mode>

[オプション]

<mode>

- enable
  外部ネットワーク回り込みパケット検出機能を使用します。
- disable
  外部ネットワーク回り込みパケット検出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]

自発パケットの外部ネットワークからの回り込みパケット検出機能を有効にするかどうかを設定します。

[未設定時]

外部ネットワーク回り込みパケット検出機能を使用するとみなされます。

```
loopintercept external enable
```

第 26 章 証明書関連情報の設定

26.1 証明書関連情報

26.1.1 certificate local name

[機能]

自装置証明書識別名の設定

[適用機種]

Si-R G110

[入力形式]

certificate local [<number>] name <name>

[オプション]

<number>

自装置証明書識別番号を指定します。

・ 自装置証明書識別番号
自装置証明書の識別番号を、0～4 の 10 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。

<name>

自装置証明書識別名を指定します。

・ 自装置証明書識別名
0x21,0x23～0x7e の 16 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]

自装置証明書識別名の設定を行います。
通常は、crypto certificate generate コマンド、crypto certificate local コマンドで設定を行います。

[注意]

crypto certificate generate コマンド、crypto certificate local コマンドで設定を行った場合は上書きされます。

[未設定時]

自装置証明書識別名を設定しないものとみなされます。

26.1.2 certificate local line

[機能]

自装置証明書の設定

[適用機種]

Si-R G110

[入力形式]

certificate local [<number>] line <line_number> <string>

[オプション]

<number>

自装置証明書識別番号を指定します。

・ 自装置証明書識別番号

自装置証明書の識別番号を、0～4 の 10 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。

<line_number>

自装置証明書の行番号を指定します。

・ 行番号

行番号を、0～99 の 10 進数で指定します。

<string>

Base64 形式の証明書を指定します。

・ 証明書データ

Base64 形式の自装置証明書を、 +、/、=、A～Z、a～z、0～9 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]

自装置証明書を Base64 形式で 1 行ずつ設定を行います。

通常は、crypto certificate generate コマンド、crypto certificate local コマンドで設定を行います。

[注意]

crypto certificate generate コマンド、crypto certificate local コマンドで設定を行った場合は上書きされます。

[未設定時]

自装置証明書を設定しないものとみなされます。

26.1.3 certificate remote name

[機能]

相手装置証明書識別名の設定

[適用機種]

Si-R G110

[入力形式]

certificate remote [<number>] name <name>

[オプション]

<number>

相手装置証明書識別番号を指定します。

・ 相手装置証明書識別番号
相手装置証明書の識別番号を、10 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。
機種ごとの相手装置証明書識別番号の範囲は以下のとおりです。

範囲	機種
0～49	Si-R G110

<name>

相手装置証明書識別名を指定します。

・ 相手装置証明書識別名
0x21,0x23～0x7e の 16 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]

相手装置証明書識別名の設定を行います。
通常は、crypto certificate remote コマンドで設定を行います。

[注意]

crypto certificate remote コマンドで設定を行った場合は上書きされます。

[未設定時]

相手装置証明書識別名を設定しないものとみなされます。

26.1.4 certificate remote line

[機能]

相手装置証明書の設定

[適用機種]

Si-R G110

[入力形式]

certificate remote [<number>] line <line_number> <string>

[オプション]

<number>

相手装置証明書識別番号を指定します。

・ 相手装置証明書識別番号
相手装置証明書の識別番号を、10 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。
機種ごとの相手装置証明書識別番号の範囲は以下のとおりです。

範囲	機種
0～49	Si-R G110

<line_number>

相手装置証明書の行番号を指定します。

・ 行番号
行番号を、0～99 の 10 進数で指定します。

<string>

Base64 形式の証明書を指定します。

・ 証明書データ
Base64 形式の相手装置証明書を、 +、/、=、A～Z、a～z、0～9 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]

相手装置証明書を Base64 形式で 1 行ずつ設定を行います。
通常は、crypto certificate remote コマンドで設定を行います。

[注意]

crypto certificate remote コマンドで設定を行った場合は上書きされます。

[未設定時]

相手装置証明書を設定しないものとみなされます。

26.1.5 certificate ca name

[機能]

認証局証明書識別名の設定

[適用機種]

Si-R G110

[入力形式]

certificate ca [<number>] name <name>

[オプション]

<number>

認証局証明書識別番号を指定します。

・ 認証局証明書識別番号
認証局証明書の識別番号を、0～4 の 10 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。

<name>

認証局証明書識別名を指定します。

・ 認証局証明書識別名
0x21,0x23～0x7e の 16 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]

認証局証明書識別名の設定を行います。
通常は、crypto certificate ca コマンドで設定を行います。

[注意]

crypto certificate ca コマンドで設定を行った場合は上書きされます。

[未設定時]

認証局証明書識別名を設定しないものとみなされます。

26.1.6 certificate ca line

[機能]

認証局証明書の設定

[適用機種]

Si-R G110

[入力形式]

certificate ca [<number>] line <line_number> <string>

[オプション]

<number>

認証局証明書識別番号を指定します。

・ 認証局証明書識別番号
認証局証明書の識別番号を、0～4 の 10 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。

<line_number>

認証局証明書の行番号を指定します。

・ 行番号
行番号を、0～99 の 10 進数で指定します。

<string>

Base64 形式の証明書を指定します。

・ 証明書データ
Base64 形式の相手装置証明書を、 +、/、=、A～Z、a～z、0～9 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]

認証局証明書を Base64 形式で 1 行ずつ設定を行います。
通常は、crypto certificate ca コマンドで設定を行います。

[注意]

crypto certificate ca コマンドで設定を行った場合は上書きされます。

[未設定時]

認証局証明書を設定しないものとみなされます。

26.1.7 certificate request line

[機能]

証明書要求の設定

[適用機種]

Si-R G110

[入力形式]

certificate request [<number>] line <line_number> <string>

[オプション]

<number>

証明書要求識別番号を指定します。

・ 証明書要求識別番号
証明書要求の識別番号を、0～4 の 10 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。

<line_number>

証明書要求の行番号を指定します。

・ 行番号
行番号を、0～99 の 10 進数で指定します。

<string>

Base64 形式の証明書要求を指定します。

・ 証明書要求データ
Base64 形式の証明書要求を、 +、/、=、A～Z、a～z、0～9 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]

証明書要求を Base64 形式で 1 行ずつ設定を行います。
通常は、crypto certificate generate コマンドで設定を行います。

[注意]

crypto certificate generate コマンドで設定を行った場合は上書きされます。

[未設定時]

証明書要求を設定しないものとみなされます。

26.1.8 certificate private line

[機能]

秘密鍵の設定

[適用機種]

Si-R G110

[入力形式]

certificate private [<number>] line <line_number> <string>

[オプション]

<number>

秘密鍵識別番号を指定します。

・ 秘密鍵識別番号
秘密鍵の識別番号を、0～4 の 10 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。

<line_number>

秘密鍵の行番号を指定します。

・ 行番号
行番号を、0～99 の 10 進数で指定します。

<string>

暗号化された秘密鍵を指定します。

・ 秘密鍵データ
暗号化された秘密鍵を指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

暗号化された秘密鍵の設定を行います。
通常は、crypto certificate generate コマンドで設定を行います。

[注意]

crypto certificate generate コマンドで設定を行った場合は上書きされます。

[未設定時]

秘密鍵を設定しないものとみなされます。

第 27 章 構成定義情報表示、削除、および操作コマンド

27.1 構成定義情報表示

27.1.1 show candidate-config

[機能]

編集中構成定義情報の表示

[適用機種]

Si-R G110

[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
ip address 192.168.0.1/24 3
ip rip use v1 v1 0 off
vlan 1
#
```

27.1.2 show running-config

[機能]

動作中構成定義情報の表示

[適用機種]

Si-R G110

[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
ip address 192.168.1.1/24 3
ip rip use v1 v1 0 off
vlan 2
#
```

27.1.3 show startup-config

[機能]

起動用構成定義情報の表示

[適用機種]

Si-R G110

[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
ether 1 1 vlan untag 1
ether 2 1 vlan untag 2
lan 0 ip address 192.168.0.1/24 3
lan 0 ip rip use v1 v1 0 off
lan 0 vlan 1
lan 1 ip address 192.168.1.1/24 3
lan 1 ip rip use v1 v1 0 off
lan 1 vlan 2
syslog facility 23
time zone 0900
resource system vlan 4084-4094
consoleinfo autologout 8h
telnetinfo autologout 5m
#
```

27.1.4 diff

[機能]

構成定義情報の差分の表示

[適用機種]

Si-R G110

[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
- /um0/任意のファイル名

[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。

[メッセージ]

```
<ERROR> diff failed: specified file is not configuration [<dst_filename>]
```

<dst_filename>で指定したファイルは構成定義ファイルではありません。

```
<ERROR> diff failed: file not found
```

比較するファイルが見つかりませんでした。

```
<ERROR> diff failed: cannot allocate temporary area
```

diff コマンドに必要な領域を割り当てることができませんでした。

```
<ERROR> diff: signal error
```

Control-C で実行中断されました。

```
<ERROR> diff failed: file read error
```

比較するファイルを読むことができませんでした。

```
<ERROR> diff failed: Permission denied
```

指定された操作は許可されていません。

```
<ERROR> diff: Cannot open file
```

比較するファイルを開くことができませんでした。

［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
#
```

27.2 構成定義情報削除

27.2.1 delete

[機能]

編集中構成定義情報の削除

[適用機種]

Si-R G110

[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 admin 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
```

27.3 構成定義情報操作

27.3.1 load

[機能]

構成定義の読み込み

[適用機種]

Si-R G110

[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
- /um0/任意のファイル名

[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。

[注意]

本コマンドはcandidate-configを上書きし、編集中のすべての構成定義情報が新規反映として扱われます。
装置起動後にはじめて第2構成定義ファイル(config2)を読み込む場合、セッション監視タイムアウトが発生するなど、ほかの通信処理に影響する可能性がありますので注意してください。

[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が下がった後に再度本コマンドを実行してください。

```
<WARNING> weak admin's password: set the password
```

管理者パスワードが設定されていません。
管理者パスワードを設定してください。

```
<WARNING> weak admin's password: contain at least 8 characters
```

管理者パスワードが7文字以下です。
8文字以上の管理者パスワードを設定してください。

```
<WARNING> weak admin's password: contain a different kind of character
```

管理者パスワードが英字のみ、または数字のみです。
英字、数字、記号を混ぜて管理者パスワードを設定してください。

```
<WARNING> weak user's password: contain at least 8 characters
```

一般ユーザパスワードが 7 文字以下です。
8 文字以上の一般ユーザパスワードを設定してください。

```
<WARNING> weak user's password: contain a different kind of character
```

一般ユーザパスワードが英字のみ、または数字のみです。
英字、数字、記号を混ぜて一般ユーザパスワードを設定してください。

```
<ERROR> load failed: config read error
```

USB メモリ上の構成定義ファイルの読み込みに失敗しました。

［実行例］

第 1 構成定義ファイルを読み込む場合

```
# load config1
#
```

27.3.2 save

[機能]

構成定義情報の保存

[適用機種]

Si-R G110

[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
- /um0/任意のファイル名

[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。
ファイル名の省略時は、起動時の構成定義ファイルに保存します。

[注意]

装置起動後にはじめて第2構成定義ファイル(config2)に保存する場合、セッション監視タイムアウトが発生するなど、ほかの通信処理に影響する可能性がありますので注意してください。

[メッセージ]

```
<ERROR> save failed: Permission denied
```

指定された操作は許可されていません。

```
<ERROR> save failed: cannot create file
```

構成定義ファイルを作成することができませんでした。

```
<ERROR> save failed: file write error
```

構成定義ファイルに書き込むことができませんでした。

[実行例]

```
# save
#
```

27.3.3 commit

[機能]

構成定義情報の動的反映

[適用機種]

Si-R G110

[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。

load コマンドまたは discard コマンド実行後に構成定義情報の動的反映を行うと、編集中のすべての構成定義情報が新規反映として扱われます。そのため、通信中に実行すると通信が一度切断されますのでご注意ください。

[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
#
```

27.3.4 commit try time

[機能]

構成定義情報の動的反映の切り戻し

[適用機種]

Si-R G110

[入力形式]

commit try time <time>

[オプション]

<time>

構成定義の切り戻しの時間を、1分～24時間の範囲で指定します。
単位は、h(時間)、m(分)、s(秒)のいずれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

commit コマンド動作を実行し、指定時間経過後に起動時構成定義(startup-config)への切り戻しを行います。

[注意]

切り戻しの予約後は、以下の動作は行えません。

- commit および commit try time コマンドによる動的反映
- save による構成定義保存

これらの動作を行いたい場合は、commit try cancel コマンドにより切り戻しの予約をキャンセルしてください。
構成定義の切り戻し時には、load startup-config と commit の実行が行われます(フラッシュ ROM に保存されている構成定義に切り替わります)。
したがって、フラッシュ ROM 上の構成定義が書き換えられている場合は、構成定義の切り替え前の構成定義に戻らないことがあります。

[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。

```
<ERROR> Waiting switch-back to old configuration.
```

構成定義切り戻しのタイマ動作中であるため、新たに動的反映を行えません。
commit try cancel コマンドによるキャンセル後に再度実行してください。

```
<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 try time 10m
#
```

27.3.5 commit try cancel

[機能]

構成定義情報の動的反映の切り戻しのキャンセル

[適用機種]

Si-R G110

[入力形式]

commit try cancel

[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]

構成定義の切り戻しの予約後に、切り戻し動作をキャンセルします。

[メッセージ]

<ERROR> Not waiting switch-back

予約された構成定義の切り戻しがありません。

[実行例]

```
# commit try cancel
#
```

27.3.6 discard

[機能]

構成定義情報の変更破棄

[適用機種]

Si-R G110

[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。

[注意]

本コマンドは candidate-config を上書きし、編集中のすべての構成定義情報が新規反映として扱われます。

[メッセージ]

```
<WARNING> weak admin's password: set the password
```

管理者パスワードが設定されていません。
管理者パスワードを設定してください。

```
<WARNING> weak admin's password: contain at least 8 characters
```

管理者パスワードが 7 文字以下です。
8 文字以上の管理者パスワードを設定してください。

```
<WARNING> weak admin's password: contain a different kind of character
```

管理者パスワードが英字のみ、または数字のみです。
英字、数字、記号を混ぜて管理者パスワードを設定してください。

```
<WARNING> weak user's password: contain at least 8 characters
```

一般ユーザパスワードが 7 文字以下です。
8 文字以上の一般ユーザパスワードを設定してください。

```
<WARNING> weak user's password: contain a different kind of character
```

一般ユーザパスワードが英字のみ、または数字のみです。
英字、数字、記号を混ぜて一般ユーザパスワードを設定してください。

[実行例]

```
# discard
```

27.4 ファイル操作コマンド

27.4.1 dir

[機能]

USB メモリのファイル一覧の表示

[適用機種]

Si-R G110

[入力形式]

dir [<filename>]

[オプション]

<filename>

表示するファイル名またはディレクトリ名を指定します。dir コマンドは一致したファイルまたはディレクトリのみを表示します。ディレクトリが指定された場合は、指定されたディレクトリ内に存在するファイルを表示します。

本オプションではワイルドカードが使用できます。使用可能なワイルドカードを以下に示します。

*****

すべての文字列が一致します。文字列の長さは関係しません。

?

任意の 1 文字と一致します。

[<char>]

<char>に記述された文字のいずれかが含まれる場合に一致します。

本オプションは複数指定することが可能です。

[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]

USB メモリのファイル一覧の表示を行います。

[メッセージ]

```
<ERROR> the specified directory cannot be found [<dirname>]
```

<dirname>で指定したディレクトリが見つかりません。

```
<ERROR> the specified file or directory cannot be found [<filename>]
```

<filename>で指定したファイルまたはディレクトリが見つかりません。

```
<ERROR> dir: signal error
```

Control-C で出力が中断されました。

［実行例］

```
# dir
Directory of /um0

    (1)                (2)        (3)      (4)
2005/06/10  11:55                  1445 CONFIG2.TXT
2005/06/10  11:55                  1445 CONFIG3.TXT
2005/06/10  11:55                  1445 CONFIG4.TXT
2005/06/10  11:55                  1445 CONFIG11.TXT
2005/06/10  11:55                  1445 CONFIG1.TXT
2005/06/13  03:16               2337531 FIRM
2005/06/13  01:58      <DIR>           TEST

                      total file                6
                      total directory           1
# dir test/*.*
Directory of /um0/test

2005/06/12  10:23                  3142 CONFIG2.TXT
2005/06/13  01:58      <DIR>           BKUP

                      total file                1
                      total directory           1
```

1) ファイルの更新日が表示されます。
2) ディレクトリであれば<DIR>と表示されます。
3) 通常ファイルであればファイルサイズが表示されます。単位は byte です。
4) ファイル名またはディレクトリ名が表示されます。

27.4.2 copy

[機能]

ファイルのコピー

[適用機種]

Si-R G110

[入力形式]

copy <src_filename> <dst_filename>

[オプション]

<src_filename>
コピー元のファイル名を指定します。

<dst_filename>
コピー先のファイル名を指定します。

[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]

ファイルのコピーを行います。ファイル名としては以下のものが指定できます。

<src_filename>として指定可能なファイル名

all	ソフトウェアおよび構成定義ファイル
candidate-config	編集中の構成定義ファイル
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
firmware	ソフトウェア
/um0/任意のファイル名	

<dst_filename>として指定可能なファイル名

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
firmware	ソフトウェア
/um0/任意のファイル名	

[注意]

<src_filename>に all を指定した場合、<dst_filename>は "/um0/"だけを指定してください。
"/um0/" 以降にファイル名を指定しても無効になります。

[メッセージ]

```
<ERROR> copy failed: Permission denied
```

指定された操作は許可されていません。

```
<ERROR> copy failed: file not found
```

コピー元のファイルが見つかりませんでした。

```
<ERROR> copy failed: cannot create file
```

コピー先のファイルを作成することができませんでした。

```
<ERROR> copy failed: file read error
```

コピー元のファイルを読むことができませんでした。

```
<ERROR> copy failed: file write error
```

コピー先のファイルに書き込むことができませんでした。

```
<ERROR> copy: signal error
```

Control-C で実行中断されました。

```
<ERROR> copy failed: file system is full
```

USB メモリ上のファイルシステムに空きがなく、コピー先のファイルに書き込むことができませんでした。

```
<ERROR> <src_filename> and <dst_filename> are identical (no execution)
```

<src_filename> と <dst_filename>に同一のファイルを指定しています。

```
<ERROR> copy: cannot allocate temporary memory
```

copy コマンドに必要な一時メモリを割り当てることができませんでした。

[実行例]

```
# copy config1 /um0/config1
#
```

27.4.3 remove

[機能]

ファイルの削除

[適用機種]

Si-R G110

[入力形式]

remove <filename>

[オプション]

<filename>
削除するファイル名を指定します。

[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]

USB メモリのファイルの削除を行います。

[メッセージ]

```
<ERROR> remove failed: file not found
```

削除するファイルが見つかりませんでした。

```
<ERROR> remove failed: this is not file
```

ファイルではないものを削除しようとしました。

```
<ERROR> remove failed: this is not operatable file
```

このファイルに対する操作は許可されていません。

```
<ERROR> remove: signal error
```

Control-C で実行中断されました。

[実行例]

```
# remove config1_um
#
```

27.4.4 rename

[機能]

USB メモリのファイル名の変更

[適用機種]

Si-R G110

[入力形式]

rename <old_filename> <new_filename>

[オプション]

<old_filename>
変更前のファイル名を指定します。

<new_filename>
変更後の新しいファイル名を指定します。

[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]

USB メモリのファイル名の変更を行います。

[メッセージ]

```
<ERROR> rename failed: cannot rename between different partition
```

異なるパーティションにはファイルを移動できません。

```
<ERROR> rename failed: file not found
```

移動元のファイルが見つかりませんでした。

```
<ERROR> rename failed: this is not file
```

ファイルではないものを移動しようとしました。

```
<ERROR> rename failed: this is not operatable file
```

このファイルに対する操作は許可されていません。

```
<ERROR> rename: signal error
```

Control-C で実行中断されました。

```
<ERROR> rename failed: file write error
```

移動先のファイルを書き込むのに失敗しました。

[実行例]

```
# rename config1_um config1_um_old
#
```

27.4.5 format

[機能]

USB メモリのフォーマット

[適用機種]

Si-R G110

[入力形式]

format

[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]

USB メモリのフォーマットを行い、出荷状態に初期化します。

[メッセージ]

```
<ERROR> format: signal error
```

Control-C で実行中断されました。

```
<ERROR> cannot format USB memory
```

USB メモリをフォーマットすることができませんでした。

[実行例]

```
# format
#
```

第 28 章 モード操作コマンド／ターミナル操作コマンド

28.1 モード操作

28.1.1 admin

[機能]

管理者クラスに移行する

[適用機種]

Si-R G110

[入力形式]

admin [<user>]

[オプション]

<user>

・管理者名
省略時は、"admin"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、管理者クラス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。

```
<WARNING> weak <user>'s password: set the password
```

管理者パスワードが設定されていません。
管理者パスワードを設定してください。

```
<WARNING> weak <user>'s password: contain at least 8 characters
```

管理者パスワードが 7 文字以下です。
8 文字以上の管理者パスワードを設定してください。

```
<WARNING> weak <user>'s password: contain a different kind of character
```

管理者パスワードが英字のみ、または数字のみです。
英字、数字、記号を混ぜて管理者パスワードを設定してください。

［実行例］

```
> admin
Password:
# exit
> admin administrator
Password:
# exit
>
```

28.1.2 su

[機能]

管理者クラスに移行する

[適用機種]

Si-R G110

[入力形式]

su [<user>]

[オプション]

<user>

・ 管理者名
省略時は、"admin"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、管理者クラス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。

```
<WARNING> weak <user>'s password: set the password
```

管理者パスワードが設定されていません。
管理者パスワードを設定してください。

```
<WARNING> weak <user>'s password: contain at least 8 characters
```

管理者パスワードが 7 文字以下です。
8 文字以上の管理者パスワードを設定してください。

```
<WARNING> weak <user>'s password: contain a different kind of character
```

管理者パスワードが英字のみ、または数字のみです。
英字、数字、記号を混ぜて管理者パスワードを設定してください。

［実行例］

```
> su
Password:
# exit
> su administrator
Password:
# exit
>
```

28.1.3 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 G110

[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。

[注意]

一般ユーザクラスで設定した terminal コマンドおよび alias コマンドの内容は、ログアウト時に破棄されます。

[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。

[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:
```

28.1.4 configure

[機能]

構成定義モードに移行する

[適用機種]

Si-R G110

[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、コマンドユーザーズガイドの「シェル機能を使う」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)#
```

28.1.5 end

[機能]

運用管理モードに戻る

[適用機種]

Si-R G110

[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
#
```

28.1.6 quit

[機能]

運用管理モードに戻る

[適用機種]

Si-R G110

[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
#
```

28.1.7 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 G110

[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)#
```

28.1.8 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 G110

[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)#
```

28.1.9 !

[機能]

クラス、モード、構成定義階層を戻る

[適用機種]

Si-R G110

[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)
#
```

28.2 ターミナル操作

28.2.1 terminal pager

[機能]

ページャー機能の設定

[適用機種]

Si-R G110

[入力形式]

terminal pager {enable|disable}

[オプション]

enable
ページャー機能を使用します。

disable
ページャー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]

ページャー機能を使用するかどうかを指定します。

ページャー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みバイト数の割合)
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(以下のキー入力前に1以上を指定)
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

入力キー	動作
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 (ほかの文字と組み合わせて使用)
$	行末 (ほかの文字と組み合わせて使用)
\<	単語開始 (ほかの文字と組み合わせて使用)
\>	単語終了 (ほかの文字と組み合わせて使用)
\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]

画面行数が 3 行以下の場合はページャー機能は動作しません。また、画面桁数がプロンプト文字列の長さ以下の場合は表示が乱れます。

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]

ページャー機能を使用しないものとみなされます。

```
terminal pager disable
```

28.2.2 terminal window

[機能]

ターミナル画面サイズの設定

[適用機種]

Si-R G110

[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 進数で指定します。

line <line>

ターミナルの画面行数を、10 進数で指定します。

[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。

通知されたあと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
```

28.2.3 terminal charset

[機能]

漢字コードの設定

[適用機種]

Si-R G110

[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
```

28.2.4 terminal prompt

[機能]

入力プロンプト文字列の設定

[適用機種]

Si-R G110

[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)
\u	ログインユーザ名
\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	ソフトウェアバージョン

特殊文字	展開文字列
\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 config1 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"の後ろの文字が空白の場合は、空白が 1 つ削除されます。

config2 の構成定義情報で起動している場合は、"config2"が表示され、"\c"の前の文字が空白でない場合は、空白が 1 つ挿入されます。

"\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	#

[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。

[実行例]

```
# terminal prompt login "Welcome: "
# terminal prompt user "[\!]\h\w\p"
# terminal prompt admin "\h bank/\C\w\p"
#
```

[未設定時]

以下を設定するものとみなされます。

```
terminal prompt login "Login: "
terminal prompt user "\h \c\w\p"
terminal prompt admin "\h \c\w\p"
```

28.2.5 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 G110

[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
```

28.2.6 terminal bell

[機能]

操作エラーベル機能の設定

[適用機種]

Si-R G110

[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
```

28.2.7 terminal logging

[機能]

コマンド実行履歴機能の設定

[適用機種]

Si-R G110

[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
```

28.2.8 show terminal

[機能]

ターミナル情報の表示

[適用機種]

Si-R G110

[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
#
```

28.3 コマンド実行履歴

28.3.1 show logging command

[機能]

コマンド実行履歴の表示

[適用機種]

Si-R G110

[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。

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、以下のいずれかの方法で"*"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、適する小さい履歴番号に戻ります。

[実行例]

```
# show logging command
12/01 15:58:55       1  show system information
12/01 15:59:04       2  show date
12/01 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
#
```

28.3.2 clear logging command

[機能]

コマンド実行履歴の消去

[適用機種]

Si-R G110

[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
#
```

28.4 コマンドエイリアス

28.4.1 alias

[機能]

コマンドエイリアス情報の設定

[適用機種]

Si-R G110

[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。

28.4.2 show alias

[機能]

コマンドエイリアス情報の表示

[適用機種]

Si-R G110

[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"
#
```

28.4.3 clear alias

[機能]

コマンドエイリアス情報の削除

[適用機種]

Si-R G110

[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
#
```

28.5 コマンド出力操作

28.5.1 more

[機能]

コマンドの出力を画面単位に表示

[適用機種]

Si-R G110

[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)
#
```

28.5.2 tail

[機能]

コマンド出力の末尾部分の表示

[適用機種]

Si-R G110

[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末尾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。

ページャー(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末尾部分)に対してページャーが動作します。

[注意]

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-R G110: protocol: master port link recover
Jul 10 09:30:30 192.168.0.1 Si-R G110: sshd: generated public/private host key pair.
Jul 10 09:30:52 192.168.0.1 Si-R G110: logon: login admin on console
#
```

28.5.3 grep

[機能]

コマンドの出力の条件指定表示

[適用機種]

Si-R G110

[入力形式]

<command> | grep [invert] [around <lines>] pattern <pattern> <command>

[オプション]

<command>
実行するコマンドを指定します。

invert
一致行非表示を指定します。

around <lines>
前後表示行数指定を指定します。

pattern <pattern>
検索文字列指定を指定します。

[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]

指定したコマンドを実行し、そのコマンドの出力を指定した条件に一致した部分だけ表示します。
指定したコマンドの出力に指定した条件が見つからなかった場合、何も表示されません。

[注意]

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、grep 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。

［実行例］

```
# show ether statistics | grep pattern Octets
Octets                   : 0
Octets                   : 0
Octets                   : 0
Octets                   : 0
Octets                   : 420
Octets                   : 0
Octets                   : 0
Octets                   : 0
Octets                   : 0
Octets                   : 0
Octets                   : 0
Octets                   : 0
Octets                   : 0
Octets                   : 0
Octets                   : 0
Octets                   : 0
Octets                   : 0
Octets                   : 0
Octets                   : 0
Octets                   : 0
Octets                   : 0
Octets                   : 0
Octets                   : 0
#
```

第 29 章 システム操作および表示コマンド

29.1 システム操作および表示

29.1.1 show system information

[機能]

静的なシステム情報の表示

[適用機種]

Si-R G110

[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]

```
# show system information
Current-time : Thu Apr 16 06:23:59 2015                 ---(1)
Startup-time : Thu Apr 16 06:23:52 2015                 ---(2)
System : Si-R G110                                      ---(3)
Serial No. : 10000472                                   ---(4)
ROM Ver. : 1.0                                          ---(5)
Firm Ver. : V03.00 NY0005 Thu Apr 16 10:11:05 JST 2015  ---(6)
Startup-config : Wed Apr 15 09:05:38 2015 config1       ---(7)
Running-config : Thu Apr 16 06:23:52 2015               ---(8)
MAC : 2cd444fd02c4-2cd444fd02ca                         ---(9)
Memory : 256MB                                          ---(10)
USB   : ------                                          ---(11)
#
```

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-R G110 :
   Si-R G110 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.
   ソフトウェアの版数、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 進数で表示されます。

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) USB(Si-R G110)
USB ポートに実装された USB デバイスの名称が表示されます。

29.1.2 show system status

[機能]

動的なシステム情報の表示

[適用機種]

Si-R G110

[入力形式]

show system 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]

装置の動的なシステム情報を表示します。

[実行例]

```
# show system status
Current-time         : Thu May 14 13:38:56 2015                  ---(1)
Startup-time         : Thu May 14 13:20:52 2015                  ---(2)
restart_cause        : power on                                  ---(3)
machine_state        : RUNNING                                   ---(4)
power_consumption    : 9 W                                       ---(5)
internal_state       : NORMAL                                    ---(6)
sfp_cage_state       : NORMAL
internal_temp        : 33 C                                      ---(7)
sfp_cage_temp        : 30 C
CONNECTOR                                                        ---(8)
 usb      :
```

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) restart_cause
   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

   thermal reset
   ： 温度異常によるリセット発生
4) machine_state
   装置の状態が表示されます。

RUNNING

: 動作中

FALLBACK

: 縮退モードで起動中

5) power_consumption

消費電力量が表示されます。

コマンド投入時の瞬間的な電流量から算出した概算値になります。

※消費電力量の目安として参照ください。

6) internal_state

内部温度の状態が表示されます。

sfp_cage_state

SFP ケージ付近温度の状態が表示されます。

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) internal_temp

内部温度が表示されます。

sfp_cage_temp

SFP ケージ付近の温度が表示されます。

8) CONNECTOR

USB ポートに実装された USB デバイス、データ通信モジュールの名称が表示されます。

29.1.3 show system funcswitch

[機能]

SELECT ボタンで選択した機能の制御状態の表示

[適用機種]

Si-R G110

[入力形式]

show system funcswitch

[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]

SELECT ボタンで選択した機能の制御状態を表示します。

[実行例]

```
# show system funcswitch
[ECO lamp]
  status          : enable                          ---(1)
  Execution time  : Mon Jan 31 08:40:05 2011        ---(2)
#
```

1) status
ECO モードランプ機能による現在のランプ状態が表示されます。

-
未実行

enable
ランプ点灯

disable
ランプ消灯

2) Execution time
ECO モードランプ機能を実行した時間が表示されます。未実行の場合は"-"が表示されます。

29.1.4 show tech-support

[機能]

解析情報の一括表示

[適用機種]

Si-R G110

[入力形式]

show tech-support [detail] [save]

[オプション]

なし

結果を表示します。

detail

結果を詳細表示します。

save

結果をUSBメモリに書き込みます。

[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するか、USBメモリに書き込んでください。

[注意]

ページャー機能(terminal pager enable コマンド参照)が有効でも、本コマンドの出力は停止することなく表示されます。

29.1.5 show logging error

[機能]

エラーログの表示

[適用機種]

Si-R G110

[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]

```
# show logging error
------------------ Error logs in FLASH ------------------
[0] Error Log:
flag=80,mode=00,unit=10,regsp=00000000
Firm information:
Si-R G110 V03.00 PTF:NY0001
Error information:
error code [c8007000]
Logging time:
Tue Jan  6 09:34:17 2015
Hardware diagnostic error information:
Detail [016077e8 016077ec 0000000d 00000000]
       [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-R G110 V03.00 PTF:NY0001
Error information:
error code [c8012005]
Logging time:
Tue Jan  6 15:02:57 2015
Hardware diagnostic error information:
Detail [0164c818 0164c81c 8a000301 00000000]
       [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=05ff93e0,thread=cmdexec
Firm information:
Si-R G110 V03.00 PTF:NY0001
System down information:
down code [00000080:0000000d]
Logging time:
Fri Jan  9 11:33:16 2015
Register:
    srr0    [007f5b60] srr1    [0002d200] csrr0   [00000000] csrr1   [00000000]
    mcsrr0  [00000000] mcsrr1  [00000000] mcar    [00000000] mcsr    [00000000]
    lr      [007f5d70] dear    [00000001] esr     [00800000] tsr     [00000000]
    gpr00   [007f5d60] gpr01   [05ff94e0] gpr02   [00000005] gpr03   [00000001]
    gpr04   [00000000] gpr05   [00000008] gpr06   [0126a0c0] gpr07   [00000000]
    gpr08   [00000000] gpr09   [00000000] gpr10   [00000000] gpr11   [00000000]
    gpr12   [00000000] gpr13   [00000000] gpr14   [00000000] gpr15   [00000000]
    gpr16   [00000000] gpr17   [00000000] gpr18   [00000000] gpr19   [00000000]
    gpr20   [00000000] gpr21   [0126a0c0] gpr22   [00000003] gpr23   [00000003]
    gpr24   [00000000] gpr25   [0126a0c0] gpr26   [00000008] gpr27   [00000001]
    gpr28   [00000001] gpr29   [00000000] gpr30   [05bdd6f0] gpr31   [05bdd6f0]
Peripheral Register:
    err_det [00000000] l2errdet[00000000] eedr    [00000000] ltesr   [00000000]

User Stack:
          +0       +4       +8       +C         +0  +4  +8  +C
05ff94e0  05ff9510 007f5d60 05bdd7bf 0126aff4   ......]`.....&..
05ff94f0  05ff9510 01563570 0126a0c0 05ff9520   .....V5p.&.....
05ff9500  05bdd6f0 05d96d04 05bdd6f0 0126a0c0   ......m......&..
05ff9510  05ff9560 00a80698 00000000 00000000   ...`............
05ff9520  0126b098 0126aff4 ffffd7b8 05ff9540   .&...&.........@
05ff9530  00000000 00000000 00000003 0126a0c0   .............&..
05ff9540  00000000 01563570 00000000 00090044   .....V5p.......D
05ff9550  05bdd6f0 00000003 00000000 0126a0c0   .............&..
05ff9560  05ff9590 00a80ae8 05ff96a8 05bdc108   ................
05ff9570  05ff9660 01563570 00000000 00000000   ...`.V5p........
05ff9580  00000003 00000000 05bdd6f0 00000003   ................
05ff9590  05ff96a0 00a80f34 00000000 00000000   .......4........
05ff95a0  00000000 00000000 00000000 00000000   ................
05ff95b0  00000000 00000000 00000000 00000000   ................
05ff95c0  05ff95e0 00000000 00000000 00000000   ................
05ff95d0  00000000 01630000 00000007 00000000   .....c..........
05ff95e0  05ff9610 00524410 05ff9578 00000000   .....RD....x....
05ff95f0  05ff9610 00000000 016ca86c 00000000   .........l.l....
05ff9600  05bdd7b8 00000000 00000002 016ca834   .............l.4
05ff9610  05ff96ac 00000003 00000000 00000000   ................
05ff9620  01630000 01630000 05ff96a8 05bdc108   .c...c..........
05ff9630  05ff9660 0052caec 05ff96a8 05bdc108   ...`.R..........
05ff9640  05ff9660 00000003 05bdc124 00000000   ...`.......$....
05ff9650  05ff9670 05bdd6f0 00000003 00000003   ...p............
05ff9660  05ff96a0 0052807c 05bdd6f0 05bdc108   .....R.|........
05ff9670  05ff96a0 00527c40 00000000 016ca834   .....R|@.....l.4
05ff9680  0126a0c0 016ca86c 00000000 00000000   .&...l.l........
05ff9690  00000000 00000000 00000000 0126a0c0   .............&..
05ff96a0  05ff96d0 00a810b8 00000003 05bdd6f0   ................
05ff96b0  00000000 00000000 00000003 01650488   .............e..
05ff96c0  016ca834 00000000 00000000 05bdc108   .l.4............
05ff96d0  05ff9710 00a589a8 00000000 00000000   ................
05ff96e0  00000000 00000000 00000000 00000002   ................
05ff96f0  05bdc108 00000002 0126a0c0 016ca86c   .........&...l.l
05ff9700  00000003 00000000 00000000 05bdc108   ................
05ff9710  05ff9750 0052efd0 00000000 00000000   ...P.R..........
05ff9720  00000009 00000000 00000000 00000000   ................
05ff9730  00000000 00000000 00000000 00000000   ................
05ff9740  00408c0c 05bdc108 20000000 016ca7ec   .@...... ....l..
05ff9750  05ff9770 00523658 00004e43 00000020   ...p.R6X..NC...
05ff9760  05ff9770 0002d200 20000000 42000022   ...p.... ...B..″
05ff9770  00000000 00409ce8 00000000 00000000   .....@..........
05ff9780  00000000 00000000 00000000 00000000   ................
```

```
05ff9790  00000000 00000000 00000000 00000000  ................
05ff97a0  00000000 00000000 00000000 00000000  ................
05ff97b0  00000000 00000000 00000000 00000000  ................
05ff97c0  00000000 00000000 00000000 00000000  ................
05ff97d0  00000000 00000000 00000000 00000000  ................
05ff97e0  00000000 00000000 00000000 00000000  ................
05ff97f0  00000000 00000000 00000000 00000000  ................
05ff9800  00000000 00000000 00000000 00000000  ................
05ff9810  00000000 00000000 80000000 01650488  .............e..
05ff9820  00000000 00523449 00000400 00013c3c  .....R4I......<<
05ff9830  00a6b45c 00a69ecc 00003708 0000371c  ...\......7...7.
05ff9840  2d2d2d2d 2d2d2d2d 2d2d2d2d 2d2d2d2d  ----------------
05ff9850  2d2d2045 72726f72 206c6f67 7320696e  -- Error logs in
05ff9860  20464c41 5348202d 2d2d2d2d 2d2d2d2d   FLASH ---------
05ff9870  2d2d2d2d 2d2d2d2d 2d0a2d2d 2d2d2d2d  ---------.------
05ff9880  2d2d2d2d 2d2d2d2d 2d2d2d2d 20457272  ------------ Err
05ff9890  6f72206c 6f677320 696e2044 52414d20  or logs in DRAM
05ff98a0  2d2d2d2d 2d2d2d2d 2d2d2d2d 2d2d2d2d  ----------------
05ff98b0  2d2d2d0a 00000000 00000000 00000000  ---.............
05ff98c0  00000000 00000000 00000000 00000000  ................
05ff98d0  00000000 00000000 00000000 00000000  ................

Interrupt Stack:
          +0       +4       +8       +C       +0  +4  +8  +C
05ff93e0  00a6f5a8 05ff94d0 00000027 fffffff5  ...........'....
05ff93f0  007f5d60 05ff94e0 00000005 00000001  ..]`............
05ff9400  00000000 00000008 0126a0c0 00000000  .........&......
05ff9410  00000000 00000000 00000000 00000000  ................
05ff9420  00000000 00000000 00000000 00000000  ................
05ff9430  00000000 00000000 00000000 0.........
05ff9440  00000000 0126a0c0 00000003 00000003  .....&..........
05ff9450  00000000 0126a0c0 00000008 00000001  .....&..........
05ff9460  00000001 00000000 05bdd6f0 05bdd6f0  ................
05ff9470  007f5b60 0002d200 00000000 00000000  ..[`............
05ff9480  007f5d70 00860abc 20000000 20000002  ..]p.... ... ...
05ff9490  00000009 00000001 00800000 00000000  ................
05ff94a0  00000000 00000000 00000000 00000000  ................
05ff94b0  00000000 00000000 00000000 00000000  ................
05ff94c0  00000000 00000000 00000000 00000001  ................
05ff94d0  00000001 0164c7a0 00004e43 00000034  .....d....NC...4
#
```

29.1.6 clear logging error

[機能]

エラーログのクリア

[適用機種]

Si-R G110

[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
#
```

29.1.7 show logging syslog

[機能]

システムログ情報の表示

[適用機種]

Si-R G110

[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、例外としてソフトウェ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-R G110: init: system startup now.
Nov 11 08:31:06 192.168.1.1 Si-R G110: protocol: ether 1 1 link up
Nov 11 08:31:06 192.168.1.1 Si-R G110: protocol: lan 0 link up
```

29.1.8 clear logging syslog

[機能]

システムログ情報のクリア

[適用機種]

Si-R G110

[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
#
```

29.1.9 clear statistics

[機能]

全統計情報のクリア

[適用機種]

Si-R G110

[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
#
```

29.1.10 show date

[機能]

現在の装置の日付、時刻の表示

[適用機種]

Si-R G110

[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
Wed Jan  5 12:30:00 2011  ---(1)
```

1) 現在の日付、時刻が表示されます。

29.1.11 date

[機能]

現在の装置の日付、時刻の表示/設定

[適用機種]

Si-R G110

[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
Sat Jan  1 12:30:00 2011
#
```

日付、時刻を設定する場合

```
# date 2011/01/01.12:30:00
#
```

29.1.12 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 G110

[入力形式]

rdate

[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]

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
Sat Jan  1 12:30:00 2011
#
```

29.1.13 reset

[機能]

装置の再起動

[適用機種]

Si-R G110

[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
```

29.1.14 update

[機能]

ソフトウェアの更新

[適用機種]

Si-R G110

[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 で指定したソフトウェア更新情報に従ってリモートホスト(ftp サーバ)からソフトウェアを取得し、本装置の FLASH メモリに格納されたソフトウェアを書き換えます。
更新したソフトウェアは本装置の再起動後に有効になります。

[注意]

ソフトウェアの更新中は、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。

```
detected HARD ERROR, cannot execute
```

［実行例］

```
# 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 '/SIRG110SOFT.ftp' (5169106 bytes).
Hash mark printing on (4096 bytes/hash mark).
#################
#################
         :
#################
###############
5169106 bytes received in 4.569 seconds (186.834 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-R G110 V03.00 PTF:NY0001
[new] Si-R G110 V03.00 PTF:NY0002
update: File information check ok.

update: Rom firm write now!
target file type 'firm' (5169106 bytes)
Erase now...
@@@@@@@@@@@@@@@@   ..[ 16 s]
@@                 ..[ 18 s]
Erase end. (34 seconds)
Write now...
@@@@@@@@@@@@@@@@   ..[  1 %]
@@@@@@@@@@@@@@@@   ..[  2 %]
         :
@@@@@@@@@@@@@@@@   ..[ 98 %]
@@@@@@@@@@@@@@     ..[100 %]
5168994 bytes wrote in 48.274 seconds (148.684 Kbytes/sec)
update: Rom firm write ok.

#
```

29.1.15 getdomainlist

[機能]

ドメインリストの取得

[適用機種]

Si-R G110

[入力形式]

getdomainlist

[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]

domainlistinfo で指定したドメインリスト情報に従ってリモートホスト(ftp サーバ)からドメインリストを取得し、本装置のドメインリストを書き換えます。更新が完了次第、そのドメインリストは有効になります。

[注意]

ProxyDNS 順引き動作の設定を変更したものを動的反映した場合、取得したドメインリスト情報はクリアされ、ACL に取得された動的 IP アドレスも削除されます。

[実行例]

```
# getdomainlist
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 '/domainlist' (174 bytes).
Hash mark printing on (4096 bytes/hash mark).
#
174 bytes received in 0.0015 seconds (11.328 Kbytes/sec)
226 Transfer complete.
221 Goodbye.
update: File transfer ok.

#
```

第 30 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

・ グループ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〈group〉(ether グループ定義番号)に指定するグループ番号の通し番号(10 進数)は、以下に示す範囲で指定してください。

範囲	機種
1～2	Si-R G110

・ ポ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〈port〉(ether ポート定義番号)に指定するポート番号の通し番号(10 進数)は、以下に示す範囲で指定してください。

範囲	機種
1	Si-R G110 (グループ 1)
1～4	Si-R G110 (グループ 2)

30.1 Ethernet のカウンタ・ログ・統計・状態などの表示

30.1.1 show ether

[機能]

Ethernet 物理ポートの情報の表示

[適用機種]

Si-R G110

[入力形式]

show ether [group <group> [port <port>]]

[オプション]

なし

すべての情報を表示します。

group <group>

・ ether グループ番号
ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

port <port>

・ ether ポート番号
ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

[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]

Ethernet ポートの情報を表示します。
group オプションのみ指定した場合は、対象グループの全ポートの情報が表示されます。
group オプション、port 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]

```
# show ether group 1 port 1

[ETHER GROUP-1 PORT-1]
description      : Ether_Group_1_Port_1                    ---(1)
status           : auto 1000M Full MDI-X                   ---(2)
media            : Metal                                   ---(3)
flow control     : send on, receive on                     ---(4)
type             : Normal                                  ---(5)
since            : Mar  2 16:01:50 2011                    ---(6)
config           : mode(auto), mdi(auto), media(auto)      ---(7)

#
```

```
# show ether group 2 port 1-2

[ETHER GROUP-2 PORT-1]
description      : Ether_Group_2_Port_1                    ---(1)
status           : auto 1000M Full MDI-X                   ---(2)
media            : Metal                                   ---(3)
flow control     : send on, receive on                     ---(4)
type             : Backup (group 1, master)                ---(5)
since            : Mar  2 16:01:50 2011                    ---(6)
config           : mode(auto), mdi(auto), media(-)         ---(7)

[ETHER GROUP-2 PORT-2]
description      : Ether_Group_2_Port_2
status           : auto 1000M Full MDI-X
media            : Metal
flow control     : send on, receive on
type             : Backup (group 1, backup, standby)
since            : Mar  2 16:01:50 2011
config           : mode(auto), mdi(auto), media(-)

#
```

1) ether ポートの説明文

ether description で設定された内容が表示されます。

2) ポートの状態

接続完了時の速度、状態が表示されます。

disable

定義により使用しない状態であることを示します。

offline

オフライン状態であることを示します。

要因によっては、以下のように示します。

offline (backup) : バックアップポート機能によるポート閉塞(ether グループ 2 のみ)

offline (startup down) : 起動時閉塞機能によるポート閉塞

offline (recovery manual): 自動復旧停止機能によるポート閉塞

down

リンクダウン状態であることを示します。

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 ether ポートの通信速度(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。

3) ether ポートのメディア種別

ether ポートのメディア種別が表示されます。

Fiber

SFP ポートを使用していることを示します。

Metal

10/100/1000BASE-TX ポートを使用していることを示します。

-

リンクアップ状態にないため不定であることを示します。

4) フロー制御状態

フロー制御が送信／受信の順で表示されます。

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。

-

リンクアップ状態にないため不定であることを示します。

5) ポート種別

ポート種別が表示されます。

Normal

通常ポートとして使用していることを示します。

Backup

バックアップポートとして使用していることを示します。

所属するバックアップグループ番号、およびmaster/backup種別も表示されます。

※待機状態のポートについては、"standby"の表示を付与します。

Mirror

ミラーターゲットポートとして使用していることを示します。

-

未使用ポートまたは定義矛盾により不定であることを示します。

6) 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が表示されます。

7) 設定情報

ether mode, ether mdi, ether media コマンド設定値が表示されます。

mode(設定値)

ether modeの設定値を、mode(auto)のように表示します。

mdi(設定値)

ether mdiの設定値を、mdi(auto)のように表示します。(メディア種別がMetalの場合)

media(設定値)

ether media の設定値を、media(auto)のように表示します。(ethernetグループ1のみ)

30.1.2 show ether brief

[機能]

Ethernet 物理ポートの情報の簡易表示

[適用機種]

Si-R G110

[入力形式]

show ether brief

[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]

Ethernet ポートの情報を簡易表示します。

[実行例]

```
# show ether brief

port  status   type                media  mdi   speed  duplex  flow
----- -------- ------------------ ------ ----- ------ ------- -----
(1)   (2)      (3)                (4)    (5)   (6)    (7)     (8)
1 1   up       normal             metal  MDIX  100M   full    TxRx
      ・                          ・
      ・                          ・
2 1   offline  normal             -      -     -      -       -
      ・                          ・
      ・                          ・
#
```

1) ポート番号
2) ポートの状態

up
リンクアップ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。

standby
スタンバイ状態であることを示します。(backup ポートのみ)
※リンクアップ状態で待機ポートとして成立しない(切り替われない)状態である場合は"*standby"の表示を付与します。

offline
オフライン状態であることを示します。

disable
定義により使用しない状態であることを示します。

3) ポート種別

normal
通常ポートとして使用していることを示します。

backup
バックアップポートとして使用していることを示します。

所属するバックアップグループ番号も表示されます。

mirror

ミラーターゲットポートとして使用していることを示します。

-

未使用ポートまたは定義矛盾により不定であることを示します。

4) ether ポートのメディア種別

fiber

SFP ポートを使用していることを示します。

metal

10/100/1000BASE-T ポートを使用していることを示します。

-

リンクアップ状態にないため不定であることを示します。

5) ether ポートの MDI 状態

MDI/MDIX

現在リンクしている MDI の種別を示します。(メディア種別が metal の場合)

-

リンクアップ状態にないため不定であることを示します。

6) ether ポートの通信速度状態

10M/100M/1000M

現在リンクしている ether ポートの通信速度(10Mbps/100Mbps/1000Mbps)を示します。

-

リンクアップ状態にないため不定であることを示します。

7) ether ポートのデュプレックス状態

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。

-

リンクアップ状態にないため不定であること、または SFP ポートであることを示します。

8) ether ポートのフロー制御状態

Tx

フロー制御の送信機能が有効であることを示します。

Rx

フロー制御の受信機能が有効であることを示します。

-

リンクアップ状態にないため不定であること、フロー制御機能が無効であることを示します。

30.1.3 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 G110

[入力形式]

show ether statistics [group <group> [port <port>]] [detail]

[オプション]

なし

すべての統計情報を表示します。

group <group>

・ ether グループ番号

ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。
指定されたグループ上の情報を表示します。
また、該当するグループが無効の場合は情報は表示されません。

範囲	機種
1～2	Si-R G110

port <port>

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。

範囲	機種
1,c1～c4	Si-R G110 (グループ 1)
1～4,c1～c4	Si-R G110 (グループ 2)

複数のポート番号を指定する場合、", "(カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例: "1-8")。
c1～c4 は、CPU とスイッチデバイスをつないだ内部接続ポートを示します。
c1～c4 を指定する場合、group 指定は無効になります。
port 指定を省略した場合は、group 指定にかかわらず c1～c4 の情報が表示されます。

detail

Ether ポートの統計情報に詳細情報を追加して表示します。

[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]

Ethernet 物理ポートの統計情報を表示します。
<port>を省略時は、対象<group>上に搭載される全ポートの統計情報が表示されます。
<port> および <group>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。
内部接続ポート番号とグループとデバイスの関係を示します。

内部接続ポート番号	グループ	デバイス
c1	1	スイッチデバイス

内部接続ポート番号	グループ	デバイス
c2	2	スイッチデバイス
c3	1	CPU
c4	2	CPU

内部接続ポートの接続は、c1 と c3 が、c2 と c4 が接続されています。

[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]

```
# show ether statistics group 1 port 1

[ETHER GROUP-1 PORT-1 STATISTICS]
[Input Statistics]
 Octets                  : 0            ---(1-1)
  bits/sec               : 0            ---(1-2)
 Frames                  : 0            ---(1-3)
  frames/sec             : 0            ---(1-4)
 Unicast                 : 0            ---(1-5)
  frames/sec             : 0            ---(1-6)
 Multicast               : 0            ---(1-7)
  frames/sec             : 0            ---(1-8)
 Broadcast               : 0            ---(1-9)
  frames/sec             : 0            ---(1-10)
 Pause frames            : 0            ---(1-11)

 Discards
  All DiscardsPkts       : 0            ---(1-12)
 Errors
  Undersize              : 0            ---(1-13)
  FCSErrors              : 0            ---(1-14)
  AlignmentErrors        : 0            ---(1-15)
  FragmentErrors         : 0            ---(1-16)
  Jabbers                : 0            ---(1-17)
  SymbolErrors           : 0            ---(1-18)
  UnknownOpcodes         : 0            ---(1-19)

[Output Statistics]
 Octets                  : 0            ---(1-20)
  bits/sec               : 0            ---(1-21)
 Frames                  : 0            ---(1-22)
  frames/sec             : 0            ---(1-23)
 Unicast                 : 0            ---(1-24)
 Multicast               : 0            ---(1-25)
  frames/sec             : 0            ---(1-26)
 Broadcast               : 0            ---(1-27)
  frames/sec             : 0            ---(1-28)
 Pause frames            : 0            ---(1-29)

 Discards
  DelayExceededDiscards  : 0            ---(1-30)
  Queue Full Discards    : 0            ---(1-31)
 Errors
  FCSErrors              : 0            ---(1-32)
  FragmentErrors         : 0            ---(1-33)
  CarrierSenseErrors     : 0            ---(1-34)
  ExcessiveCollisions    : 0            ---(1-35)
  LateCollisions         : 0            ---(1-36)

 SingleCollisionFrames   : 0            ---(1-37)
 MultipleCollisionFrames : 0            ---(1-38)
 DeferredTransmissions   : 0            ---(1-39)
```

内部接続ポートの実行例

```
# show ether statistics group 1 port c1

[INTERNAL CONNECTION PORT-1 STATISTICS]   ---(1-40)
 Packets from             : group1        ---(1-41)
 Connected to             : C3            ---(1-42)

[Input Statistics]
 Octets                   : 0             ---(1-1)
  bits/sec                : 0             ---(1-2)
 Frames                   : 0             ---(1-3)
  frames/sec              : 0             ---(1-4)
 Unicast                  : 0             ---(1-5)
  frames/sec              : 0             ---(1-6)
 Multicast                : 0             ---(1-7)
  frames/sec              : 0             ---(1-8)
 Broadcast                : 0             ---(1-9)
  frames/sec              : 0             ---(1-10)
 Pause frames             : 0             ---(1-11)

 Discards
  All DiscardsPkts        : 0             ---(1-12)
 Errors
  Undersize               : 0             ---(1-13)
  FCSErrors               : 0             ---(1-14)
  AlignmentErrors         : 0             ---(1-15)
  FragmentErrors          : 0             ---(1-16)
  Jabbers                 : 0             ---(1-17)
  SymbolErrors            : 0             ---(1-18)
  UnknownOpcodes          : 0             ---(1-19)

[Output Statistics]
 Octets                   : 0             ---(1-20)
  bits/sec                : 0             ---(1-21)
 Frames                   : 0             ---(1-22)
  frames/sec              : 0             ---(1-23)
 Unicast                  : 0             ---(1-24)
 Multicast                : 0             ---(1-25)
  frames/sec              : 0             ---(1-26)
 Broadcast                : 0             ---(1-27)
  frames/sec              : 0             ---(1-28)
 Pause frames             : 0             ---(1-29)

 Discards
  DelayExceededDiscards   : 0             ---(1-30)
  Queue Full Discards     : 0             ---(1-31)
 Errors
  FCSErrors               : 0             ---(1-32)
  FragmentErrors          : 0             ---(1-33)
  CarrierSenseErrors      : 0             ---(1-34)
  ExcessiveCollisions     : 0             ---(1-35)
  LateCollisions          : 0             ---(1-36)

 SingleCollisionFrames    : 0             ---(1-37)
 MultipleCollisionFrames  : 0             ---(1-38)
 DeferredTransmissions    : 0             ---(1-39)
```

1-1)　受信したデータのオクテット数
1-2)　1 秒あたりの受信ビット数(bits/sec)
1-3)　受信した総フレーム数
1-4)　1 秒あたりの受信フレーム数(frames/sec)
1-5)　受信したユニキャストフレーム数
1-6)　1 秒あたりの受信したユニキャストフレーム数(frames/sec)
1-7)　受信したマルチキャストフレーム数
1-8)　1 秒あたりの受信したマルチキャストフレーム数(frames/sec)
1-9)　受信したブロードキャストフレーム数
1-10) 1 秒あたりの受信したブロードキャストフレーム数(frames/sec)

1-11) PAUSE フレーム(MAC 制御フレーム)受信数
1-12) 受信した全フレームのうち、廃棄した数
1-13) ショートサイズ(64 バイト未満)フレーム受信数
1-14) データサイズ 64～1518 バイトで FCS エラーを検出したフレーム数
1-15) アライメントエラーを検出した受信フレーム数
1-16) ショートサイズ(64 バイト未満)フレームで FCS エラーまたはアライメントエラーを検出したフレーム数
10M/100M half での接続時の通信でカウントアップする場合があります。
1-17) オーバサイズ(タグなしでは 1579 バイト以上、タグありでは 1583 バイト以上)で廃棄したフレーム受信数または、データサイズ 1519 バイト以上で FCS エラーまたは FCS アライメントエラーを検出したフレーム数
1-18) シンボルエラー発生回数
1-19) 未サポートの MAC 制御フレーム受信数
1-20) 全送信オクテット数
1-21) 1 秒あたりの送信ビット数(bits/sec)
1-22) 送信フレーム数
1-23) 1 秒あたりの送信フレーム数(frames/sec)
1-24) 送信したユニキャストフレーム数
1-25) 送信したマルチキャストフレーム数
1-26) 1 秒あたりの送信したマルチキャストフレーム数(frames/sec)
1-27) 送信したブロードキャストフレーム数
1-28) 1 秒あたりの送信したブロードキャストフレーム数(frames/sec)
1-29) PAUSE フレーム(MAC 制御フレーム)送信数
1-30) 過度な遅延による廃棄フレーム数
1-31) キューフルで破棄されたフレーム数
1-32) FCS エラーフレーム送信数
1-33) ショートサイズ(64 バイト未満)フレームで FCS エラーまたは FCS アライメントエラーを検出したフレーム送信数
1-34) キャリア未検出エラー発生回数
1-35) コリジョン多発によって送信が失敗したフレーム数
1-36) レイトコリジョン発生回数
1-37) 1 回のコリジョン発生後、送信が成功したフレーム数
1-38) 複数回のコリジョン発生後、送信が成功したフレーム数
1-39) 伝送路ビジーにより送信が遅延したフレーム数
1-40) 内部接続ポートの統計情報
1-41) 内部接続ポートに属する外部ポート
1-42) 対向する内部接続ポート

detail 指定時の実行例

```
# show ether statistics group 2 port 1 detail
[ETHER GROUP-2 PORT-1 STATISTICS]
[Input Statistics]
 Octets                  : 0
  bits/sec               : 0
 Frames                  : 0
  frames/sec             : 0
 Unicast                 : 0
  frames/sec             : 0
 Multicast               : 0
  frames/sec             : 0
 Broadcast               : 0
  frames/sec             : 0
 Pause frames            : 0
 Mac Control frames      : 0            ---(2-1)

 Discards
  All DiscardsPkts       : 0
  Resource Full          : 0            ---(2-2)
  Discards by Filter     : 0            ---(2-3)
  Policy Discards        : 0            ---(2-4)
```

```
  Port In Discards        : 0            ---(2-5)
  Input Discards          : 0            ---(2-6)
 Errors
  Undersize               : 0
  FCSErrors               : 0
  AlignmentErrors         : 0
  FragmentErrors          : 0
  Jabbers                 : 0
  SymbolErrors            : 0
  UnknownOpcodes          : 0

[Output Statistics]
 Octets                   : 0
  bits/sec                : 0
 Frames                   : 0
  frames/sec              : 0
 Unicast                  : 0
 Multicast                : 0
  frames/sec              : 0
 Broadcast                : 0
  frames/sec              : 0
 Pause frames             : 0
 Mac Control frames       : 0            ---(2-7)
 Jabbers                  : 0            ---(2-8)

 Discards
  DelayExceededDiscards   : 0
  Internal Discards       : 0            ---(2-9)
  Queue Full Discards     : 0
 Errors
  FCSErrors               : 0
  FragmentErrors          : 0
  CarrierSenseErrors      : 0
  ExcessiveCollisions     : 0
  LateCollisions          : 0
  InternalCellErrors      : 0

 SingleCollisionFrames    : 0
 MultipleCollisionFrames  : 0
 DeferredTransmissions    : 0

[Input Detail Statistics]
  Frame size                frames      frames/sec
        64                : 0           0                   ---(2-10)
        65-127            : 0           0                   ---(2-11)
        128-255           : 0           0                   ---(2-12)
        256-511           : 0           0                   ---(2-13)
        512-1023          : 0           0                   ---(2-14)
        1024-1518         : 0           0                   ---(2-15)
        1519-1582         : 0           0                   ---(2-16)

[Output Detail Statistics]
  Frame size                frames      frames/sec
        64                : 0           0                   ---(2-17)
        65-127            : 0           0                   ---(2-18)
        128-255           : 0           0                   ---(2-19)
        256-511           : 0           0                   ---(2-20)
        512-1023          : 0           0                   ---(2-21)
        1024-1518         : 0           0                   ---(2-22)
        1519-1582         : 0           0                   ---(2-23)
```

detail 指定時には以下の情報を追加して表示します。

2-1) MAC 制御フレーム受信数

2-2) リソース不足、またはバックプレッシャで廃棄した受信フレーム数

2-3) フィルタリングによって廃棄された受信フレーム数

2-4) Tag 付き vlan 登録したポートに Tag なしフレームを受信した場合に破棄された受信フレーム数
または、受信破棄設定により破棄された受信フレーム数

2-5) backup 設定により待機ポートとなったポートで廃棄された受信フレーム数
または、STP がフォワーディング状態でないことにより廃棄された受信フレーム数

2-6) その他の理由で廃棄された受信フレーム数

- MAC ヘッダが以下の値の場合

  Source MAC Address が FF:FF:FF:FF:FF:FF である、Source MAC Address がマルチキャストアドレス形式である

- 入力ポートで異常なフレームと認識されずに転送されたフレームのうち、出力されずに破棄された場合
- 入力フレームの負荷が高いため、内部接続ポートでフロー制御が動作し、フレームが破棄された場合

2-7) MAC 制御フレーム送信数

2-8) オーバサイズ(1519 バイト以上)フレームで FCS エラーまたは FCS アライメントエラーを検出したフレーム数

2-9) チップ内で廃棄されたフレーム数

2-10) データサイズ 64 バイトのフレーム受信数、および 1 秒あたりのデータサイズ 64 バイトのフレーム受信数(frames/sec)

2-11) データサイズ 65～ 127 バイトのフレーム受信数、および 1 秒あたりのデータサイズ 65～ 127 バイトのフレーム受信数(frames/sec)

2-12) データサイズ 128～ 255 バイトのフレーム受信数、および 1 秒あたりのデータサイズ 128～ 255 バイトのフレーム受信数(frames/sec)

2-13) データサイズ 256～ 511 バイトのフレーム受信数、および 1 秒あたりのデータサイズ 256～ 511 バイトのフレーム受信数(frames/sec)

2-14) データサイズ 512～1023 バイトのフレーム受信数、および 1 秒あたりのデータサイズ 512～1023 バイトのフレーム受信数(frames/sec)

2-15) データサイズ 1024～1518 バイトのフレーム受信数、および 1 秒あたりのデータサイズ 1024～1518 バイトのフレーム受信数(frames/sec)

2-16) データサイズ 1519 バイト以上のフレーム受信数、および 1 秒あたりのデータサイズ 1519 バイト以上のフレーム受信数(frames/sec)

2-17) データサイズ 64 バイトのフレーム送信数、および 1 秒あたりのデータサイズ 64 バイトのフレーム送信数(frames/sec)

2-18) データサイズ 65～ 127 バイトのフレーム送信数、および 1 秒あたりのデータサイズ 65～ 127 バイトのフレーム送信数(frames/sec)

2-19) データサイズ 128～ 255 バイトのフレーム送信数、および 1 秒あたりのデータサイズ 128～ 255 バイトのフレーム送信数(frames/sec)

2-20) データサイズ 256～ 511 バイトのフレーム送信数、および 1 秒あたりのデータサイズ 256～ 511 バイトのフレーム送信数(frames/sec)

2-21) データサイズ 512～1023 バイトのフレーム送信数、および 1 秒あたりのデータサイズ 512～1023 バイトのフレーム送信数(frames/sec)

2-22) データサイズ 1024～1518 バイトのフレーム送信数、および 1 秒あたりのデータサイズ 1024～1518 バイトのフレーム送信数(frames/sec)

2-23) データサイズ 1519 バイト以上のフレーム送信数、および 1 秒あたりのデータサイズ 1519 バイト以上のフレーム送信数(frames/sec)

内部接続ポートの実行例(c3,c4)

```
# show ether statistics group 1 port c3

[INTERNAL CONNECTION PORT-3 STATISTICS]   ---(3-1)
 Packets from             : group1        ---(3-2)
 Connected to             : C1            ---(3-3)

Input packets             : 0             ---(3-4)
Input error packets       : 0             ---(3-5)
 frames too long          : 0             ---(3-6)
 alignment errors         : 0             ---(3-7)
 frames too short         : 0             ---(3-8)
 FCS errors               : 0             ---(3-9)
 overrun                  : 0             ---(3-10)
 late collision           : 0             ---(3-11)
Output packets            : 0             ---(3-12)
Output error packets      : 0             ---(3-13)
 late collision           : 0             ---(3-14)
 excessive collisions     : 0             ---(3-15)
 underrun                 : 0             ---(3-16)
 carrier sense errors     : 0             ---(3-17)
```

3-1)　内部接続ポートの統計情報
3-2)　内部接続ポートに属する外部ポート
3-3)　対向する内部接続ポート
3-4)　受信したパケット数
3-5)　受信時にエラーを検出したパケット数
3-6)　最大値を超えてエラーとなった受信パケット数
3-7)　アライメントでエラーとなった受信パケット数
3-8)　最小値以下でエラーとなった受信パケット数
3-9)　FCS 異常でエラーとなった受信パケット数
3-10)　バッファオーバーランでエラーとなったパケット数
3-11)　Late コリジョンでエラーとなったパケット数
3-12)　送信したパケット数
3-13)　送信時にエラーを検出したエラーパケット数
3-14)　Late コリジョンでエラーとなった送信パケット数
3-15)　Excessive コリジョンでエラーとなった送信パケット数
3-16)　バッファアンダーランでエラーとなった送信パケット数
3-17)　キャリア検出でエラーとなった送信パケット数

30.1.4 show ether utilization

[機能]

Ethernet 物理ポートの使用率情報の表示

[適用機種]

Si-R G110

[入力形式]

show ether utilization

[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]

Ethernet 物理ポートの使用率情報を表示します。

[注意]

使用率情報は、本装置を再起動するとクリアされます。

[実行例]

```
# show ether utilization

[Group 1]
Port    TX/sec      Util      RX/sec      Util
------  ----------  -------   ----------  -------
    (1)         (2)       (3)         (4)       (5)
      1           0         0           0         0
      .                                 .
      .                                 .

[Group 2]
Port    TX/sec      Util      RX/sec      Util
------  ----------  -------   ----------  -------
     1           0         0           0         0
      .                                 .
      .                                 .

[Connection port]
Port    TX/sec      Util      RX/sec      Util
------  ----------  -------   ----------  -------
     1           0         0           0         0
     2           0         0           0         0
```

1) Port
   ポート番号が表示されます。
2) TX/sec
   1 秒間に送信したフレーム数(pps)が表示されます。
3) Util
   物理ポートの送信使用率(%)が表示されます。
4) RX/sec
   1 秒間に受信したフレーム数(pps)が表示されます。
5) Util

物理ポートの受信使用率(%)が表示されます。

30.1.5 show ether queue

[機能]

Ethernet 物理ポートの COS Queue に滞留しているパケット数の表示

[適用機種]

Si-R G110

[入力形式]

show ether queue [group <group> [port <port>]]

[オプション]

なし

すべてのポートの COS Queue に滞留しているパケット数を表示します。

group <group>

指定されたグループのポートの COS Queue に滞留しているパケット数を表示します。
また、該当するグループが無効の場合は内部テーブル情報は表示されません。

範囲	機種
1～2	Si-R G110

port <port>

指定されたポートの COS Queue に滞留しているパケット数を表示します。
また、該当するポート番号が無効の場合は情報は表示しません。

範囲	機種
1,c1～c2	Si-R G110（グループ 1）
1～4,c1～c2	Si-R G110（グループ 2）

複数のポート番号を指定する場合、″,″(カンマ)で区切ります。
複数の番号が続く場合、″-″(ハイフン)で区切ります(例: ″1-8″)。
c1～c2 は、CPU とスイッチデバイスをつないだ内部接続ポートを示します。
c1～c2 を指定する場合、group 指定は無効になります。

[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]

Ethernet 物理ポートの COS Queue に滞留しているパケット数を表示します。
group、port オプションを指定した場合は、対象ポートの情報を表示します。

[注意]

COS Queue に滞留しているパケット数は、本装置を再起動するとクリアされます。

［実行例］

```
# show ether queue
[ETHER GROUP-1 PORT-1]
  CoS Queue 0      : 0       ---(1)
  CoS Queue 1      : 0
  CoS Queue 2      : 0
  CoS Queue 3      : 0

   ・                ・
   ・                ・
```

1） CoS Queue 0

ハードウェア COS Queue 0 に滞留しているパケット数が表示されます。

30.1.6 show ether media-info

[機能]

Ethernet 物理ポートのメディア情報の表示

[適用機種]

Si-R G110

[入力形式]

show ether media-info

[オプション]

なし

SFP ポー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]

メディア情報が表示されます。

[実行例]

```
# show ether media-info

Group Port media type Vendor PN
----- ---- ---------- ----------------
 (1)   (2)  (3)         (4)
  1     1  BASE-PX    XXX-0123
```

1) グループ番号
2) ポート番号
3) メディア情報
   実装されているモジュールの種別が表示されます。

   BASE-PX
   BASE-PX モジュールが実装されています。
   Si-R G110 V03.00 では BASE-PX モジュールのみサポートします。

   SFP(SX)
   SFP(1000BASE-SX)モジュールが実装されています。

   SFP(LX)
   SFP(1000BASE-LX)モジュールが実装されています。

   SFP(BX-D)
   SFP(1000BASE-BX-D)モジュールが実装されています。

   SFP(BX-U)
   SFP(1000BASE-BX-U)モジュールが実装されています。

   SFP(ZX)
   SFP(1000BASE-ZX)モジュールが実装されています。

   UNKNOWN
   実装されているモジュールの種別が不明です。

   NONE
   SFP モジュールが実装されていません。

   ERROR
   モジュール故障などで、モジュール内の識別情報が読めない場合はこの表示となります。

OFFLINE

モジュールが実装されているが、offline ether コマンドが発行された場合はこの表示となります。

4) ベンダー型番

実装されているモジュールのメーカ型番が表示されます。

メディア種別が不明な場合でも、モジュール内の情報が表示されます。

30.2 Ethernet のカウンタ・ログ・統計などのクリア

30.2.1 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 G110

[入力形式]

clear ether statistics [group <group> [port <port>]]

[オプション]

なし

指定されたグループまたはポート上の統計情報をクリアします。

group <group>

指定されたグループ上の統計情報をクリアします。
また、該当するグループが無効の場合は統計情報はクリアされません。

範囲	機種
1～2	Si-R G110

port <port>

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。

範囲	機種
1,c1～c4	Si-R G110 (グループ 1)
1～4,c1～c4	Si-R G110 (グループ 2)

複数のポート番号を指定する場合、", "(カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例: "1-8")。
c1～c4 は、CPU とスイッチデバイスをつないだ内部接続ポートを示します。
c1～c4 を指定する場合、group 指定は無効になります。

[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]

Ethernet 物理ポートの統計情報をクリアします。
<port>の省略時は、対象<group>上に搭載される全ポートの統計情報がクリアされます。
<port> および <group>の省略時は、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]

```
# clear ether statistics
#
```

第 31 章 VLAN 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

31.1 VLANのカウンタ・ログ・統計・状態などの表示

31.1.1 show vlan

[機能]

VLAN設定情報の表示

[適用機種]

Si-R G110

[入力形式]

show vlan
show vlan summary
show vlan interface
show vlan vid <vlan_id>

[オプション]

なし
登録されているVLAN構成の全VLAN情報とVLAN数を表示します。

summary
登録されているVLAN構成のVLAN数のみを表示します。

interface
登録されているVLAN構成の全VLAN情報を表示します。

vid <vlan_id>
VLAN IDで指定されたVLANの構成情報を表示します。

・ VLAN ID
1～4094の10進数で指定します。

[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]

VLANの設定情報を表示します。

[注意]

ethergroup vlan mode disable設定時は、ethergroup 1に設定されているVLAN情報だけが対象となります。

[実行例]

```
# show vlan

VID  Interface          Tag           Type     Description
---- ------------------ ------------- -------- --------------------------------
(1)  (2)                (3)           (4)      (5)
100  ether 1 1          dot1q-tagged  port     v100
200  ether 2 1          dot1q-tagged  port     v200
     ether 2 2          untagged
     ether 2 3          untagged

Total Count : 2       ---(6)

#
```

1) VLAN番号

2) インタフェース

ether

ether グループ番号、ポート番号

pseudo-ether

pseudo-ether インタフェース番号

3) Tag 種別

untagged

Untagged VLAN

dot1q-tagged

Tagged VLAN

4) VLAN 種別

port

ポート VLAN

5) VLAN 名

6) VLAN 種別ごとのエントリ数 および VLAN エントリ総数

登録されている VLAN 数のみを表示する場合

```
# show vlan summary

Total Count : 2

#
```

登録されている VLAN 構成のみを表示する場合

```
# show vlan interface

VID  Interface          Tag           Type     Description
---- ------------------ ------------- -------- --------------------------------
(1)  (2)                (3)           (4)      (5)
100  ether 1 1          dot1q-tagged  port     v100
200  ether 2 1          dot1q-tagged  port     v200
     ether 2 2          untagged
     ether 2 3          untagged

#
```

指定 VLAN のみを表示する場合

```
# show vlan vid 100

VID  Interface          Tag           Type     Description
---- ------------------ ------------- -------- --------------------------------
(1)  (2)                (3)           (4)      (5)
100  ether 1 1          dot1q-tagged  port     v100

#
```

第 32 章 データ通信モジュール接続のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

・ USB 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 usb <line>(USB 番号)に指定する挿入されている USB の番号(10 進数)は、機種ごとに以下に示す範囲で指定してください。ただし、USB ポートが 1 つの機種は、USB 番号の指定はできません。

範囲	機種
指定不可	Si-R G110

32.1 データ通信モジュール接続のカウンタ・ログ・統計・状態などの表示

32.1.1 show modemmodule

[機能]

データ通信モジュール接続の状態情報表示

[適用機種]

Si-R G110

[入力形式]

show modemmodule [usb <line>]

[オプション]

なし

すべてのデータ通信モジュール接続の状態情報を表示します。

usb <line>

USB に挿入されているデータ通信モジュール接続の状態情報を表示します。

・ USB 番号

挿入されている USB の番号を指定します。

USB 番号の指定方法の詳細については、本章の冒頭を参照してください。

[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]

データ通信モジュール接続の現在の状態情報を表示します。

[実行例]

```
# show modemmodule
[USB]                                                   ---(1)
description           : L03D                            ---(2)
module name           : NTT DOCOMO, INC. docomo L03D    ---(3)
status                : connected(normal)               ---(4)
call status           : call-out                        ---(5)
remote target         : rmt0.ap0 [remote 0 ap 0]        ---(6)
remote TEL no         : *99***1#                        ---(7)
line speed            : 64000 bps                       ---(8)
communicated time     : 0000.00:01:54                   ---(9)
IPCP                  : opened                          ---(10)
negotiated IP address : local    1.1.1.1                ---(11)
                      : remote   2.2.2.2                ---(11)
DNS server address    : 3.3.3.3 4.4.4.4                 ---(12)
IPV6CP                : closed                          ---(13)
BCP                   : closed                          ---(14)
send/receive traffic  : 592 bps/944 bps                 ---(15)
```

1) データ通信モジュールが挿入されている USB の情報

2) 説明文

使用している回線についての説明文が表示されます。

3) データ通信モジュール名称

データ通信モジュールの名称が表示されます。

データ通信モジュール抜けなどにより名称が不明の場合は、何も表示されません。

4) 回線状態

以下のいずれかが表示されます。

waiting
データ通信モジュールが挿入されていない状態
disable
定義により使用しない状態
enabling
同期確立中
synchronization failed
同期はずれ状態
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
データ通信モジュールの状態が()内に表示されます。
normal
正常
not ready
定義なしのため利用不可
not usable
電波状態不良検出により利用不可
error
エラー検出により利用不可
offline
閉塞中のため利用不可

以下の情報は、通信中(「status」が connected)の場合だけ表示されます。

5) 接続方向
以下のどちらかが表示されます。
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
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) 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
以下のいず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 のプライマリ DNS サーバアドレス/セカンダリ 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

以下のいず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

以下のいず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) 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量が bps 単位で表示されます。

32.1.2 show modemmodule account

[機能]

データ通信モジュール接続のアカウント情報の表示

[適用機種]

Si-R G110

[入力形式]

show modemmodule 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]

データ通信モジュール接続のアカウント情報を表示します。

[実行例]

```
# show modemmodule account
[wan 1]
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
15）接続先定義番号
16）発信接続の合計時間
17）接続の合計パケット数

32.1.3 show modemmodule condition status

[機能]

データ通信モジュールの電波状態監視の状態情報表示

[適用機種]

Si-R G110

[入力形式]

show modemmodule condition status [usb <line>]

[オプション]

なし

すべてのデータ通信モジュールの電波状態監視の状態情報を表示します。

usb <line>

USB に挿入されているデータ通信モジュールの電波状態監視の状態情報を表示します。

・ USB 番号

挿入されている USB の番号を指定します。

USB 番号の指定方法の詳細については、本章の冒頭を参照してください。

[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]

データ通信モジュールの電波状態監視の状態情報を表示します。

[実行例]

電波状態監視を有効化した場合

```
# show modemmodule condition status
[USB]                                                    ---(1)
description           : L05A-1                           ---(2)
module name           : FOMA L05A LG Electronics Inc.    ---(3)
status                : idle                             ---(4)
periodic check level  : 1                                ---(5)
confirm check level   : 2                                ---(6)
current condition     : good                             ---(7)
previous condition    : bad                              ---(8)
updated               : Oct  2 17:31:26 2010             ---(9)
time to next check    : 30s                              ---(10)
last level                                               ---(11)
  check level         : 2                                ---(12)
  updated             : Oct  2 17:31:26 2010             ---(13)
info                                                     ---(14)
  mode                : enable                           ---(15)
  at_command          : "AT*DANTE"                       ---(16)
  result format       : "*DANTE:"                        ---(17)
  result position     :                                  ---(18)
  range               : 0-3                              ---(19)
  out of range        :                                  ---(20)
  level               : 1                                ---(21)
  watch               : 1m                               ---(22)
  connect mode        : level                            ---(23)
```

電波状態監視を有効化した場合(電波監視結果未取得の状態)

```
[USB]                                                   ---(1)
description           : L05A-2                          ---(2)
module name           : FOMA L05A LG Electronics Inc.   ---(3)
status                : check                           ---(4)
periodic check level  : -                               ---(5)
confirm check level   : -                               ---(6)
current condition     : -                               ---(7)
previous condition    : -                               ---(8)
updated               : Oct  2 17:31:26 2010            ---(9)
time to next check    : -                               ---(10)
last level                                              ---(11)
  check level         : -                               ---(12)
  updated             : -                               ---(13)
info                                                    ---(14)
  mode                : enable                          ---(15)
  at_command          : "AT*DANTE"                      ---(16)
  result format       : "*DANTE:"                       ---(17)
  result position     :                                 ---(18)
  range               : 0-3                             ---(18)
  out of range        :                                 ---(20)
  level               : 1                               ---(21)
  watch               : 1m                              ---(22)
  connect mode        : level                           ---(23)

#
```

電波状態監視を無効化した場合

```
# show modemmodule condition status
[USB]                                                   ---(1)
description           : L05A-1                          ---(2)
module name           : FOMA L05A LG Electronics Inc.   ---(3)
status                : disable                         ---(4)

#
```

電波状態監視を有効化した場合(commit 実施後、1 度だけ電波状態監視を実行した状態)

```
# show modemmodule condition status
[USB]                                                   ---(1)
description           : L05A-1                          ---(2)
module name           : FOMA L05A LG Electronics Inc.   ---(3)
status                : idle                            ---(4)
periodic check level  : 1                               ---(5)
confirm check level   : 2                               ---(6)
current condition     : good                            ---(7)
previous condition    : -                               ---(8)
updated               : Oct  2 17:31:26 2010            ---(9)
time to next check    : 30s                             ---(10)
last level                                              ---(11)
  check level         : 2                               ---(12)
  updated             : Oct  2 17:31:26 2010            ---(13)
info                                                    ---(14)
  mode                : enable                          ---(15)
  at_command          : "AT*DANTE"                      ---(16)
  result format       : "*DANTE:"                       ---(17)
  result position     :                                 ---(18)
  range               : 0-3                             ---(19)
  out of range        :                                 ---(20)
  level               : 1                               ---(21)
  watch               : 1m                              ---(22)
  connect mode        : level                           ---(23)

#
```

定期監視と再監視で電波状態の判定結果に差があった場合

```
# show modemmodule condition status
[USB]                                                      ---(1)
description           : L05A-1                             ---(2)
module name           : FOMA L05A LG Electronics Inc.      ---(3)
status                : idle                               ---(4)
periodic check level  : 1                                  ---(5)
confirm check level   : 0                                  ---(6)
current condition     : good                               ---(7)
previous condition    : bad                                ---(8)
updated               : Oct  2 17:31:26 2010 (confirm failed) ---(9)
time to next check    : 30s                                ---(10)
last level                                                 ---(11)
  check level         : 0                                  ---(12)
  updated             : Oct  2 17:31:26 2010               ---(13)
info                                                       ---(14)
  mode                : enable                             ---(15)
  at_command          : "AT*DANTE"                         ---(16)
  result format       : "*DANTE:"                          ---(17)
  result position     :                                    ---(18)
  range               : 0-3                                ---(19)
  out of range        :                                    ---(20)
  level               : 1                                  ---(21)
  watch               : 1m                                 ---(22)
  connect mode        : level                              ---(23)

#
```

1) データ通信モジュールが挿入されているUSBの情報
2) 説明文
   使用している回線についての説明文が表示されます。
3) データ通信モジュール名称
   データ通信モジュールのモジュール名称が表示されます。
4) 監視状態
   電波状態の監視状態が表示されます。監視無効の場合は、以下の項目以降が表示されません。

   disable
   監視無効

   init
   監視開始待ち

   idle
   監視実施待ち

   check
   定期監視実施中

   confirm
   再監視実施中
5) 定期監視電波レベル
   監視間隔ごとにデータ通信モジュールから取得した電波状態が表示されます。
   未取得の場合は"-"が表示されます。
6) 再監視電波レベル
   定期監視直後にデータ通信モジュールから取得した電波状態が表示されます。
   未取得の場合は"-"が表示されます。
7) 現在の電波状態監視結果
   電波状態監視の結果が表示されます。
   connect modeがforceの場合は、本項目の表示内容にかかわらず常に回線接続可能と判断されます。

   good
   電波状態良好(回線接続可能)

   bad
   電波状態不良(回線接続不可)

–

監視結果が未決(回線接続不可)

8) 前回の電波状態監視結果

前回の電波状態監視の結果が表示されます。

connect mode が force の場合は、本項目の表示内容にかかわらず常に回線接続可能と判断されます。

good

電波状態良好(回線接続可能)

bad

電波状態不良(回線接続不可)

–

監視結果が未決(回線接続不可)

9) 最終更新時刻

定期監視電波レベル、再監視電波レベル、現在の電波状態監視結果、前回の電波状態監視結果のいずれかが更新された時刻が表示されます。

定期監視と再監視で電波状態の判定結果に差があった場合、(confirm failed)が表示され、電波状態監視結果は更新されません。

10) 次回の定期監視実施までの時間

次回の定期監視実施までの時間が表示されます。

監視状態が監視開始待ちの場合は、"-"が表示されます。

11) 最新の電波レベルに関する情報

12) 最新の電波レベル

データ通信モジュールから取得した最新の電波状態が表示されます。

未取得の場合は"-"が表示されます。

13) 更新時刻

最新の電波レベルが更新された時刻が表示されます。

最新の電波レベルが未取得の場合は"-"が表示されます。

14) 電波状態監視の動作パラメタ

電波状態監視の動作パラメタの設定内容が表示されます。

15) 電波状態監視の動作モード

16) 電波状態監視に使用する AT コマンド

電波状態監視に使用する AT コマンドがダブルクォーテーション(")で囲まれて表示されます。

17) 電波状態監視の応答フォーマット

電波状態監視に使用する AT コマンドがダブルクォーテーション(")で囲まれて表示されます。

18) 電波状態監視の取得位置

19) 電波状態監視の電波レベル有効範囲

20) 電波状態監視の圏外判定条件

21) 電波状態監視の電波状態判定レベル

22) 電波状態監視の監視間隔

23) 電波状態監視の接続指示

32.1.4 show modemmodule condition history

[機能]

データ通信モジュールの電波状態監視の履歴情報表示

[適用機種]

Si-R G110

[入力形式]

show modemmodule condition history [usb <line>]

[オプション]

なし

すべてのデータ通信モジュールの電波状態監視の履歴情報を表示します。

usb <line>

USB に挿入されているデータ通信モジュールの電波状態監視の履歴情報を表示します。

・ USB 番号

挿入されている USB の番号を指定します。

USB 番号の指定方法の詳細については、本章の冒頭を参照してください。

[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]

データ通信モジュールの電波状態監視の履歴情報を表示します。

以下に、履歴情報の最大表示件数を示します。

履歴情報の最大表示件数	機種
2000 件(回線ごと)	Si-R G110

[実行例]

電波状態監視を有効化した場合

(wan modemmodule condition history dupcut を disable に設定)

```
# show modemmodule condition history
[USB]                                                   ---(1)
description           : L05A-1                          ---(2)
module name           : FOMA L05A LG Electronics Inc.   ---(3)
status                : idle                            ---(4)
[0001] Oct 25 06:28:37 2010: condition initialized.
-(5)-- ---------(6)--------  ---------(7)----------
[0002] Oct 25 06:28:40 2010: received=p2/c2 level=3 condition=bad.
                             -------------------(7)----------------------
[0003] Oct 25 06:29:40 2010: received=p3/c3 level=3 condition=good(changed).
[0004] Oct 25 06:30:40 2010: received=p3/c3 level=3 condition=good.
[0005] Oct 25 06:31:00 2010: condition initialized.
[0006] Oct 25 06:31:04 2010: received=p3/c3 level=3 condition=good.
[0007] Oct 25 06:32:04 2010: received=p1/c3(confirm failed).
[0008] Oct 25 06:33:04 2010: received=p1/c0 level=3 condition=bad(changed).
[0009] Oct 25 06:34:04 2010: received=p1/c0 level=3 condition=bad.
[0010] Oct 25 06:35:04 2010: received=p1/c0 level=3 condition=bad.
[0011] Oct 25 06:36:04 2010: received=p1/c0 level=3 condition=bad.
[0012] Oct 25 06:37:04 2010: condition initialized.

#
```

電波状態監視を有効化した場合

(wan modemmodule condition history dupcut を enable に設定)

```
# show modemmodule condition history
[USB]                                                   ---(1)
description           : L05A-1                          ---(2)
module name           : FOMA L05A LG Electronics Inc.   ---(3)
status                : idle                            ---(4)
[0001] Oct 25 06:28:37 2010: condition initialized.
-(5)-- ---------(6)--------  ---------(7)----------
[0002] Oct 25 06:28:40 2010: received=p2/c2 level=3 condition=bad.
                             -------------------(7)----------------------
[0003] Oct 25 06:29:40 2010: received=p3/c3 level=3 condition=good(changed).
[0004] Oct 25 06:30:40 2010: received=p3/c3 level=3 condition=good.
[0005] Oct 25 06:31:00 2010: condition initialized.
[0006] Oct 25 06:31:04 2010: received=p3/c3 level=3 condition=good.
[0007] Oct 25 06:32:04 2010: received=p1/c3(confirm failed).
[0008] Oct 25 06:33:04 2010: received=p1/c0 level=3 condition=bad(changed).
[0009] Oct 25 06:34:04 2010: received=p1/c0 level=3 condition=bad.
[0010] Oct 25 06:37:04 2010: same message repeated 2 times.
[0011] Oct 25 06:37:04 2010: condition initialized.

#
```

電波状態監視を無効化した場合

```
# show modemmodule condition history
[USB]                                                   ---(1)
description           : L05A-1                          ---(2)
module name           : FOMA L05A LG Electronics Inc.   ---(3)
status                : disable                         ---(4)

#
```

1) データ通信モジュールが挿入されている USB の情報
2) 説明文
   使用している回線についての説明文が表示されます。
3) データ通信モジュール名称
   データ通信モジュールのモジュール名称が表示されます。
4) 監視状態
   電波状態の監視状態が表示されます。監視無効の場合は、以下の項目以降が表示されません。

   disable
   監視無効

   init
   監視開始待ち

   idle
   監視実施待ち

   check
   定期監視実施中

   confirm
   再監視実施中
5) 連番
6) 発生時刻
7) 発生内容
   電波状態の監視内容が表示されます。

   condition initialized
   監視状態が監視開始待ちに変化した場合に表示されます。
   本メッセージは、wan modemmodule condition history dupcut による重複出力の抑止対象外であり、常に表示されます。

   received
   定期監視電波レベルと再監視電波レベルが p<value>/c<value>の形式で表示されます。

定期監視と再監視で電波状態の判定結果に差があった場合、(confirm failed)が表示され、電波状態監視結果は更新されません。

level

接続可能レベルが表示されます。

condition

電波状態監視結果が"good"または"bad"で表示されます。

電波状態監視結果が前回と異なる場合は、(changed)が表示されます。

same message repeated

wan modemmodule condition history dupcut により重複出力を抑止している場合、
重複した監視内容、回数が表示されます。重複した回数は<count> times の形式で表示されます。

32.1.5 show modemmodule condition statistics

[機能]

データ通信モジュールの電波状態監視の統計情報表示

[適用機種]

Si-R G110

[入力形式]

show modemmodule condition statistics [usb <line>]

[オプション]

なし

すべてのデータ通信モジュールの電波状態監視の統計情報を表示します。

usb <line>

USB に挿入されているデータ通信モジュールの電波状態監視の統計情報を表示します。

・ USB 番号

挿入されている USB の番号を指定します。

USB 番号の指定方法の詳細については、本章の冒頭を参照してください。

[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]

データ通信モジュールの電波状態監視の統計情報を表示します。

[実行例]

電波状態監視を有効化した場合

```
# show modemmodule condition statistics

[USB]                                                   ---(1)
description           : L05A-1                          ---(2)
module name           : FOMA L05A LG Electronics Inc.   ---(3)
status                : idle                            ---(4)
periodic check                                          ---(5)
  exec                : 240                             ---(6)
  reply               : 240                             ---(7)
  failed              : 0                               ---(8)
  error               : 0                               ---(9)
confirm check                                           ---(10)
  exec                : 240                             ---(6)
  reply               : 240                             ---(7)
  failed              : 0                               ---(8)
  error               : 0                               ---(9)
condition                                               ---(11)
  good                : 4                               ---(12)
  bad                 : 3                               ---(13)
  confirm failed      : 1                               ---(14)
  change to good      : 0                               ---(15)
  change to bad       : 1                               ---(16)
  initialized         : 1                               ---(17)
on other control      : 0                               ---(18)

#
```

電波状態監視を無効化した場合

```
# show modemmodule condition statistics
[USB]                                                   ---(1)
description           : L05A-1                          ---(2)
module name           : FOMA L05A LG Electronics Inc.   ---(3)
status                : disable                         ---(4)

#
```

1) データ通信モジュールが挿入されているUSBの情報
2) 説明文
   使用している回線についての説明文が表示されます。
3) データ通信モジュール名称
   データ通信モジュールのモジュール名称が表示されます。
4) 監視状態
   電波状態の監視状態が表示されます。監視無効の場合は、以下の項目以降が表示されません。
   disable
   監視無効
   init
   監視開始待ち
   idle
   監視実施待ち
   check
   定期監視実施中
   confirm
   再監視実施中
5) 定期監視に関する統計
6) 監視を実施した回数
7) 結果を取得した回数
8) 制御タイムアウト、制御受付不可により監視結果が取得できなかった回数
9) 制御エラー発生により監視結果が取得できなかった回数
10) 再監視に関する統計
11) 電波状態監視結果に関する統計
12) 電波状態監視結果が電波状態良好であった回数
13) 電波状態監視結果が電波状態不良であった回数
14) 定期監視と再監視で電波状態監視結果に差があったため、電波状態監視結果を更新しなかった回数
15) 電波状態監視結果が、電波状態不良から電波状態良好に変わった回数
16) 電波状態監視結果が、電波状態良好から電波状態不良に変わった回数
17) 監視状態が監視開始待ちに変化し、電波状態の監視情報が初期化された回数
18) ほかの機能と競合が発生し、監視が実施できなかった回数

32.1.6 show modemmodule statistics

[機能]

データ通信モジュールの統計情報表示

[適用機種]

Si-R G110

[入力形式]

show modemmodule statistics [usb <line>]

[オプション]

なし

すべてのデータ通信モジュールの統計情報を表示します。

usb <line>

USB に挿入されているデータ通信モジュールの統計情報を表示します。

・ USB 番号

挿入されている USB の番号を指定します。

USB 番号の指定方法の詳細については、本章の冒頭を参照してください。

[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]

データ通信モジュール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、データ通信モジュールの抜き取りや挿入でもクリアされます。

[実行例]

```
# show modemmodule statistics

[MODEM USB STATUS]
Interface status     : OPEN                          ---(1)
 since               : Jan 11 13:21:15 2006          ---(2)

[MODEM USB 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 USB 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が表示されます。

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が表示されます。

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

32.2 データ通信モジュール接続のカウンタ・ログ・統計などのクリア

32.2.1 clear modemmodule account

[機能]

データ通信モジュール接続のアカウント情報のクリア

[適用機種]

Si-R G110

[入力形式]

clear modemmodule 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]

データ通信モジュール接続のアカウント情報をクリアします。

[実行例]

```
# clear modemmodule account
#
```

32.2.2 clear modemmodule condition history

[機能]

データ通信モジュールの電波状態監視の履歴情報クリア

[適用機種]

Si-R G110

[入力形式]

clear modemmodule condition history

[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]

データ通信モジュールの電波状態監視の履歴情報をクリアします。

[実行例]

```
# clear modemmodule condition history
#
```

32.2.3 clear modemmodule condition statistics

[機能]

データ通信モジュールの電波状態監視の統計情報クリア

[適用機種]

Si-R G110

[入力形式]

clear modemmodule condition 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]

データ通信モジュールの電波状態監視の統計情報をクリアします。

[実行例]

```
# clear modemmodule condition statistics
#
```

32.2.4 clear modemmodule statistics

[機能]

データ通信モジュールの統計情報クリア

[適用機種]

Si-R G110

[入力形式]

clear modemmodule 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]

データ通信モジュールの統計情報をクリアします。

[実行例]

```
# clear modemmodule statistics
#
```

第 33 章 USB 接続のカウンタ・ログ・統計・状態などの表示コマンド

・ USB 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 usb <line>(USB 番号)に指定する挿入されている USB の番号(10 進数)は、機種ごとに以下に示す範囲で指定してください。ただし、USB ポートが 1 つの機種は、USB 番号の指定はできません。

範囲	機種
指定不可	Si-R G110

33.1 USB 接続のカウンタ・ログ・統計・状態などの表示

33.1.1 show usb hcd status

[機能]

USB ポートの状態表示

[適用機種]

Si-R G110

[入力形式]

show usb hcd status [usb <line>]

[オプション]

なし

全 USB ポートの状態を表示します。

usb <line>

USB の状態を表示します。

・ USB ポート番号

挿入されている USB の番号を指定します。

USB 番号の指定方法の詳細については、本章の冒頭を参照してください。

[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]

USB ポートの状態を表示します。

[実行例]

```
# show usb hcd status usb

[USB HCD STATUS USB]
status              : enable                          ---(1)
```

1) USB ポート状態

USB ポートの状態が表示されます。

disable

使用不可能状態、または安全な取り外し可能状態

enable

使用可能状態

33.1.2 show usb storage status

[機能]

USB マスストレージ制御状態の表示

[適用機種]

Si-R G110

[入力形式]

show usb storage status [usb <line>]

[オプション]

なし

全 USB ポートの USB マスストレージ制御状態を表示します。

usb <line>

USB の情報を表示します。

・ USB ポート番号

挿入されている USB の番号を指定します。

USB 番号の指定方法の詳細については、本章の冒頭を参照してください。

[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/CE クラス)

構成定義モード(管理者クラス/CE クラス)

[説明]

USB マスストレージ制御の現在の状態を表示します。

［実行例］

```
# show usb storage status

[Thread]
Status                  : Active              ---(1)

[USB]
Status                  : Idle                ---(2)
Speed                   : Full                ---(3)
Geometry probing        : Success             ---(4)
 Test unit ready        : Success             ---(5)
 Inquiry                : Success
 Mode sense             : Success
 Read capacity          : Success
 Read format capacities : ----
Hold data               : Not exist           ---(6)
Error status            : Get device specs [5/5] (Read format capacities) ---(7)
 Error reason           : Transfer URB failure ---(8)
 Error event            : 0x3200000d          ---(9)
 Request sense code     : (02, 10, 00)        ---(10)
[Storage specs]
Vendor                  : FUJITSU             ---(11)
Product                 : USB   PortableDrive ---(12)
Product Rev.            : 3.96                ---(13)
Total sectors           : 500400              ---(14)
Cylinders               : 695                 ---(15)
Heads                   : 15                  ---(16)
Sectors per track       : 48                  ---(17)
[USB specs]
Speed                   : Full                ---(18)
Max LUN                 : 3                   ---(19)
[USB configuration]
Device address          : 1                   ---(20)
Interface               : 0                   ---(21)
Sub class               : 6                   ---(22)
LUN                     : 0                   ---(23)
BulkInEP                : 0x82                ---(24)
BulkOutEP               : 0x02                ---(25)
```

1) USB マスストレージ制御スレッド状態

以下のいずれかが表示されます。

Uninit

未初期化

Waiting for USBD active

起動中(USBD 起動待ち)

Waiting for entry class completed

起動中(エントリクラス処理完了待ち)

Active

活性

以下の情報は、USB デバイスの接続を認識した場合だけ表示されます。

2) USB デバイス制御状態

以下のいずれかが表示されます。

Uninit

未初期化

Initializing [1/2] (Set configuration)

初期化中(Set configuration)

Initializing [2/2] (Get max lun)

初期化中(Get max lun)

Get device specs [1/5] (Test unit ready)

デバイス諸元獲得中(Test unit ready)

Get device specs [2/5] (Inquiry)
デバイス諸元獲得中(Inquiry)
Get device specs [3/5] (Mode sense)
デバイス諸元獲得中(Mode sense)
Get device specs [4/5] (Read capacity)
デバイス諸元獲得中(Read capacity)
Get device specs [5/5] (Read format capacities)
デバイス諸元獲得中(Read format capacities)
Idle
アイドル(転送要求待ち)
Transferring
転送中
Waiting for unplugging
USB デバイス抜去待ち(異常検出)
Unplugging
抜去処理中

3) 速度
以下のいずれかが表示されます。
注意: 表示は USB デバイスとの通信速度ですが、転送スループットを表すものではありません。
High
ハイスピードモード (480Mbps)
Full
フルスピードモード (12Mbps)
Low
ロースピードモード (1.5Mbps)

4) ジオメトリ検出状況
マスストレージデバイスの全セクタ数、シリンダ数、ヘッド数、1 トラックあたりのセクタ数をジオメトリと呼びます。
以下のいずれかが表示されます。
Success
成功
Success(partly guessed)
成功(情報の一部は推測されました)
Failed
失敗
Not yet
検出はまだ行われていません

5) ジオメトリ検出状況 詳細表示
ジオメトリ検出は、SCSI コマンド(TEST_UNIT_READY, INQUIRY, MODE SENSE(6),READ CAPACITY, READ FORMAT CAPACITIES)によって、行われます。
各コマンドの実施状態が、以下のいずれかで表示されます。
Success
成功
Failed (no data)
失敗(データなし)
Failed (retry out)
失敗(リトライアウト)
Failed
失敗(その他)

実施されていない

6) 保持しているデータの有無

ファイルシステムから受けた転送要求の有無が表示されます。
以下のどちらかが表示されます。

Exists
存在する

Not exists
存在しない

以下、7)，8)，9)，10)の情報は、エラーが発生し転送動作を継続できなくなった場合だけ表示されます。

7) エラー発生時の状態
エラーが発生したときのUSBデバイス制御状態(2)が表示されます。

8) エラー原因
転送動作を継続できなくなった原因が表示されます。

9) エラーイベント
内部情報が表示されます。

10) リクエストセンスコード
USBデバイス側でエラーを検出した際に設定されるUSBデバイス側のエラー情報が表示されます。

11) ベンダー情報
USBデバイスのベンダー情報が表示されます。

12) プロダクト情報
USBデバイスのプロダクト情報が表示されます。

13) プロダクトリビジョン情報
USBデバイスのプロダクトリビジョン情報が表示されます。

14) 全セクタ数
USBデバイスの保持する全セクタ数が表示されます。

15) シリンダ数
USBデバイスのシリンダ数が表示されます。

16) ヘッド数
USBデバイスのヘッド数が表示されます。

17) トラックあたりのセクタ数
USBデバイスの1トラック(1ヘッド、1シリンダ)あたりのセクタ数が表示されます。

18) 速度
USBプロトコル速度が表示されます。(3)と同一です。

19) 最大LUN
USBデバイスの持つLUNの最大値が表示されます。本装置では、LUN=0以外のデバイスをサポートしません。

20) デバイスアドレス
USBバス上でデバイスを一意に指定するために、USBDによって割り当てられたデバイス番号が表示されます。

21) インタフェース
USBマスストレージ制御スレッドが選択したインタフェースの番号が表示されます。

22) サブクラス
USBデバイスのサブクラス情報が表示されます。クラス情報は、0(=マスストレージクラス)です。

23) LUN
USBマスストレージ制御スレッドが選択したLUN番号が表示されます。

24) BulkInEP
USBマスストレージ制御スレッドが選択したバルクインエンドポイント番号が表示されます。

25) BulkOutEP
USBマスストレージ制御スレッドが選択したバルクアウトエンドポイント番号が表示されます。

第 34 章 pseudo ether 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

34.1 pseudo ether インタフェースのカウンタ・ログ・統計・状態などの表示

34.1.1 show pseudo-ether

[機能]

pseudo ether インタフェース状態の表示

[適用機種]

Si-R G110

[入力形式]

show pseudo-ether

[オプション]

なし

pseudo ether 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]

pseudo ether の情報を表示します。

[実行例]

```
# show pseudo-ether
[PSEUDO-ETHER1]                                          ---(1)
description           : LTE                              ---(2)
module name           : HUAWEI HWD12                     ---(3)
status                : up                               ---(4)
updated               : Mar 2 16:01:50 2013              ---(5)
communicated time     : 0000.00:01:18                    ---(6)

#
```

1) pseudo ether インタフェース名
2) pseudo ether の説明文
   pseudo-ether description で設定された内容が表示されます。
3) pseudo ether モジュールの名称
   pseudo ether モジュールの名称が表示されます。
4) pseudo ether インタフェースの状態が表示されます。
   waiting
   pseudo ether モジュール挿入待ちであることを示します。
   disable
   定義により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。
   up
   リンクアップ状態であることを示します。
5) 4)の状態になった時刻が表されます。
6) 接続時間
   リンクアップ時は接続時間が以下の形式で表示されます。

dddd.hh:mm:ss(日.時:分:秒)

34.1.2 show pseudo-ether statistics

[機能]

pseudo ether インタフェースの統計情報の表示

[適用機種]

Si-R G110

[入力形式]

show pseudo-ether statistics

[オプション]

なし

pseudo ether 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]

pseudo ether インタフェース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 pseudo ether デバイスの挿抜でクリアされます。
統計情報は clear statistics コマンドでクリアされません。

[実行例]

```
# show pseudo-ether statistics
[PSEUDO-ETHER1]                                          ---(1)
description              : LTE                           ---(2)
module name              : HUAWEI HWD12                  ---(3)
[Input Statistics]                                       ---(4)
  OK packets             : 0                             ---(5)
  CRC error packets      : 0                             ---(6)
  Protocol error packets : 0                             ---(7)
  Buffer error packets   : 0                             ---(8)
[Output Statistics]                                      ---(9)
  OK packets             : 0                             ---(10)
  Error packets          : 0                             ---(11)
```

1) pseudo ether インタフェース名
2) pseudo ether の説明文
   pseudo-ether description で設定された内容が表示されます。
3) pseudo ether モジュールの名称
   pseudo ether モジュールの名称が表示されます。
4) 受信側統計情報
5) 受信 OK パケット数
   本情報が取得できない場合は、'-'(ハイフン)が表示されます。
6) 受信 CRC エラーパケット数
   本情報が取得できない場合は、'-'(ハイフン)が表示されます。
7) 受信プロトコルエラーパケット数
   本情報が取得できない場合は、'-'(ハイフン)が表示されます。
8) 受信バッファ不足でのエラーパケット数

本情報が取得できない場合は、'-'(ハイフン)が表示されます。

9) 送信側統計情報

10) 送信 OK パケット数

本情報が取得できない場合は、'-'(ハイフン)が表示されます。

11) 送信エラーパケット数

本情報が取得できない場合は、'-'(ハイフン)が表示されます。

第 35 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

35.1 インタフェースのカウンタ・ログ・統計・状態などの表示

35.1.1 show interface

[機能]

インタフェース情報の表示

[適用機種]

Si-R G110

[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］

```
# show interface
lan0               MTU 1500    <UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST>
-(1)-                  -(2)-   ------------------(3)-------------------
    Description: private_0                                              ┐
    Type: port vlan                                                     │
    VLAN ID is 20                                                       │
    MAC address: 00:00:0e:f1:41:dc                                      │
    Status: up since Mar  2 16:01:53 2011                               │
    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>
    Description: private_1                                              ┐
    Type: port vlan                                                     │
    VLAN ID is 30                                                       │
    MAC address: 00:00:0e:f1:41:dc                                      │
    Status: up since Mar  2 16:01:50 2011                               │(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>
    Description: Internet_1                                             ┐
    Type: pseudo P2P interface                                          │
    Status: up since Mar  2 16:01:53 2011                               │
    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>
    Description: Internet_2                                             ┐
    Type: template P2P interface                                        │
    Status: up since Mar  2 19:23:45 2011                               │(4)
    IP address:                                                         │
      192.168.10.1 -> 192.168.20.1                                      ┘
lo0                MTU 16384   <UP,LOOPBACK,RUNNING,MULTICAST>
    Type: loopback                                                      ┐
    Status: up since Mar  2 16:01:50 2011                               │
    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) Description

lan description または remote description で定義された内容が表示されます。

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。

port vlan

ポート 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
ポート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。
ethergroup vlan mode disable設定時にlan vlan 0が設定されている場合、UNTAG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

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。
anycast
エニーキャストアドレスであることを示します。
autoconfig
自動生成されたアドレスであることを示します。

35.1.2 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 G110

[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]

```
# show interface brief
Interface        Status     Type
-------------   -------    -------------------
(1)             (2)        (3)
lan0            up         port vlan
lan1            up         port 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

3) Type

インタフェースタイプが表示されます。

port vlan

ポート 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

35.1.3 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 G110

[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]

```
# show interface summary
There are 4 interfaces (up status 4 interfaces)
    Loopback interface      :    1 (up status    1 interfaces)  ---(1)
    Port VLAN interface     :    2 (up status    2 interfaces)  ---(2)
    Pseudo P2P interface    :    1 (up status    1 interfaces)  ---(3)
    Template P2P interface  :    1 (up status    1 interfaces)  ---(4)
#
```

1) ループバックインタフェース
2) ポート VLAN
3) 仮想 P2P インタフェース
4) 仮想 P2P インタフェース(template で利用されるもの)

35.1.4 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 G110

[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]

```
# show interface detail
lan0               MTU 1500    <UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST>
-(1)-                  -(2)-   ------------------(3)-------------------
    Description:
    Type: port vlan                                                      ┐
    VLAN ID is 20                                                        │
    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>
    Description:
    Type: port vlan                                                      ┐
    VLAN ID is 30                                                        │
    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>
    Description:
    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>
    Description:
    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 ┘
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) Description

インタフェースの説明文が表示されます。

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。

port vlan

ポート 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

ポート 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

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。
anycast :
エニーキャストアドレス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。

```
#show interface detail interface pseudoeth1

pseudoeth1     MTU 1500    <UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST>
---(1)---     ----(2)----  ----(3)---------------------------------

    Description: LTE
    ----(4)----------
    Type: Wireless Man/Wan
    ----(5)---------------
    Status: up since Dec  5 15:58:35 2011
    ----(6)------------------------------
    statistics:
    ----(7)----
      in packets:                 1861578 out packets:                 3422127
      ----(8)---------------------------- ---(9)------------------------------
         bytes:                  96964338     bytes:                401012537
         -(10)---------------------------     -(10)---------------------------

         unicasts:               1861573     unicasts:               3422122
         -(11)---------------------------     -(11)---------------------------
         multicasts/broadcasts:        5     multicasts/broadcasts:        5
         -(12)---------------------------     -(12)---------------------------

         discards:                     0     discards:                     0
         -(13)---------------------------     -(13)---------------------------
                                              drop:                         0
                                              -(14)---------------------------
```

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) pseudo ether の説明文
5) インタフェースタイプ
6) インタフェース状態
7) 統計情報
8) 受信パケット数
9) 送信パケット数
10) バイト数
11) unicast パケット数
12) multicast/broadcast パケット数
13) 破棄パケット数
14) drop パケット数

35.1.5 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 G110

[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］

```
# 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

3) Type

インタフェースタイプが表示されます。

port vlan

ポート 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

35.1.6 show access-point

[機能]

接続先情報の表示

[適用機種]

Si-R G110

[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
0～99	Si-R G110

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
0～99	Si-R G110

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。
論理リンクの場合、バンドル回線の状態は表示されません。

［実行例］

```
# show access-point
remote 0 ap 0         : Internet.isp                          ---(1)
  status              : connected                             ---(2)
    detail            : connected                             ---(3)
    since             : Mar  3 14:42:33 2011                  ---(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                : MODEM                                 ---(9)
    IPCP              : opened                                ---(10)
      local address   : 27.231.100.62                         ---(11)
      DNS server      : 220.159.212.200 220.159.212.201       ---(12)
    IPV6CP            : opened                                ---(13)
    BCP               : opened                                ---(14)

remote 2 ap 0         : kawasaki.vpn
  status              : connected
    since             : Mar  3 14:23:04 2011
  speed               : not available
    send traffic      : not available
    receive traffic   : not available
  type                : IPsec/IKE
    IKE Version       : 1                                     ---(15)
    exchange type     : aggressive                            ---(16)
    IKE SA            : established                           ---(17)
    IPsec SA          : established                           ---(18)
    auto ignore       : enable                                ---(19)
                        192.168.2.0/24                        ---(20)
                        192.168.3.0/24

remote 3 ap 0         : 192.168.1.1
  status              : connected
    since             : Mar  3 14:23:04 2011
  speed               : not available
    send traffic      : not available
    receive traffic   : not available
  type                : overlap
    nexthop           : 192.168.1.1(static)                   ---(21)

remote 4 ap 0         : 192.168.1.1
  status              : connected
    since             : Mar  3 14:23:04 2011
  speed               : not available
    send traffic      : not available
    receive traffic   : not available
  type                : overlap
    nexthop           : 192.168.1.1(dhcp)                     ---(21)

remote 5 ap 0         : 192.168.1.1
  status              : connected
    since             : Mar  3 14:23:04 2011
  speed               : not available
    send traffic      : not available
    receive traffic   : not available
  type                : overlap
    nexthop           : not available                         ---(21)
```

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

現在の接続状態が表示されます。以下のいず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 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

接続中に同期はずれを検出し、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

4) 状態遷移時刻

「status」が現在の状態に変化した時刻が表示されます。

5) 通信時間

dddd.hh:mm:ss の形式で通信時間が表示されます。dddd=日数、hh=時間、mm=分、ss=秒を示します。「Type」が PPPoE または MODEM の場合にだけ表示されます。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 の場合にだけ表示されます。

6) 伝送速度

現在の伝送速度が表示されます。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が表示されます。

8) 受信レート

最新のデータ受信レートが表示されます。

9) 通信手段

相手システムとの通信手段が表示されます。以下のいずれかが表示されます。

－ IPv4

IPv4 tunnel

－ IPv6

IPv6 tunnel

－ 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
－ MODEM
データ通信モジュール

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 通信の状態が表示されます。以下のいず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プライマリ DNS サーバアドレス/セカンダリ DNS サーバアドレスが表示されます。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 通信の状態が表示されます。以下のいず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が表示されます。以下のいず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。

15) IKE バージョン

IKE のバージョンが表示されます。以下のどちらかが表示されます。

－ 1
IKEv1 を利用
－ 2
IKEv2 を利用

16) 鍵交換モード

IKE の鍵交換モードが表示されます。以下のどちらかが表示されます。

IKEv2 を利用する場合は表示されません。

－ main
Main モードを利用

－ aggressive
Aggressive モードを利用

17) IKE SA 状態
IKE SA の状態が表示されます。以下のいず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 の状態が表示されます。以下のいず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

19) 動的 VPN 接続 INVITE 自動 ignore 状態
動的 VPN 接続 INVITE 自動 ignore 状態が表示されます。以下のどちらかが表示されます。
IKEv2 を利用する場合は表示されません。
－ enable
INVITE 自動 ignore 使用
－ disable
INVITE 自動 ignore 未使用

20) 接続先情報 動的 VPN 接続 INVITE 自動 ignore 対象アドレス
動的 VPN 接続 INVITE 自動 ignore により対象となるアドレス/ネットワークが表示されます。
IKEv2 を利用する場合は表示されません。

以下の情報は overlap を利用して通信する場合に限り表示されます。

21) nexthop
以下のいずれかが表示されます。
－ 192.168.1.1(static)
nexthop <address>で指定された IP アドレスが表示されます。
－ 192.168.1.1(dhcp)
nexthop dhcp で、DHCP クライアントで取得した IP アドレスが表示されます。
－ not available
overlap to の<kind>で lan を指定しない場合に表示されます。
overlap to の<kind>で lan を指定した場合、転送先 IP ルータ未設定のときに表示されます。
overlap to の<kind>で lan を指定した場合、かつ remote ap overlap nexthop で dhcp を設定したとき、DHCP クライアントで IP アドレスを取得できない場合に表示されます。

35.1.7 show template

[機能]

テンプレート着信の通信状態

[適用機種]

Si-R G110

[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]

```
# show template
[template 0]
description           : template_0                          ---(1)
status                : active                              ---(2)
Number of interfaces  :  Active: 1, Free: 7                 ---(3)

rmt40(user id:sayama-1@domainname)                          ---(4)
  status              : connected                           ---(5)
    since             : Mar  3 14:15:29 2011                ---(6)
  speed               : not available                       ---(7)
    send traffic      : not available                       ---(8)
    receive traffic   : not available                       ---(9)
  type                : IPsec/IKE                           ---(10)
    IKE Version       : 1                                   ---(11)
    exchange type     : aggressive                          ---(12)
    IKE SA            : established                         ---(13)
    IPsec SA          : established                         ---(14)
```

1) template description で定義された内容が表示されます。
2) 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
3) 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。
4) 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。)
5) 接続状態
   現在の接続状態が表示されます。以下が表示されます。
   - 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が表示されます。

7) 伝送速度

現在の伝送速度が表示されます。MP の場合は合計速度が表示されます。

8) 送信レート

最新のデータ送信レートが表示されます。

9) 受信レート

最新のデータ受信レートが表示されます。

10) 通信手段

相手システムとの通信手段が表示されます。以下が表示されます。

－ IPsec/IKE

IPsec(IKE による鍵交換を利用)

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。

11) IKE バージョン

IKE のバージョンが表示されます。以下のどちらかが表示されます。

－ 1

IKEv1 を利用

－ 2

IKEv2 を利用

12) 鍵交換モード

IKE の鍵交換モードが表示されます。以下のどちらかが表示されます。
IKEv2 を利用する場合は表示されません。

－ main

Main モードを利用

－ aggressive

Aggressive モードを利用

13) IKE SA 状態

IKE SA の状態が表示されます。以下のいず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

14) IPsec SA 状態

IPsec SA の状態が表示されます。以下のいず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

35.1.8 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 G110

[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]

```
# 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

35.2 インタフェースのカウンタ・ログ・統計などのクリア

35.2.1 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 G110

[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
#
```

35.2.2 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 G110

[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 36 章 ARP エントリの表示、削除コマンド

36.1 ARP エントリの表示

36.1.1 show arp

[機能]

ARP エントリの表示

[適用機種]

Si-R G110

[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]

```
# 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 アドレスが表示されます。

2) MAC Address
ARP エントリの MAC アドレスが表示されます。
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。

36.2 ARP エントリの削除

36.2.1 clear arp

[機能]

ARP エントリの削除

[適用機種]

Si-R G110

[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 37 章 Neighbor Cache テーブルエントリの表示、削除コマンド

37.1 Neighbor Cache テーブルエントリの表示

37.1.1 show ndp

[機能]

Neighbor Cache テーブルエントリの表示

[適用機種]

Si-R G110

[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]

```
# 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 アドレスが表示されます。

2) MAC Address
Neighbor Cache エントリの MAC アドレスが表示されます。
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。

37.2 Neighbor Cache テーブルエントリの削除

37.2.1 clear ndp

[機能]

Neighbor Cache エントリの削除

[適用機種]

Si-R G110

[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 38 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

38.1 IPv4 ルーティングテーブル情報・統計などの表示、クリア

38.1.1 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 G110

[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]

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(F)および経路を注入したプロトコルの種別(P)が表示されます。
以下に、表示されるカーネルフラグ(F)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、経路注入元プロトコル種別(P)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。

38.1.2 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 G110

[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]

```
# 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

経路を注入したプロトコルの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。

38.1.3 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 G110

[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。

動的 VPN 機能を使用する場合は、経路削除により動的 VPN のセッションが切断されることがあります。

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]

```
# clear ip route
```

38.1.4 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 G110

[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
IP 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 <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]

```
# show ip route kernel
Routing Tables for Internet

Destination/Masklen Gateway           Flag   Interface
------------------- ----------------- ------ ---------
(1)                 (2)               (3)    (4)
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                                                    ---(5)


# 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。
2) Gateway
   ゲートウェイアドレスが表示されます。
   ダイレクト経路はゲートウェイのMACアドレスが表示されます。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)で表示されます。
3) Flag
   エントリ種別が表示されます。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送信あり)であることを示します。

   B (Blackhole)
   破棄経路(ICMP unreach送信なし)であることを示します。
4) Interface
   送出先インタフェースを示します。
5) 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。

38.1.5 show ip route kernel ecmp statistics

[機能]

ECMP 統計情報の表示

[適用機種]

Si-R G110

[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]

```
# 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

38.1.6 clear ip route kernel ecmp statistics

[機能]

ECMP 統計情報のクリア

[適用機種]

Si-R G110

[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
#
```

38.2 IPv6 ルーティングテーブル情報・統計などの表示、クリア

38.2.1 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 G110

[入力形式]

```
show ipv6 route [all]
show ipv6 route connected [all]
show ipv6 route static [all]
show ipv6 route ra [all]
show ipv6 route rip [all]
show ipv6 route bgp [all]
show ipv6 route ospf [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。

ra

RA 受信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。

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]

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)
--  ------------------------------------------  ---------   ------------------
*RA ::/0                                        00:00:05          12
        fe80::2                                                lan0
*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(F)および経路を注入したプロトコルの種別(P)が表示されます。
以下に、表示されるカーネルフラグ(F)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、経路注入元プロトコル種別(P)を示します。

RA
: RA 受信経路情報を示します。

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。

DH

: DHCP 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。

38.2.2 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 G110

[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]

```
# show ipv6 route summary
Route Source    Networks
 (1)              (2)
------------    --------
RA                     0
Static                 3
OSPF                   0 (O:0, A:0, E1:0, E2:0)
RIP                    0
BGP                    0 (Be:0, Bi:0)
DHCP                   0
DNS                    0
IKE                    0
Connected              7
Total                 10
```

1) Route Source

経路を注入したプロトコルの種別が表示されます。

RA

: RA 受信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。

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。

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。

38.2.3 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 G110

[入力形式]

```
clear ipv6 route
clear ipv6 route rip
clear ipv6 route bgp
clear ipv6 route ospf
clear ipv6 route dns
clear ipv6 route dhcp
clear ipv6 route ra
```

[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。

dhcp

DHCP 経路のみ再登録します。

ra

RA 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。
動的 VPN 機能を使用する場合は、経路削除により動的 VPN のセッションが切断されることがあります。
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]

```
# clear ipv6 route
```

38.2.4 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 G110

[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]

```
# 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が表示されます。
ダイレクト経路はゲートウェイの MAC アドレスが表示されます。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)で表示されます。

Flag
エントリ種別が表示されます。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 送信あり)であることを示します。

B (Blackhole)
破棄経路(ICMP unreach 送信なし)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。

38.2.5 show ipv6 ra default-router-list

[機能]

デフォルトルータリストの表示

[適用機種]

Si-R G110

[入力形式]

show ipv6 ra default-router-list

[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]

RA パケットから生成したデフォルトルータ候補を一覧表示します。

[メッセージ]

```
<ERROR> No IPv6 RA(host) is configured.
```

原因：
RA 受信機能が設定されていません。
対処：
RA 受信機能を設定してください。

[実行例]

```
# show ipv6 ra default-router-list
lan0:
  Advertise Router          Flag Lifetime Time
  (1)                       (2)      (3)   (4)
  fe80::1                   MO       1800  300
  fe80::1:1                 M-       1800   55
  fe80::1111:1111:1111:1111 -O       9000 9000
lan1:
  Advertise Router          Flag Lifetime Time
  fe80::1                   --       1800  300

The number of entries : 4                              ---(5)
```

1) Advertise Router
RA パケットの送信元アドレスが表示されます。
2) Flag
M、O flag の状態が表示されます。
M
Managed flag bit が on の状態
O
Otherconfig flag bit が on の状態
-
flag bit が off の状態
3) Lifetime
RA パケットの Router Lifetime(秒)が表示されます。

4) Time
Router Lifetime が満了するまでの残り時間(秒)が表示されます。
5) The number of entries
本装置で保持するデフォルトルータのエントリ数が表示されます。

38.2.6 show ipv6 ra prefix-list

[機能]

プレフィックスリストの表示

[適用機種]

Si-R G110

[入力形式]

show ipv6 ra prefix-list

[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]

RA パケットから生成したプレフィックス情報を一覧表示します。

[メッセージ]

```
<ERROR> No IPv6 RA(host) is configured.
```

原因：
RA 受信機能が設定されていません。
対処：
RA 受信機能を設定してください。

[実行例]

```
# show ipv6 ra prefix-list
Prefix/Prefixlen         Flag    Preferred Lifetime     Valid Lifetime
(1)                      (2)     (3)                    (4)
  Advertise Router          Interface
  (5)                       (6)
1000::/64                LA      602800(604800)         2590000(2592000)
  fe80::1                   lan0
2000::/64                LA      0(604800)              3599(2592000)
  fe80::2                   lan0
2000:2000:2000:2000::/64 -A      4800(604800)           1992000(2592000)
  fe80::1000:1000:1000:1001 lan0
2001::/64                LA      infinity               infinity
  fe80::10                  lan1

The number of entries : 4                               ---(7)
```

1) Prefix/Prefixlen
RA パケットの Prefix と Prefixlen が表示されます。

2) Flag
RA パケットの L、A フラグの状態が表示されます。

L
オンリンクフラグが 1 の状態

A
自動アドレス生成フラグが 1 の状態

-
フラグが 0 の状態

3) Preferred Lifetime

Preferred LifeTime が満了するまでの残り時間(秒)が表示されます。()内には RA パケットの Preferred LifeTime 値(秒)が表示されます。0 は満了したことを示します。

無限の場合は infinity が表示されます。

4) Valid Lifetime

Valid LifeTime が満了するまでの残り時間(秒)が表示されます。()内には RA パケットのプレフィックス情報オプションの Valid LifeTime 値(秒)が表示されます。

満了するとエントリが削除されます。

無限の場合は infinity が表示されます。

5) Advertise Router

RA パケットの送信元アドレスが表示されます。

6) Interface

RA パケット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

本装置で保持するプレフィックスのエントリ数が表示されます。

第 39 章 RIP 情報の表示、クリア操作コマンド

39.1 RIP 情報の表示、クリア

39.1.1 show ip rip route

[機能]

RIP 経路情報の表示

[適用機種]

Si-R G110

[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]

```
# 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)および経路を注入したプロトコルの種別(P)が表示されます。
以下に、ベストパスを示すフラグ(F)を示します。

*****
: ベストパスを示します。

空白

：スペア経路情報を示します。

以下に、経路注入元プロトコル種別(P)を示します。

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

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。

39.1.2 show ip rip protocol

[機能]

RIP プロトコル情報の表示

[適用機種]

Si-R G110

[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]

```
# 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が表示されます。

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
本装置の RIP の優先度が表示されます。

15) The number of entries
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。

39.1.3 clear ip rip statistics

[機能]

RIP 統計情報のクリア

[適用機種]

Si-R G110

[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
#
```

39.2 IPv6 RIP 情報の表示

39.2.1 show ipv6 rip route

[機能]

IPv6 RIP 経路情報の表示

[適用機種]

Si-R G110

[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]

```
# 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)および経路を注入したプロトコルの種別(P)が表示されます。
以下に、ベストパスを示すフラグ(F)を示します。

*****
: ベストパスを示します。

空白

：スペア経路情報を示します。

以下に、経路注入元プロトコル種別(P)を示します。

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。

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。

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

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。

39.2.2 show ipv6 rip protocol

[機能]

IPv6 RIP プロトコル情報の表示

[適用機種]

Si-R G110

[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]

```
# 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が表示されます。

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。

DHCP

: DHCP 経路情報を示します。

7) Distance

本装置の RIP の優先度が表示されます。

8) The number of entries

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 40 章 BGP 情報の表示、クリア操作コマンド

40.1 BGP 情報の表示、クリア

40.1.1 show ip bgp route

[機能]

BGP 経路情報の表示

[適用機種]

Si-R G110

[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]

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, p stale, * 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 0.65000 1.65001
    2.65002 3.65003 4.65004 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 0.65000 1.65001
    2.65002 3.65003 4.65004 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, p stale, * 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 0.65000 1.65001
    2.65002 3.65003 4.65004 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。

p

： グレースフルリスタート処理によって保護されている(stale 経路)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。

オリジン(ORIGIN 属性)には以下が表示されます。

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
  0.65000 1.65001 2.65002 3.65003 4.65004                                  (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.

: ベストパスが aggregate コマンドの summary-only 指定の集約経路により抑制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) 0.65000 1.65001 2.65002 3.65003 4.65004

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。

経路情報が無効な場合は、"inaccessible"と表示されます。

6) Origin IGP, metric 0, localpref 100, valid, external, best

Origin

: オリジン(ORIGIN 属性)が表示されます。

"IGP"、"EGP"または"incomplete"のいず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

: aggregate コマンドで作成し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。

preserved

: グレースフルリスタート処理が始まったことによって、保護されている場合(stale 経路)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。

40.1.2 show ip bgp route summary

[機能]

BGP 経路情報数の表示

[適用機種]

Si-R G110

[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 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]

```
# 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
BGP 受信経路と再配布経路の合計が表示されます。network 経路と aggregate 経路は含まれません。
3) Total Entries
BGP 受信経路、再配布経路、network 経路と aggregate 経路の合計が表示されます。
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。

また、AS_PATH 属性がない経路の場合も、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。

40.1.3 show ip bgp status

[機能]

BGP IPv4 セッションの状態表示

[適用機種]

Si-R G110

[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]

IPv4 で接続している 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]

```
# show ip bgp status
Local AS number 65535.65535                                                (1)
Neighbor                AS    MsgRcvd    MsgSent Up/Down   State       PfxRcvd
   (2)                 (3)        (4)        (5)      (6)      (7)         (8)
192.168.10.2        0.65000         92        103 00:00:06  Active            0
192.168.20.3    65535.65535         93        104 00:45:10  Estab             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

OpenConf
: BGP 接続確立のための KEEPALIVE メッセージ待ち状態

Estab
: BGP 接続が確立した状態

8) PfxRcvd
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。

40.1.4 show ip bgp neighbors

[機能]

BGP IPv4 隣接情報の表示

[適用機種]

Si-R G110

[入力形式]

show ip bgp neighbors [address <ip_address>]

[オプション]

なし

すべての BGP IPv4 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 IPv4 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 IPv4 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］

```
# show ip bgp neighbors
BGP neighbor is 192.168.10.2,                                          (1)
  remote AS 0.65000, local AS 65535.65535, external link
  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)
    Support for 4-octet AS number: advertised and received
    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)
    Graceful restart: advertised, received                            (13)
      can retain stale routes and already preserve forwarding states
  NEXT_HOP is always this router                                      (14)
  2 accepted prefixes                                                 (15)
  3 announced prefixes                                                (16)

 Connections established 4; dropped 3                                 (17)
 Graceful restart status:
     not restart yet, restart time is 10 sec                          (18)

Local host: 192.168.10.1, Local port: 1055                            (19)
Foreign host: 192.168.10.2, Foreign port: 179                         (20)
Nexthop: 192.168.10.1                                                 (21)
Read thread: on  Write thread: off                                    (22)
```

1) BGP neighbor is 192.168.10.2
   remote AS 0.65000, local AS 65535.65535, 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が以下の情報で表示されます。

Support for 4-octet AS number:

4 バイトの AS 番号をサポートしていることを示します。

Route refresh:

ルートリフレッシュ能力をサポートしていることを示します。

Address family IPv4 Unicast:

IPv4 ユニキャストの経路情報をサポートしていることを示します。

Address family IPv6 Unicast:

IPv6 ユニキャストの経路情報をサポートしていることを示します。

ケイパビリティ名に続く文字の意味は以下のとおりです。

advertised and received

対象のケイパビリティを送受信したことを示します。

advertised

対象のケイパビリティを送信したが受信していないことを示します。

received

対象のケイパビリティを送信していないが受信したことを示します。

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。

13) Graceful restart:

12)で表示されたアドレスファミリに関するグレースフルリスタートのネゴシエーションの結果が以下の情報で表示されます。

- advertised

  このアドレスファミリの能力値を隣接装置に送信したことを示します。

- received

  このアドレスファミリの能力値を隣接装置から受信したことを示します。

- can retain stale routes

  隣接装置とアドレスファミリの設定が一致したため、相手装置からの要求でグレースフルリスタートを開始した場合に、本装置でのパケット転送を継続する能力があることを示します。

- and already preserve forwarding states

  グレースフルリスタート処理を開始し、隣接装置から受信した経路を保護中であることを示します。

14) NEXT_HOP is always this router

ネクストホップセルフが有効な場合に表示されます。

15) 2 accepted prefixes

隣接装置から受信した現在の経路情報の数が表示されます。

16) 3 announced prefixes

本装置から広報した現在の経路情報の数が表示されます。

17) 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。

18) not restart yet, restart time is 10 sec

グレースフルリスタートの状態が以下の情報で表示されます。restart time は相手装置から OPEN メッセージで通知された Restart timer 値です。

グレースフルリスタートの状態は以下のとおりです。

restart finish

: グレースフルリスタート処理完了

already restart

: グレースフルリスタート処理中

not restart yet

: BGP セッション確立後、グレースフルリスタート処理をまだ一度も行っていない

19) 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。

20) 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。

21) Nexthop: 192.168.10.1

ネクストホップとして通知する IP アドレスが表示されます。

22) 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。

40.1.5 clear ip bgp neighbors

[機能]

BGP IPv4セッションのクリア

[適用機種]

Si-R G110

[入力形式]

clear ip bgp neighbors [address <ip_address>] [soft <mode>]

[オプション]

なし

すべてのBGP IPv4セッションをクリアします。

address <ip_address>

BGP IPv4セッションをクリアする隣接装置を指定します。

soft <mode>

BGP IPv4セッションを切断しないで、隣接装置と経路情報の再交換を実施します。
省略時は、BGP IPv4セッションを切断します。

- in
  隣接装置にUPDATEメッセージ送信を要求するROUTE REFRESHメッセージを送信します。
- out
  隣接装置にUPDATEメッセージを送信します。
- both
  in と out の両方の動作を行います。

[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]

隣接装置とのBGP IPv4セッションを再接続します。"soft"オプションを指定した場合は、BGP IPv4セッションを維持したまま経路情報の再交換のみを行います。

[注意]

"soft in"および"soft both"オプションを使用する場合は、隣接装置がルートリフレッシュ機能をサポートしている必要があります。

[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］

a)すべての隣接装置とのBGP IPv4セッションを再接続する場合

```
# clear ip bgp neighbors
#
```

b)特定の隣接装置とのBGP IPv4セッションを再接続する場合

```
# clear ip bgp neighbors address 192.168.1.1
#
```

c)すべての隣接装置とのBGP経路の再交換を行う場合

```
# clear ip bgp neighbors soft both
#
```

d)特定の隣接装置とのBGP経路の再交換を行う場合

```
# clear ip bgp neighbors address 192.168.1.1 soft both
#
```

40.1.6 clear ip bgp statistics

[機能]

BGP IPv4セッションの統計情報クリア

[適用機種]

Si-R G110

[入力形式]

clear ip bgp 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]

BGP IPv4セッションの統計情報をクリアします。

[実行例]

```
# clear ip bgp statistics
#
```

40.2 BGP IPv6 情報の表示、クリア

40.2.1 show ipv6 bgp route

[機能]

BGP IPv6 経路情報の表示

[適用機種]

Si-R G110

[入力形式]

show ipv6 bgp route
show ipv6 bgp route address <ipv6_address>/<prefixlen> detail
show ipv6 bgp route address <ipv6_address>/<prefixlen> longer-prefixes

[オプション]

なし
BGP の IPv6 経路情報を表示します。

address <ipv6_address>/<prefixlen> detail
指定されたアドレスとプレフィックス長に一致する経路のみ詳細表示します。

address <ipv6_address>/<prefixlen> longer-prefixes
指定されたアドレスとプレフィックス長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。

[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 IPv6 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］

パラメタなしの場合

```
# show ipv6 bgp route
Local router ID is 192.168.20.1                                          (1)
Status Codes: s suppressed, v valid, p stale, * best, i - internal
Origin Codes: i - IGP, e - EGP, ? - incomplete

   Network                                      Metric  LocalPref
      (2)                                          (3)      (4)
       Next Hop                              Path
          (5)                                (6)
v* 1000::/64
       ::                                   i
v*i1000:1000:1000:1000::/64
       ::                                   i
v i1000:1000:1000:1000::/64                           0         99
       1000::1                              10.65010 i
v* 2000:2000::/64                                     0        100
       1000::1                              10.65010 i
v* 3000:3000::/64                                     0      10000
       4000::1                              0.65005 0.65004 i
The number of routes is 5                                                (7)

# show ipv6 bgp route address 1000:1000::/32 longer-prefixes
Local router ID is 192.168.20.1
Status Codes: s suppressed, v valid, p stale, * best, i - internal
Origin Codes: i - IGP, e - EGP, ? - incomplete

   Network                                      Metric  LocalPref
       Next Hop                              Path
v*i1000:1000:1000:1000::/64
       ::                                   i
v i1000:1000:1000:1000::/64                           0         99
       1000::1                              10.65010 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。

   p
   ： グレースフルリスタート処理によって保護されている(stale経路)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) 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) Next Hop
   ネクストホップのIPv6アドレスが表示されます。
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。
   オリジン(ORIGIN属性)には以下が表示されます。

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。

アドレスとプレフィックス長に一致する経路の詳細表示の場合

```
# show ipv6 bgp route address 9000::/16 detail
BGP routing table entry for 9000::/16                                    (1)
Paths: (2 available, best #1)                                            (2)
  Advertised to non peer-group peers:                                    (3)
  8000::8 7000::7 6000::6
  0.65008 0.65007 0.65006                                                (4)
    5000:5000::5 (fe80::5)                                               (5)
      from 4000::4 (192.168.10.4)
      Origin IGP, metric 0, localpref 200, valid, external, best         (6)
      Community: no-export                                               (7)
      Last update: Thu Mar 1 14:39:40 2007                               (8)
  0.65005 0.65004
    3000:3000::3 (fe80::3)
      from 2000::2 (192.168.10.2)
      Origin IGP, metric 0, localpref 100, valid, external
      Community: no-export
      Last update: Thu Mar 1 14:39:40 2007
```

1) BGP routing table entry for

指定した経路情報が表示されます。

2) Paths: (2 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

: ベストパスがある場合、ベストパスが重複経路内で上から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.

: ベストパスが aggregate コマンドの summary-only 指定の集約経路により抑制されている場合に表示されます。

3) Advertised to non peer-group peers:

8000::8 7000::7 6000::6

この経路情報を BGP で広報している場合は、すべての広報先の隣接装置の IPv6 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) 0.65008 0.65007 0.65006

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 ルータ ID が表示されます。

本コマンドで指定した経路が重複している場合は、4)から 8)の情報が経路数分表示されます。

5) 5000:5000::5 (fe80::5)

from 4000::4 (192.168.10.4)

ネクストホップアドレスと、送信元 IPv6 アドレス(BGP ルータ ID)が表示されます。

ネクストホップアドレスには、MP_REACH_NLRI 属性の先頭ネクストホップアドレスが表示されます。

次ネクストホップアドレスが存在する場合は続けて()内に表示されます。

経路情報が無効な場合は続けて"inaccessible"が表示されます。
送信元 IPv6 アドレスには、UPDATE メッセージの送信元アドレスが表示されます。

6) Origin IGP, metric 0, localpref 200, valid, external, best

Origin
: オリジン(ORIGIN 属性)が表示されます。
"IGP"、"EGP"または"incomplete"のいず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 で受信した経路の場合に表示されます。

internal
: IBGP で受信した経路の場合に表示されます。

aggregated, local
: aggregate コマンドで作成し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。

preserved
: グレースフルリスタート処理が始まったことによって、保護されている場合(stale 経路)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。

40.2.2 show ipv6 bgp route summary

[機能]

BGP IPv6 経路情報数の表示

[適用機種]

Si-R G110

[入力形式]

show ipv6 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 IPv6 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]

```
# show ipv6 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
BGP 受信経路と再配布経路の合計が表示されます。network 経路と aggregate 経路は含まれません。
3) Total Entries
BGP 受信経路、再配布経路、network 経路と aggregate 経路の合計が表示されます。
4) Total Prefixes
プレフィックス数が表示されます。同一のプレフィックスは 1 として数えられます。
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。

また、AS_PATH 属性がない経路の場合も、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。

40.2.3 show ipv6 bgp status

[機能]

BGP IPv6 セッションの状態表示

[適用機種]

Si-R G110

[入力形式]

show ipv6 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]

IPv6 で接続している 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]

```
# show ipv6 bgp status
Local AS number 65535.65535                                                    (1)
Neighbor
  (2)        AS    MsgRcvd    MsgSent Up/Down   State          PfxRcvd
            (3)      (4)        (5)     (6)      (7)           (8)
1111::1
        0.65000         92        103 00:00:06  Active               0
1111::2
    65535.65535         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 IPv6 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) PfxRcvd

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。

40.2.4 show ipv6 bgp neighbors

[機能]

BGP IPv6 隣接情報の表示

[適用機種]

Si-R G110

[入力形式]

show ipv6 bgp neighbors [address <ipv6_address>]

[オプション]

なし

すべての BGP IPv6 隣接情報を表示します。

address <ipv6_address>

指定した隣接アドレスの BGP IPv6 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 IPv6 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］

```
# show ipv6 bgp neighbors
BGP neighbor is 2000::2,                                                  (1)
  remote AS 0.65000, local AS 65535.65535, external link
  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)
    Support for 4-octet AS number: advertised and received
    Route refresh: advertised and received (old and new)
    Address family IPv6 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 1000::1                                                 (11)

For address family: IPv6 Unicast                                          (12)
  NEXT_HOP is always this router                                          (13)
  2 accepted prefixes                                                     (14)
  3 announced prefixes                                                    (15)

 Connections established 4; dropped 3                                     (16)
  External BGP neighbor may be up to 2 hops away.                         (17)
Local host: 1000::1, Local port: 179                                      (18)
Foreign host: 2000::2, Foreign port: 2346                                 (19)
Nexthop global: 1000::1                                                   (20)
Nexthop local: fe80::1                                                    (21)
Read thread: on Write thread: off                                         (22)
```

1) BGP neighbor is 2000::2,

   remote AS 0.65000, local AS 65535.65535, external link

   隣接装置の IPv6 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、BGP 接続形態が表示されます。"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が以下の情報で表示されます。

Support for 4-octet AS number:

4バイトの AS 番号をサポートしていることを示します。

Route refresh:

ルートリフレッシュ能力をサポートしていることを示します。

Address family IPv4 Unicast:

IPv4ユニキャストの経路情報をサポートしていることを示します。

Address family IPv6 Unicast:

IPv6ユニキャストの経路情報をサポートしていることを示します。

ケイパビリティ名に続く文字の意味は以下のとおりです。

advertised and received

対象のケイパビリティを送受信したことを示します。

advertised

対象のケイパビリティを送信したが受信していないことを示します。

received

対象のケイパビリティを送信していないが受信したことを示します。

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 2000::1
BGPセッションの自側に設定されているIPv6アドレスが表示されます。

12) For address family: IPv6 Unicast
アドレスファミリが表示されます。

13) NEXT_HOP is always this router
ネクストホップセルフが有効な場合に表示されます。

14) 2 accepted prefixes
隣接装置から受信している現在の経路情報の数が表示されます。

15) 3 announced prefixes
本装置から広報している現在の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) External BGP neighbor may be up to 2 hops away.
EBGPマルチホップ接続の場合にホップ数が表示されます。

18) Local host: 1000::1, Local port: 179
BGP接続に使用している本装置のIPv6アドレスとポート番号が表示されます。

19) Foreign host: 2000::2, Foreign port: 2346
BGP接続に使用している隣接装置のIPv6アドレスとポート番号が表示されます。

20) Nexthop: 1000::1
ネクストホップとして通知するIPv6アドレスが表示されます。

21) Nexthop local: fe80::1
ネクストホップとして通知するリンクローカルアドレスが表示されます。

22) 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。

40.2.5 clear ipv6 bgp neighbors

[機能]

BGP IPv6セッションのクリア

[適用機種]

Si-R G110

[入力形式]

clear ipv6 bgp neighbors [address <ipv6_address>] [soft <mode>]

[オプション]

なし

すべての隣接装置とのBGP IPv6セッションをクリアします。

address <ipv6_address>

BGP IPv6セッションをクリアする隣接装置を指定します。

soft <mode>

BGP IPv6セッションを切断しないで、隣接装置と経路情報の再交換を実施します。

省略時は、BGP IPv6セッションを切断します。

- in
  隣接装置にUPDATEメッセージ送信を要求するROUTE REFRESHメッセージを送信します。
- out
  隣接装置にUPDATEメッセージを送信します。
- both
  in と out の両方の動作を行います。

[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]

隣接装置とのBGP IPv6セッションを再登録します。"soft"オプションを指定した場合は、BGP IPv6セッションを維持したまま経路情報の再交換のみを行います。

[注意]

"soft in"および"soft both"オプションを使用する場合は、隣接装置がルートリフレッシュ機能をサポートしている必要があります。

[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]

a)すべての隣接装置とのBGP IPv6セッションを再接続する場合

```
# clear ipv6 bgp neighbors
#
```

b)特定の隣接装置とのBGP IPv6セッションを再接続する場合

```
# clear ipv6 bgp neighbors address 2001:db8::1
#
```

c)すべての隣接装置とのBGP経路の再交換を行う場合

```
# clear ipv6 bgp neighbors soft both
#
```

d)特定の隣接装置とのBGP経路の再交換を行う場合

```
# clear ipv6 bgp neighbors address 2001:db8::1 soft both
#
```

40.2.6 clear ipv6 bgp statistics

[機能]

BGP IPv6セッションの統計情報クリア

[適用機種]

Si-R G110

[入力形式]

clear ipv6 bgp 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]

BGP IPv6セッションの統計情報をクリアします。

[実行例]

```
# clear ipv6 bgp statistics
#
```

第 41 章 OSPF 情報の表示、クリア操作コマンド

41.1 OSPF 情報の表示、クリア

41.1.1 show ip ospf route

[機能]

OSPF 経路情報の表示

[適用機種]

Si-R G110

[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］

```
# 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。

インタフェース経路の場合、"0.0.0.0"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
経路の nexthop が属するエリアのエリア ID が表示されます。
Type2 AS 外部経路の場合は、表示されません。
6) Interface
出力インタフェース名が表示されます。
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。
ネットワーク経路数に、インタフェース経路は含みません。

41.1.2 show ip ospf protocol

[機能]

OSPF 情報の表示

[適用機種]

Si-R G110

[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］

```
# 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
 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 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

エリアの種類が表示されます。

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。

41.1.3 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 G110

[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]

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。

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。

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。

41.1.4 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 G110

[入力形式]

show ip ospf interface [detail]

[オプション]

なし

OSPF インタフェース情報を表示します。

detail

OSPF インタフェース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]

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］

```
# show ip ospf interface detail

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)
  Packet statistics for 00:03:40                                   ---+----(17)
                      sent    received                                  |
    Hello:               6           6                                  |
    Description:         3           3                                  |
    Request:             1           1                                  |
    Update:              3           2                                  |
    Ack:                 1           4                             ---+

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
  Packet statistics for 00:10:03
                      sent    received
    Hello:              43          43
    Description:         6           6
    Request:             2           2
    Update:              4           4
    Ack:                 3           7

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
  Packet statistics for 00:10:03
                      sent    received
    Hello:              25          25
    Description:         8           5
    Request:             3           1
    Update:              4           4
    Ack:                 3           7
```

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
: ブロードキャストネットワークを示します。

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) Packet statistics for
OSPF パケットの統計情報が表示されます。
統計情報には、OSPF パケット送受信数、および採取を開始してからの経過時間が表示されます。
なお、loopback インタフェースに統計情報は表示されません。
本情報は OSPF インタフェースが活性状態の場合のみ表示されます。
ダウン状態となった場合、統計情報はクリアされます。

41.1.5 show ip ospf neighbor

[機能]

OSPF 隣接情報の表示

[適用機種]

Si-R G110

[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］

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 が表示されます。
2) Pri
   優先度(Priority)が表示されます。
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。

41.1.6 clear ip ospf statistics

[機能]

OSPF 統計情報のクリア

[適用機種]

Si-R G110

[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
#
```

41.2 IPv6 OSPF 情報の表示、クリア

41.2.1 show ipv6 ospf route

[機能]

IPv6 OSPF 経路情報の表示

[適用機種]

Si-R G110

[入力形式]

show ipv6 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]

IPv6 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 IPv6 OSPF is configured.
```

原因：
IPv6 OSPF が設定されていません。または、定義が不足しており IPv6 OSPF が動作していません。

対処：
IPv6 OSPF を設定してください。

［実行例］

```
# show ipv6 ospf route

Type          Destination/Prefixlen                       Area
(1)           (2)                                         (3)
                  Nexthop                                       Cost Interface
                  (4)                                           (5)  (6)
Network Intra 2001:db8:ffff:1000::/64                     0.0.0.0
                  ::                                              10 lan0
Network Intra 2001:db8:ffff:2000::/64                     0.0.0.0
                  fe80::20b:5dff:fe18:10                          20 lan0
Network Inter 2001:db8:ffff:3000::/64                     0.0.0.0
                  fe80::20b:5dff:fe18:10                          20 lan0
Network Type1 2001:db8:ffff:4000::/64                     0.0.0.0
                  fe80::20b:5dff:fe18:10                          40 lan0
Network Type2 2001:db8:ffff:5000::/64
                  fe80::20b:5dff:fe18:10                        1000 lan0
Network Type2 2001:db8:ffff:6000::/64
                  fe80::20b:5dff:fe18:10                        1000 lan0
Router  Inter 3.3.3.3                                     0.0.0.0
                  fe80::20b:5dff:fe18:10                          20 lan0
5 Network entries, and 1 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

： AS 境界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。

Discard

： 集約経路定義時の破棄経路を示します。

2) Destination/Prefixlen

ネットワーク経路の場合は、あて先ネットワークとプレフィックス長が表示されます。

AS 境界ルータ経路の場合は、プレフィックス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) Area

経路の nexthop が属するエリアのエリア ID が表示されます。

Type2 AS 外部経路の場合は、本情報は空白となります。

4) 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ゲートウェイのアドレスが表示されます。

インタフェース経路の場合、"::"が表示されます。

5) 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。

6) Interface

出力インタフェース名が表示されます。

7) 5 Network entries, and 1 Router entries.

ネットワーク経路とAS境界ルータ経路の数が表示されます。
ネットワーク経路数に、インタフェース経路は含みません。

41.2.2 show ipv6 ospf protocol

[機能]

IPv6 OSPF 情報の表示

[適用機種]

Si-R G110

[入力形式]

show ipv6 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]

IPv6 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 IPv6 OSPF is configured.
```

原因：
IPv6 OSPF が設定されていません。または、定義が不足しており IPv6 OSPF が動作していません。

対処：
IPv6 OSPF を設定してください。

［実行例］

```
# show ipv6 ospf protocol
 ospf(v3) daemon is running.                                          ---(1)
 Global statistics and variables:
 SPF schedule delay 5 secs, Hold time between next SPF 10 secs        ---(2)
  Router ID: 10.10.10.10                                              ---(3)
  AS boundary router.                                                 ---(4)
  Redistributing external routes from,                                ---(5)
    Connected
    Static
  Area border router.                                                 ---(6)
  Number of AS scope LSA in Database is 1. Checksum Sum is 0x395e     ---(7)
  Number of LSA is 22                                                 ---(8)
  Number of network route is 1                                        ---(9)
  Number of router route is 0                                         ---(10)
  Number of configured areas is 2                                     ---(11)

  Area(0.0.0.0) statistics and variables:                             ---(12)
    This area seems to be normal area                                 ---(13)
    SPF algorithm executed 3 times                                    ---(14)
    Number of LSA in Database is 11. Checksum Sum is 0x689ac          ---(15)
    Number of fully adjacent neighbor is 2                            ---(16)
    Number of active interface is 2                                   ---(17)
    Number of interfaces attached in this area is 2                   ---(18)
    "Area" address range(for route aggregation):                      ---(19)
      2001:db8:1000::/48                              (Advertise)

  Area(0.0.0.1) statistics and variables:
    This area seems to be normal area
    SPF algorithm executed 4 times
    Number of LSA in Database is 6. Checksum Sum is 0x313ea
    Number of fully adjacent neighbor is 1
    Number of active interface is 1
    Number of interfaces attached in this area is 1
    "Area" address range(for route aggregation):
```

1) ospf(v3) 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: 10.10.10.10
   ルータ ID が表示されます。
4) 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。
5) 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。

   Connected
   ： インタフェース経路を示します。

   Static
   ： スタティック経路を示します。

   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。

   DHCP
   ： DHCP 経路を示します。
6) 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。

7) Number of AS scope LSA in Database is 1. Checksum Sum is 0x395e
ASスコープLSA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。

8) Number of LSA is 22
LSAの数が表示されます。

9) Number of network route is 1
ネットワーク経路の数が表示されます。

10) Number of router route is 0
AS境界ルータ経路の数が表示されます。

11) Number of configured areas is 2
設定されているエリアの総数が表示されます。

12) 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。

13) This area seems to be normal area
エリアの種類が表示されます。

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が表示されます。

14) SPF algorithm executed 3 times
SPF計算アルゴリズムの実行回数が表示されます。

15) Number of LSA in Database is 11. Checksum Sum is 0x689ac
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。

16) Number of fully adjacent neighbor is 2
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。

17) Number of active interface is 2
このエリアに属しているOSPFインタフェースのうちUP状態のインタフェース数が表示されます。

18) Number of interfaces attached in this area is 2
このエリアに属するOSPFインタフェースの総数が表示されます。

19) "Area" address range(for route aggregation):
エリア内部集約経路の定義がある場合、一覧が表示されます。

41.2.3 show ipv6 ospf database

[機能]

IPv6 OSPF LSA データベース情報の表示

[適用機種]

Si-R G110

[入力形式]

```
show ipv6 ospf database
show ipv6 ospf database detail
show ipv6 ospf database self-originate
show ipv6 ospf database lsa <type> detail
show ipv6 ospf database lsa <type> ls-id <link_id> detail
show ipv6 ospf database lsa <type> self-originate detail
show ipv6 ospf database lsa <type> adv-router <router_id> detail
show ipv6 ospf database lsa <type> adv-router <router_id> ls-id <link_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。

detail

OSPF データベースの全 LSA を詳細表示します。

self-originate

OSPF データベースの自ルータが生成した 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、inter-prefix、inter-router、external、link、intra-prefix 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 種別で自ルータが生成した 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。

lsa <type> adv-router <router_id> ls-id <link_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、リンク 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]

IPv6 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 IPv6 OSPF is configured.
```

原因：

IPv6 OSPF が設定されていません。または、定義が不足しており IPv6 OSPF が動作していません。

対処：

IPv6 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]

OSPF データベースの全 LSA の簡易表示の場合

```
# show ipv6 ospf database

LSA list in the LSDB for interface lan0 (2 LSAs, Checksum Sum:0x15134)
                                         (1)           (2)
Type     Link ID         Advertiser      Age  Seq#     Sum
 (3)      (4)             (5)            (6)   (7)      (8)
Link     0.0.0.1         10.10.10.10     0068 80000002 5561
Link     0.0.0.1         20.20.20.20     0073 80000001 fbd3

LSA list in the LSDB for interface lan1 (2 LSAs, Checksum Sum:0xf9f5)
Type     Link ID         Advertiser      Age  Seq#     Sum
Link     0.0.0.2         10.10.10.10     0068 80000002 b3f0
Link     0.0.0.1         30.30.30.30     0075 80000002 4605

LSA list in the LSDB for area 0.0.0.0 (6 LSAs, Checksum Sum:0x2d9ee)
Type     Link ID         Advertiser      Age  Seq#     Sum
Router   0.0.0.0         10.10.10.10     0027 80000004 1f78
Router   0.0.0.0         20.20.20.20     0028 80000003 f080
Network  0.0.0.1         20.20.20.20     0033 80000001 6cf2
InterPre 0.0.0.1         10.10.10.10     0066 80000002 cfeb
InterRtr 0.0.0.1         10.10.10.10     0013 80000001 2358
Intra    0.0.0.2         20.20.20.20     0027 80000001 69c1

LSA list in the LSDB for area 0.0.0.1 (5 LSAs, Checksum Sum:0x27cb5)
Type     Link ID         Advertiser      Age  Seq#     Sum
Router   0.0.0.0         10.10.10.10     0026 80000003 6609
Router   0.0.0.0         30.30.30.30     0028 80000003 011e
Network  0.0.0.1         30.30.30.30     0029 80000001 947a
InterPre 0.0.0.1         10.10.10.10     0066 80000002 be0d
Intra    0.0.0.2         30.30.30.30     0028 80000001 c307

LSA list in the LSDB for AS (4 LSAs, Checksum Sum:0x20460)
Type     Link ID         Advertiser      Age  Seq#     Sum
External 0.0.0.1         30.30.30.30     0079 80000001 2f04
External 0.0.0.2         30.30.30.30     0079 80000001 e53c
External 0.0.0.3         30.30.30.30     0079 80000001 9c74
External 0.0.0.4         30.30.30.30     0079 80000001 53ac
```

1) 2 LSAs
   インタフェースごとまたは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:0x15134
   スコープ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。

InterPre

：Inter Area Prefix LSA を示します。

InterRtr

：Inter Area Router LSA を示します。

External

：AS external LSA を示します。

Link

：Link LSA を示します。

Intra

：Intra Area Prefix LSA を示します。

Unknown

：未定義の LSA を示します。

4) Link ID

LSA の Link State ID が表示されます。

5) Advertiser

LSA を広報したルータのルータ ID が表示されます。

6) Age

LSA が生成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 LSA(Router LSA)情報表示の場合

```
# show ipv6 ospf database lsa router detail

LSA list in the LSDB for area 0.0.0.0 (3 LSAs, Checksum Sum:0x17cea)

Router    Id 0.0.0.0          Router 10.10.10.10
 (1)      (2)                 (3)
Age 0110  Seq 80000004  Sum 1f78  Length 40
 (4)      (5)           (6)       (7)
  Flag 0x01 (-|-|-|B)  Option 0x13 (-|R|-|-|E|V6)
  (8)                  (9)
  Transit         Metric 10  If-Id 1
    Neighbor-Id 20.20.20.20  Neighbor-If-Id 1

Router    Id 0.0.0.0          Router 20.20.20.20
Age 0116  Seq 80000003  Sum f080  Length 40
  Flag 0x00 (-|-|-|-)  Option 0x13 (-|R|-|-|E|V6)
  Transit         Metric 10  If-Id 1
  (10)            (11)       (12)
    Neighbor-Id 20.20.20.20  Neighbor-If-Id 1
    (13)                     (14)
LSA list in the LSDB for area 0.0.0.1 (5 LSAs, Checksum Sum:0x26801)

Router    Id 0.0.0.0          Router 10.10.10.10
Age 0023  Seq 80000006  Sum 1794  Length 56
  Flag 0x01 (-|-|-|B)  Option 0x13 (-|R|-|-|E|V6)
  Transit         Metric 10  If-Id 2
    Neighbor-Id 30.30.30.30  Neighbor-If-Id 1
  Transit         Metric 10  If-Id 3
    Neighbor-Id 40.40.40.40  Neighbor-If-Id 1

Router    Id 0.0.0.0          Router 30.30.30.30
Age 0058  Seq 80000003  Sum fa26  Length 40
  Flag 0x00 (-|-|-|-)  Option 0x13 (-|R|-|-|E|V6)
  Transit         Metric 10  If-Id 1
    Neighbor-Id 30.30.30.30  Neighbor-If-Id 1

Router    Id 0.0.0.0          Router 40.40.40.40
Age 0019  Seq 80000003  Sum 05cb  Length 40
  Flag 0x00 (-|-|-|-)  Option 0x13 (-|R|-|-|E|V6)
  Transit         Metric 10  If-Id 1
    Neighbor-Id 40.40.40.40  Neighbor-If-Id 1
```

1) Router
   Router LSA であることを示します。
2) Id
   LSA の Link State ID が表示されます。
3) Router
   LSA を広報したルータのルータ ID が表示されます。
4) Age
   LSA が生成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) Flag
   このルータの役割が表示されます。

   0x01 (-|-|-|B)
   ： エリア境界ルータであることを示します。

   0x02 (-|-|E|-)
   ： AS 境界ルータであることを示します。

0x08 (W|-|-|-)

: ワイルドカード・マルチキャスト・レシーバであることを示します。

9) 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。

0x01 (-|-|-|-|-|V6)

: IPv6 をサポートしていることを示します。

0x02 (-|-|-|-|E|-)

: AS External LSA をサポートしていることを示します。

0x04 (-|-|-|MC|-|-)

: MOSPF をサポートしていることを示します。

0x08 (-|-|N|-|-|-)

: NSSA をサポートしていることを示します。

0x10 (-|R|-|-|-|-)

: ルーティング機能をサポートしていることを示します。

0x20 (DC|-|-|-|-|-)

: デマンドサーキットをサポートしていることを示します。

10) Transit

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

: トランジットリンクであることを示します。

11) Metric

そのリンクのコストが表示されます。

12) If-Id

インタフェース ID が表示されます。

13) Neighbor-Id

隣接ルータのルータ ID が表示されます。

Transit リンクの場合は DR のルータ ID が表示されます。

14) Neighbor-If-Id

隣接ルータのインタフェース ID が表示されます。

Transit リンクの場合は DR のインタフェース ID が表示されます。

ネットワーク LSA(Network LSA)情報表示の場合

```
# show ipv6 ospf database lsa network detail

LSA list in the LSDB for area 0.0.0.0 (6 LSAs, Checksum Sum:0x26d51)

Network   Id 0.0.0.1          Router 20.20.20.20
 (1)      (2)                 (3)
Age 0020  Seq 80000001  Sum 6cf2  Length 32
 (4)      (5)           (6)       (7)
  Option 0x13 (-|R|-|-|E|V6)
   (8)
    Attached Router: 20.20.20.20     ---(9)
    Attached Router: 10.10.10.10
```

1) Network

Network LSA であることを示します。

2) Id

LSA の Link State ID が表示されます。

3) Router

LSA を広報したルータのルータ ID が表示されます。

4) Age

LSA が生成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。

0x01 (-|-|-|-|-|V6)
: IPv6 をサポートしていることを示します。

0x02 (-|-|-|-|E|-)
: AS External LSA をサポートしていることを示します。

0x04 (-|-|-|MC|-|-)
: MOSPF をサポートしていることを示します。

0x08 (-|-|N|-|-|-)
: NSSA をサポートしていることを示します。

0x10 (-|R|-|-|-|-)
: ルーティング機能をサポートしていることを示します。

0x20 (DC|-|-|-|-|-)
: デマンドサーキットをサポートしていることを示します。

9) Attached Router
リン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。

エリア間プレフィックス LSA(Inter Area Prefix LSA)情報表示の場合

```
# show ipv6 ospf database lsa inter-prefix detail

LSA list in the LSDB for area 0.0.0.0 (6 LSAs, Checksum Sum:0x31254)

InterPre  Id 0.0.0.2          Router 10.10.10.10
 (1)      (2)                 (3)
Age 0057  Seq 80000002  Sum b416  Length 36
 (4)      (5)           (6)       (7)
  Prefix 2001:db8:ffff:1000::/64 Option 0x00 (-|-|-|-)
  (8)                            (9)
    Metric  10
    (10)
```

1) InterPre
Inter Area Prefix LSA であることを示します。
2) Id
LSA の Link State ID が表示されます。
3) Router
LSA を広報したルータのルータ ID が表示されます。
4) Age
LSA が生成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) Prefix
エリア外ネットワークのプレフィックス/プレフィックス長が表示されます。
9) Option
プレフィックスオプションが表示されます。

0x01 (-|-|-|NU)

: ユニキャスト計算に含まれないことを示します。

0x02 (-|-|LA|-)

: 広報ルータのインタフェースアドレスであることを示します。

0x04 (-|MC|-|-)

: マルチキャスト計算に含まれることを示します。

0x08 (P|-|-|-)

: NSSA 境界ルータで再広報される NSSA エリアプレフィックスであることを示します。

10) Metric

エリア外ネットワークまでコストが表示されます。

エリア間ルータ LSA(Inter Area Router LSA)情報表示の場合

```
# show ipv6 ospf database lsa inter-router detail

LSA list in the LSDB for area 0.0.0.0 (4 LSAs, Checksum Sum:0x3ac7e)

InterRtr  Id 0.0.0.8          Router 10.10.10.10
 (1)      (2)                  (3)
Age 0012  Seq 80000001  Sum e6b5  Length 32
 (4)      (5)           (6)       (7)
  Option 0x13 (-|R|-|-|E|V6)  Metric  10   Router-Id 20.20.20.20
   (8)                        (9)          (10)
```

1) InterRtr

Inter Area Router LSA であることを示します。

2) Id

LSA の Link State ID が表示されます。

3) Router

LSA を広報したルータのルータ ID が表示されます。

4) Age

LSA が生成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。

0x01 (-|-|-|-|-|V6)

: IPv6 をサポートしていることを示します。

0x02 (-|-|-|-|E|-)

: AS External LSA をサポートしていることを示します。

0x04 (-|-|-|MC|-|-)

: MOSPF をサポートしていることを示します。

0x08 (-|-|N|-|-|-)

: NSSA をサポートしていることを示します。

0x10 (-|R|-|-|-|-)

: ルーティング機能をサポートしていることを示します。

0x20 (DC|-|-|-|-|-)

: デマンドサーキットをサポートしていることを示します。

9) Metric

エリア外 AS 境界ルータまでのコストが表示されます。

10) Router-Id

エリア外 AS 境界ルータのルータ ID が表示されます。

AS 外部ネットワーク LSA(AS External LSA)情報表示の場合

```
# show ipv6 ospf database lsa external detail

LSA list in the LSDB for AS (2 LSAs, Checksum Sum:0x16420)

External  Id 0.0.0.1          Router 30.30.30.30
 (1)      (2)                 (3)
Age 0029  Seq 80000002  Sum ae9c  Length 36
 (4)      (5)           (6)       (7)
  flag 0x04 (E|-|-)   Type2  Metric 20
   (8)                (9)    (10)
    Prefix 2001:db8:ffff:1000::/64 Option 0x00 (-|-|-|-)
     (11)                          (12)
  Forwarder 2001:db8:111::1111/128                ---(13)
  Tag 0                                           ---(14)
  Ref-LS-Type 0x0000            Ref-Link-Id 0.0.0.0
    (15)                                 (16)

External  Id 0.0.0.2          Router 30.30.30.30
Age 0029  Seq 80000002  Sum b584  Length 36
  flag 0x04 (E|-|-)   Type2  Metric 20
    Prefix 2001:db8:ffff:2000::/64 Option 0x00 (-|-|-|-)
```

1) External
   AS external LSA であることを示します。
2) Id
   Link State ID が表示されます。
3) Router
   LSA を広報したルータのルータ ID が表示されます。
4) Age
   LSA が生成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) flag
   この LSA に含まれる情報が表示されます。

   0x01 (-|-|T)
   ： 外部経路タグを含んでいることを示します。

   0x02 (-|F|-)
   ： フォワーディングアドレスを含んでいることを示します。

   0x04 (E|-|-)
   ： 外部メトリックの種別を示します。
   ビット E が設定されているときは Type2、設定されていないときは Type1 であることを示します。
9) Type2
   外部メトリックの種別が表示されます。

   Type1
   ： Type1 外部メトリックであることを示します。

   Type2
   ： Type2 外部メトリックであることを示します。
10) Metric
   このネットワークまでのメトリックが表示されます。
11) Prefix
   AS 外部ネットワークのプレフィックス/プレフィックス長が表示されます。
12) Option
   プレフィックスオプションが表示されます。

0x01 (-|-|-|NU)

：ユニキャスト計算に含まれないことを示します。

0x02 (-|-|LA|-)

：広報ルータのインタフェースアドレスであることを示します。

0x04 (-|MC|-|-)

：マルチキャスト計算に含まれることを示します。

0x08 (P|-|-|-)

：NSSA 境界ルータで再広報される NSSA エリアプレフィックスであることを示します。

13) Forwarder

フォワーディングアドレスが表示されます。

フォワーディングアドレスが設定されている場合に表示されます。

14) Tag

外部経路タグが表示されます。

タグ情報が設定されている場合に表示されます。

15) Ref-LS-Type

Referenced LS Type が表示されます。

Referenced LS Type が設定されている場合に表示されます。

16) Ref-Link-Id

Referenced Link State ID が表示されます。

Referenced Link State ID が設定されている場合に表示されます。

リンク LSA(Link LSA)情報表示の場合

```
# show ipv6 ospf database lsa link detail

LSA list in the LSDB for interface lan0 (1 LSAs, Checksum Sum:0xe8a0)

Link      Id 0.0.0.1          Router 10.10.10.10
 (1)      (2)                 (3)
Age 0085  Seq 80000002  Sum e8a0  Length 92
 (4)      (5)           (6)       (7)
  Priority 1   Option 0x13 (-|R|-|-|E|V6)
   (8)          (9)
  Link-Local Address fe80::20b:5dff:fe18:10       ---(10)
  Number of Prefixes 4                            ---(11)
    Prefix 2001:db8:ffff:1000::/64 Option 0x00 (-|-|-|-)
     (12)                            (13)
    Prefix 2001:db8:ffff:2000::/64 Option 0x00 (-|-|-|-)
    Prefix 2001:db8:ffff:3000::/64 Option 0x00 (-|-|-|-)
    Prefix 2001:db8:ffff:4000::/64 Option 0x00 (-|-|-|-)
```

1) Link

Link LSA であることを示します。

2) Id

LSA の Link State ID が表示されます。

3) Router

LSA を広報したルータのルータ ID が表示されます。

4) Age

LSA が生成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) Priority

このリンクでの生成元ルータの指定ルータ優先度が表示されます。

9) 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。

0x01 (-|-|-|-|-|V6)

: IPv6 をサポートしていることを示します。

0x02 (-|-|-|-|E|-)

: AS External LSA をサポートしていることを示します。

0x04 (-|-|-|MC|-|-)

: MOSPF をサポートしていることを示します。

0x08 (-|-|N|-|-|-)

: NSSA をサポートしていることを示します。

0x10 (-|R|-|-|-|-)

: ルーティング機能をサポートしていることを示します。

0x20 (DC|-|-|-|-|-)

: デマンドサーキットをサポートしていることを示します。

10) Link-Local Address

広報元ルータのリンクローカルアドレスが表示されます。

11) Number of Prefixes

LSA に含まれているプレフィックスの数が表示されます。

12) Prefix

広報元ルータのリンクに設定されたプレフィックス/プレフィックス長が表示されます。

13) Option

プレフィックスオプションが表示されます。

0x01 (-|-|-|NU)

: ユニキャスト計算に含まれないことを示します。

0x02 (-|-|LA|-)

: 広報ルータのインタフェースアドレスであることを示します。

0x04 (-|MC|-|-)

: マルチキャスト計算に含まれることを示します。

0x08 (P|-|-|-)

: NSSA 境界ルータで再広報される NSSA エリアプレフィックスであることを示します。

エリア内プレフィックス LSA(Intra Area Prefix LSA)情報表示の場合

```
# show ipv6 ospf database lsa intra-prefix detail

LSA list in the LSDB for area 0.0.0.0 (2 LSAs, Checksum Sum:0x144e8)

Intra     Id 0.0.0.1          Router 10.10.10.10
 (1)      (2)                 (3)
Age 0087  Seq 80000003  Sum 45e1  Length 80
 (4)      (5)           (6)       (7)
  Number of Prefixes 4                          ---(8)
  Ref-LS-Type 0x2001 (Router)  Ref-Link-Id 0.0.0.0
   (9)                          (10)
  Ref-Adv-Rtr 10.10.10.10                       ---(11)
    Prefix 2001:db8:ffff:1000::/64 Option 0x00 (-|-|-|-)
     (12)                            (13)
      Metric 10                                 ---(14)
    Prefix 2001:db8:ffff:2000::/64 Option 0x00 (-|-|-|-)
      Metric 10
    Prefix 2001:db8:ffff:3000::/64 Option 0x00 (-|-|-|-)
      Metric 10
    Prefix 2001:db8:ffff:4000::/64 Option 0x00 (-|-|-|-)
      Metric 10
```

1) Intra

Intra-Area-Prefix LSA であることを示します。

2) Id

LSA の Link State ID が表示されます。

3) Router

LSA を広報したルータのルータ ID が表示されます。

4) Age

LSA が生成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) Number of Prefixes

LSA に含まれているプレフィックスの数が表示されます。

9) Ref-LS-Type

この LSA が参照する LSA の種別が表示されます。

0x2001 (Router)

: Router LSA を参照することを示します。

0x2002 (Network)

: Network LSA を参照することを示します。

10) Ref-Link-Id

この LSA が参照する LSA の Link State ID が表示されます。

Ref-LS-Type が Router の場合、0 が表示されます。

11) Ref-Adv-Rtr

この LSA が参照する LSA の広報元ルータ ID が表示されます。

12) Prefix

ルータ・ネットワークに存在するプレフィックス/プレフィックス長が表示されます。

13) Option

プレフィックスオプションが表示されます。

0x01 (-|-|-|NU)

: ユニキャスト計算に含まれないことを示します。

0x02 (-|-|LA|-)

: 広報ルータのインタフェースアドレスであることを示します。

0x04 (-|MC|-|-)

: マルチキャスト計算に含まれることを示します。

0x08 (P|-|-|-)

: NSSA 境界ルータで再広報される NSSA エリアプレフィックスであることを示します。

14) Metric

このプレフィックスのコストが表示されます。

41.2.4 show ipv6 ospf interface

[機能]

IPv6 OSPF インタフェース情報の表示

[適用機種]

Si-R G110

[入力形式]

show ipv6 ospf interface [detail]

[オプション]

なし

OSPF インタフェース情報を表示します。

detail

OSPF インタフェース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]

IPv6 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 IPv6 OSPF is configured.
```

原因：

IPv6 OSPF が設定されていません。または、定義が不足しており IPv6 OSPF が動作していません。

対処：

IPv6 OSPF を設定してください。

［実行例］

OSPF インタフェース情報詳細表示の場合

```
# show ipv6 ospf interface detail

lan0:                                                                  ---(1)
  Line physical status is (Up)                                         ---(2)
  Line ospf status is (DR), priority is 1, transmit delay is 1
   (3)                        (4)            (5)
  Interface ID 1, Instance ID 0                                        ---(6)
  Neighbor Count is 0, Adjacent neighbor count is 0                    ---(7)
  Internet Address 2001:db8:ffff:1000:20b:5dff:fe18:10/64,             ---(8)
  Link Local Address fe80::20b:5dff:fe18:10, Area 0.0.0.0
   (9)                                        (10)
  Timer intervals(in seconds): Hello 10, Dead 40, Wait 40, Retransmit 5  ---(11)
  Router ID 10.10.10.10, Network Type BROADCAST, Cost: 10
   (12)                      (13)                     (14)
  Designated Router ID 10.10.10.10
    Interface Address fe80::20b:5dff:fe18:10, Interface ID 1           ---(15)
  Backup Designated Router ID 0.0.0.0                                  ---(16)
  Next hello packet due in 00:00:00                                    ---(17)
  Packet statistics for 00:01:14                                   ---+---(18)
                      sent    received                                 |
    Hello:               7           0                               |
    Description:         0           0                               |
    Request:             0           0                               |
    Update:              0           0                               |
    Ack:                 0           0                           ---+

lan1:
  Line physical status is (Up)
  Line ospf status is (DR), priority is 1, transmit delay is 1
  Interface ID 2, Instance ID 0
  Neighbor Count is 1, Adjacent neighbor count is 1
  Internet Address 2001:db8:ffff:2000::11/64,
  Link Local Address fe80::20b:5dff:fe18:11, Area 0.0.0.1
  Timer intervals(in seconds): Hello 10, Dead 40, Wait 40, Retransmit 5
  Router ID 10.10.10.10, Network Type BROADCAST, Cost: 10
  Designated Router ID 10.10.10.10
    Interface Address fe80::20b:5dff:fe18:11, Interface ID 2
  Backup Designated Router ID 30.30.30.30
    Interface Address fe80::200:eff:fed0:bd53
  Next hello packet due in 00:00:08
  Packet statistics for 00:03:45
                      sent    received
    Hello:              23          20
    Description:         8           7
    Request:             1           4
    Update:             26          14
    Ack:                10          17
```

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 でのインタフェースの状態が表示されます。

   Down
   ： Down 状態であることを示します。

   DR
   ： 指定ルータであることを示します。

   BDR
   ： 副指定ルータであることを示します。

   Other
   ： 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
   ： Point-to-Point であることを示します。

Waiting

: DR/BDR 選出待ち状態であることを示します。

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 1

LSU パケット送信遅延時間が表示されます。

6) Interface ID 1, Instance ID 0

このインタフェースのインタフェース ID とインスタンス ID が表示されます。

7) 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。

8) Internet Address 2001:db8:ffff:1000:20b:5dff:fe18:10/64

このインタフェースのグローバルアドレスが表示されます。

9) Link Local Address fe80::20b:5dff:fe18:10

このインタフェースのリンクローカルアドレスが表示されます。

10) 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。

11) 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。

Wait

: DR/BDR 選出待ち時間を示します。

Retransmit

: パケット再送間隔の時間を示します。

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"

12) Router ID

ルータ ID が表示されます。

13) 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

: ブロードキャストネットワークを示します。

14) Cost

インタフェースの出力コストが表示されます。

15) Designated Router ID 10.10.10.10

Interface Address fe80::20b:5dff:fe18:10, Interface ID 1

指定ルータのルータ ID とそのインタフェースのリンクローカルアドレスとインタフェース ID が表示されます。

未決定の場合は 0.0.0.0 と表示されます。

16) Backup Designated Router ID 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のリンクアドレスが表示されます。

未決定の場合は 0.0.0.0 と表示されます。

17) Next hello packet due in

次の Hello が送信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)"

18) Packet statistics for

OSPF パケットの統計情報が表示されます。

統計情報には、OSPF パケット送受信数、および採取を開始してからの経過時間が表示されます。
本情報は OSPF インタフェースが活性状態の場合のみ表示されます。
ダウン状態となった場合、統計情報はクリアされます。

41.2.5 show ipv6 ospf neighbor

[機能]

IPv6 OSPF 隣接情報の表示

[適用機種]

Si-R G110

[入力形式]

show ipv6 ospf neighbor [detail]
show ipv6 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 IPv6 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 IPv6 OSPF is configured.
```

原因：
IPv6 OSPF が設定されていません。または、定義が不足しており IPv6 OSPF が動作していません。

対処：
IPv6 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］

OSPF 隣接情報表示の場合

```
# show ipv6 ospf neighbor

Neighbor information with all interfaces, result:

Neighbor with lan0 (DR) result:                                        ---(1)
 Neighbor ID            If ID Pri State          Deadtime   DDL  ReqL  RtrL
   (2)                   (3)  (4)  (5)            (6)       (7)   (8)   (9)
   20.20.20.20              1    1 Full/BDR      00:00:38    0     0     0
   30.30.30.30              1    1 Full/Other    00:00:39    0     0     0
```

1) Neighbor with lan0 (DR) result:
   本装置のインタフェース名とそのインタフェースの状態が表示されます。
   なお、インタフェースの状態は、ブロードキャストネットワークのときに表示されます。
   Down
   ： Down 状態であることを示します。
   Waiting
   ： 指定ルータ／副指定ルータ選出待ち状態であることを示します。
   DR
   ： 本装置が、指定ルータであることを示します。
   BDR
   ： 本装置が、副指定ルータであることを示します。
   Other
   ： 本装置が、指定ルータでも副指定ルータでもないことを示します。
2) Neighbor ID
   隣接ルータのルータ ID が表示されます。
3) If ID
   隣接ルータのインタフェース ID が表示されます。
4) Pri
   隣接ルータの指定ルータ優先度(Priority)が表示されます。
5) 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。

6) 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。

7) 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。

8) ReqL

リンクステート要求リスト中の LSA 数が表示されます。

9) RtrL

リンクステート再送リスト中の LSA 数が表示されます。

OSPF 隣接ルータ情報の詳細表示の場合

```
# show ipv6 ospf neighbor router-id 20.20.20.20 detail
Neighbor 20.20.20.20, interface address fe80::20b:5dff:fe18:14        ----(1)
   In the area 0.0.0.0 via interface lan0                              ----(2)
   Neighbor priority is 1, State is Full, 5 state changes, If id  1    ----(3)
   DR is 10.10.10.10, BDR is 20.20.20.20                               ----(4)
   Option is 0x13 (-|R|-|-|E|V6)                                       ----(5)
   Dead timer due in 00:00:33                                          ----(6)
   Neighbor is up for 00:00:46                                         ----(7)
   Database Summary List 0                                             ----(8)
   Link State Request List 0                                           ----(9)
   Link State Retransmission List 0                                    ----(10)
```

1) Neighbor 20.20.20.20, interface address fe80::20b:5dff:fe18:14

隣接ルータのルータ ID とリンクローカル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, 5 state changes, If id 1

隣接ルータの指定ルータ優先度、状態、状態の遷移回数、およびインタフェース ID が表示されます。

4) DR is 10.10.10.10, BDR is 20.20.20.20

指定ルータおよび副指定ルータのルータ ID が表示されます。

5) Option is 0x13 (-|R|-|-|E|V6)

Hello パケットに設定されたオプションが表示されます。

0x01 (-|-|-|-|-|V6)

：IPv6 をサポートしていることを示します。

0x02 (-|-|-|-|E|-)

：AS External LSA をサポートしていることを示します。

0x04 (-|-|-|MC|-|-)

：MOSPF をサポートしていることを示します。

0x08 (-|-|N|-|-|-)

：NSSA をサポートしていることを示します。

0x10 (-|R|-|-|-|-)

：ルーティング機能をサポートしていることを示します。

0x20 (DC|-|-|-|-|-)

：デマンドサーキットをサポートしていることを示します。

6) Dead timer due in 00:00:33

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 00:00:46

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。

41.2.6 clear ipv6 ospf statistics

[機能]

IPv6 OSPF 統計情報のクリア

[適用機種]

Si-R G110

[入力形式]

clear ipv6 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]

IPv6 OSPF 統計情報をクリアします。

[実行例]

```
# clear ipv6 ospf statistics
#
```

第 42 章 パケットの統計情報の表示、クリア操作コマンド

42.1 IPv4パケットの統計情報の表示、クリア

42.1.1 show ip traffic

[機能]

IP関連の統計情報の表示

[適用機種]

Si-R G110

[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]

```
# 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
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 because 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
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
#
```

42.1.2 clear ip traffic

[機能]

IP 関連の統計情報のクリア

[適用機種]

Si-R G110

[入力形式]

clear ip traffic

[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 関連の統計情報をクリアします。

[実行例]

```
# clear ip traffic
#
```

42.2 IPv6パケットの統計情報の表示、クリア

42.2.1 show ipv6 traffic

[機能]

IPv6パケットの統計情報の表示

[適用機種]

Si-R G110

[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]

```
# 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
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
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
#
```

42.2.2 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 G110

[入力形式]

clear ipv6 traffic

[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 パケットの統計情報をクリアします。

[実行例]

```
# clear ipv6 traffic
#
```

第 43 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

43.1 IPv4 フィルタのカウンタ・ログ・統計・状態などの表示、クリア

43.1.1 show ip filter

[機能]

IP フィルタテーブル表示

[適用機種]

Si-R G110

[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］

```
# 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                             proto SYN remain
              dst(src) IP/mask:port
 [  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行います。

・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 と表示されます。
21) SPI フィルタテーブル数

43.1.2 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 G110

[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]

```
# 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

43.1.3 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 G110

[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]

```
# show ip filter summary total
[lan0]---(1)
IPv4 filter
  static table                          1---(2)
  dynamic table                         0---(3)
  SPI table                             1---(4)

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

43.1.4 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 G110

[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
#
```

43.2 IPv6 フィルタのカウンタ・ログ・統計・状態などの表示、クリア

43.2.1 show ipv6 filter

[機能]

IPv6 フィルタテーブル表示

[適用機種]

Si-R G110

[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]

```
# 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行います。
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 と表示されます。
20) SPI フィルタテーブル数
21) Traffic Class 値

43.2.2 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 G110

[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]

```
# 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

43.2.3 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 G110

[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]

```
# show ipv6 filter summary total
[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

43.2.4 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 G110

[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 44 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

44.1 IPv4 IDSのカウンタ・ログ・統計・状態などの表示、クリア

44.1.1 show ip ids statistics

[機能]

IDSの統計情報の表示

[適用機種]

Si-R G110

[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］

```
# 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とき
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とき
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

44.1.2 clear ip ids statistics

[機能]

IDS の統計情報のクリア

[適用機種]

Si-R G110

[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 45 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

45.1 NATのカウンタ・ログ・統計・状態などの表示

45.1.1 show ip nat

[機能]

NAT変換テーブルの表示

[適用機種]

Si-R G110

[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］

```
# show ip nat
nat table is normal   ---(1)
[rmt0]  ---(2)
ap 0: ap-001
-(3)- -(4)--
dynamic NAT table queue
table:3   ---(5)
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
-(6)-- ------(7)------ -(8)- ----(9)---- (10)      -----(11)----- -(12)-  -(13)-
[   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
[   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         10.36.195.136         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) NAT 変換テーブル数の拡張状態

nat table is normal

通常動作

2) インタフェース名
3) 接続先定義番号
4) 接続先名
5) 変換テーブル数
6) 変換テーブル通番
7) グローバル IP アドレス
8) グローバルポート番号、またはグローバル ICMP_ID
9) プライベート IP アドレス
10) プライベートポート番号、またはプライベート ICMP_ID
11) 相手側 IP アドレス
12) 相手側ポート番号
13) 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 と表示されます。

45.1.2 show ip nat statistics

[機能]

NAT の統計情報の表示

[適用機種]

Si-R G110

[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]

```
# show ip nat statistics
nat table is normal   ---(1)
           to Global   to Private
translate         85 ---(2)    63 ---(3)
error              0 ---(4)     0 ---(5)

            fragment
translate          0 ---(6)
error              0 ---(7)

             current         peak        limit
nat table         12 ---(8)    12 ---(9) 23031 ---(10)

error accounting
  lack of memory                0 ---(11)
  table not found               0 ---(12)
  too small packet              0 ---(13)
  same node                     0 ---(14)
  other reason                  0 ---(15)
```

1) NAT 変換テーブル数の拡張状態
   nat table is normal
   通常動作
2) プライベート→グローバル変換回数
3) グローバル→プライベート変換回数
4) プライベート→グローバルエラー発生回数
5) グローバル→プライベートエラー発生回数
6) フラグメントパケットの正常変換回数
7) フラグメントパケットのエラー発生回数
8) 現在使用中の NAT 変換テーブル個数
9) 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)
10) NAT 変換テーブルの最大制限個数
11) メモリ枯渇回数
12) 変換テーブルにないパケットの受信回数

13) 異常に短いパケットの受信回数

14) dynamic NAT table queue に接続された既存の NAT 変換テーブルとプライベート IP アドレス、プライベートポート番号、相手側 IP アドレス、相手側ポート番号、プロトコル番号が同一の NAT 変換テーブルをさらに dynamic NAT table queue に接続しようとして失敗した回数、および、dynamic NAT table queue に接続された既存の NAT 変換テーブルとグローバル IP アドレス、グローバルポート番号、相手側 IP アドレス、相手側ポート番号、プロトコル番号が同一の NAT 変換テーブルをさらに dynamic NAT table queue に接続しようとして失敗した回数の合計

15) その他のエラー回数

45.1.3 show ip nat summary

[機能]

NAT 変換テーブル数の表示

[適用機種]

Si-R G110

[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]

```
# show ip nat summary
nat table is normal   ---(1)
[rmt0]  ---(2)
ap 0: ap-001
-(3)- -(4)--
dynamic NAT table queue
table:3   ---(5)
application table queue
table:1
static NAT table queue
table:3
address table queue
table:1
```

1) NAT 変換テーブル数の拡張状態

nat table is normal

通常動作

2) インタフェース名
3) 接続先定義番号
4) 接続先名
5) 変換テーブル数

45.2 NATのカウンタ・ログ・統計などのクリア

45.2.1 clear ip nat statistics

[機能]

NATの統計情報のクリア

[適用機種]

Si-R G110

[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 46 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

46.1 マルチキャストのカウンタ・ログ・統計・状態などの表示

46.1.1 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 G110

[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]

```
# show ip multicast group
IPv4 Multicast Groups

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 IPv4 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

46.1.2 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 G110

[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]

```
# 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

46.1.3 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 G110

[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]

```
# 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

46.1.4 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 G110

[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]

```
# 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
   スタティック RP の場合は infinity と表示されます。
7) RP の総数

46.1.5 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 G110

[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]

```
# 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

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。

46.1.6 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 G110

[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]

```
# show ip multicast route
IPv4 Multicast Routing Table

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・ルータを再び元に戻します。

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。

46.1.7 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 G110

[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]

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

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

46.1.8 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 G110

[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]

```
# 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

46.1.9 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 G110

[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]

```
# show ip multicast statistics
IPv4 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

46.2 マルチキャストのカウンタ・ログ・統計などのクリア

46.2.1 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 G110

[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]

```
# clear ip multicast interface statistics
#
```

46.2.2 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 G110

[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]

```
# clear ip multicast route kernel statistics
#
```

46.2.3 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 G110

[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]

```
# clear ip multicast statistics
#
```

第 47 章 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

47.1 IPv4 DHCP のカウンタ・ログ・統計・状態などの表示

47.1.1 show ip dhcp

[機能]

IPv4 DHCP 運用状況の表示

[適用機種]

Si-R G110

[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、DECLINE メッセージによる配布不可能な IP アドレスおよび期間を表示します。

配布不可能な IP アドレスが存在しない場合、DECLINE IP Address List は表示されません。

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］

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)
DNS Server Address        : 192.168.1.1                   ---(4)
TIME Server Address       : 192.168.1.1                   ---(5)
NTP Server Address        : 192.168.1.1                   ---(6)
WINS Server Address       : 192.168.1.1                   ---(7)
SIP Server Name/Address   : 192.168.1.1                   ---(8)
Domain Name               : fujitsu.com                   ---(9)
Lease Time                : 0001.00:00:00                 ---(10)

Active Client List:
No.  IP address        MAC address         Lease remain
--- ----------------   -----------------   -------------
(11)(12)               (13)                (14)
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

DECLINE IP Address List:
No.  IP address          Reusable time
--- ----------------     -------------
    (15)                 (16)
001 192.168.1.7          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 DNS サーバアドレス
5) 配布タイムサーバアドレス
6) 配布 NTP サーバアドレス
7) 配布 WINS サーバアドレス
8) 配布 SIP サーバアドレス
9) 配布ドメイン名
10) リース時間
11) 通番
12) IP アドレス
13) MAC アドレス
14) 残りリース時間
15) 配布不可能な IP アドレス
16) 配布不可能な時間

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       : 192.168.1.1                  ---(5)
NTP Server Address        : 192.168.1.1                  ---(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              : Fri Mar  4 11:48:19 2011     ---(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

47.2 IPv6 DHCP のカウンタ・ログ・統計・状態などの表示、クリア

47.2.1 show ipv6 dhcp

[機能]

IPv6 DHCP 運用状況の表示

[適用機種]

Si-R G110

[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

配布アドレス／プレフィックス情報、リース中のアドレス／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 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。

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、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］

IPv6 DHCP サーバの場合

```
# show ipv6 dhcp

[rmt0] IPv6 DHCP Server Informations

Server DUID               : 0003000100000e58a00b ---(1)
Server Preference         : 0 ---(2)
Lease Address             : from 2001:db8::100 ---(3)
                            to   2001:db8::1ff ---(4)
DNS Server Address        : 2001:db8::1 ---(5)
                            2001:db8::3 ---(6)
DNS Domain Name           : fujitsu.com ---(7)
SIP Server Address        : 2001:db8::2 ---(8)
                            2001:db8::4 ---(9)
SIP Domain Name           : voip.fujitsu.com ---(10)
                            voip2.fujitsu.com ---(11)
SNTP Server Address       : 2001:db8::9 ---(12)
                            2001:db8::10 ---(13)

Active Client List:
No.  IPv6 address                              Lease remain
     Client DUID                               IAID
--- ---------------------------------------- -------------
(14)(15)                                       (16)
001 2001:db8::100                              0000.23:59:00
    (17)                                       (18)
    000100010d9e75e70019db134032                134224347

Active PD Client:
--------------------------------------------------------------------------------
Client DUID             : 0003000100000a65f034 ---(19)
IAID                    : 2 ---(20)
Prefix/Prefixlen        : 2001:db8::/48 ---(21)
Preferred Lifetime      : infinity ---(22)
Valid Lifetime          : infinity ---(23)
Delegated Time          : Fri Mar  4 11:48:19 2011 ---(24)
Lease remain            : infinity ---(25)
#
```

1) サーバ DUID
2) サーバプリファレンス値
3) 割り当て先頭 IPv6 アドレス
4) 割り当て末尾 IPv6 アドレス
5) 配布 DNS サーバアドレス
6) 配布セカンダリ DNS サーバアドレス
7) 配布 DNS ドメイン名
8) 配布 SIP サーバアドレス
9) 配布セカンダリ SIP サーバアドレス
10) 配布 SIP ドメイン名
11) 配布セカンダリ SIP ドメイン名
12) 配布 SNTP サーバアドレス
13) 配布セカンダリ SNTP サーバアドレス
14) 通番
15) 配布 IPv6 アドレス
16) 残りリース時間
17) クライアントの DUID
18) クライアントの IAID
19) PD クライアントの DUID
20) PD クライアントの IAID
21) 配布プレフィックス
22) Preferred Lifetime

23) Valid Lifetime
24) 配布時間
25) リース有効期限

IPv6 DHCP リレーエージェントの場合

```
# show ipv6 dhcp

[rmt0] IPv6 DHCP Relay Agent Information

Forwarding Interface   : lan0 ---(1)
Forwarding DHCP Server : ff05::1:3 ---(2)
#
```

1) リレー先インタフェース
2) リレー先サーバアドレス

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               : 0003000100000e58a00b ---(3)
Server DUID               : 000100010ee29225000d56918090 ---(4)
Server Preference         : 0 ---(5)
DNS Server Address        : 2001:db8::1 ---(6)
                            2001:db8::3 ---(7)
DNS Domain Name           : fujitsu.com ---(8)
SIP Server Address        : 2001:db8::2 ---(9)
                            2001:db8::4 ---(10)
SIP Domain Name           : voip.fujitsu.com ---(11)
                            voip2.fujitsu.com ---(12)
SNTP Server Address       : 2001:db8::9 ---(13)
                            2001:db8::10 ---(14)
IPv6 Address
  Assigned Time           : Fri Mar  4 11:48:19 2011 ---(15)
  Uptime                  : 0000.00:00:41 ---(16)
  T1 (Renewal Time)       : infinity ---(17)
  T2 (Rebind Time)        : infinity ---(18)
  Preferred Lifetime      : infinity ---(19)
  Valid Lifetime          : infinity ---(20)
  Address                 : 2001:db8:1234::abcd ---(21)
Prefix Delegation
  Delegated Time          : Fri Mar  4 11:48:19 2011 ---(22)
  Uptime                  : 0000.00:00:41 ---(23)
  T1 (Renewal Time)       : infinity ---(24)
  T2 (Rebind Time)        : infinity ---(25)
  Preferred Lifetime      : infinity ---(26)
  Valid Lifetime          : infinity ---(27)
  Prefix/Prefixlen        : 2001:db8::/48 ---(28)

Assign Interface List
-------------------------------------------------------------------------------
I/F Name   Prefix/Prefixlen
rmt1       2001:db8:0:1::/64 ---(29)
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 DNS ドメイン名
9) 獲得 SIP サーバアドレス

10) 獲得セカンダリ SIP サーバアドレス
11) 獲得 SIP ドメイン名
12) 獲得セカンダリ SIP ドメイン名
13) 獲得 SNTP サーバアドレス
14) 獲得セカンダリ SNTP サーバアドレス
15) IPv6 アドレス獲得時間
16) IPv6 アドレス獲得からの経過時間
17) 獲得 IPv6 アドレスの T1 時間
18) 獲得 IPv6 アドレスの T2 時間
19) 獲得 IPv6 アドレスの Preferred Lifetime
20) 獲得 IPv6 アドレスの Valid Lifetime
21) 獲得 IPv6 アドレス
22) プレフィックス獲得時間
23) プレフィックス獲得からの経過時間
24) 獲得プレフィックスの T1 時間
25) 獲得プレフィックスの T2 時間
26) 獲得プレフィックスの Preferred Lifetime
27) 獲得プレフィックスの Valid Lifetime
28) 獲得プレフィックス
29) 割り当てプレフィックス情報

47.2.2 clear ipv6 dhcp server

[機能]

IPv6 DHCP サーバ情報のクリア

[適用機種]

Si-R G110

[入力形式]

clear ipv6 dhcp server

[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]

DHCP の以下の情報をクリアします。

IPv6 DHCP サーバのリース情報クリア

IPv6 DHCP サーバのリース情報をクリアします。

[実行例]

```
# clear ipv6 dhcp server
#
```

第 48 章 動的 VPN の状態などの表示、情報の削除コマンド

48.1 動的VPNの情報交換クライアントの状態などの表示

48.1.1 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 G110

[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]

```
# 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

: 登録済み

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、ポート番号が表示されます。

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。

48.1.2 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 G110

[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]

```
# show dvpn client session
No.(1)  Status (2)    Elapsed Time   Expire    Session ID (5)
        User Agent Client (6) (3)       (4)
        User Agent Server (7)
------  ------------------------------------------------------------
[0001]  CONNECTED     0000.00:00:30     300            1
       *IPsecIKE)20010db8000000000000000000000000/64@fujitsu.com
        IPsecIKE)20010db8000000001000000000000000/64@fujitsu.com
[0002]  INVITE        0000.00:00:00  infinity          2
        TOKYO@fujitsu.com
       *KAWASAKI@fujitsu.com
[0003]  CONNECTED     0000.00:00:45     300            3
       *IPsecIKE)c0a80100/24@fujitsu.com
        IPsecIKE)c0a80200/24@fujitsu.com

Total Sessions      3   (8)
#

# show dvpn client session summary
Total Sessions      3
#
```

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) Session ID
セッション ID が表示されます。
6) 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。
7) User Agent Server
セッションの着呼側ユーザ 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。
8) Total Sessions
セッションの合計数が表示されます。

48.2 動的VPNサーバの状態などの表示

48.2.1 show dvpn server

[機能]

動的VPNサーバ情報の表示

[適用機種]

Si-R G110

[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]

```
# 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。

48.2.2 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 G110

[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]

```
# 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が表示されます。

4) Trs
登録されているトランスポート種別が表示されます。

UDP
: UDPで通信

5) Contact
登録されているユーザのContactアドレス、ポート番号が表示されます。
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。

48.2.3 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 G110

[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]

```
# 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が表示されます。

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。

48.3 動的VPNサーバの情報の削除

48.3.1 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 G110

[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]

```
# clear dvpn server user
#
```

48.3.2 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 G110

[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]

```
# clear dvpn server session
#
```

第 49 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

49.1 IPsec/IKE のカウンタ・ログ・統計・状態などの表示

49.1.1 show ipsec sa

[機能]

システムの IPsec SA 情報の表示

[適用機種]

Si-R G110

[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]

(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 2012), 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 2012), 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 2012), 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 2012), 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 2012), 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 2012), 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 2012), 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 2012), 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 2012), 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 2012), 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 2012), 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 2012), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(0Kbyte), Current(1Kbyte), Remain(0Kbyte)

[13]    Remote Name(ISP-3), rmt6, ap0
        Side(Initiator), Gateway(210.1.2.1, 210.1.1.1), OUT
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=171237444(0x0a34e050), ESN(enable)
        Created(Jun 26 17:59:03 2012), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(0Kbyte), Current(300Kbyte), Remain(0Kbyte)

[14]    Remote Name(ISP-3), rmt6, 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(0x0ad7c851), ESN(enable)
        Created(Jun 26 17:59:03 2012), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(0Kbyte), Current(200Kbyte), Remain(0Kbyte)

[15]    Remote Name(ISP-4), rmt7, ap0
        Side(Initiator), Gateway(2001:db8:15:2::38, 2001:db8:15:1::38), OUT
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=171237446(0x0a34e052), ESN(enable)
        Created(Jun 26 17:59:03 2012), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(0Kbyte), Current(50Kbyte), Remain(0Kbyte)

[16]    Remote Name(ISP-4), rmt7, ap0
        Side(Initiator), Gateway(2001:db8:15:1::38, 2001:db8:15:2::38), IN
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=181913671(0x0ad7c853), ESN(enable)
        Created(Jun 26 17:59:03 2012), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(0Kbyte), Current(50Kbyte), 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)
        IKE Version(1), Authmethod(shared-key), DPD(disable)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        Created(Jun 26 17:59:03 2012)
        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)
        IKE Version(1), Authmethod(rsa-signature), DPD(disable)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        Created(Jun 26 17:59:03 2012)
        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)
        IKE Version(1), Authmethod(shared-key), DPD(disable)
        Enctype(3des-cbc), Hashtype(hmac-sha1), PFS(modp1024)
        Created(Jun 26 17:59:03 2012)
        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)
        IKE Version(1), Authmethod(shared-key), DPD(enable)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        Created(Jun 26 17:59:03 2012)
        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)
        IKE Version(1), Authmethod(shared-key), DPD(enable)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        Created(Jun 26 17:59:03 2012)
        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)
        IKE Version(1), Authmethod(shared-key), DPD(enable)
        Enctype(3des-cbc), Hashtype(hmac-sha1), PFS(modp1024)
        Created(Jun 26 17:59:03 2012)
        Lifetime(86400sec), Current(10sec), Remain(86390sec)
        NAT-T VendorID(0x4a131c81070358455c5728f20e95452f)

[7]     Destination(210.1.1.1.500), Source(210.1.2.1.500), rmt6
        Cookies(2ee33635dcc2a837:ece2a45bc12889ef)
        Side(Initiator), Status(ESTABLISHED)
        IKE Version(2), Authmethod(shared-key), PRF(hmac-md5), DPD(disable)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768), EAP(disable)
        Created(Jun 26 17:59:03 2012)
        Lifetime(86400sec), Current(10sec), Remain(86390sec)
```

```
[8]     Destination(2001:db8:15:1::38.500), Source(2001:db8:15:2::38.500), rmt7
        Cookies(6ee33635dcc2a837:dce2a45bc12889ef)
        Side(Initiator), Status(ESTABLISHED)
        IKE Version(2), Authmethod(rsa-signature), PRF(hmac-md5), DPD(disable)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768), EAP(disable)
        Created(Jun 26 17:59:03 2012)
        Lifetime(86400sec), Current(10sec), Remain(86390sec)
```

(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)
        IKE Version(1), Authmethod(shared-key), DPD(disable)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        Created(Jun 26 17:59:03 2012)
        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)
        IKE Version(1), Authmethod(rsa-signature), DPD(disable)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        Created(Jun 26 17:59:03 2012)
        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)
        IKE Version(1), Authmethod(shared-key), DPD(disable)
        Enctype(3des-cbc), Hashtype(hmac-sha1), PFS(modp1024)
        Created(Jun 26 17:59:03 2012)
        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)
        IKE Version(1), Authmethod(shared-key), DPD(enable)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        Created(Jun 26 17:59:03 2012)
        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)
        IKE Version(1), Authmethod(shared-key), DPD(enable)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        Created(Jun 26 17:59:03 2012)
        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)
        IKE Version(1), Authmethod(shared-key), DPD(enable)
        Enctype(3des-cbc), Hashtype(hmac-sha1), PFS(modp1024)
        Created(Jun 26 17:59:03 2012)
        Lifetime(86400sec), Current(10sec), Remain(86390sec)
        NAT-T VendorID(0x4a131c81070358455c5728f20e95452f)

[7]     Destination(210.1.1.1.500), Source(210.1.2.1.500), rmt6
        Cookies(2ee33635dcc2a837:ece2a45bc12889ef)
        Side(Initiator), Status(ESTABLISHED)
        IKE Version(2), Authmethod(shared-key), PRF(hmac-md5), DPD(disable)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768), EAP(disable)
        Created(Jun 26 17:59:03 2012)
        Lifetime(86400sec), Current(10sec), Remain(86390sec)

[8]     Destination(2001:db8:15:1::38.500), Source(2001:db8:15:2::38.500), rmt7
        Cookies(6ee33635dcc2a837:dce2a45bc12889ef)
        Side(Initiator), Status(ESTABLISHED)
        IKE Version(2), Authmethod(rsa-signature), PRF(hmac-md5), DPD(disable)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768), EAP(disable)
        Created(Jun 26 17:59:03 2012)
        Lifetime(86400sec), Current(10sec), Remain(86390sec)
```

(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 2012), 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 2012), 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 2012), 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 2012), 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 2012), 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 2012), 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 2012), 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 2012), 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 2012), 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 2012), 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 2012), 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 2012), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(0Kbyte), Current(1Kbyte), Remain(0Kbyte)

[13]    Remote Name(ISP-3), rmt6, ap0
        Side(Initiator), Gateway(210.1.2.1, 210.1.1.1), OUT
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=171237444(0x0a34e050), ESN(enable)
        Created(Jun 26 17:59:03 2012), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(0Kbyte), Current(300Kbyte), Remain(0Kbyte)

[14]    Remote Name(ISP-3), rmt6, 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(0x0ad7c851), ESN(enable)
        Created(Jun 26 17:59:03 2012), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(0Kbyte), Current(200Kbyte), Remain(0Kbyte)

[15]    Remote Name(ISP-4), rmt7, ap0
        Side(Initiator), Gateway(2001:db8:15:2::38, 2001:db8:15:1::38), OUT
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=171237446(0x0a34e052), ESN(enable)
        Created(Jun 26 17:59:03 2012), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(0Kbyte), Current(50Kbyte), Remain(0Kbyte)

[16]    Remote Name(ISP-4), rmt7, ap0
        Side(Initiator), Gateway(2001:db8:15:1::38, 2001:db8:15:2::38), IN
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=181913671(0x0ad7c853), ESN(enable)
        Created(Jun 26 17:59:03 2012), NewSA(23040sec, 3276Kbyte)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        Lifebyte(0Kbyte), Current(50Kbyte), 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), ESN(enable)
        --------------  --------------------------  -----------
             (15)           (16)                        (17)
        Created(Apr 26 17:59:03 2012), NewSA(23040sec, 3276Kbyte)
        ------------------------------  ----------------------------
             (18)                            (19)
        Lifetime(28800sec), Current(332sec), Remain(28468sec)
        ------------------  ---------------  -----------------
             (20)                (21)              (22)
        Lifebyte(4096Kbyte), Current(2528Kbyte), Remain(1568Kbyte)
        -------------------  -------------------  ------------------
             (23)                (24)              (25)
```

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) ポリシーの方向

OUT:
出力用ポリシー

IN:
入力用ポリシー

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
※SHA2 の場合、"hmac-sha"に続く数字は鍵長を表しています。
ただし、SHA1 の場合、"hmac-sha1"と表示されます。
14) PFS 使用時の DH(Diffie-Hellman)グループ

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)

modp2048 :
Diffie-Hellman グループの MODP2048(グループ 14)

off :
Diffie-Hellman グループを使用しません。
※IKE Version2 初回接続時には"off"で動作します。

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) ESN(Extended Sequence Number:拡張シーケンス番号)の有無
IKE Version2 使用時のみ表示されます。
18) IPsec SA 作成時間(秒)
19) 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)

20) IPsec SA 有効時間(秒)
21) IPsec SA 作成からの経過時間(秒)
22) IPsec SA 削除までの残存時間(秒)
23) IPsec SA 有効パケット量(キロバイト)
24) 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

25) 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)
        IKE Version(2), Authmethod(shared-key), PRF(hmac-md5), DPD(disable)
        --------------  ----------------------  -------------  ------------
             (10)             (11)                  (12)         (13)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768) EAP(disable)
        ----------------  ------------------  ------------ -----------
             (14)             (15)                  (16)     (17)
        Created(Apr 26 17:59:03 2012)
        -----------------------------
             (18)
        Lifetime(86400sec), Current(10sec), Remain(86390sec)
        ------------------  --------------  ----------------
             (19)             (20)              (21)
        NAT-T VendorID(0x7d9419a65310ca6f2c179d9215529d56)
        --------------------------------------------------
             (22)
```

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

IKE Version1 の場合は以下が表示されます。

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。

IKE Version2の場合は以下が表示されます。

IKE_INIT_SA_SENT
IKE_INIT_SA_RECEIVED
IKE_AUTH_SENT
IKE_AUTH_RECEIVED
CREATE_CHILD_SA_SENT
CREATE_CHILD_SA_RECEIVED
ESTABLISHED
EXPIRED

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

※ IKE Version2使用時には表示されません。

10) IKEバージョン

1:
IKE Version1

2:
IKE Version2

11) 認証方式

shared-key:
共有鍵認証方式

rsa-signature:
RSAデジタル署名認証方式

none:
未使用(IKEv2のみ)

なし:
ネゴシエーション中(IKEv2のみ)

12) PRF(Pseudo-Random Function:擬似乱数関数)

※ IKE Version1使用時には表示されません。

13) DPD(Dead Peer Detection)の使用

disable:
未使用

enable:
使用

※ IKE Version1使用時には、自装置と相手装置でDPDの使用が確認された場合"enable"と表示します。

14) 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。

15) 認証アルゴリズム

※SHA2の場合、"hmac-sha"に続く数字は鍵長を表しています。
ただし、SHA1の場合、"hmac-sha1"と表示されます。

16) PFSグループ

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)
modp2048：
Diffie-Hellman グループの MODP2048(グループ 14)

17) EAP(Extensible Authentication Protocol)の使用
disable:
未使用
enable:
使用
※ IKE Version1 使用時には表示されません。

18) IKE SA 作成時間
19) IKE SA 有効時間(秒)
20) IKE SA 作成からの経過時間(秒)
21) IKE SA 削除までの残存時間(秒)
22) 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

49.1.2 show ike statistics

[機能]

IKE 統計情報表示

[適用機種]

Si-R G110

[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ときに、インタフェース IKE 統計情報がクリアされます。

[実行例]

```
# 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 Dead Peer Detection               ---(30)
                        0 invalid replay check(DPD)         ---(31)
                        0 others Notify Message             ---(32)
                        0 invalid Notify Message type       ---(33)
                0 there is no valid ISAKMP-SA               ---(34)
                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   ---(35)
                0 invalid Vendor ID
                0 invalid NAT Discovery
                0 invalid NAT Original Address
                0 invalid Next Payload type
        0 Quick Mode Exchange                               ---(36)
                0 there is no valid ISAKMP-SA               ---(37)
                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                               ---(38)
        0 Acknowledged Informational Exchange               ---(39)
        0 invalid Exchange type                             ---(40)
sent isakmp packet:
 0 isakmp packet send error                                 ---(41)
 0 total isakmp packet sent                                 ---(42)
sent isakmp packet phase1:
        0 isakmp phase1 packet resent                       ---(43)
        0 phase1 give up                                    ---(44)
sent isakmp packet phase2:
        0 isakmp phase2 packet resent                       ---(45)
        0 phase2 give up                                    ---(46)
sent isakmp packet information:
        0 No Proposal Chosen                                ---(47)
        0 Initial Contact                                   ---(48)
        0 Dead Peer Detection                               ---(49)
        0 others Notify Message                             ---(50)
others:
        0 phase1 count > phase1_max                         ---(51)
        0 encrypting failed                                 ---(52)
        0 decrypting failed                                 ---(53)
        0 failed to create inbound IPsec SA                 ---(54)
        0 failed to create outbound IPsec SA                ---(55)
        0 IKE SA information no entry                       ---(56)
        0 IPsec SA information no entry                     ---(57)
        0 shared key no entry                               ---(58)
        0 IPsec remote interface Down                       ---(59)
        0 invalid remote address                            ---(60)
        0 invalid local address                             ---(61)
```

```
        0 failed to allocate buffer                          ---(62)
        0 radius/aaa authentication succeeded                ---(63)
        0 radius/aaa authentication failed                   ---(64)
        0 access interface allocation failed                 ---(65)
        0 resolving of FQDN failed                           ---(66)
        0 resolving of RA address failed                     ---(67)
        0 other                                              ---(68)
#
```

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) ベンダー 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) 相手到達確認(DPD)メッセージ受信数
31) 相手到達確認(DPD)メッセージシーケンス番号不正
32) その他の通知メッセージ受信数
33) 無効な通知メッセージの受信数
34) ISAKMP SA がない Informational 受信数
35) 無効な削除メッセージ受信数
36) Quick Mode 受信数
37) ISAKMP SA がない Quick Mode 受信数
38) New group Mode 受信数
39) Acknowledged Informational 受信数
40) 無効な交換タイプ受信数
41) パケット送信エラー数
42) 送信パケットの合計数
43) Phase1 パケット再送数
44) Phase1 ネゴシエーション失敗数
45) Phase2 パケット再送数

46) Phase2 ネゴシエーション失敗数
47) SA Proposal が受け入れられない通知メッセージ送信数
48) 初めての SA 確立通知メッセージ送信数
49) 相手到達確認(DPD)メッセージ送信数
50) その他の通知メッセージ送信数
51) 装置内での ISAKMP SA 最大数超過数
52) ISAKMP パケット暗号化失敗数
53) ISAKMP パケット復号化失敗数
54) 受信用 IPsec SA 作成失敗数
55) 送信用 IPsec SA 作成失敗数
56) IKE SA 情報検索失敗数
57) IPsec SA 情報検索失敗数
58) 共有鍵検索失敗
59) 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
60) 相手側アドレス不正数
61) 自側アドレス不正数
62) 領域獲得失敗数
63) RADIUS/AAA 認証成功数
64) RADIUS/AAA 認証失敗数
65) アクセスインタフェース獲得失敗数
66) FQDN 名前解決失敗数
67) RA アドレス取得失敗数
68) 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

49.2 IPsec/IKE のカウンタ・ログ・統計などのクリア

49.2.1 clear ike statistics

[機能]

IKE 統計情報のクリア

[適用機種]

Si-R G110

[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 50 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

50.1 VRRPのカウンタ・ログ・統計・状態などの表示

50.1.1 show vrrp

[機能]

VRRP機能の各種情報の表示

[適用機種]

Si-R G110

[入力形式]

show vrrp [interface <interface_name> [vrid <vrid>]] [brief]

[オプション]

なし

稼動しているすべての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-R G110

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、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、本装置で稼動しているすべての 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:00:02:0a                              ---(11)
    Virtual Router IP Address:
        fe80::1                                                          ---(12)
    VRRP advertisement interval 1                                        ---(13)
    Shutdown interface trigger:
        lan1   reduce 200  OFF                                           ---(14)
        rmt11  reduce 100  OFF
    Shutdown route trigger:
        2001:db8::/32      lan0   reduce 100  OFF                        ---(15)
        10.232.79.200/32   rmt1   reduce 100  OFF
    Shutdown node trigger:
        192.168.100.100    rmt0   reduce 254  OFF                        ---(16)
        2001:db8:dd72::5   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/HopLimit 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/HopLimit 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/HopLimit 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

50.2 VRRPのカウンタ・ログ・統計などのクリア

50.2.1 clear vrrp statistics

[機能]

VRRP統計情報のクリア

[適用機種]

Si-R G110

[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 51 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

51.1 ブリッジのカウンタ・ログ・統計・状態などの表示

51.1.1 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 G110

[入力形式]

show bridge
show bridge vlan <vid>
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。

vlan <vid>
指定された VLAN で学習された学習テーブルの内容を表示します。
・ VLAN ID
VLAN ID を、1～4094 の 10 進数で指定します。

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, A - Authenticated entry
Address           VLAN Interface       Status
----------------- ---- --------------- ------
(1)               (2)  (3)             (4)
00:0e:00:78:2f:7a 10   ether 1 1       D
00:a0:c9:f0:20:e9 20   ether 2 1       D
8c:73:6e:b3:01:01 10   cpu 0           S
8c:73:6e:b3:01:02 20   cpu 1           S
```

1) 学習テーブルに登録されている MAC アドレス
2) VLAN ID
3) エントリされた端末が存在するポート
ether
ether ポート
4) 学習テーブルの状態
以下のいずれかが表示されます。
D
動的学習テーブル

A

動的学習テーブル(認証成功端末)

S

静的学習テーブル

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 :     4                          ---(1)
    Dynamic entry         :     2                          ---(2)
    Static entry          :     2                          ---(3)
    Authenticated entry   :     0                          ---(4)
    System entry          :     0                          ---(5)
Free station blocks       :  8188                          ---(6)
```

1) 使用中の学習テーブル数
2) 動的学習による学習テーブル数
3) 静的学習による学習テーブル数
4) 動的学習による学習テーブル数(認証成功端末)
5) 装置内部使用による学習テーブル数
6) 未使用の学習テーブル数

51.2 ブリッジのカウンタ・ログ・統計・状態などのクリア

51.2.1 clear bridge

[機能]

動的に学習したテーブルの初期化

[適用機種]

Si-R G110

[入力形式]

```
clear bridge
clear bridge vlan <vid>
clear bridge mac <macaddr> <vid>
```

[オプション]

なし

動的に学習されているすべての MAC アドレスを学習テーブルから削除します。

vlan <vid>

指定された VLAN で学習されているすべての MAC アドレスを学習テーブルから削除します。

・ VLAN ID
  VLAN ID を、1～4094 の 10 進数で指定します。

mac <macaddr> <vid>

指定された VLAN で学習されている指定された MAC アドレスを学習テーブルから削除します。

・ MAC アドレス
  学習テーブルから削除する MAC アドレスを指定します。
  (XX:XX:XX:XX:XX:XX の形式で、XX は 2 桁の 16 進数です。)
・ VLAN ID
  VLAN ID を、1～4094 の 10 進数で指定します。

[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]

動的に学習されている MAC アドレスを学習テーブルから削除します。

[注意]

以下のアドレスは削除されません。

・ vlan forward コマンド定義によって静的に登録されたアドレス

[実行例]

```
# clear bridge
#
```

51.3 スパニングツリーのカウンタ・ログ・統計・状態などの表示

51.3.1 show spanning-tree

[機能]

スパニングツリー情報の表示

[適用機種]

Si-R G110

[入力形式]

```
show spanning-tree
show spanning-tree root
show spanning-tree bridge
show spanning-tree active
show spanning-tree interface ether group <group> port <port>
show spanning-tree detail
```

[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 ether group <group> port <port>
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。

[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］

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
Spanning tree enabled protocol IEEE
Root ID     Priority    32768                                          ---(1)
            Address     00:00:e2:08:57:89                              ---(2)
            Cost        200000                                         ---(3)
            Port        3 (ether 2 1)                                  ---(4)
            Hello Time 2sec  Max Age 20sec  Forward Delay 15sec
            ---------------  -------------  --------------------
            (5)              (6)            (7)
Bridge ID   Priority    32768                                          ---(8)
            Address     00:0b:5d:89:00:aa                              ---(9)
            Hello Time 2sec  Max Age 20sec  Forward Delay 15sec
            ---------------  -------------  --------------------
            (10)             (11)           (12)
            STP Mode stp
            ------------
            (13)

Interface       Port ID  Cost        Status(Role)            Sent
                                     Designated Bridge ID    Received
--------------- -------- ----------- ----------------------- ----------
ether 2 1          128.3     200000* Forwarding(Root)                5
---------          -----     ------- -----------------              ---
(14)               (15)      (16)    (17)                           (18)
                   128.1          0  32768 00:00:e2:08:57:89        24
                   -----        ---- -----------------------        ---
                   (19)         (20) (21)                           (22)
ether 2 2          128.4     200000* Forwarding(Designated)         25
---------          -----     ------- ----------------------         ---
(14)               (15)      (16)    (17)                           (18)
                   128.2     200000  32768 00:0b:5d:89:00:aa         0
                   -----     ------- -----------------------        ---
                   (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。
   本装置がルートブリッジの場合は以下が表示されます。

   Port　　0 (This bridge is the root)

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) STP 動作モード
本装置の STP 動作モード(disable/stp)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
ポート状態が以下のいずれかで表示されます。

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いず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

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。

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:e2:08:57:89                       ---(2)
            Cost        200000                                  ---(3)
            Port        3 (ether 2 1)                           ---(4)
            Hello Time 2sec  Max Age 20sec  Forward Delay 15sec
            ---------------  -------------  -------------------
            (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。

本装置がルートブリッジの場合は以下が表示されます。

```
Port        0 (This bridge is the root)
```

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     00:0b:5d:89:00:aa                           ---(2)
            Hello Time 2sec  Max Age 20sec  Forward Delay 15sec
            ---------------  -------------  -------------------
            (3)              (4)            (5)
            STP Mode stp
            ------------
            (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) STP 動作モード

本装置の STP 動作モード(disable/stp)が表示されます。

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する場合

```
# show spanning-tree active
ether 2 1 is Forwarding  Port Version 0(STP)
-----------------------  -------------------
(1)                      (2)
    Port path cost 200000(auto), Port priority 128, Port Identifier 128.3
    ----------------------------  -----------------  -----------------------
    (3)                           (4)                (5)
    Port role is Root
    -----------------
    (6)
    Designated root has priority 32768, address 00:00:e2:08:57:89
    ----------------------------------  -------------------------
    (7)                                 (8)
    Designated bridge has priority 32768, address 00:00:e2:08:57:89
    -----------------------------------  -------------------------
    (9)                                  (10)
    Designated port id is 128.1, Designated path cost 0
    ---------------------------  -----------------------
    (11)                         (12)
    BPDU statistics:
      Config BPDU: sent 3, sent error 0
                   ------  ------------
                   (13)    (14)
                   received 112, discarded 0
```

```
                  -------------  -----------
                   (15)           (16)
      TCN BPDU:    sent 2, sent error 0
                   ------  ------------
                   (17)    (18)
                   received 0, discarded 0
                   ----------  -----------
                   (19)        (20)
      Other error: bad protocol 0, bad version 0
                   --------------  -------------
                   (21)            (22)
                   bad BPDU type 0
                   ---------------
                   (23)

ether 2 2 is Forwarding  Port Version 0(STP)
------------------------  --------------------
(1)                       (2)
    Port path cost 200000(auto), Port priority 128, Port Identifier 128.4
    ----------------------------  -----------------  -----------------------
    (3)                           (4)                (5)
    Port role is Designated
    -----------------------
    (6)
    Designated root has priority 32768, address 00:00:e2:08:57:89
    ----------------------------------  -------------------------
    (7)                                 (8)
    Designated bridge has priority 32768, address 00:0b:5d:89:00:aa
    -------------------------------------  -------------------------
    (9)                                    (10)
    Designated port id is 128.2, Designated path cost 200000
    ----------------------------  ---------------------------
    (11)                          (12)
    BPDU statistics:
      Config BPDU: sent 292, sent error 0
                   --------- ------------
                   (13)      (14)
                   received 0, discarded 0
                   ----------  -----------
                   (15)        (16)
      TCN BPDU:    sent 0, sent error 0
                   ------  ------------
                   (17)    (18)
                   received 0, discarded 0
                   ----------  -----------
                   (19)        (20)
      Other error: bad protocol 0, bad version 0
                   --------------  -------------
                   (21)            (22)
                   bad BPDU type 0
                   ---------------
                   (23)
```

1) インタフェース名とポート状態

ポート状態が以下のいずれかで表示されます。

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 STP バージョン

STP バージョンは以下のいずれかが表示されます。

-(OFF)
STP 未使用ポート
0(STP)
802.1d STP

3) 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。
4) ポート優先度
該当ポートの優先度が表示されます。
5) 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。
6) ポート役割
ポートの役割状態が以下のいず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
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) 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。
10) 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。
11) 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。
12) 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。
13) 構成 BPDU 送信回数
構成 BPDU の送信回数が表示されます。
14) 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。
15) 構成 BPDU 受信回数
構成 BPDU の受信回数が表示されます。
16) 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。
17) TCN BPDU 送信回数
TCN BPDU の送信回数が表示されます。
18) TCN BPDU 送信エラー回数
TCN BPDU の送信エラー回数が表示されます。
19) TCN BPDU 受信回数
TCN BPDU の受信回数が表示されます。
20) TCN BPDU 受信破棄回数
TCN BPDU の受信破棄回数が表示されます。
21) 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。
22) 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。

23) 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。

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 ether group 2 port 1
ether 2 1 is Forwarding  Port Version 0(STP)
------------------------  --------------------
(1)                       (2)
    Port path cost 200000(auto), Port priority 128, Port Identifier 128.3
    ----------------------------  -----------------  -----------------------
    (3)                           (4)                (5)
    Port role is Root
    -----------------
    (6)
    Designated root has priority 32768, address 00:00:e2:08:57:89
    ----------------------------------  -------------------------
    (7)                                 (8)
    Designated bridge has priority 32768, address 00:00:e2:08:57:89
    -------------------------------------  -------------------------
    (9)                                    (10)
    Designated port id is 128.1, Designated path cost 0
    ----------------------------  -----------------------
    (11)                          (12)
    BPDU statistics:
      Config BPDU: sent 3, sent error 0
                   ------  ------------
                   (13)    (14)
                   received 112, discarded 0
                   ------------  -----------
                   (15)          (16)
      TCN BPDU:    sent 2, sent error 0
                   ------  ------------
                   (17)    (18)
                   received 0, discarded 0
                   ----------  -----------
                   (19)        (20)
      Other error: bad protocol 0, bad version 0
                   --------------  -------------
                   (21)            (22)
                   bad BPDU type 0
                   ---------------
                   (23)
```

1) インタフェース名とポート状態

ポート状態が以下のいずれかで表示されます。

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 STP バージョン

STP バージョンが以下のいずれかで表示されます。

-(OFF)

STP 未使用ポート

0(STP)

802.1d STP

3) 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。

4) ポート優先度
該当ポートの優先度が表示されます。
5) 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。
6) ポート役割
ポートの役割状態が以下のいず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

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) 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。
10) 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。
11) 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。
12) 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。
13) 構成 BPDU 送信回数
構成 BPDU の送信回数が表示されます。
14) 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。
15) 構成 BPDU 受信回数
構成 BPDU の受信回数が表示されます。
16) 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。
17) TCN BPDU 送信回数
TCN BPDU の送信回数が表示されます。
18) TCN BPDU 送信エラー回数
TCN BPDU の送信エラー回数が表示されます。
19) TCN BPDU 受信回数
TCN BPDU の受信回数が表示されます。
20) TCN BPDU 受信破棄回数
TCN BPDU の受信破棄回数が表示されます。
21) 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。
22) 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。
23) 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 00:0b:5d:89:00:aa
```

```
  ------------------------------------  -------------------------
  (1)                                    (2)
  Configured hello time 2, max age 20, forward delay 15
  -----------------------  ----------  ----------------
  (3)                      (4)         (5)
  Current root has priority 32768, address 00:00:e2:08:57:89
  --------------------------------  -------------------------
  (6)                               (7)
  Root port is ether 2 1, cost of root path is 200000
  ----------------------  ---------------------------
  (8)                     (9)
  STP Mode stp
  ------------
  (10)
  Topology changes        1  Detected date Tue Nov  1 05:30:28 2005
  -------------------------  ---------------------------------------
  (11)                        (12)
                              (time since 05:30:28)
                               -------------------
                               (13)

ether 2 1 is Forwarding  Port Version 0(STP)
-----------------------  -------------------
(14)                     (15)
    Port path cost 200000(auto), Port priority 128, Port Identifier 128.3
    ---------------------------  -----------------  ---------------------
    (16)                         (17)               (18)
    Port role is Root
    -----------------
    (19)
    Designated root has priority 32768, address 00:00:e2:08:57:89
    ----------------------------------  -------------------------
    (20)                                (21)
    Designated bridge has priority 32768, address 00:00:e2:08:57:89
    -------------------------------------  -------------------------
    (22)                                   (23)
    Designated port id is 128.1, Designated path cost 0
    ---------------------------  ----------------------
    (24)                         (25)
    BPDU statistics:
      Config BPDU: sent 3, sent error 0
                   ------  ------------
                   (26)    (27)
                   received 901, discarded 0
                   ------------  -----------
                   (28)          (29)
      TCN BPDU:    sent 0, sent error 0
                   ------  ------------
                   (30)    (31)
                   received 0, discarded 0
                   ----------  -----------
                   (32)        (33)
      Other error: bad protocol 0, bad version 0
                   --------------  -------------
                   (34)            (35)
                   bad BPDU type 0
                   ---------------
                   (36)
    Other statistics:
      changed to forwarding state 1
                                  ---
                                  (37)

ether 2 2 is Forwarding  Port Version 0(STP)
-----------------------  -------------------
(14)                     (15)
    Port path cost 200000(auto), Port priority 128, Port Identifier 128.4
    ---------------------------  -----------------  ----------------------
    (16)                         (17)               (18)
    Port role is Designated
    -----------------------
```

```
(19)
Designated root has priority 32768, address 00:00:e2:08:57:89
-----------------------------------  -------------------------
(20)                                 (21)
Designated bridge has priority 32768, address 00:0b:5d:89:00:aa
-------------------------------------  --------------------------
(22)                                   (23)
Designated port id is 128.2, Designated path cost 20000
----------------------------  --------------------------
(24)                          (25)
BPDU statistics:
  Config BPDU: sent 902, sent error 0
               --------- ------------
               (26)      (27)
               received 0, discarded 0
               ------------  -----------
               (28)          (29)
  TCN BPDU:    sent 0, sent error 0
               ------  ------------
               (30)    (31)
               received 0, discarded 0
               ----------  -----------
               (32)        (33)
  Other error: bad protocol 0, bad version 0
               --------------  -------------
               (34)            (35)
               bad BPDU type 0
               ---------------
               (36)
Other statistics:
  changed to forwarding state 1
                              ---
                              (37)
```

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) 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) 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。
本装置がルートブリッジの場合は 8) ルートポート、9) ルートパスコストは表示されずに、以下のメッセージが表示されます。

```
This bridge is the root
```

9) 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。

10) STP 動作モード
本装置の STP 動作モード(disable/stp)が表示されます。

11) トポロジチェンジ検出回数
トポロジチェンジを検出した回数が表示されます。

12) トポロジチェンジ検出時刻
最後にトポロジチェンジを検出した時刻が表示されます。

13) トポロジチェンジ検出経過時間
最後にトポロジチェンジ検出してからの経過時間が表示されます。
14) インタフェース名とポート状態
ポート状態が以下のいずれかで表示されます。
Disabled
STP は無効
Blocking
Blocking 状態
Listening
Listening 状態
Learning
Learning 状態
Forwarding
Forwarding 状態
15) ポート STP バージョン
STP バージョンが以下のいずれかで表示されます。
-(OFF)
STP 未使用ポート
0(STP)
802.1d STP
16) 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。
17) ポート優先度
該当ポートの優先度が表示されます。
18) 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。
19) ポート役割
ポートの役割状態が以下のいず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
20) 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。
21) 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。
22) 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。
23) 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。
24) 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。
25) 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。
26) 構成 BPDU 送信回数
構成 BPDU の送信回数が表示されます。
27) 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。

28) 構成 BPDU 受信回数

構成 BPDU の受信回数が表示されます。

29) 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。

30) TCN BPDU 送信回数

TCN BPDU の送信回数が表示されます。

31) TCN BPDU 送信エラー回数

TCN BPDU の送信エラー回数が表示されます。

32) TCN BPDU 受信回数

TCN BPDU の受信回数が表示されます。

33) TCN BPDU 受信破棄回数

TCN BPDU の受信破棄回数が表示されます。

34) 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。

35) 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。

36) 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。

37) 転送状態に遷移した回数

ポート状態が転送(Forwarding)状態に遷移した回数

51.4 スパニングツリーのカウンタ・ログ・統計・状態などのクリア

51.4.1 clear spanning-tree statistics

[機能]

スパニングツリー関連の統計情報のクリア

[適用機種]

Si-R G110

[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 52 章 ブリッジグループのカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

52.1 ブリッジグループのカウンタ・ログ・統計・状態などの表示、クリア

52.1.1 show bridgegroup

[機能]

ブリッジグループに関する状態および統計情報の表示

[適用機種]

Si-R G110

[入力形式]

show bridgegroup
show bridgegroup group [<group_id>]
show bridgegroup 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 の省略時は、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-R G110

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]

ブリッジグループに関する状態、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 bridgegroup
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        vlan1           S    infinity
00:a0:c9:13:f3:37         0        vlan2           D         164
00:a0:c9:f0:20:e9         0        vlan3           D         196
00:b0:d0:6f:94:78         0        vlan4           D         196
00:0c:6e:63:25:77         1        vlan5           D         204
00:04:96:1a:a7:b0         1        vlan6           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
以下のどちらかが表示されます。

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 bridgegroup 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

52.1.2 show bridgegroup 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 G110

[入力形式]

```
show bridgegroup status
show bridgegroup status interface <interface_name>
show bridgegroup 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 の省略時は、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-R G110

[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 bridgegroup status
Name       Group   Status  IPv4     IPv6     D_if             In     Out
--------   -----   ------  ----     ----     ---              --     ---
(1)        (2)      (3)    (4)      (5)      (6)              (7)    (8)

vlan1      *0      valid   Bridge   Routing  *                 0       2
vlan2      *0      valid   Bridge   Routing                    0       1
vlan100     1      valid   Bridge   Routing  *                 0       0
vlan4000    1      valid   Bridge   Routing                    0       0
rmt0        1      valid   Bridge   Routing                    0       0
```

1) インタフェース名
   vlan、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
   ether グループで透過モードを使用しているグループには、先頭に*が表示されます。
3) ブリッジの状態
   以下のどちらかが表示されます。
   valid
   ブリッジは有効

invalid

ブリッジは無効

4) IPv4 転送方式

以下のどちらかが表示されます。

Bridge

ブリッジで転送

Routing

ルーティングで転送

5) IPv6 転送方式

以下のどちらかが表示されます。

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

52.1.3 clear bridgegroup statistics

[機能]

ブリッジ関連の統計情報クリア

[適用機種]

Si-R G110

[入力形式]

clear bridgegroup 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 bridgegroup statistics
#
```

第 53 章 認証機能のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

・ グループ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〈group〉(ether グループ定義番号)に指定するグループ番号の通し番号(10 進数)は、以下に示す範囲で指定してください。

範囲	機種
2	Si-R G110

・ ポ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〈port〉(ether ポート定義番号)に指定するポート番号の通し番号(10 進数)は、以下に示す範囲で指定してください。

範囲	機種
1～4	Si-R G110 (グループ 2)

53.1 認証成功端末情報のカウンタ・ログ・統計・状態などの表示

53.1.1 show auth port ether

[機能]

認証成功端末情報の表示

[適用機種]

Si-R G110

[入力形式]

show auth port ether [group <group> [port <port>]]

[オプション]

なし

すべての認証成功端末情報を表示します。

group <group>

・ ether グループ番号
ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

port <port>

・ ether ポート番号
ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

[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]

認証機能(IEEE802.1X 認証、MAC アドレス認証)での認証成功端末情報を表示します。
group オプションのみ指定した場合は、対象グループの全ポートの情報が表示されます。
group オプション、port 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]

```
# show auth port ether
[ether]
Group  Port  Mode  MAC Address        Function  VLAN
------ ----- ----- ------------------ --------- -----
(1)    (2)   (3)   (4)                (5)       (6)
2      1     mac   00:13:21:f6:01:11  macauth   10
2      2     mac   00:13:21:f6:02:22  dot1x     20
#
```

1) ether グループ番号
2) ether ポート番号
3) 認証方法(各ポートの先頭行に表示)

mac

MAC アドレスごとの認証を行う

4) MAC アドレス
5) 認証成功した機能

dot1x

IEEE802.1X 認証

macauth

MAC アドレス認証

6) VLAN ID

※

認証成功端末が存在しないインタフェースは、ether グループ番号および ether ポート番号以外の項目が"-"で表示されます。

53.2 IEEE802.1X 認証のカウンタ・ログ・統計・状態などの表示

53.2.1 show dot1x port ether

[機能]

IEEE802.1X 認証状態の表示

[適用機種]

Si-R G110

[入力形式]

show dot1x port ether [group <group> [port <port>]]

[オプション]

なし

すべての IEEE802.1X 認証状態を表示します。

group <group>

・ ether グループ番号
ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

port <port>

・ ether ポート番号
ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

[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]

認証機能情報として認証により許容された端末(Supplicant)についてユーザ名、認証方式、認証状態、統計情報を表示します。
group オプションのみ指定した場合は、対象グループの全ポートの情報が表示されます。
group オプション、port 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]

```
# show dot1x port ether
[ether]
Group Port User              EAP-Type Authentication OK times NG times Status VLAN
(1)   (2)  (3)               (4)      (5)            (6)      (7)      (8)    (9)
                             MAC address             Since
                             (10)                    (11)
-----------------------------------------------------------------------------------
2     1    user01            TTLS     Authenticated  2        2        S2     1
                             00:0e:13:25:0f:01       Mar 31 18:35:01 2012
2     2    admin             TLS      Authenticated  2        0        S2     1
                             00:0e:13:8e:55:02       Mar 31 18:37:15 2012
#
```

1) ether グループ番号
2) ether ポート番号
3) ユーザ名
4) 認証方式

5) 認証状態

-

未設定または未接続ポートであることを示します。

Authenticating

認証中

Authenticated

認証済み

Failure

認証失敗

6) 認証により許容された回数

7) 認証失敗の回数

認証サーバまたはAAAから認証失敗が通知された場合またはユーザに割り当てるVLAN IDの設定に失敗した場合にカウントされます。

8) IEEE802.1X認証の内部状態

S0

認証前の状態

S1

認証処理中の状態

S2

通常状態

9) VLAN ID

10) 端末(Supplicant)のMACアドレス

11) 認証に成功した時刻(再認証時は更新されません)

※

認証を行っていないポートでは、ユーザ名や認証方式などが"-"で表示されます。

53.2.2 show dot1x statistics port ether

[機能]

IEEE802.1X 認証統計情報の表示

[適用機種]

Si-R G110

[入力形式]

show dot1x statistics port ether [group <group> [port <port>]]

[オプション]

なし

すべての IEEE802.1X 認証統計情報を表示します。

group <group>

・ ether グループ番号
ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

port <port>

・ ether ポート番号
ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-" (ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

[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]

IEEE802.1X 認証の統計情報を表示します。
group オプションのみ指定した場合は、対象グループの全ポートの情報が表示されます。
group オプション、port 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。

[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]

```
# show dot1x statistics port ether
[ether]
Group 2 Port 1 statistics:
                     EAPOL frame received count : 0                 ---(1)
                         EAPOL frame sent count : 0                 ---(2)
               EAPOL Start frame received count : 0                 ---(3)
              EAPOL Logoff frame received count : 0                 ---(4)
           EAP Identity Response received count : 0                 ---(5)
                   EAP response received count : 0                 ---(6)
                EAP Identity Request sent count : 1                 ---(7)
                         EAP request sent count : 0                 ---(8)
             Invalid EAPOL frame received count : 0                 ---(9)
    EAP with illegal length frame received count : 0                ---(10)
           Version of EAPOL last received frame : 0                 ---(11)
       Supplicant address of last received frame : 00:00:00:00:00:00 ---(12)

#
```

1) 受信 EAPOL フレーム数
2) 送信 EAPOL フレーム数
3) 受信 EAPOL-Start フレーム数
4) 受信 EAPOL-Logoff フレーム数
5) 受信 EAP Identity response フレーム数
6) EAP Identity 以外の受信 EAP response フレーム数
7) 送信 EAP Identity request フレーム数
8) EAP Identity 以外の送信 EAP request フレーム数
9) 受信した無効な EAPOL フレーム数
10) 受信した不当なパケット長の EAPOL フレーム数
11) 最後に受信した EAPOL フレームのバージョン番号
12) 最後に受信した端末(Supplicant)の MAC アドレス

53.3 IEEE802.1X 認証のカウンタ・ログ・統計などのクリア

53.3.1 clear dot1x statistics

[機能]

IEEE802.1X 認証統計情報のクリア

[適用機種]

Si-R G110

[入力形式]

clear dot1x statistics

[オプション]

なし

すべてのポートの IEEE802.1X 認証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]

IEEE802.1X 認証の統計情報をクリアします。

[注意]

以下の内容についてはクリアされません。

- 最後に受信した EAPOL フレームのバージョン番号
- 最後に受信した端末(Supplicant)の MAC アドレス

[実行例]

```
# clear dot1x statistics
#
```

53.4 MAC アドレス認証のカウンタ・ログ・統計・状態などの表示

53.4.1 show macauth port ether

[機能]

MAC アドレス認証状態の表示

[適用機種]

Si-R G110

[入力形式]

show macauth port ether [group <group> [port <port>]]

[オプション]

なし

すべての MAC アドレス認証状態を表示します。

group <group>

・ ether グループ番号
ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

port <port>

・ ether ポート番号
ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

[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]

MAC アドレス認証状態を表示します。
group オプションのみ指定した場合は、対象グループの全ポートの情報が表示されます。
group オプション、port 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]

```
# show macauth port ether
[ether]
Group  Port  Mode  MAC Address        Status     VLAN  Since
------ ----- ----- ------------------ ---------- ----- ---------------------
(1)    (2)   (3)   (4)                (5)        (6)   (7)
2      1     mac   00:13:22:f6:01:13  success    10    Apr  1 10:50:53 2012
                   00:13:22:f6:01:43  failure    -     Apr  1 10:51:12 2012
2      2     mac   00:13:22:f6:02:23  success    20    Apr  1 10:55:30 2012
                   00:13:22:f6:02:43  failure    -     Apr  1 10:56:03 2012
                   00:13:22:f6:02:74  failure    -     Apr  1 10:57:22 2012
#
```

1) ether グループ番号
2) ether ポート番号
3) 認証方法(各ポートの先頭行に表示)

mac

MAC アドレスごとの認証を行う

4) MAC アドレス

5) 認証状態

idle

認証端末が未検出

response

認証結果待ち

success

認証成功

permanent

認証不要端末

failure

認証失敗または認証制限数超過

6) VLAN ID

7) 認証開始、認証成功または認証失敗した時刻

53.4.2 show macauth statistics port ether

[機能]

MAC アドレス認証統計情報の表示

[適用機種]

Si-R G110

[入力形式]

show macauth statistics port ether [group <group> [port <port>]]

[オプション]

なし

すべての MAC アドレス認証統計情報を表示します。

group <group>

・ ether グループ番号
ether グループ番号を、10 進数で指定します。
グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

port <port>

・ ether ポート番号
ether ポート番号を、10 進数で指定します。
複数のポート番号を設定する場合、"," (カンマ)で区切ります。
複数の番号が続く場合、"-" (ハイフン)で区切ります(例:"1-2")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

[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]

MAC アドレス認証の統計情報を表示します。
group オプションのみ指定した場合は、対象グループの全ポートの情報が表示されます。
group オプション、port 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]

```
# show macauth statistics port ether
[ether]
Group 2 Port 1 statistics:
  MAC authentication request  : 8                          ---(1)
  MAC authentication success  : 5                          ---(2)
  MAC authentication failure  : 2                          ---(3)
  MAC authentication logout   : 4                          ---(4)
  MAC authentication excess   : 1                          ---(5)

#
```

1) MAC アドレス認証要求回数
2) MAC アドレス認証成功回数
3) MAC アドレス認証失敗回数
4) MAC アドレス認証ログアウト回数
5) MAC アドレス認証未実行回数(認証制限数超過)

53.5 MAC アドレス認証のカウンタ・ログ・統計などのクリア

53.5.1 clear macauth statistics

[機能]

MAC アドレス認証統計情報のクリア

[適用機種]

Si-R G110

[入力形式]

clear macauth statistics

[オプション]

なし

すべてのポートの MAC アドレス認証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]

MAC アドレス認証の統計情報をクリアします。

[実行例]

```
# clear macauth statistics
#
```

53.6 ARP 認証のカウンタ・ログ・統計・状態などの表示

53.6.1 show arpauth vlan

[機能]

ARP 認証状態の表示

[適用機種]

Si-R G110

[入力形式]

show arpauth vlan [<vid>]

[オプション]

なし

すべての VLAN の ARP 認証状態を表示します。

<vid>

・ VLAN ID

ARP 認証状態を表示する VLAN を指定します。

VLAN ID を、1～4094 の 10 進数で指定します。

[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]

ARP 認証状態を表示します。

[実行例]

```
# show arpauth vlan

VLAN  Num   MAC Address        IP address       Status   Remain
----- ----- ------------------ ---------------- -------- --------
(1)   (2)   (3)                (4)              (5)      (6)
1     1     00:13:21:f6:01:13  192.168.100.100  success  00:20:12
2     2     00:13:21:f6:02:23  192.168.200.201  success  00:00:22
            00:13:21:f6:02:43  192.168.200.205  failure  00:00:22
5     3     00:13:21:f6:05:33  192.168.1.10     permanent   -
            00:13:21:f6:02:73  192.168.1.20     failure  12:11:00
            00:13:21:f6:02:74  192.168.1.30     failure  12:11:01
8     0
#
```

1) VLAN ID

2) 端末数

3) MAC アドレス

4) IP アドレス

5) 認証状態

response

認証結果待ち

success

認証成功

failure

認証失敗

permanent

認証不要

retry

資源不足で再認証

6）認証状態保持時間の残り

53.6.2 show arpauth statistics

[機能]

ARP 認証統計情報の表示

[適用機種]

Si-R G110

[入力形式]

show arpauth statistics [<vid>]

[オプション]

なし

すべての VLAN の ARP 認証統計情報を表示します。

<vid>

・ VLAN ID

ARP 認証統計情報を表示する VLAN を指定します。

VLAN ID を、1～4094 の 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]

ARP 認証の統計情報を表示します。

[実行例]

```
# show arpauth statistics

VLAN 1 :
  Authentication request  : 7                          --- (1)
                 success  : 5                          --- (2)
                 failure  : 2                          --- (3)
  Non-authentication      : 2                          --- (4)
                 success  : 1                          --- (5)
                 failure  : 1                          --- (6)
  Authenticated           : 1                          --- (7)
VLAN 10 :
  Authentication request  : 4
                 success  : 1
                 failure  : 3
  Non-authentication      : 1
                 success  : 1
                 failure  : 0
  Authenticated           : 0
#
```

1) AAA への認証要求回数
2) AAA からの応答回数（成功）
3) AAA からの応答回数（失敗）
4) 認証結果保持時間内の要求回数
5) 認証結果保持時間内の応答回数（成功）
6) 認証結果保持時間内の応答回数（失敗）
7) 認証不要 IP アドレスからの要求回数

53.7 ARP 認証のカウンタ・ログ・統計などのクリア

53.7.1 clear arpauth statistics

[機能]

ARP 認証統計情報のクリア

[適用機種]

Si-R G110

[入力形式]

clear arpauth statistics

[オプション]

なし

すべての VLAN の ARP 認証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]

ARP 認証の統計情報をクリアします。

[実行例]

```
# clear arpauth statistics
#
```

第 54 章 トラッキング情報の表示、クリア操作コマンド

・ トラッキング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>(トラッキング定義番号)に指定するトラッキング定義の通し番号(10 進数)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-R G110

54.1 トラッキング情報の表示

54.1.1 show tracking

[機能]

トラッキング情報表示

[適用機種]

Si-R G110

[入力形式]

show tracking [<number>]

[オプション]

なし

すべてのトラッキング情報を表示します。

<number>

・トラッキング定義番号

表示するトラッキング定義番号を、10 進数で指定します。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

[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]

トラッキング情報を表示します。

<number>を指定した場合は、トラッキング定義番号のトラッキング情報を表示します。

［実行例］

```
# show tracking
[TRACKING 0]                                                    ---(1)
  Trigger                                                       ---(2)
    Node trigger                                                ---(3)
      down  192.168.1.2  192.168.2.10                           ---(4)
  Action                                                        ---(5)
    Down action                                                 ---(6)
      Executed last time : Wed Jun 26 10:50:46 2013             ---(7)
      Executed count     : 1                                    ---(8)
      Command                                                   ---(9)
        offline ether group 1 port 1                            ---(10)
    Up action                                                   ---(11)
      Executed last time : Wed Jun 26 10:52:46 2013             ---(12)
      Executed count     : 1                                    ---(13)
      Command                                                   ---(14)
        online ether group 1 port 1                             ---(15)

[TRACKING 1]
  Trigger
    Node trigger
      up    10.1.1.1  10.1.1.2
  Action
    Down action
      Executed last time : --
      Executed count     : 0
    Up action
      Executed last time : Sun Jun 30 21:15:11 2013
      Executed count     : 2
      Command
        online remote 0

#
```

1) トラッキング定義番号
2) トリガ情報
3) ノードトリガ情報
4) 監視状態，送信元 IP アドレス，監視対象 IP アドレス

監視状態

監視の現在の状態

－ --
状態取得中

－ down
異常状態

－ up
正常状態

5) アクション情報
6) down アクション情報
7) down アクション適用時刻
最後に適用した down アクションの時刻を表示します。
適用がない場合には"--"を表示します。
8) down アクション適用回数
9) down アクション適用コマンド情報
10) down アクション適用コマンド
11) up アクション情報
12) up アクション適用時刻
最後に適用した up アクションの時刻を表示します。
適用がない場合には"--"を表示します。
13) up アクション適用回数

14）up アクション適用コマンド情報
15）up アクション適用コマンド

54.1.2 show tracking brief

[機能]

トラッキング簡易情報表示

[適用機種]

Si-R G110

[入力形式]

show tracking brief

[オプション]

なし

すべてのトラッキング簡易情報を表示します。

[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]

トラッキング簡易情報を表示します。

[実行例]

```
# show tracking brief
[TRACKING 0]                    ---(1)
  Trigger    Num  Status
  ---------- ---- -------
  (2)        (3)  (4)
  Node       0    up
[TRACKING 1]
  Trigger    Num  Status
  ---------- ---- -------
  Node       0    down
#
```

1) トラッキング定義番号
2) トリガ情報
3) トリガ定義番号
4) 監視状態
   監視の現在の状態
   - --
     状態取得中
   - down
     down 状態
   - up
     up 状態

54.2 トラッキング統計情報のクリア

54.2.1 clear tracking statistics

[機能]

トラッキング統計情報のクリア

[適用機種]

Si-R G110

[入力形式]

clear tracking statistics [<number>]

[オプション]

なし

すべてのトラッキング情報をクリアします。

<number>

・ トラッキング定義番号

クリアするトラッキング定義番号を、10 進数で指定します。

定義番号の指定方法の詳細については、本章の冒頭を参照してください。

[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]

トラッキング統計情報をクリアします。

show tracking コマンドで表示される以下の情報がクリアされます。

・ down アクション適用時刻
・ down アクション適用回数
・ up アクション適用時刻
・ up アクション適用回数

[実行例]

```
# clear tracking statistics
#
```

第 55 章 SNMP 統計情報の表示、クリア操作コマンド

55.1 SNMP 統計情報の表示

55.1.1 show snmp statistics

[機能]

SNMP 機能の統計情報の表示

[適用機種]

Si-R G110

[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］

```
# 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)
SNMPv3 statistics information:
          0 Input Unknown Security Models                ---(28)
          0 Input Invalid Msgs                           ---(29)
          0 Input Unknown PDU Handlers                   ---(30)
          0 Input Unsupported SecLevels                  ---(31)
          0 Input Not InTimeWindows                      ---(32)
          0 Input Unknown User Names                     ---(33)
          0 Input Unknown EngineIds                      ---(34)
          0 Input Wrong Digests                          ---(35)
          0 Input Decryption Errors                      ---(36)
#
```

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
28) 未サポートまたは不正な Security Models 受信の総数
29) 不正な SNMP メッセージ受信の総数
30) 未サポートまたは不正な PDU Handler 受信の総数
31) 未サポートまたは不正な Security Level 受信の総数
32) TimeWindows 外の SNMP メッセージ受信の総数
33) 不正な User Names 受信の総数
34) 不正な EngineId 受信の総数
35) 認証失敗の総数
36) 暗号失敗の総数

55.2 SNMP 統計などのクリア

55.2.1 clear snmp statistics

[機能]

SNMP 統計情報のクリア

[適用機種]

Si-R G110

[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 56 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

56.1 NETTIME(time/sntp)統計情報の表示

56.1.1 show nettime statistics

[機能]

NETTIME(time/sntp)機能の統計情報の表示

[適用機種]

Si-R G110

[入力形式]

show nettime statistics [<mode> [<protocol>]]

[オプション]

なし

稼動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、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、本装置で稼動しているすべての 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

56.2 NETTIME(time/sntp)統計などのクリア

56.2.1 clear nettime statistics

[機能]

NETTIME(time/sntp)統計情報のクリア

[適用機種]

Si-R G110

[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 57 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

57.1 UPnPのカウンタ・ログ・統計・状態などの表示

57.1.1 show upnp

[機能]

UPnP状態情報の表示

[適用機種]

Si-R G110

[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

57.1.2 show upnp statistics

[機能]

UPnP 統計情報の表示

[適用機種]

Si-R G110

[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。

57.1.3 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 G110

[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

57.2 UPnPのカウンタ・ログ・統計などのクリア

57.2.1 clear upnp statistics

[機能]

UPnP統計情報のクリア

[適用機種]

Si-R G110

[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
#
```

57.2.2 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 G110

[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 58 章 ポリシーグループの状態の表示コマンド

58.1 ポリシーグループの状態の表示

58.1.1 show policy-group

[機能]

ポリシーグループ情報表示

[適用機種]

Si-R G110

[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 進数で指定します。

範囲	機種
0～99	Si-R G110

[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]

```
# 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が表示されます。
ただし、「status」が「inactive」「down」の場合は表示されません。

第 59 章 ドメインリストの状態の表示コマンド

59.1 ドメインリストの状態の表示

59.1.1 show domainlist

[機能]

ドメインリスト情報表示

[適用機種]

Si-R G110

[入力形式]

show domainlist [ip]

[オプション]

なし

すべてのドメインリスト情報を表示します。

ip

ドメインリストを使用する場合に指定した ACL で保持されている IP アドレスとその残存時間を表示します。

[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]

ドメインリストについての情報を表示します。

[注意]

domainlist 情報が何も設定されていないドメインリスト情報は表示しません。

［実行例］

```
# show domainlist
COUNT [ 0] ID [0]
       (1)    (2)
Domain NAME
[  1] *sample.com                                                    ---(3)
      use :          57                                              ---(4)
[  2] test?site.com
      use :          3
COUNT [ 1] ID [1]
Domain NAME
(5)

COUNT [ 0] ID [0]
Domain NAME CNAME
[  1] test.sample.com.net                                            ---(6)
      use :          1  ttl :   591
                    (7)         (8)
[  2] test2site.com.akamai.net
      use :          0  ttl :   58

COUNT [ 1] ID [1]
Domain NAME CNAME
(9)

# show domainlist ip
acl [   0]                                                           ---(10)
         dst_ip             remain_time     use_count
         (11)               (12)            (13)
[   1]   192.168.100.10             450         49530
[   2]   192.168.100.11             440         60150
acl [   1]
  inactive                                                           ---(14)
#
```

1) ProxyDNS 転送先定義番号
2) ドメイン ID 番号
3) ドメイン名
4) ドメイン名使用回数
5) ドメインリスト情報の設定はされているがドメイン名が反映されていない場合、表示しません。
6) ProxyDNS の応答が CNAME で返ってきた場合、表示されます。
7) CNAME 使用回数
8) CNAME 保持時間(単位：秒)
9) ドメインリスト情報の設定はされているがドメイン名が反映されていない場合、または、ProxyDNS の応答が CNAME で返ってこない場合、表示しません。
10) ACL 定義番号
11) 動的 IP アドレス
12) 動的 IP アドレス保持時間(単位：秒)
13) 動的 IP アドレス使用回数
14) 動的 IP アドレスが保持されていない場合、"inactive"と表示されます。

第 60 章 SSH ホスト認証用公開鍵の表示コマンド

60.1 SSH ホスト認証用公開鍵の表示

60.1.1 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 G110

[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
P31K2u3XAEoAzLa0JQCo6VjoDQh15YIzKFo2AVaK4lCeS3q81q8A4+jttJ0Dt0U0
rVucQo0q+BdIgaCMDuaqmJQAotGvZvZQ/RMTSh6pMh+z9DdB1DLnPNxEyt61Sftz
Vk+rjgZ29In2V7ai4yu0fIhNL61yb0rrfoZ9YQW4P9rJuDxhvn2xvZQ/RMTSh6pM
6WIwA9mlzAst/YBxbb9Jc07uPVhN8M624q8yKsQaMClW1AAAWOO+ZkaqccWLy9GU
xPksjfC+N7022akmykT8V6iMh4+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 AA94UAATdVfYAAxsAArx3AAIF7QAsTsTwAEeKogAFAlNoAAOOAAAAj3F
AAD3C1yc2EAAAABIwAAAHsMXKAAB+shGQAHDmIABBSpjAARVYAAERAAJZ/IAAAAB
OAB9QAB+2kSY6AAUAygACvAAB3NzaA7wtAAJ/kAADRQgABwmQAThHAAUtOySgAEJ
JMBAAX4= root@localhost    ---(1)
#
```

1) 本装置のホスト認証用 RSA 公開鍵

第 61 章 AAA の状態の表示、クリア操作コマンド

61.1 AAAの状態の表示

61.1.1 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 G110

[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]

```
# 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

61.1.2 show aaa radius client statistics

[機能]

RADIUS クライアント機能の統計情報表示

[適用機種]

Si-R G110

[入力形式]

show aaa radius client statistics [group <group_id> [{auth|accounting} [<number>]]]

[オプション]

なし
AAA グループすべての統計情報を表示します。

group <group_id>
指定したグループに関する統計情報を表示します。

group <group_id> auth
指定したグループの認証に関する統計情報を表示します。

group <group_id> auth <number>
指定したグループの指定した認証定義番号に関する統計情報を表示します。

group <group_id> accounting
指定したグループのアカウンティングに関する統計情報を表示します。

group <group_id> accounting <number>
指定したグループの指定したアカウンティング定義番号に関する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]

RADIUS クライアントの統計情報を表示します。

［実行例］

```
# show aaa radius client statistics
aaa 0 auth 0 statistics information:
         100 Round Trip Time(ms)                          ---(1)
           2 Access Requests                              ---(2)
           0 Access Retransmissions                       ---(3)
           1 Access Accepts                               ---(4)
           0 Access Rejects                               ---(5)
           0 Access Challenges                            ---(6)
           0 Malformed Access Responses                   ---(7)
           0 Bad Authenticators                           ---(8)
           0 Pending Requests                             ---(9)
           0 Timeouts                                     ---(10)
           0 Unknown Types                                ---(11)
           0 Packets Dropped                              ---(12)
aaa 0 accounting 0 statistics information:
         100 Round Trip Time(ms)                          ---(13)
           1 Requests                                     ---(14)
           0 Retransmissions                              ---(15)
           1 Responses                                    ---(16)
           0 Malformed Responses                          ---(17)
           0 Bad Authenticators                           ---(18)
           0 Pending Requests                             ---(19)
           0 Timeouts                                     ---(20)
           0 Unknown Types                                ---(21)
           0 Packets Dropped                              ---(22)
```

1) 認証サーバの RTT 値
2) Access-Request 送信数
3) Access-Request 再送数
4) Access-Accept 受信数
5) Access-Rejects 受信数
6) Access-Challenges 受信数
7) 異常な Access-Responses 受信数
8) 不正な Authenticator 受信数
9) 応答を受信していないパケット数
10) タイムアウトになった回数
11) パケットの種別を特定できなかった回数
12) 破棄されたパケット数
13) アカウンティングサーバの RTT 値
14) Accounting-Request 送信数
15) Accounting-Request 再送数
16) Accounting-Response 受信数
17) 異常な Accounting-Response 受信数
18) 不正な Authenticator 受信数
19) 応答を受信していないパケット数
20) タイムアウトになった回数
21) パケットの種別を特定できなかった回数
22) 破棄されたパケット数

61.2 MAC アドレス収集情報の表示、クリア

61.2.1 show aaa mac collect status

[機能]

端末 MAC アドレスの収集状態の表示

[適用機種]

Si-R G110

[入力形式]

show aaa mac collect 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]

端末 MAC アドレス収集の状態を表示します。

[実行例]

```
# show aaa mac collect status
  Target AAA Group    : 0                                     ---(1)
  Status              : RUNNING                               ---(2)
  Listed              : 3 / 1000                              ---(3)
  Marked              : 2                                     ---(4)
  Last Change Time    : Oct 13 11:14:28 2006                  ---(5)
```

1) 収集の対象の AAA 定義番号
   収集停止中(運用モード)で、収集されている端末 MAC アドレスがない場合は NONE が表示されます。
2) 現在の端末 MAC アドレス収集の状態
   - RUNNING
     収集動作中(収集モード)
   - STOPPED
     収集停止中(運用モード)
3) 収集された端末 MAC アドレスの個数／最大個数
4) 選択中の端末 MAC アドレスの個数
5) 端末 MAC アドレス収集の状態が最後に更新された日時

61.2.2 show aaa mac collect list

[機能]

収集した端末MACアドレスの表示

[適用機種]

Si-R G110

[入力形式]

show aaa mac collect list [{marked|unmarked}]

[オプション]

なし

収集したすべての端末MACアドレスの情報を表示します。

marked

aaactl mac collect mark コマンドにより選択されている端末MACアドレスの情報を表示します。

unmarked

aaactl mac collect mark コマンドにより選択されていない端末MACアドレ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]

収集した端末MACアドレスの情報を表示します。

[実行例]

```
# show aaa mac collect list
ListNo. Marked  MAC Address        User ID      Times
------- ------  -----------------  ------------ -----
  (1)     (2)         (3)               (4)        (5)
   1      *     00:00:0e:13:4d:c5  00000e134dc5   1
   2      *     00:16:d3:20:87:21  0016d3208721   2
   3            00:16:d3:d1:77:14  0016d3d17714   1
3/100 Entries Listed, 2 Entries Marked.
```

1) 収集した端末MACアドレスのリスト番号
2) 選択の状態

＊

： 登録候補として選択されていることを示します。

空白

： 登録候補として選択されていないことを示します。

3) 端末MACアドレス
4) 端末MACアドレスに対応するユーザID
5) 収集された回数

61.2.3 clear aaa mac collect list

[機能]

収集した端末MACアドレスのクリア

[適用機種]

Si-R G110

[入力形式]

clear aaa mac collect list

[オプション]

なし

収集したすべての端末MACアドレスの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]

収集した端末MACアドレスの情報をクリアします。

[実行例]

```
# clear aaa mac collect list
#
```

第 62 章 ソケット状態の表示コマンド

62.1 ソケット状態の表示

62.1.1 show socket

[機能]

ソケット状態の表示

[適用機種]

Si-R G110

[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]

```
# 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  127.0.0.1.2600         127.0.0.1.1030         ESTABLISHED
tcp        0      0  127.0.0.1.1030         127.0.0.1.2600         ESTABLISHED
tcp        0      0  127.0.0.1.2700         127.0.0.1.1029         ESTABLISHED
tcp        0      0  127.0.0.1.1029         127.0.0.1.2700         ESTABLISHED
tcp        0      0  *.22                   *.*                    LISTEN
tcp        0      0  127.0.0.1.2600         127.0.0.1.1028         ESTABLISHED
tcp        0      0  127.0.0.1.1028         127.0.0.1.2600         ESTABLISHED
tcp        0      0  127.0.0.1.65432        127.0.0.1.1027         ESTABLISHED
tcp        0      0  127.0.0.1.1027         127.0.0.1.65432        ESTABLISHED
tcp        0      0  127.0.0.1.60546        *.*                    LISTEN
tcp        0      0  127.0.0.1.60547        *.*                    LISTEN
tcp        0      0  127.0.0.1.65432        127.0.0.1.1026         ESTABLISHED
tcp        0      0  *.37                   *.*                    LISTEN
tcp        0      0  127.0.0.1.1026         127.0.0.1.65432        ESTABLISHED
tcp        0      0  127.0.0.1.65433        *.*                    LISTEN
tcp        0      0  127.0.0.1.60548        *.*                    LISTEN
tcp        0      0  127.0.0.1.65060        *.*                    LISTEN
tcp        0      0  127.0.0.1.65432        *.*                    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  127.0.0.1.2602         *.*                    LISTEN
tcp        0      0  127.0.0.1.2600         *.*                    LISTEN
tcp        0      0  127.0.0.1.2700         *.*                    LISTEN
udp        0      0  127.0.0.1.2680         *.*
udp        0      0  127.0.0.1.161          *.*
udp        0      0  *.520                  *.*
udp        0      0  127.0.0.1.2611         *.*
udp        0      0  *.67                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.67                   *.*
udp        0      0  127.0.0.1.2640         *.*
udp        0      0  *.68                   *.*
udp        0      0  *.67                   *.*
```

```
udp        0      0  *.68                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.53                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.67                   *.*
udp        0      0  127.0.0.1.52000        *.*
udp        0      0  *.68                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.37                   *.*
udp        0      0  *.68                   *.*
udp        0      0  *.67                   *.*
udp        0      0  *.68                   *.*
udp        0      0  127.0.0.1.2639         *.*
udp        0      0  127.0.0.1.2638         *.*
udp        0      0  127.0.0.1.2631         *.*
udp        0      0  *.123                  *.*
udp        0      0  *.68                   *.*
udp        0      0  *.67                   *.*
udp        0      0  127.0.0.1.2633         *.*
udp        0      0  127.0.0.1.2632         *.*
udp        0      0  127.0.0.1.2636         *.*
udp        0      0  127.0.0.1.2634         *.*
udp        0      0  127.0.0.1.2635         *.*
udp        0      0  127.0.0.1.2630         *.*
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  127.0.0.1.2626         *.*
udp        0      0  127.0.0.1.2623         *.*
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  127.0.0.1.2705         *.*
udp        0      0  *.514                  *.*
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  *.37                   *.*
udp6       0      0  *.123                  *.*
#
```

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、以下のいず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 63 章 トレースの表示、クリア操作コマンド

63.1 トレースの表示

63.1.1 show trace ppp

[機能]

PPP フレームトレースの表示

[適用機種]

Si-R G110

[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]

```
# show trace ppp

[001] internet.ISP     : PPP session start                02.08.07 09:55:01.697
-(1)- ----(2)-----       ------(3)--------                ----------(4)--------
        port=vlan:1
             --(5)--

[002] internet.ISP     : Send LCP       Configure-Request 02.08.07 09:55:01.697
                         -(6)- -(7)-     -------(8)-------
        port=vlan:1
        data=c021 0100 000a 0506 f01e 028e
             -----------(9)---------------

[003] internet.ISP     : Recv LCP       Configure-Request 02.08.07 09:55:02.116
        port=vlan:1
        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=vlan:1
        data=c021 0401 000e 0802 0702 0206 0000 0000

[005] internet.ISP     : Recv LCP       Configure-Nak     02.08.07 09:55:02.116
        port=vlan:1
        data=c021 0300 0008 0104 05ae
```

1) ログ番号
   ログ番号が、001～999 の 10 進数で表示されます。
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。

－ データ通信モジュールの場合

usb

－ PPPoE の場合

vlan:<vid>

利用した VLAN VID が表示されます。

6) 送受信

以下のどちらかが表示されます。

－ 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。

(※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。)

0xc021 LCP : Link Control Protocol

0xc023 PAP : Password Authentication Protocol

0xc223 CHAP : Challenge-Handshake Authentication Protocol

0x8021 IPCP : Internet Protocol Control Protocol

0x8031 BCP : Bridge Control Protocol

0x8057 IPV6CP : IPv6 Control Protocol

0x80fd CCP : Compression Control Protocol

0x80fb ICCP : Individual Compression Control Protocol

0xc02d BAP : Bandwidth Allocation Protocol

0xc02b BACP : Bandwidth Allocation Control Protocol

0xc029 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

0x01 Configure-Request

0x02 Configure-Ack

0x03 Configure-Nak

0x04 Configure-Reject

0x05 Terminate-Request

0x06 Terminate-Ack

0x07 Code-Reject

－ プロトコル種別が LCP の場合

0x08 Protocol-Reject

0x09 Echo-Request

0x0a Echo-Reply

0x0b Discard-Request

－ プロトコル種別が CCP、ICCP の場合

0x0e Reset-Request

0x0f Reset-Act

－ プロトコル種別が PAP の場合

0x01 Authenticate-Request

0x02 Authenticate-Ack

0x03 Authenticate-Nak

－ プロトコル種別が CHAP の場合

0x01 Challenge
0x02 Response
0x03 Success
0x04 Failure

－ プロトコル種別が BAP の場合

0x01 Call-Request
0x02 Call-Response
0x03 Callback-Request
0x04 Callback-Response
0x05 Link-Drop-Request
0x06 Link-Drop-Response
0x07 Call-Status-Ind
0x08 Call-Status-Rsp

－ プロトコル種別が CBCP の場合

0x01 Callback-Request
0x02 Callback-Response
0x03 Callback-Ack

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 64 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。

63.1.2 show trace pppoe

[機能]

PPPoE フレームトレースの表示

[適用機種]

Si-R G110

[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]

```
# 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
以下のどちらかが表示されます。
－ 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 進数で表示されます。
8) data=
送受信したフレームの内容が 16 進数で表示されます。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。

63.1.3 show trace ike

[機能]

IKE トレース情報表示

[適用機種]

Si-R G110

[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
30	Si-R G110

[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]

```
# 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

[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

以下のいず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 が(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。

63.1.4 show trace modemmodule

[機能]

データ通信モジュール制御トレースの表示

[適用機種]

Si-R G110

[入力形式]

show trace modemmodule

[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]

データ通信モジュールの発着呼トレースデータを表示します。

[注意]

データ通信モジュール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]

```
# show trace modemmodule

[01]  USB   : ModemModule Status                        15.05.14 14:19:40.509
        sig_on=()
        ModemModule Inserted

[02]  USB   : ModemModule Status                        15.05.14 14:19:40.509
        sig_on=()
        ModemModule Open

[03]  USB   : Change Signal                             15.05.14 14:19:40.513
        sig_on=(CS,ER,RS)
        CS OFF -> ON

[04]  USB   : Change Signal                             15.05.14 14:19:40.513
        sig_on=(DR,CS,ER,RS)
        DR OFF -> ON

[05]  USB   : Change Signal                             15.05.14 14:19:40.513
        sig_on=(CD,DR,CS,ER,RS)
        CD OFF -> ON

[06]  USB   : Send                                      15.05.14 14:19:42.513
(1)-  (2)---   (3)-                                     ----------(4)--------
        sig_on=(CD,DR,CS,ER,RS)
        -------(5)-------------
        data=4154 5a0d 0a                               ATZ..
        ----(6)----------                               -(7)-

[07]  USB   : Recv                                      15.05.14 14:19:42.513
        sig_on=(CD,DR,CS,ER,RS)
        data=4154 5a                                    ATZ

[08]  USB   : Recv                                      15.05.14 14:19:42.519
        sig_on=(CD,DR,CS,ER,RS)
```

```
        data=4f4b                                   OK
#
```

1) ログ番号
ログ番号が、01～99 の 10 進数で表示されます。
2) データ通信モジュールが挿入されている USB の情報
3) 送受信
以下のいずれかが表示されます。

Send
ルータがデータ通信モジュールへデータを送信したことを示します。

Recv
ルータがデータ通信モジュール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。

ModemModule Status
以下の状態を示します。

表示	状態
ModemModule Inserted	データ通信モジュールの挿入の検出
ModemModule Ejected	データ通信モジュールの抜去の検出
ModemModule Open	データ通信モジュールの活性化
ModemModule Close	データ通信モジュールの非活性化
Start Modemmodule Reset	データ通信モジュールのリセット開始
Complete Modemmodule Reset	データ通信モジュールのリセット完了

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
データ通信モジュール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
データ通信モジュール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。
データ通信モジュール接続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 文字列で表示されます。

63.1.5 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 G110

[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 Mar  3 13:12:44 2011
--- ----        ------------------------
(1)  (2)                    (3)
        This platform does not support both privilege separation and
        ------------------------------------------------------------
                                    (4)
compression
-----------
    (4)
[2] sshd        Thu Mar  3 13:12:44 2011
        Compression disabled
[3] sshd        Thu Mar  3 13:12:44 2011
        info1: sshd version unknown
[4] sshd        Thu Mar  3 13:12:44 2011
        info1: read PEM private key done: type RSA
[5] sshd        Thu Mar  3 13:12:44 2011
        info1: private host key: #0 type 1 RSA
[6] sshd        Thu Mar  3 13:12:44 2011
        info1: read PEM private key done: type DSA
[7] sshd        Thu Mar  3 13:12:44 2011
        info1: private host key: #1 type 2 DSA
[8] sshd        Thu Mar  3 13:12:44 2011
        info1: Bind to port 22 on 0.0.0.0.
[9] sshd       Thu Mar  3 13:12:44 2011
        Server listening on 0.0.0.0 port 22.
[10] sshd       Thu Mar  3 13:12:44 2011
        info1: Bind to port 22 on ::.
[11] sshd       Thu Mar  3 13:12:44 2011
        Server listening on :: port 22.
```

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。

63.2 トレースのクリア

63.2.1 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 G110

[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 64 章 証明書関連の表示コマンド

64.1 証明書関連の表示

64.1.1 show crypto certificate

[機能]

証明書情報の表示

[適用機種]

Si-R G110

[入力形式]

show crypto certificate [base64] [candidate]

[オプション]

なし

動作中のすべての証明書情報(証明書要求、自装置証明書、相手装置証明書、認証局証明書)を表示します。

base64

Base64 形式で証明書情報(証明書要求、自装置証明書)を表示する場合に指定します。

candidate

編集中の構成定義から証明書情報を表示する場合に指定します。

[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/CE クラス)
構成定義モード(管理者クラス)

[説明]

証明書に関する情報を表示します。

[注意]

証明書によっては[実行例]と異なる表示が行われることがあります。

[実行例]

(1) オプションなし

```
# show crypto certificate
[Certificate Request]
[1]   Number : 0
      Version : 0
      Subject : C=JP, ST=Kanagawa, L=Kawasaki,
                O=Fujitsu Limited, OU=Tech Div.,
                CN=shisya.fujitsu.com, emailAddress=hoge@fujitsu.com
      Subject Public Key Info:
          Public Key Algorithm : rsaEncryption
          RSA Public Key : (1024 bit)
      Requested Extensions:
          X509v3 Key Usage:
                Digital Signature, Certificate Sign
          X509v3 Subject Alternative Name:
                IP Address:192.168.1.1
          X509v3 Subject Alternative Name:
                DNS:shisya-a.fujitsu.com
      Signature Algorithm : sha1WithRSAEncryption

[Local Certificate]
[1]   Number : 0,  Name : mycert.pem
      Version : 1
      Serial Number : 1 (0x1)
      Signature Algorithm : sha1WithRSAEncryption
```

```
      Issuer : C=JP, ST=Kanagawa, L=Kawasaki,
               O=Fujitsu Limited, OU=Tech Div.,
               CN=shisya.fujitsu.com, emailAddress=hoge@fujitsu.com
      Validity
          Not Before: Wed Mar  2 11:07:58 2011
          Not After : Mon Dec 31 11:07:58 2015
      Subject : C=JP, ST=Kanagawa, L=Kawasaki,
                O=Fujitsu Limited, OU=Tech Div.,
                CN=shisya.fujitsu.com, emailAddress=hoge@fujitsu.com
      Subject Public Key Info:
          Public Key Algorithm : rsaEncryption
          RSA Public Key : (1024 bit)
      X509v3 extensions:
          X509v3 Key Usage:
                Digital Signature, Certificate Sign
          X509v3 Subject Alternative Name:
                IP Address:192.168.1.1
          X509v3 Subject Alternative Name:
                DNS:shisya-a.fujitsu.com
          X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:1
      Signature Algorithm : sha1WithRSAEncryption
          5c:3c:df:94:6f:35:ce:55:83:78:45:9e:b3:71:ba:67:ed:80:
          b0:bf:fc:bb:a1:24:79:a6:94:dc:65:99:55:0a:05:8d:60:54:
          08:cf:5f:cc:08:db:f5:c8:69:3d:6a:df:12:3a:54:20:33:9c:
          e2:d1:b5:f2:a4:3d:29:d4:e0:77:52:cb:74:9b:31:b1:de:2d:
          e3:b1:5b:8a:24:a6:e7:d2:ab:32:b1:46:50:12:93:05:4b:b2:
          5d:60:7b:88:44:de:67:58:f0:63:a8:7e:bc:0a:a4:03:f3:33:
          de:27:69:55:73:07:2c:52:88:45:14:a0:3c:9a:bf:66:b0:48:
          95:35

[Remote Certificate]
[1]   Number : 0,  Name : peercert.pem
      Version : 3
      Serial Number: 0
      Signature Algorithm : md5WithRSAEncryption
      Issuer : C=JP, ST=Kanagawa, L=kawasaki,
               O=Fujitsu Limited
               OU=Tech Div.,
               CN=honsya.fujitsu.com,
               emailAddress=hoge@fujitsu.com
      Validity
          Not Before: Mar  2 07:50:53 2011
          Not After : Dec 31 07:50:53 2015
      Subject : C=JP, ST=Kanagawa, L=kawasaki,
                O=Fujitsu Limited
                OU=Tech Div.,
                CN=honsya.fujitsu.com,
                emailAddress=hoge@fujitsu.com
      Subject Public Key Info:
          Public Key Algorithm : rsaEncryption
          RSA Public Key : (1024 bit)
      X509v3 extensions:
          X509v3 Key Usage:
                Digital Signature, Certificate Sign
          X509v3 Subject Alternative Name:
                IP Address:192.168.2.1
          X509v3 Subject Alternative Name:
                DNS:shisya-b.fujitsu.com
          X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:1
      Signature Algorithm : md5WithRSAEncryption
          c2:9b:e5:cb:f0:24:e9:dd:6f:32:07:6d:70:86:18:e5:2d:78:
          8d:02:9d:da:d9:c1:f4:2b:47:cf:e6:f2:1b:89:7b:e4:88:2a:
          87:6b:85:c5:92:29:6d:8b:92:1a:f5:4e:4b:ec:c8:97:5c:a2:
          21:e9:71:33:9a:7b:40:f5:2c:fc:10:16:53:57:8f:52:6a:cb:
          ad:ab:1e:b4:46:e0:20:55:f4:a5:7c:a5:58:5f:02:6d:6d:3c:
          1f:d4:8c:20:37:e4:77:a7:62:9d:dc:69:90:0d:d5:99:59:4f:
          40:a4:b0:0a:46:80:17:69:00:f8:b0:1a:a3:42:1a:b2:c9:23:
          9b:4e
```

```
[CA Certificate]
[1]   Number : 0,  Name : cacert.pem
      Version : 3
      Serial Number: 0
      Signature Algorithm : md5WithRSAEncryption
      Issuer : C=JP, ST=Kanagawa, L=kawasaki,
               O=Fujitsu Limited
               OU=Tech Div.,
               CN=honsya.fujitsu.com,
               emailAddress=hoge@fujitsu.com
      Validity
          Not Before: Mar  2 07:50:53 2011
          Not After : Dec 31 07:50:53 2015
      Subject : C=JP, ST=Kanagawa, L=kawasaki,
                O=Fujitsu Limited
                OU=Tech Div.,
                CN=honsya.fujitsu.com,
                emailAddress=hoge@fujitsu.com
      Subject Public Key Info:
          Public Key Algorithm : rsaEncryption
          RSA Public Key : (1024 bit)
      Signature Algorithm : md5WithRSAEncryption
          c2:9b:e5:cb:f0:24:e9:dd:6f:32:07:6d:70:86:18:e5:2d:78:
          8d:02:9d:da:d9:c1:f4:2b:47:cf:e6:f2:1b:89:7b:e4:88:2a:
          87:6b:85:c5:92:29:6d:8b:92:1a:f5:4e:4b:ec:c8:97:5c:a2:
          21:e9:71:33:9a:7b:40:f5:2c:fc:10:16:53:57:8f:52:6a:cb:
          ad:ab:1e:b4:46:e0:20:55:f4:a5:7c:a5:58:5f:02:6d:6d:3c:
          1f:d4:8c:20:37:e4:77:a7:62:9d:dc:69:90:0d:d5:99:59:4f:
          40:a4:b0:0a:46:80:17:69:00:f8:b0:1a:a3:42:1a:b2:c9:23:
          9b:4e
#
```

(2) 編集中の構成定義からすべての証明書情報(証明書要求、自装置証明書、相手装置証明書)を表示

```
# show crypto certificate candidate
[Certificate Request]
[1]   Number : 0
      Version : 0
      Subject : C=JP, ST=Kanagawa, L=Kawasaki,
                O=Fujitsu Limited, OU=Tech Div.,
                CN=shisya.fujitsu.com, emailAddress=hoge@fujitsu.com
      Subject Public Key Info:
          Public Key Algorithm : rsaEncryption
          RSA Public Key : (1024 bit)
      Requested Extensions:
          X509v3 Key Usage:
                Digital Signature, Certificate Sign
          X509v3 Subject Alternative Name:
                IP Address:192.168.1.1
          X509v3 Subject Alternative Name:
                DNS:shisya-a.fujitsu.com
      Signature Algorithm : sha1WithRSAEncryption

[Local Certificate]
[1]   Number : 0,  Name : mycert.pem
      Version : 1
      Serial Number : 1 (0x1)
      Signature Algorithm : sha1WithRSAEncryption
      Issuer : C=JP, ST=Kanagawa, L=Kawasaki,
               O=Fujitsu Limited, OU=Tech Div.,
               CN=shisya.fujitsu.com, emailAddress=hoge@fujitsu.com
      Validity
          Not Before: Fri Mar  2 11:07:58 2011
          Not After : Tue Dec 31 11:07:58 2015
      Subject : C=JP, ST=Kanagawa, L=Kawasaki,
                O=Fujitsu Limited, OU=Tech Div.,
                CN=shisya.fujitsu.com, emailAddress=hoge@fujitsu.com
      Subject Public Key Info:
          Public Key Algorithm : rsaEncryption
          RSA Public Key : (1024 bit)
      X509v3 extensions:
```

```
        X509v3 Key Usage:
              Digital Signature, Certificate Sign
        X509v3 Subject Alternative Name:
              IP Address:192.168.1.1
        X509v3 Subject Alternative Name:
              DNS:shisya-a.fujitsu.com
        X509v3 Basic Constraints: critical
              CA:TRUE, pathlen:1
    Signature Algorithm : sha1WithRSAEncryption
        5c:3c:df:94:6f:35:ce:55:83:78:45:9e:b3:71:ba:67:ed:80:
        b0:bf:fc:bb:a1:24:79:a6:94:dc:65:99:55:0a:05:8d:60:54:
        08:cf:5f:cc:08:db:f5:c8:69:3d:6a:df:12:3a:54:20:33:9c:
        e2:d1:b5:f2:a4:3d:29:d4:e0:77:52:cb:74:9b:31:b1:de:2d:
        e3:b1:5b:8a:24:a6:e7:d2:ab:32:b1:46:50:12:93:05:4b:b2:
        5d:60:7b:88:44:de:67:58:f0:63:a8:7e:bc:0a:a4:03:f3:33:
        de:27:69:55:73:07:2c:52:88:45:14:a0:3c:9a:bf:66:b0:48:
        95:35

[Remote Certificate]
[1]   Number : 0,  Name : peercert.pem
      Version : 3
      Serial Number: 0
      Signature Algorithm : md5WithRSAEncryption
      Issuer : C=JP, ST=Kanagawa, L=kawasaki,
               O=Fujitsu Limited
               OU=Tech Div.,
               CN=honsya.fujitsu.com,
               emailAddress=hoge@fujitsu.com
      Validity
          Not Before: Mar  2 07:50:53 2011
          Not After : Dec 31 07:50:53 2015
      Subject : C=JP, ST=Kanagawa, L=kawasaki,
                O=Fujitsu Limited
                OU=Tech Div.,
                CN=honsya.fujitsu.com,
                emailAddress=hoge@fujitsu.com
      Subject Public Key Info:
          Public Key Algorithm : rsaEncryption
          RSA Public Key : (1024 bit)
      X509v3 extensions:
          X509v3 Key Usage:
                Digital Signature, Certificate Sign
          X509v3 Subject Alternative Name:
                IP Address:192.168.2.1
          X509v3 Subject Alternative Name:
                DNS:shisya-b.fujitsu.com
          X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:1
      Signature Algorithm : md5WithRSAEncryption
          c2:9b:e5:cb:f0:24:e9:dd:6f:32:07:6d:70:86:18:e5:2d:78:
          8d:02:9d:da:d9:c1:f4:2b:47:cf:e6:f2:1b:89:7b:e4:88:2a:
          87:6b:85:c5:92:29:6d:8b:92:1a:f5:4e:4b:ec:c8:97:5c:a2:
          21:e9:71:33:9a:7b:40:f5:2c:fc:10:16:53:57:8f:52:6a:cb:
          ad:ab:1e:b4:46:e0:20:55:f4:a5:7c:a5:58:5f:02:6d:6d:3c:
          1f:d4:8c:20:37:e4:77:a7:62:9d:dc:69:90:0d:d5:99:59:4f:
          40:a4:b0:0a:46:80:17:69:00:f8:b0:1a:a3:42:1a:b2:c9:23:
          9b:4e

[CA Certificate]
[1]   Number : 0,  Name : cacert.pem
      Version : 3
      Serial Number: 0
      Signature Algorithm : md5WithRSAEncryption
      Issuer : C=JP, ST=Kanagawa, L=kawasaki,
               O=Fujitsu Limited
               OU=Tech Div.,
               CN=honsya.fujitsu.com,
               emailAddress=hoge@fujitsu.com
      Validity
          Not Before: Mar  2 07:50:53 2011
          Not After : Dec 31 07:50:53 2015
```

```
      Subject : C=JP, ST=Kanagawa, L=kawasaki,
                O=Fujitsu Limited
                OU=Tech Div.,
                CN=honsya.fujitsu.com,
                emailAddress=hoge@fujitsu.com
      Subject Public Key Info:
          Public Key Algorithm : rsaEncryption
          RSA Public Key : (1024 bit)
      Signature Algorithm : md5WithRSAEncryption
          c2:9b:e5:cb:f0:24:e9:dd:6f:32:07:6d:70:86:18:e5:2d:78:
          8d:02:9d:da:d9:c1:f4:2b:47:cf:e6:f2:1b:89:7b:e4:88:2a:
          87:6b:85:c5:92:29:6d:8b:92:1a:f5:4e:4b:ec:c8:97:5c:a2:
          21:e9:71:33:9a:7b:40:f5:2c:fc:10:16:53:57:8f:52:6a:cb:
          ad:ab:1e:b4:46:e0:20:55:f4:a5:7c:a5:58:5f:02:6d:6d:3c:
          1f:d4:8c:20:37:e4:77:a7:62:9d:dc:69:90:0d:d5:99:59:4f:
          40:a4:b0:0a:46:80:17:69:00:f8:b0:1a:a3:42:1a:b2:c9:23:
          9b:4e
#
```

(3) base64 オプションを指定して動作中の証明書情報(証明書要求、自装置証明書)を表示

```
# show crypto certificate base64
[Certificate Request]
[1]   Number : 0
-----BEGIN CERTIFICATE REQUEST-----
MIICMDCCAZkCAQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYDVQQIEwhLYW5hZ2F3YTER
MA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0c3UgTGltaXRlZDESMBAG
A1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJzaGlzeWEuZnVqaXRzdS5jb20xHzAd
BgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBAMk7Bq9Ciaxh17fYIkwbRLI64EAjP1RnDrEnLJ/ds9ErIoT4sPBc
Z9a0mvdz0nRlK8HmNmDGMo1DRufBWueSvs9Qgl0zykQu+R3YKPMNMJ3gL06tiNkl
6TtNNUAK+OGda0brLL6t6+jE/U1Kskjt7UzdH1an1AroLkLtkrVqcBPjAgMBAAGg
UDBOBgkqhkiG9w0BCQ4xQTA/MAsGA1UdDwQEAwIChDAPBgNVHREECDAGhwTAqAEB
MB8GA1UdEQQYMBaCFHNoaXN5YS1hLmZ1aml0c3UuY29tMA0GCSqGSIb3DQEBBQUA
A4GBACRKhbhx8kl08Jf7w9YNgzHN+ORyY2sIrqhqpytSquNonvcZZaEgVeqygUqQ
WOIqhggINKSRW82odtTFi97Ttga1yijj5GeaVCLaSE6FH9lLhcLlArY2dArRYM/x
Zv62xudPCLvwe+w49N8gA+Dq+9G3wCSYA0kFQNJmm/HIpUnb
-----END CERTIFICATE REQUEST-----

[Local Certificate]
[1]   Number : 0,  Name : mycert.pem
-----BEGIN CERTIFICATE-----
MIIDBjCCAm8CAQEwDQYJKoZIhvcNAQEFBQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYD
VQQIEwhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
c3UgTGltaXRlZDESMBAGA1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJzaGlzeWEu
ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
MDcwNzIwMDIwNzU4WhcNMDcxMjMxMDIwNzU4WjCBnzELMAkGA1UEBhMCSlAxETAP
BgNVBAgTCEthbmFnYXdhMREwDwYDVQQHEwhLYXdhc2FraTEYMBYGA1UEChMPRnVq
aXRzdSBMaW1pdGVkMRIwEAYDVQQLEwlUZWNoIERpdi4xGzAZBgNVBAMTEnNoaXN5
YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAyTsGr0KJrGHXt9giTBtEsjrgQCM/
VGc0sScsn92z0SsihPiw8Fxn1rSa93PSdGUrweY2YMYyjUNG58Fa55K+z1CCXTPK
RC75Hdgo8w0wneAvTq2I2SXp0001QAr44Z1rRussvq3r6MT9TUqyS03tTN0fVqfU
CuguQu2StWpwE+MCAwEAAaNVMFMwCwYDVR0PBAQDAgKEMA8GA1UdEQQIMAaHBMCo
AQEwHwYDVR0RBBgwFoIUc2hpc3lhLWEuZnVqaXRzdS5jb20wEgYDVR0TAQH/BAgw
BgEB/wIBATANBgkqhkiG9w0BAQUFAAOBgQBcPN+UbzXOVYN4RZ6zcbpn7YCwv/y7
oSR5ppTcZZlVCgWNYFQIz1/MCNv1yGk9at8SOlQgM5zi0bXypD0p10B3Ust0mzGx
3i3jsVuKJKbn0qsysUZQEpMFS7JdYHuIRN5nWPBjqH68CqQD8zPeJ2lVcwcsUohF
FKA8mr9msEiVNQ==
-----END CERTIFICATE-----

#
```

(4) base64 オプションを指定して編集中の構成定義から証明書情報(証明書要求、自装置証明書)を表示

```
# show crypto certificate base64 candidate
[Certificate Request]
[1]   Number : 0
-----BEGIN CERTIFICATE REQUEST-----
MIICMDCCAZkCAQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYDVQQIEwhLYW5hZ2F3YTER
MA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0c3UgTGltaXRlZDESMBAG
A1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJzaGlzeWEuZnVqaXRzdS5jb20xHzAd
BgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBAMk7Bq9Ciaxh17fYIkwbRLI64EAjP1RnDrEnLJ/ds9ErIoT4sPBc
Z9a0mvdz0nRlK8HmNmDGMo1DRufBWueSvs9Qgl0zykQu+R3YKPMNMJ3gL06tiNkl
6TtNNUAK+OGda0brLL6t6+jE/U1Kskjt7UzdH1an1AroLkLtkrVqcBPjAgMBAAGg
UDBOBgkqhkiG9w0BCQ4xQTA/MAsGA1UdDwQEAwIChDAPBgNVHREECDAGhwTAqAEB
MB8GA1UdEQQYMBaCFHNoaXN5YS1hLmZ1aml0c3UuY29tMA0GCSqGSIb3DQEBBQUA
A4GBACRKhbhx8kl08Jf7w9YNgzHN+ORyY2sIrqhqpytSquNonvcZZaEgVeqygUqQ
WOIqhggINKSRW82odtTFi97Ttga1yijj5GeaVCLaSE6FH91LhcLlArY2dArRYM/x
Zv62xudPCLvwe+w49N8gA+Dq+9G3wCSYA0kFQNJmm/HIpUnb
-----END CERTIFICATE REQUEST-----

[Local Certificate]
[1]   Number : 0,  Name : mycert.pem
-----BEGIN CERTIFICATE-----
MIIDBjCCAm8CAQEwDQYJKoZIhvcNAQEFBQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYD
VQQIEwhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
c3UgTGltaXRlZDESMBAGA1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJzaGlzeWEu
ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
MDcwNzIwMDIwNzU4WhcNMDcxMjMxMDIwNzU4WjCBnzELMAkGA1UEBhMCSlAxETAP
BgNVBAgTCEthbmFnYXdhMREwDwYDVQQHEwhLYXdhc2FraTEYMBYGA1UEChMPRnVq
aXRzdSBMaW1pdGVkMRIwEAYDVQQLEwlUZWNoIERpdi4xGzAZBgNVBAMTEnNoaXN5
YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAyTsGr0KJrGHXt9giTBtEsjrgQCM/
VGc0sScsn92z0SsihPiw8Fxn1rSa93PSdGUrweY2YMYyjUNG58Fa55K+z1CCXTPK
RC75Hdgo8w0wneAvTq2I2SXp0001QAr44Z1rRussvq3r6MT9TUqyS03tTN0fVqfU
CuguQu2StWpwE+MCAwEAAaNVMFMwCwYDVR0PBAQDAgKEMA8GA1UdEQQIMAaHBMCo
AQEwHwYDVR0RBBgwFoIUc2hpc3lhLWEuZnVqaXRzdS5jb20wEgYDVR0TAQH/BAgw
BgEB/wIBATANBgkqhkiG9w0BAQUFAAOBgQBcPN+UbzXOVYN4RZ6zcbpn7YCwv/y7
oSR5ppTcZZlVCgWNYFQIz1/MCNv1yGk9at8SOlQgM5zi0bXypD0p10B3Ust0mzGx
3i3jsVuKJKbn0qsysUZQEpMFS7JdYHuIRN5nWPBjqH68CqQD8zPeJ2lVcwcsUohF
FKA8mr9msEiVNQ==
-----END CERTIFICATE-----

#
```

```
[1]   Number : 0,  Name : peercert.pem
---   ----------   -------------------
(1)         (2)          (3)
      Version : 3
      -----------
            (4)
      Serial Number: 0
      ----------------
            (5)
      Signature Algorithm : md5WithRSAEncryption
      -------------------------------------------
                (6)
      Issuer : C=JP, ST=Kanagawa, L=kawasaki,
               ----  -----------  ----------
                (7)      (8)          (9)
               O=Fujitsu Limited
               -----------------
                (10)
               OU=Tech Div.,
               ------------
                (11)
               CN=shisya.fujitsu.com,
               ----------------------
                (12)
               emailAddress=hoge@fujitsu.com
               -----------------------------
                (13)
```

```
Validity
    Not Before: Mar  2 07:50:53 2011
    --------------------------------
          (14)
    Not After : Dec 31 07:50:53 2015
    --------------------------------
          (15)
Subject : C=JP, ST=Kanagawa, L=kawasaki,
          ----  -----------  ----------
          (16)    (17)         (18)
          O=Fujitsu Limited
          -----------------
          (19)
          OU=Tech Div.,
          ------------
          (20)
          CN=shisya.fujitsu.com,
          ----------------------
          (21)
          emailAddress=hoge@fujitsu.com
          -----------------------------
          (22)
Subject Public Key Info:
    Public Key Algorithm : rsaEncryption
    ------------------------------------
          (23)
    RSA Public Key : (1024 bit)
    ---------------------------
          (24)
X509v3 extensions:
    X509v3 Key Usage:
          Digital Signature, Certificate Sign
    ---------------------------------------
          (25)
    X509v3 Subject Alternative Name:
          IP Address:192.168.1.1
    -------------------------------
          (26)
    X509v3 Subject Alternative Name:
          DNS:shisya-a.fujitsu.com
    --------------------------------
          (27)
    X509v3 Basic Constraints: critical
          CA:TRUE, pathlen:1
    ----------------------------------
          (28)
Signature Algorithm : md5WithRSAEncryption
-------------------------------------------
          (29)
    c2:9b:e5:cb:f0:24:e9:dd:6f:32:07:6d:70:86:18:e5:2d:78:
    8d:02:9d:da:d9:c1:f4:2b:47:cf:e6:f2:1b:89:7b:e4:88:2a:
    87:6b:85:c5:92:29:6d:8b:92:1a:f5:4e:4b:ec:c8:97:5c:a2:
    21:e9:71:33:9a:7b:40:f5:2c:fc:10:16:53:57:8f:52:6a:cb:
    ad:ab:1e:b4:46:e0:20:55:f4:a5:7c:a5:58:5f:02:6d:6d:3c:
    1f:d4:8c:20:37:e4:77:a7:62:9d:dc:69:90:0d:d5:99:59:4f:
    40:a4:b0:0a:46:80:17:69:00:f8:b0:1a:a3:42:1a:b2:c9:23:
    9b:4e
    -----------------------------------------------------
          (30)
```

1) 証明書の表示番号
2) 識別番号
3) 識別名
4) バージョン
5) シリアル番号
6) 署名アルゴリズム
7) 国コード
8) 都道府県
9) 市区町村

10) 組織または会社
11) 組織ユニットまたは部門
12) ホスト名
13) E メールアドレス
14) 証明書の発行日時
15) 証明書の有効期限
16) 国コード
17) 都道府県
18) 市区町村
19) 組織または会社
20) 組織ユニットまたは部門
21) 通常名
22) E メールアドレス
23) 公開鍵アルゴリズム
24) 公開鍵の内容
25) 証明書の利用方法
26) サブジェクト代替名称(IP アドレス)
27) サブジェクト代替名称(DNS 名)
28) 証明書の規制
29) 署名アルゴリズム
30) 署名の内容

第 65 章 認証関連制御コマンド

・ グループ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〈group〉(ether グループ定義番号)に指定するグループ番号の通し番号(10 進数)は、以下に示す範囲で指定してください。

範囲	機種
2	Si-R G110

・ ポ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〈port〉(ether ポート定義番号)に指定するポート番号の通し番号(10 進数)は、以下に示す範囲で指定してください。

範囲	機種
1～4	Si-R G110（グループ 2）

65.1 IEEE802.1X 認証制御

65.1.1 dot1xctl initialize port ether

[機能]

IEEE802.1X 認証状態の初期化

[適用機種]

Si-R G110

[入力形式]

dot1xctl initialize port ether <group> <port> [<macaddr>]

[オプション]

<group> <port>

指定されたポートの認証状態を変更します。

<group>

ether グループ番号を、10 進数で指定します。

グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

ether ポート番号を、10 進数で指定します。

ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<macaddr>

指定された MAC アドレスを持つ端末(Supplicant)の認証状態を変更します。

(XX:XX:XX:XX:XX:XX の形式で、XX は 2 桁の 16 進数です。)

[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]

指定されたポートまたは端末(Supplicant)の認証状態を初期状態に戻します。

[実行例]

```
# dot1xctl initialize port ether 2 1
#
```

65.1.2 dot1xctl reconfirm port ether

[機能]

IEEE802.1X 再認証の実行

[適用機種]

Si-R G110

[入力形式]

dot1xctl reconfirm port ether <group> <port> [<macaddr>]

[オプション]

<group> <port>

指定されたポートの認証状態を変更します。

<group>

ether グループ番号を、10 進数で指定します。

グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

ether ポート番号を、10 進数で指定します。

ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<macaddr>

指定された MAC アドレスを持つ端末(Supplicant)の認証状態を変更します。

(XX:XX:XX:XX:XX:XX の形式で、XX は 2 桁の 16 進数です。)

[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]

指定されたポートまたは端末(Supplicant)の再認証を開始します。

[注意]

本コマンドを連続することにより、ネットワークを不安定にするだけでなく、接続中の端末(Supplicant)が切断されてしまう場合があります。

[実行例]

```
# dot1xctl reconfirm port ether 2 1
#
```

65.2 MAC アドレス認証制御

65.2.1 macauthctl initialize port ether

[機能]

MAC アドレス認証状態の解除

[適用機種]

Si-R G110

[入力形式]

macauthctl initialize port ether <group> <port> [<macaddr>]

[オプション]

<group> <port>

指定されたポートの認証状態を変更します。

<group>

ether グループ番号を、10 進数で指定します。

グループ番号の指定方法の詳細については、本章の冒頭を参照してください。

<port>

ether ポート番号を、10 進数で指定します。

ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<macaddr>

指定された MAC アドレスを持つ端末の認証状態を変更します。

(XX:XX:XX:XX:XX:XX の形式で、XX は 2 桁の 16 進数です。)

[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]

指定されたポートまたは端末の認証状態を初期状態に戻します。

[実行例]

```
# macauthctl initialize port ether 2 1
#
```

65.3 ARP 認証制御

65.3.1 arpauthctl initialize

[機能]

ARP 認証状態を変更します。

[適用機種]

Si-R G110

[入力形式]

arpauthctl initialize <vid> [<macaddr>]

[オプション]

initialize

認証状態を初期状態に戻します。

<vid>

・ VLAN ID

指定された VLAN の端末の認証状態を変更します。

VLAN ID を、1～4094 の 10 進数で指定します。

<macaddr>

・ MAC アドレス

認証端末の MAC アドレスを指定します。

省略した場合は、指定された VLAN のすべての端末の認証状態を変更します。

XX:XX:XX:XX:XX:XX の形式で指定します。XX は 2 桁の 16 進数です。

[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]

指定された端末の認証状態を変更します。

[実行例]

```
# arpauthctl initialize 1
#
```

第 66 章 回線制御コマンド

66.1 回線制御

66.1.1 offline

[機能]

切断、または閉塞の実施

[適用機種]

Si-R G110

[入力形式]

```
offline ether [group <group> [port <port>]]
offline pseudo-ether [<interface_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]

ether

すべての ether ポートを閉塞(リンクダウン)します。

ether group <group>

指定された ether グループのポートを閉塞(リンクダウン)します。

ether group <group> port <port>

指定された ether グループの指定されたポートを閉塞(リンクダウン)します。
複数の ether 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。

pseudo-ether

すべての pseudo ether インタフェースを閉塞(リンクダウン)します。

pseudo-ether <interface_number>

指定された pseudo ether インタフェースを閉塞(リンクダウン)します。
<interface_number>で指定可能な範囲は以下のとおりです。

範囲	機種
1	Si-R G110

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
0～99	Si-R G110

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
0～99	Si-R G110

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 進数で指定します。

範囲	機種
0～1	Si-R G110

<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
0～99	Si-R G110

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]

"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 ether group 1 port 1
closed [1 1]                                                    ---(1)
#
```

```
# offline policy-group 0
<ERROR> already closed [0]                                    ---(2)
#
```

```
# offline remote 0 ap 0
<ERROR> cannot close [0 0]                                    ---(3)
#
```

1) 閉塞した場合、以下のメッセージが表示されます。

   closed [<target>]

2) すでに閉塞中の ether ポートに対して閉塞した場合、以下のメッセージが表示されます。

   <ERROR> already closed [<target>] : <detail>

3) 有効になっていない ether ポートに対して閉塞した場合、以下のメッセージが表示されます。

   <ERROR> cannot close [<target>] : <detail>

   <target>は、入力コマンドごとに異なり、以下のように表示されます。

   - offline ether の場合
     <group> <port>
   - offline pseudo-ether の場合
     <interface_number>
   - offline access-point の場合
     <ap_name>
   - offline template interface の場合
     <interface_name>
   - offline template の場合
     <template_number>
   - offline policy-group の場合
     <policy-group_number>

   <detail>はエラーの詳細を表し、詳細がある場合にのみ表示されます。

66.1.2 online

[機能]

接続、または閉塞解除の実施

[適用機種]

Si-R G110

[入力形式]

online ether [group <group> [port <port>]]
online pseudo-ether [<interface_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]

ether
すべての ether ポートを閉塞解除します。

ether group <group>
指定された ether グループのポートを閉塞解除します。

ether group <group> port <port>
指定された ether グループの指定されたポートを閉塞解除します。
複数の ether 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。

pseudo-ether
すべての pseudo ether インタフェースを閉塞解除します。

pseudo-ether <interface_number>
指定された pseudo ether インタフェースを閉塞解除します。
<interface_number>で指定可能な範囲は以下のとおりです。

範囲	機種
1	Si-R G110

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
0～99	Si-R G110

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
0～99	Si-R G110

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 128 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 128 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 進数で指定します。

範囲	機種
0～1	Si-R G110

<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
0～99	Si-R G110

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。

[実行例]

```
# online ether group 1 port 1
opened [1 1]                                                    ---(1)
#
```

```
# online ether group 2 port 8
<ERROR> already opened [2 8]                                    ---(2)
#
```

```
# online remote 0 ap 0
<ERROR> cannot open [0 0]                                       ---(3)
#
```

1) 閉塞解除した場合、以下のメッセージが表示されます。

   opened [<target>]

2) すでに閉塞解除されている ether ポートに対して閉塞解除した場合、以下のメッセージが表示されます。

   <ERROR> already opened [<target>] : <detail>

3) 有効になっていない ether ポートに対して閉塞した場合、以下のメッセージが表示されます。

   <ERROR> cannot open [<target>] : <detail>

   <target>は、入力コマンドごとに異なり、以下のように表示されます。

   - online ether コマンドの場合
     <group> <port>
   - online pseudo-ether の場合
     <interface_number>
   - online access-point コマンドの場合
     <ap_name>
   - online template コマンドの場合
     <template_number>
   - online policy-group コマンドの場合
     <policy-group_number>

   <detail>はエラー詳細で、詳細がない場合は表示されません。

第 67 章 VRRP 制御コマンド

67.1 VRRP 制御

67.1.1 vrrp action

[機能]

VRRP の手動停止および再開始

[適用機種]

Si-R G110

[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-R G110

interface <interface_name>の省略時は、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>の省略時は、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、手動で停止状態にしたり、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)

[注意]

VRRP グループを手動停止した状態で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。

[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]

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 disable
vrrp: command accepted vrid10
# vrrp action interface lan0 vrid 10 enable
vrrp: command accepted vrid10
#
```

67.1.2 vrrp preempt-permit

[機能]

VRRP プリエンプトモードの制御

[適用機種]

Si-R G110

[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-R G110

interface <interface_name>の省略時は、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>の省略時は、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切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 68 章 動的 VPN サーバ制御コマンド

68.1 動的VPNサーバ制御

68.1.1 dvpnserver disable

[機能]

動的VPNサーバの手動停止

[適用機種]

Si-R G110

[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、手動で停止状態にすることができます。

[実行例]

```
# dvpnserver disable
#
```

68.1.2 dvpnserver enable

[機能]

動的VPNサーバの再開始

[適用機種]

Si-R G110

[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]

```
# dvpnserver enable
#
```

第 69 章 RADIUS 制御コマンド

69.1 RADIUS 制御

69.1.1 radius recovery

[機能]

RADIUS サーバの復旧

[適用機種]

Si-R G110

[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 70 章 AAA 制御コマンド

70.1 端末MACアドレス収集

・ 収集したMACアドレスのリスト番号の範囲

範囲	機種
1～1000	Si-R G110

70.1.1 aaactl mac collect start

[機能]

端末MACアドレス収集開始

[適用機種]

Si-R G110

[入力形式]

aaactl mac collect start <group_id>

[オプション]

<group_id>

端末MACアドレス収集を開始する対象となるAAA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]

端末MACアドレスの収集を開始し、収集モードに移行します。収集モードではすべての端末MACアドレスの認証は、AAAユーザ情報定義またはRADIUSの認証結果に関係なく認証成功となります。

AAAユーザ定義情報を利用して認証を行う場合は、本来認証失敗となるはずの端末MACアドレスの収集が行われます。端末MACアドレスは、認証が失敗したものの中から収集可能なMACアドレス数まで収集を行い、それを超える分は収集は行われません。

RADIUSを利用して認証を行う場合は、端末MACアドレスの収集は行われません。

端末MACアドレス収集がすでに動作中の場合はエラーメッセージを出力して終了します。また、端末MACアドレスを収集後に、別のAAA定義番号で収集を開始した場合は、それまでに収集した端末MACアドレスはすべてクリアされます。同一のAAA定義番号で収集を開始した場合は、クリアしないで継続して収集を行います。

[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。

```
aaactl: command accepted
```

端末MACアドレス収集が動作中の場合は以下のメッセージを出力します。

```
<ERROR> aaactl: mac collect is running on group <group_id>
```

<group_id>

動作中のAAA定義番号を示します。

指定したAAA定義番号が不正であった場合は以下のメッセージを出力します。

```
<ERROR> aaactl: illegal group id
```

［実行例］

```
# aaactl mac collect start 0
aaactl: command accepted
#
```

70.1.2 aaactl mac collect stop

[機能]

端末MACアドレス収集終了

[適用機種]

Si-R G110

[入力形式]

aaactl mac collect stop

[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]

端末MACアドレスの収集を終了し、端末MACアドレスの認証を通常の運用モードに移行します。

[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。

```
aaactl: command accepted
```

端末MACアドレス収集が動作していない場合は以下のメッセージを出力します。

```
<ERROR> aaactl: mac collect is not running
```

<group_id>
動作中のAAA定義番号を示します。

[実行例]

```
# aaactl mac collect stop
aaactl: command accepted
#
```

70.1.3 aaactl mac collect mark

[機能]

端末MACアドレス収集結果から登録候補を選択

[適用機種]

Si-R G110

[入力形式]

aaactl mac collect mark <mark_list>

[オプション]

<mark_list>

マーキング対象とするリスト番号を10進数で指定します。

複数のリス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、「2-35」のように"-"(ハイフン)を使用して指定します。

リスト番号は、"," (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。

- 10進数値 (例: 99 = リスト番号99)
- リスト番号-リスト番号 (例: 32-64 = 32〜64までのリスト番号)
- リスト番号- (例: 5- = 5〜100までのリスト番号)
- -リスト番号 (例: -92 = 1〜92までのリスト番号)
- リスト番号,リスト番号,… (例: 10,20,30- = 10と20と30以降のリスト番号)
- all
  すべてのリスト番号を対象とする場合に指定します。

[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]

MACアドレス収集機能を用いて収集した端末MACアドレスを、AAAユーザ情報に登録する登録候補として選択します。
候補として選択された端末MACアドレスは、show aaa mac collect list コマンドで * 印付で表示されます。

[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。

```
aaactl: command accepted
```

指定したリスト番号が存在しないリスト番号であった場合は以下のメッセージを出力します。

```
<ERROR> aaactl: illegal list number
```

[実行例]

```
# aaactl mac collect mark 1,3-7,10-21,30
aaactl: command accepted
#
```

70.1.4 aaactl mac collect unmark

[機能]

端末MACアドレス収集結果から登録候補を選択解除

[適用機種]

Si-R G110

[入力形式]

aaactl mac collect unmark <unmark_list>

[オプション]

<unmark_list>

マーキング対象外とするリスト番号を10進数で指定します。

複数のリス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、「2-35」のように"-"(ハイフン)を使用して指定します。

リスト番号は、"," (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。

- 10進数値 (例: 99 = リスト番号99)
- リスト番号-リスト番号 (例: 32-64 = 32～64までのリスト番号)
- リスト番号- (例: 5- = 5～100までのリスト番号)
- -リスト番号 (例: -92 = 1～92までのリスト番号)
- リスト番号,リスト番号,… (例: 10,20,30- = 10と20と30以降のリスト番号)
- all
  すべてのリスト番号を対象外とする場合に指定します。

[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]

MACアドレス収集機能を用いて収集した端末MACアドレスを、AAAユーザ情報に登録する登録候補の選択から外します。

候補から外れた端末MACアドレスは、show aaa mac collect list コマンドで * 印なしで表示されます。

[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。

```
aaactl: command accepted
```

指定したリスト番号が存在しないリスト番号であった場合は以下のメッセージを出力します。

```
<ERROR> aaactl: illegal list number
```

[実行例]

```
# aaactl mac collect unmark 5,13-15
aaactl: command accepted
#
```

70.1.5 aaactl mac collect commit

[機能]

選択した端末MACアドレスのAAAユーザ情報への登録

[適用機種]

Si-R G110

[入力形式]

aaactl mac collect commit [password <password>]

[オプション]

password <password>

AAAユーザ情報定義に端末MACアドレスと同時に登録する認証パスワードを、0x21,0x23～0x7eの64文字以内の文字列で指定します。

省略時はユーザIDと同じ文字列が認証パスワードとして登録されます。

[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]

MACアドレス収集機能を用いて収集した端末MACアドレスのうち、AAAユーザ情報に登録するために選択した登録候補を、編集中構成定義情報のAAAユーザ情報に登録します。

MACアドレス収集機能が収集モードで動作しているときには、本操作は行えません。

同じ端末MACアドレスがAAAユーザ情報にすでに存在する場合は、その端末MACアドレスは登録候補として選択されていても無視され、すでにあるその端末MACアドレスのAAAユーザ情報は変更されません。

登録はAAAユーザ情報定義が定義されていないもっとも小さいAAAユーザ情報定義番号に対して、選択したリストの番号順に行われます。選択した端末MACアドレスの数がユーザ情報の空きよりも多い場合は、登録できるところまで登録を行い、登録ができなかったリスト番号の先頭をエラーメッセージとともに出力して終了します。

本操作で編集中構成定義に登録したAAAユーザ情報を認証情報として使用するためには、commitコマンドを使用して編集中構成定義を運用中構成定義に反映する必要があります。

[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。

```
aaactl: command accepted
```

AAAユーザ情報の空きが、選択した端末MACアドレスよりも少なかった場合は、以下のメッセージを出力します。

```
<WARNING> aaactl: aaa <group_id> user full, list <number> and later not committed
```

<group_id>

AAA定義番号を示します。

<number>

ユーザ定義情報の空きがなく構成定義に反映されなかった先頭のリスト番号を示します。

端末MACアドレス収集が動作中の場合は以下のメッセージを出力します。

```
<ERROR> aaactl: mac collect is running on group <group_id>
```

<group_id>

動作中のAAA定義番号を示します。

指定したパスワードが長過ぎる場合は以下のメッセージを出力します。

```
<ERROR> aaactl: password too long
```

指定したパスワードが定義不能であった場合は以下のメッセージを出力します。

```
<ERROR> aaactl: illegal password
```

［実行例］

```
# aaactl mac collect commit password klj8hIGU
aaactl: command accepted
#
```

第 71 章 USB ポート制御コマンド

・ USB 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 usb <line>(USB 番号)に指定する挿入されている USB の番号(10 進数)は、機種ごとに以下に示す範囲で指定してください。ただし、USB ポートが 1 つの機種は、USB 番号の指定はできません。

範囲	機種
指定不可	Si-R G110

71.1 USB ポート制御

71.1.1 usbctl

[機能]

USB ポートの状態の制御

[適用機種]

Si-R G110

[入力形式]

usbctl <mode> [usb <line>]

[オプション]

<mode>

・ enable
USB ポートを使用可能な状態にします。

・ eject
USB ポートに実装されている USB デバイスを安全に取り外すために実行します。

・ restart
USB ポートに実装されているデータ通信モジュールを再起動し、使用可能な状態にします。

なし

全 USB ポートの状態の制御を行います。

usb <line>

指定の USB ポート番号のみの状態の制御を行います。

・ USB 番号
挿入されている USB の番号を指定します。
USB 番号の指定方法の詳細については、本章の冒頭を参照してください。

[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]

USB ポートの状態の制御を行います。

USB ポートに実装されている USB デバイスを安全に取り外すために、usbctl eject コマンドを実行します。

また、USB デバイスの取り外し後は、USB デバイスを自動認識します。

usbctl enable コマンドを実行することで、過電流検出で USB ポートが使用不可能な状態の場合に、使用可能な状態にします。過電流検出状態以外で実行した場合は何も行われません。

usbctl restart コマンドを実行することで、USB ポートに実装されているデータ通信モジュールを再起動し、使用可能な状態にします。

[注意]

usbctl restart コマンドは USB デバイスの強制的な取り外しを行いますので、USB メモリが取り付けられている USB ポートに対して使用しないでください。

usbctl eject コマンド実行後は、USB デバイスを取り外してください。

[実行例]

```
# usbctl enable usb
enable ok. [USB]
#
```

過電流状態でusbctl enableコマンドを実行し成功した場合は、上記メッセージが表示されます。

```
# usbctl enable usb
<ERROR> cannot enable. Please try again. [USB]
#
```

usbctl enableコマンドに失敗した場合は、上記メッセージが表示されます。
上記メッセージが出力された場合は、5秒以上待ってから再度同じコマンドを実行してください。

```
# usbctl eject usb
eject ok. [USB]
#
```

usbctl ejectコマンドに成功した場合は、上記メッセージが表示されます。
上記メッセージが出力された後、USBデバイスを取り外してください。

```
# usbctl eject usb
#
```

USBデバイス未実装状態、またはusbctl ejectコマンドを実行後にUSBデバイスを抜き取らない状態で再度usbctl ejectコマンドを実行した場合は、何も表示されません。

```
# usbctl eject usb
<ERROR> cannot eject. Please try again. [USB]
#
```

usbctl ejectコマンドに失敗した場合は、上記メッセージが表示されます。
上記メッセージが出力された場合は、5秒以上待ってから再度同じコマンドを実行してください。

```
# usbctl restart usb
restart accepted. [USB]
#
```

usbctl restartコマンドの実行に成功した場合は、上記メッセージが表示されます。
データ通信モジュールが使用可能な状態になったことは、システムログ(USBデバイス接続)で確認してください。

```
# usbctl restart usb
restart running now. [USB]
#
```

データ通信モジュールの再起動中にusbctlコマンドを実行した場合、上記メッセージが表示され、何も行われません。
上記メッセージが出力された場合は、3秒以上待ってから再度同じコマンドを実行してください。

```
# usbctl restart usb
<ERROR> cannot restart. Please try again. [USB]
#
```

usbctl restartコマンドに失敗した場合は、上記メッセージが表示されます。
上記メッセージが出力された場合は、5秒以上待ってから再度同じコマンドを実行してください。

第 72 章 証明書関連制御コマンド

72.1 証明書関連の制御

72.1.1 crypto certificate generate

[機能]

秘密鍵、証明書要求、自装置証明書の設定

[適用機種]

Si-R G110

[入力形式]

crypto certificate generate

[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]

対話形式で秘密鍵、証明書要求、自装置証明書の設定を行います。
コマンド実行後、指示に従い自装置の情報を:(コロン)以降に入力してください。
秘密鍵と証明書要求は同じ識別番号で設定され、鍵ペアと判断されます。
自装置証明書のみを設定する場合、事前に秘密鍵、証明書要求が設定されている必要があります。
本コマンドは運用管理コマンドですが、設定した内容は以下の構成定義コマンドとして設定されます。

秘密鍵

: certificate private line

証明書要求

: certificate request line

自装置証明書

: certificate local name
certificate local line

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、定義反映を行う場合は、commit コマンドまたは save コマンド実行後に reset コマンドを行ってください。

[注意]

すでに「crypto certificate generate」コマンド、「crypto certificate local」コマンドで設定を行っている場合は以前と違う情報で上書きされます。
本コマンドで定義した内容は、以下の構成定義情報を delete コマンドで削除できます。

秘密鍵

: certificate private line

証明書要求

: certificate request line

自装置証明書

: certificate local name
certificate local line

[実行例]

(1) 秘密鍵、証明書要求と自装置証明書の設定を行う場合

:(コロン)より後ろの部分を入力します

```
(config)# crypto certificate generate
```

```
RSA key pair number[0-4] :0
generate RSA key pair.
Are you sure?[y/n] :y
RSA key pair and Certificate request will be overwritten.  (上書きすることを通知するメッセージ
Are you sure?[y/n] :y                                      は鍵ペアが未設定の場合は表示されません)
Local certificate number[0-4] :0
Local certificate will be overwritten.  (上書きすることを通知するメッセージは自装置証明書が
Are you sure?[y/n] :y                                      未設定の場合は表示されません)
key bit(361-2048) :1024
certificate request hash(sha1 or md5) :sha1
local certificate name :cert.pem
local certificate hash(sha1 or md5) :sha1
expire date(YYYYMMDD) :20151231
Country Name(2 letter code) :JP
State or Province Name :Kanagawa
Locality Name :Kawasaki
Organization Name :Fujitsu Limited
Organizational Unit Name :Tech Div.
Common Name :shisya.fujitsu.com
Email Address :hoge@fujitsu.com
subjectAltName IP :192.168.1.1
subjectAltName DNS :shisya-A.fujitsu.com
Please wait to create RSA private key and Certificate request.
certificate private 0 line 0 HABNg39no/6PrWicHYI2Ambcsqbvwcr8d03hsDstuY8MrRKghUF20fCP7FxV2qC1S
nTnboIjjha3bPcJc18RaddXs3UsG
certificate private 0 line 1 U@GVXBb3qUablFzippI/G7RzvQIoIidVko7D3UyPqyzSmhXprLJFCkUbIro/UGy5k
qCFQlyJtEvBElrN69StqUqk0qxn
certificate private 0 line 2 8/6xVM07inyDX5uY71PgSMEI10WpPG7UXYGX/xD3bbi3q0Y@whH15nAKdqMIvfVx8
HJzVcNCdNpGg8@ty360s@rWyqas
certificate private 0 line 3 xaXDBs9Y5n0KZwSb96WZhS8vBtzs1dzhATnWvaejIXyFYdgAhPYp1rMdqBNyuBhoT
CSglN2vXZNvwXN3a0IInBWrrBNW
certificate private 0 line 4 0jLsXNgMwc8cgTCw0ZL6dWrKGU3qtnjTpYzsVoHVUcTPhb9yEwq0M2rTU/eX@77lu
k0mPXY5XrqipSbwfqrodH0us3
certificate private 0 line 5 70OAlBhmaYN7rlbaLSmzrQD07s2QDNvwI87dHypF4KC8BP0HwemUYQ6xq32vijbQ@
qlI0flH4YKB5LvAXJeJJ4qRa@IA
certificate private 0 line 6 FKjaEBAcl0NTGk9nMd1uE@2/DvoXtIzqNo9Ooo6NUn/5oz/qxpLaHzshl9@oKCL8e
0dMoYRy7g0eeQI2oU1DrF6iHdDY
certificate private 0 line 7 HFZBzMEtC9MNQeGqFlEY@edgfRo1IAM9qa3/ip2HBgcUHZHqNVgSePHeBdtrikubN
KWC@wSmZ3AdJ/@rzClhXhBrg6j
certificate private 0 line 8 bo2HYUzA6hvPtZpECc21pTYH8i401Akqh1kiK0QXS4P3gCMMIaPMN5lzMQ@QFX8jq
flSP0eRMwjFscD/TVRPTlyNAtoG
certificate private 0 line 9 8ocM49xUiyGyibznxgZNwsZ0Yy8i8GXMkb6VkBGog22TfTfmona4D1wz464IYfMPw
kw6rq/9eYqW71HXB4jJDRU1C/UK
certificate private 0 line 10 TyyPu9KD5xY0wKGLYBbDzC60aVT445YpewrHiAuo1Dpd6FcPZULLj@wa7gHu0A/7
Vzpu7VQhaXJz1xzdDOT2iRQT97MVQ
certificate private 0 line 11 2XH/r4JKRiZpn5LP4/Hr5uwZDGQ5h21fEdvwVp80bKbL4a81/lPt0cfMXoA7IbC8
Mrc0ZkMxGGkV0eMqlC2Bgt5YE1
certificate private 0 line 12 ei9ZNnGLgLtxJJrrXWq4zk9tuzH@0ZXe0INO0uAgVH5ktLiTOX2gsSz2fRq2D4Q6
hi
certificate request 0 line 0 MIICMDCCAZkCAQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYDVQQIEwhLYW5hZ2F3YTER
certificate request 0 line 1 MA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0c3UgTG1taXRlZDESMBAG
certificate request 0 line 2 A1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJzaGlzeWEuZnVqaXRzdS5jb20xHzAd
certificate request 0 line 3 BgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
certificate request 0 line 4 gY0AMIGJAoGBAMk7Bq9Ciaxh17fYIkwbRLI64EAjP1RnDrEnLJ/ds9ErIoT4sPBc
certificate request 0 line 5 Z9a0mvdz0nR1K8HmNmDGMo1DRufBWueSvs9Qgl0zykQu+R3YKPMNMJ3gL06tiNk1
certificate request 0 line 6 6TtNNUAK+OGda0brLL6t6+jE/U1Kskjt7UzdH1an1AroLkLtkrVqcBPjAgMBAAGg
certificate request 0 line 7 UDB0BgkqhkiG9w0BCQ4xQTA/MAsGA1UdDwQEAwIChDAPBgNVHREECDAGhwTAqAEB
certificate request 0 line 8 MB8GA1UdEQQYMBaCFHNoaXN5YS1hLmZ1aml0c3UuY29tMA0GCSqGSIb3DQEBBQUA
certificate request 0 line 9 A4GBACRKhbhx8kl08Jf7w9YNgzHN+0RyY2sIrqhqpytSquNonvcZZaEgVeqygUqQ
certificate request 0 line 10 WOIqhggINKSRW82odtTFi97Ttga1yijj5GeaVCLaSE6FH91LhcL1ArY2dArRYM/x
certificate request 0 line 11 Zv62xudPCLvwe+w49N8gA+Dq+9G3wCSYA0kFQNJmm/HIpUnb
Created RSA private key and Certificate request.
Please wait to create Local certificate.
certificate local 0 name cert.pem
certificate local 0 line 0 MIIDBjCCAm8CAQEwDQYJKoZIhvcNAQEFBQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYD
certificate local 0 line 1 VQQIEwhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
certificate local 0 line 2 c3UgTG1taXRlZDESMBAGA1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJzaGlzeWEu
certificate local 0 line 3 ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
certificate local 0 line 4 MDcwNzIwMDIwNzU4WhcNMDcxMjMxMDIwNzU4WjCBnzELMAkGA1UEBhMCS1AxETAP
certificate local 0 line 5 BgNVBAgTCEthbmFnYXdhMREwDwYDVQQHEwhLYXdhc2FraTEYMBYGA1UEChMPRnVq
certificate local 0 line 6 aXRzdSBMaW1pdGVkMRIwEAYDVQQLEwlUZWNoIERpdi4xGzAZBgNVBAMTEnNoaXN5
certificate local 0 line 7 YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
certificate local 0 line 8 nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAyTsGr0KJrGHXt9giTBtEsjrgQCM/
certificate local 0 line 9 VGc0sScsn92z0SsihPiw8Fxn1rSa93PSdGUrweY2YMYyjUNG58Fa55K+z1CCXTPK
certificate local 0 line 10 RC75Hdgo8w0wneAvTq2I2SXp0001QAr44Z1rRussvq3r6MT9TUqyS03tTN0fVqfU
certificate local 0 line 11 CuguQu2StWpwE+MCAwEAAaNVMFMwCwYDVR0PBAQDAgKEMA8GA1UdEQQIMAaHBMCo
certificate local 0 line 12 AQEwHwYDVR0RBBgwFoIUc2hpc3lhLWEuZnVqaXRzdS5jb20wEgYDVR0TAQH/BAgw
certificate local 0 line 13 BgEB/wIBATANBgkqhkiG9w0BAQUFAAOBgQBcPN+UbzXOVYN4RZ6zcbpn7YCwv/y7
certificate local 0 line 14 oSR5ppTcZZ1VCgWNYFQIz1/MCNv1yGk9at8S01QgM5zi0bXypD0p10B3Ust0mzGx
certificate local 0 line 15 3i3jsVuKJKbn0qsysUZQEpMFS7JdYHuIRN5nWPBjqH68CqQD8zPeJ21VcwcsUohF
certificate local 0 line 16 FKA8mr9msEiVNQ==
Created Local certificate.
(config)#
```

(2) 秘密鍵、証明書要求の設定を行う場合

：(コロン)より後ろの部分を入力します

```
(config)# crypto certificate generate
RSA key pair number[0-4] :0
generate RSA key pair.
```

```
Are you sure?[y/n] :y
RSA key pair and Certificate request will be overwritten.  (上書きすることを通知するメッセージ
Are you sure?[y/n] :y                                      は鍵ペアが未設定の場合は表示されません)
Local certificate number[0-4] :  (未入力)
key bit(361-2048) :1024
certificate request hash(sha1 or md5) :sha1
Country Name(2 letter code) :JP
State or Province Name :Kanagawa
Locality Name :Kawasaki
Organization Name :Fujitsu Limited
Organizational Unit Name :Tech Div.
Common Name :shisya.fujitsu.com
Email Address :hoge@fujitsu.com
subjectAltName IP :192.168.1.1
subjectAltName DNS :shisya-A.fujitsu.com
Please wait to create RSA private key and Certificate request.
certificate private 0 line 0 HABNg39no/6PrWicHYI2Ambcsqbvwcr8d03hsDstuY8MrRKghUF20fCP7FxV2qClS
nTnboIjjha3bPcJc18RaddXs3UsG
certificate private 0 line 1 U@GVXBb3qUablFzippI/G7RzvQIoIidVko7D3UyPqyzSmhXprLJFCkUbIro/UGy5k
qCFQlyJtEvBElrN69StqUqk0qxn
certificate private 0 line 2 8/6xVM07inyDX5uY7lPgSMEI10WpPG7UXYGX/xD3bbi3q0Y@whH15nAKdqMIvfVx8
HJzVcNCdNpGg8@ty360s@rWyqas
certificate private 0 line 3 xaXDBs9Y5n0KZwSb96WZhS8vBtzs1dzhATnWvaejIXyFYdgAhPYp1rMdqBNyuBhoT
CSglN2vXZNvwXN3a0IInBWrrBNW
certificate private 0 line 4 0jLsXNgMwc8cgTCw0ZL6dWrKGU3qtnjTpYzsVoHVUcTPhb9yEwq0M2rTU/eX@77lu
k0mPXY5XrqipSbwfqrodH0us3
certificate private 0 line 5 70OAlBhmaYN7rlbaLSmzrQDO7s2QDNvwI87dHypF4KC8BP0HwemUYQ6xq32vijbQ@
qlIOflH4YKB5LvAXJeJJ4qRa@IA
certificate private 0 line 6 FKjaEBAcl0NTGk9nMd1uE@2/DvoXtIzqNo90oo6NUn/5oz/qxpLaHzshl9@oKCL8e
0dMoYRy7g0eeQI2oU1DrF6iHdDY
certificate private 0 line 7 HFZBzMEtC9MNQeGqFlEY@edgfRo1IAM9qa3/ip2HBgcUHZHqNVgSePHeBdtrikubN
KWC@wSmZ3AdJ/@rzClhXhBrg6j
certificate private 0 line 8 bo2HYUzA6hvPtZpECc21pTYH8i401Akqh1kiK0QXS4P3gCMMIaPMN51zMQ@QFX8jq
flSP0eRMwjFscD/TVRPTlyNAtoG
certificate private 0 line 9 8ocM49xUiyGyibznxgZNwsZOYy8i8GXMkb6VkBGog22TfTfmona4D1wz464IYfMPw
kw6rq/9eYqW71HXB4jJDRU1C/UK
certificate private 0 line 10 TyyPu9KD5xY0wKGLYBbDzC60aVT445YpewrHiAuo1Dpd6FcPZULLj@wa7gHu0A/7
Vzpu7VQhaXJz1xzdDOT2iRQT97MVQ
certificate private 0 line 11 2XH/r4JKRiZpn5LP4/Hr5uwZDGQ5h21fEdvwVp80bKbL4a81/lPt0cfMXoA7IbC8
Mrc0ZkMxGGkVOeMq1C2Bgt5YE1
certificate private 0 line 12 ei9ZNnGLgLtxJJrrXWq4zk9tuzH@0ZXe0INO0uAgVH5ktLiTOX2gsSz2fRq2D4Q6
hi
certificate request 0 line 0 MIICMDCCAZkCAQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYDVQQIEwhLYW5hZ2F3YTER
certificate request 0 line 1 MA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTDOZ1aml0c3UgTG1taXR1ZDESMBAG
certificate request 0 line 2 A1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJzaG1zeWEuZnVqaXRzdS5jb20xHzAd
certificate request 0 line 3 BgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
certificate request 0 line 4 gYOAMIGJAoGBAMk7Bq9Ciaxh17fYIkwbRLI64EAjP1RnDrEnLJ/ds9ErIoT4sPBc
certificate request 0 line 5 Z9a0mvdz0nR1K8HmNmDGMo1DRufBWueSvs9Qgl0zykQu+R3YKPMNMJ3gL06tiNkl
certificate request 0 line 6 6TtNNUAK+OGda0brLL6t6+jE/U1Kskjt7UzdH1an1AroLkLtkrVqcBPjAgMBAAGg
certificate request 0 line 7 UDBOBgkqhkiG9w0BCQ4xQTA/MAsGA1UdDwQEAwIChDAPBgNVHREECDAGhwTAqAEB
certificate request 0 line 8 MB8GA1UdEQQYMBaCFHNoaXN5YS1hLmZ1aml0c3UuY29tMA0GCSqGSIb3DQEBBQUA
certificate request 0 line 9 A4GBACRKhbhx8kl08Jf7w9YNgzHN+0RyY2sIrqhqpytSquNonvcZZaEgVeqygUqQ
certificate request 0 line 10 WOIqhggINKSRW82odtTFi97Ttga1yijj5GeaVCLaSE6FH91LhcL1ArY2dArRYM/x
certificate request 0 line 11 Zv62xudPCLvwe+w49N8gA+Dq+9G3wCSYA0kFQNJmm/HIpUnb
Created RSA private key and Certificate request.
(config)#
```

(3) 自装置証明書の設定を行う場合

:(コロン)より後ろの部分を入力します

```
(config)# crypto certificate generate
RSA key pair number[0-4] :0
generate RSA key pair.
Are you sure?[y/n] :n
Local certificate number[0-4] :0
Local certificate will be overwritten.  (上書きすることを通知するメッセージは自装置証明書が
Are you sure?[y/n] :y                                          未設定の場合は表示されません)
local certificate name :cert.pem
local certificate hash(sha1 or md5) :sha1
expire date(YYYYMMDD) :20151231
Please wait to create Local certificate.
certificate local 0 name cert.pem
certificate local 0 line 0 MIIDBjCCAm8CAQEwDQYJKoZIhvcNAQEFBQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYD
certificate local 0 line 1 VQQIEwhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
certificate local 0 line 2 c3UgTGltaXRlZDESMBAGA1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJzaGlzeWEu
certificate local 0 line 3 ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
certificate local 0 line 4 MDcwNzIwMDIwNzU4WhcNMDcxMjMxMDIwNzU4WjCBnzELMAkGA1UEBhMCS1AxETAP
certificate local 0 line 5 BgNVBAgTCEthbmFnYXdhMREwDwYDVQQHEwhLYXdhc2FraTEYMBYGA1UEChMPRnVq
certificate local 0 line 6 aXRzdSBMaW1pdGVkMRIwEAYDVQQLEwlUZWNoIERpdi4xGzAZBgNVBAMTEnNoaXN5
certificate local 0 line 7 YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
certificate local 0 line 8 nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAyTsGr0KJrGHXt9giTBtEsjrgQCM/
certificate local 0 line 9 VGc0sScsn92z0SsihPiw8Fxn1rSa93PSdGUrweY2YMYyjUNG58Fa55K+z1CCXTPK
certificate local 0 line 10 RC75Hdgo8w0wneAvTq2I2SXpO001QAr44Z1rRussvq3r6MT9TUqySO3tTN0fVqfU
certificate local 0 line 11 CuguQu2StWpwE+MCAwEAAaNVMFMwCwYDVR0PBAQDAgKEMA8GA1UdEQQIMAaHBMCo
certificate local 0 line 12 AQEwHwYDVR0RBBgwFoIUc2hpc3lhLWEuZnVqaXRzdS5jb20wEgYDVR0TAQH/BAgw
certificate local 0 line 13 BgEB/wIBATANBgkqhkiG9w0BAQUFAAOBgQBcPN+UbzXOVYN4RZ6zcbpn7YCwv/y7
certificate local 0 line 14 oSR5ppTcZZlVCgWNYFQIz1/MCNv1yGk9at8SO1QgM5zi0bXypD0p10B3Ust0mzGx
certificate local 0 line 15 3i3jsVuKJKbn0qsysUZQEpMFS7JdYHuIRN5nWPBjqH68CqQD8zPeJ2lVcwcsUohF
certificate local 0 line 16 FKA8mr9msEiVNQ==
Created Local certificate.
(config)#
```

自装置の情報

```
RSA key pair number[0-4] :
--------------------------
        (1)
Local certificate number[0-4] :
-------------------------------
        (2)
key bit(361-2048) :
-------------------
        (3)
certificate request hash(sha1 or md5) :
---------------------------------------
        (4)
local certificate name :
------------------------
        (5)
local certificate hash(sha1 or md5) :
-------------------------------------
        (6)
expire date(YYYYMMDD) :
-----------------------
        (7)
Country Name(2 letter code) :
-----------------------------
        (8)
State or Province Name :
------------------------
        (9)
Locality Name :
---------------
        (10)
Organization Name :
-------------------
        (11)
Organizational Unit Name :
--------------------------
        (12)
Common Name :
-------------
        (13)
Email Address :
---------------
        (14)
subjectAltName IP :
-------------------
        (15)
subjectAltName DNS :
--------------------
        (16)
```

1) 鍵ペアの識別番号
   鍵ペアの識別番号を、0～4 の 10 進数で指定します。
2) 自装置証明書の識別番号
   自装置証明書識別番号を、0～4 の 10 進数で指定します。
   未指定の場合、自装置証明書の作成は行いません。
3) 鍵長
   鍵長(bit)を 361～2048 の 10 進数で指定します。
4) 証明書要求で使用するハッシュアルゴリズム
   ハッシュアルゴリズムを指定します。

   sha1
   ハッシュアルゴリズムとして SHA1 を使用します。

   md5
   ハッシュアルゴリズムとして MD5 を使用します。
5) 自装置証明書識別名
   0x21,0x23～0x7e の 16 文字以内の ASCII 文字列で指定します。

6) 自装置証明書で使用するハッシュアルゴリズム

ハッシュアルゴリズムを指定します。

sha1

ハッシュアルゴリズムとして SHA1 を使用します。

md5

ハッシュアルゴリズムとして MD5 を使用します。

7) 自装置証明書の有効期限

自装置証明書の有効期限を失効日指定します。

－ 証明書の有効期限失効日

自装置証明書の有効期限が失効する日付を、YYYYMMDD の形式で指定します

YYYY

西暦を、西暦 1990～2036 年まで指定できます。

MM

月を、1～12 の 10 進数で指定します。

DD

日付を、1～31 の 10 進数で指定します。

過去の日付や現在の日付は指定できません。

8) 国(C)

0x21,0x23～0x7e の 2 文字の ASCII 文字列で指定します。

9) 都道府県(ST)

0x22(ダブルクォーテーション)と 0x2f(スラッシュ)を除く[0x20-0x7e]の範囲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。

10) 市区町村(L)

0x22(ダブルクォーテーション)と 0x2f(スラッシュ)を除く[0x20-0x7e]の範囲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。

11) 組織または会社(O)

0x22(ダブルクォーテーション)と 0x2f(スラッシュ)を除く[0x20-0x7e]の範囲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。

12) 組織ユニットまたは部門(OU)

0x22(ダブルクォーテーション)と 0x2f(スラッシュ)を除く[0x20-0x7e]の範囲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。

13) ホスト名(CN)

0x22(ダブルクォーテーション)と 0x2f(スラッシュ)を除く[0x20-0x7e]の範囲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。

14) E メールアドレス

0x21,0x23～0x7e の 64 文字以内の ASCII 文字列で指定します。

15) サブジェクト代替名称(IP アドレス)

IPv4 アドレスを指定します。

16) サブジェクト代替名称(DNS 名)

0x22(ダブルクォーテーション)と 0x2f(スラッシュ)を除く[0x21-0x7e]の範囲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。(DNS 名には大文字と小文字の区別がないため、すべて小文字になります)

72.1.2 crypto certificate local

[機能]

自装置証明書の取り込み

[適用機種]

Si-R G110

[入力形式]

crypto certificate local <number> name <name>

[オプション]

<number>

自装置証明書識別番号を指定します。

・ 自装置証明書識別番号
自装置証明書の識別番号を、0～4 の 10 進数で指定します。

name <name>

自装置証明書識別名を指定します。

・ 自装置証明書識別名
0x21,0x23～0x7e の 16 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]

自装置証明書を取り込みます。
証明書の入力は Base64 形式で行い、開始行と終了行には以下の文字列を指定してください。

開始行

: -----BEGIN CERTIFICATE-----

終了行

: -----END CERTIFICATE-----

証明書の取り込みは開始と終了の行を除いた、100 行までで指定してください。
自装置証明書の設定が行われると以下の構成定義が設定されます。

自装置証明書

: certificate local name
certificate local line

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、定義反映を行う場合は、commit コマンドまたは save コマンド実行後に reset コマンドを行ってください。

[注意]

すでに<number>で指定した「crypto certificate generate」コマンド、「crypto certificate local」コマンドで設定を行っている場合は上書きされます。
取り込んだ自装置証明書情報が証明書として有効でない場合は構成定義の設定は行いません。
本コマンドで定義した内容は、以下の構成定義情報を delete コマンドで削除できます。

自装置証明書

: certificate local name
certificate local line

[実行例]

```
(config)# crypto certificate local 0 name mycert.pem
Please input.
-----BEGIN CERTIFICATE-----
```

```
MIIDBjCCAm8CAQEwDQYJKoZIhvcNAQEFBQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYD
VQQIEwhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
c3UgTGltaXRlZDESMBAGA1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJzaGlzeWEu
ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
MDcwNzIwMDIwNzU4WhcNMDcxMjMxMDIwNzU4WjCBnzELMAkGA1UEBhMCS1AxETAP
BgNVBAgTCEthbmFnYXdhMREwDwYDVQQHEwhLYXdhc2FraTEYMBYGA1UEChMPRnVq
aXRzdSBMaW1pdGVkMRIwEAYDVQQLEwlUZWNoIERpdi4xGzAZBgNVBAMTEnNoaXN5
YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAyTsGr0KJrGHXt9giTBtEsjrgQCM/
VGc0sScsn92z0SsihPiw8Fxn1rSa93PSdGUrweY2YMYyjUNG58Fa55K+z1CCXTPK
RC75Hdgo8w0wneAvTq2I2SXpO001QAr44Z1rRussvq3r6MT9TUqyS03tTN0fVqfU
CuguQu2StWpwE+MCAwEAAaNVMFMwCwYDVR0PBAQDAgKEMA8GA1UdEQQIMAaHBMCo
AQEwHwYDVR0RBBgwFoIUc2hpc3lhLWEuZnVqaXRzdS5jb20wEgYDVR0TAQH/BAgw
BgEB/wIBATANBgkqhkiG9w0BAQUFAAOBgQBcPN+UbzX0VYN4RZ6zcbpn7YCwv/y7
oSR5ppTcZZlVCgWNYFQIz1/MCNv1yGk9at8SO1QgM5zi0bXypD0p10B3Ust0mzGx
3i3jsVuKJKbn0qsysUZQEpMFS7JdYHuIRN5nWPBjqH68CqQD8zPeJ2lVcwcsUohF
FKA8mr9msEiVNQ==
-----END CERTIFICATE-----
certificate local 0 name mycert.pem
certificate local 0 line 0 MIIDBjCCAm8CAQEwDQYJKoZIhvcNAQEFBQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYD
certificate local 0 line 1 VQQIEwhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
certificate local 0 line 2 c3UgTGltaXRlZDESMBAGA1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJzaGlzeWEu
certificate local 0 line 3 ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
certificate local 0 line 4 MDcwNzIwMDIwNzU4WhcNMDcxMjMxMDIwNzU4WjCBnzELMAkGA1UEBhMCS1AxETAP
certificate local 0 line 5 BgNVBAgTCEthbmFnYXdhMREwDwYDVQQHEwhLYXdhc2FraTEYMBYGA1UEChMPRnVq
certificate local 0 line 6 aXRzdSBMaW1pdGVkMRIwEAYDVQQLEwlUZWNoIERpdi4xGzAZBgNVBAMTEnNoaXN5
certificate local 0 line 7 YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
certificate local 0 line 8 nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAyTsGr0KJrGHXt9giTBtEsjrgQCM/
certificate local 0 line 9 VGc0sScsn92z0SsihPiw8Fxn1rSa93PSdGUrweY2YMYyjUNG58Fa55K+z1CCXTPK
certificate local 0 line 10 RC75Hdgo8w0wneAvTq2I2SXpO001QAr44Z1rRussvq3r6MT9TUqyS03tTN0fVqfU
certificate local 0 line 11 CuguQu2StWpwE+MCAwEAAaNVMFMwCwYDVR0PBAQDAgKEMA8GA1UdEQQIMAaHBMCo
certificate local 0 line 12 AQEwHwYDVR0RBBgwFoIUc2hpc3lhLWEuZnVqaXRzdS5jb20wEgYDVR0TAQH/BAgw
certificate local 0 line 13 BgEB/wIBATANBgkqhkiG9w0BAQUFAAOBgQBcPN+UbzX0VYN4RZ6zcbpn7YCwv/y7
certificate local 0 line 14 oSR5ppTcZZlVCgWNYFQIz1/MCNv1yGk9at8SO1QgM5zi0bXypD0p10B3Ust0mzGx
certificate local 0 line 15 3i3jsVuKJKbn0qsysUZQEpMFS7JdYHuIRN5nWPBjqH68CqQD8zPeJ2lVcwcsUohF
certificate local 0 line 16 FKA8mr9msEiVNQ==
(config)#
```

72.1.3 crypto certificate remote

[機能]

相手装置証明書の取り込み

[適用機種]

Si-R G110

[入力形式]

crypto certificate remote <number> name <name>

[オプション]

<number>

相手装置証明書識別番号を指定します。

・ 相手装置証明書識別番号
相手装置証明書の識別番号を、10 進数で指定します。
機種ごとの相手装置証明書識別番号の範囲は以下のとおりです。

範囲	機種
0～49	Si-R G110

name <name>

相手装置証明書識別名を指定します。

・ 相手装置証明書識別名
0x21,0x23～0x7e の 16 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]

相手装置証明書を取り込みます。
証明書の入力は Base64 形式で行い、開始行と終了行には以下の文字列を指定してください。

開始行

: -----BEGIN CERTIFICATE-----

終了行

: -----END CERTIFICATE-----

相手装置証明書の取り込みは開始と終了の行を除いた、100 行までで指定してください。
相手装置証明書の設定が行われると以下の構成定義が設定されます。

相手装置証明書

: certificate remote name
certificate remote line

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、定義反映を行う場合は、commit コマンドまたは save コマンド実行後に reset コマンドを行ってください。

[注意]

すでに<number>で指定した相手装置証明書識別番号に「crypto certificate remote」コマンドで設定を行っている場合は上書きされます。
取り込んだ相手装置証明書情報が証明書として有効でない場合は構成定義の設定は行いません。
本コマンドで定義した内容は、以下の構成定義情報を delete コマンドで削除できます。

相手装置証明書

: certificate remote name

certificate remote line

[実行例]

```
(config)# crypto certificate remote 0 name peercert.pem
Please input.
-----BEGIN CERTIFICATE-----
MIIC/jCCAeYCAQAwDQYJKoZIhvcNAQEEBQAwRTELMAkGA1UEBhMCQVUxEzARBgNV
BAgTClNvbWUtU3RhdGUxITAfBgNVBAoTGEludGVybmV0IFdpZGdpdHMgUHR5IEx0
ZDAeFw0wNjAxMDUwOTUzMTlaFw0wNjAyMDQwOTUzMTlaMEUxCzAJBgNVBAYTAkFV
MRMwEQYDVQQIEwpTb211LVN0YXRlMSEwHwYDVQQKExhJbnRlcm5ldCBXaWRnaXRz
IFB0eSBMdGQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDiTb0BDCqj
PU47aBdKPyGuAfEhtdtyYAHxKaKVuuQYH8x/+mvtZCHlmrsUDNm0o+W494OguqjB
8LmzWSbRm1zM1FsJxcDvr1v89TaAPqckrnrl/Mz4dGhKyFYhcsbiYOL5AuWbtbaP
aMv04op4/Y2iL9AAeHqVVN1aX071/iVu1S0I4Fvfu3PGH8b/imiVlwhaNid98b53
10KklxU7+UT/HAClx1rutfqWve/suM7nlW4qM3qsc4aoUgy68mPlCm8SeU0mdIPm
X7X8XP1ZDpbgDruXj33LPXo5J7jQk0ILVd1zaRGZDPVw153d0kgybDLjg7+Z3uM5
s4r/Wno6pZ6nAgMBAAEwDQYJKoZIhvcNAQEEBQADggEBAEnoJG/QLWKfD+iN/zOR
sbbSn04Z7Zx7GavCdCEilwNK+qWkP+5ZkKFbNHYRX2Sv16FpR/UWvcKdlfpFt2gu
2GddS3DoUDPn3Hj8wzf5sMwJLHfkwv038DPEOsbb+AliQ3/ne4vUTrNWgMOGyDaS
4RKzMod2/xzI8+BykmHGX8e2ukcS1ZdnZM1IV16SXCFsawlJ2CPtdwxnYCxjHyq0
nfhxNYRivy3KIXeVaIYCIuijIKNnYYhpQIVFMOzcNF8ej2GYrlrp+xTQ/t6fMbq+
JniNh8LFmzSCH+jd3EgxFlGl0Wyrk/ULSzPLVwzav40K2N6X+IDw+kPi9HNOSG06
0+0=
-----END CERTIFICATE-----
certificate remote 0 name peercert.pem
certificate remote 0 line 0 MIIC/jCCAeYCAQAwDQYJKoZIhvcNAQEEBQAwRTELMAkGA1UEBhMCQVUxEzARBgNV
certificate remote 0 line 1 BAgTClNvbWUtU3RhdGUxITAfBgNVBAoTGEludGVybmV0IFdpZGdpdHMgUHR5IEx0
certificate remote 0 line 2 ZDAeFw0wNjAxMDUwOTUzMTlaFw0wNjAyMDQwOTUzMTlaMEUxCzAJBgNVBAYTAkFV
certificate remote 0 line 3 MRMwEQYDVQQIEwpTb211LVN0YXRlMSEwHwYDVQQKExhJbnRlcm5ldCBXaWRnaXRz
certificate remote 0 line 4 IFB0eSBMdGQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDiTb0BDCqj
certificate remote 0 line 5 PU47aBdKPyGuAfEhtdtyYAHxKaKVuuQYH8x/+mvtZCHlmrsUDNm0o+W494OguqjB
certificate remote 0 line 6 8LmzWSbRm1zM1FsJxcDvr1v89TaAPqckrnrl/Mz4dGhKyFYhcsbiYOL5AuWbtbaP
certificate remote 0 line 7 aMv04op4/Y2iL9AAeHqVVN1aX071/iVu1S0I4Fvfu3PGH8b/imiVlwhaNid98b53
certificate remote 0 line 8 10KklxU7+UT/HAClx1rutfqWve/suM7nlW4qM3qsc4aoUgy68mPlCm8SeU0mdIPm
certificate remote 0 line 9 X7X8XP1ZDpbgDruXj33LPXo5J7jQk0ILVd1zaRGZDPVw153d0kgybDLjg7+Z3uM5
certificate remote 0 line 10 s4r/Wno6pZ6nAgMBAAEwDQYJKoZIhvcNAQEEBQADggEBAEnoJG/QLWKfD+iN/zOR
certificate remote 0 line 11 sbbSn04Z7Zx7GavCdCEilwNK+qWkP+5ZkKFbNHYRX2Sv16FpR/UWvcKdlfpFt2gu
certificate remote 0 line 12 2GddS3DoUDPn3Hj8wzf5sMwJLHfkwv038DPEOsbb+AliQ3/ne4vUTrNWgMOGyDaS
certificate remote 0 line 13 4RKzMod2/xzI8+BykmHGX8e2ukcS1ZdnZM1IV16SXCFsawlJ2CPtdwxnYCxjHyq0
certificate remote 0 line 14 nfhxNYRivy3KIXeVaIYCIuijIKNnYYhpQIVFMOzcNF8ej2GYrlrp+xTQ/t6fMbq+
certificate remote 0 line 15 JniNh8LFmzSCH+jd3EgxFlGl0Wyrk/ULSzPLVwzav40K2N6X+IDw+kPi9HNOSG06
certificate remote 0 line 16 0+0=
(config)#
```

72.1.4 crypto certificate ca

[機能]

認証局証明書の取り込み

[適用機種]

Si-R G110

[入力形式]

crypto certificate ca <number> name <name>

[オプション]

<number>

認証局証明書識別番号を指定します。

・ 認証局証明書識別番号
認証局証明書の識別番号を、0～4 の 10 進数で指定します。

name <name>

認証局証明書識別名を指定します。

・ 認証局証明書識別名
0x21,0x23～0x7e の 16 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]

認証局証明書を取り込みます。
証明書の入力は Base64 形式で行い、開始行と終了行には以下の文字列を指定してください。

開始行

: -----BEGIN CERTIFICATE-----

終了行

: -----END CERTIFICATE-----

認証局証明書の取り込みは開始と終了の行を除いた、100 行までで指定してください。
認証局証明書の設定が行われると以下の構成定義が設定されます。

認証局証明書

: certificate ca name
certificate ca line

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、定義反映を行う場合は、commit コマンドまたは save コマンド実行後に reset コマンドを行ってください。

[注意]

すでに<number>で指定した認証局証明書識別番号に「crypto certificate ca」コマンドで設定を行っている場合は上書きされます。
取り込んだ認証局証明書情報が証明書として有効でない場合は構成定義の設定は行いません。
本コマンドで定義した内容は、以下の構成定義情報を delete コマンドで削除できます。

認証局証明書

: certificate ca name
certificate ca line

[実行例]

```
(config)# crypto certificate ca 0 name cacert.pem
Please input.
-----BEGIN CERTIFICATE-----
```

```
MIIDBjCCAm8CAQEwDQYJKoZIhvcNAQEFBQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYD
VQQIEwhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
c3UgTGltaXRlZDESMBAGA1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJzaGlzeWEu
ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
MDcwNzIwMDIwNzU4WhcNMDcxMjMxMDIwNzU4WjCBnzELMAkGA1UEBhMCS1AxETAP
BgNVBAgTCEthbmFnYXdhMREwDwYDVQQHEwhLYXdhc2FraTEYMBYGA1UEChMPRnVq
aXRzdSBMaW1pdGVkMRIwEAYDVQQLEwlUZWNoIERpdi4xGzAZBgNVBAMTEnNoaXN5
YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAyTsGr0KJrGHXt9giTBtEsjrgQCM/
VGc0sScsn92z0SsihPiw8Fxn1rSa93PSdGUrweY2YMYyjUNG58Fa55K+z1CCXTPK
RC75Hdgo8w0wneAvTq2I2SXpO001QAr44Z1rRussvq3r6MT9TUqyS03tTN0fVqfU
CuguQu2StWpwE+MCAwEAAaNVMFMwCwYDVR0PBAQDAgKEMA8GA1UdEQQIMAaHBMCo
AQEwHwYDVR0RBBgwFoIUc2hpc3lhLWEuZnVqaXRzdS5jb20wEgYDVR0TAQH/BAgw
BgEB/wIBATANBgkqhkiG9w0BAQUFAAOBgQBcPN+UbzX0VYN4RZ6zcbpn7YCwv/y7
oSR5ppTcZZlVCgWNYFQIz1/MCNv1yGk9at8SO1QgM5zi0bXypD0p10B3Ust0mzGx
3i3jsVuKJKbn0qsysUZQEpMFS7JdYHuIRN5nWPBjqH68CqQD8zPeJ2lVcwcsUohF
FKA8mr9msEiVNQ==
-----END CERTIFICATE-----
certificate ca 0 name cacert.pem
certificate ca 0 line 0 MIIDBjCCAm8CAQEwDQYJKoZIhvcNAQEFBQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYD
certificate ca 0 line 1 VQQIEwhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
certificate ca 0 line 2 c3UgTGltaXRlZDESMBAGA1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJzaGlzeWEu
certificate ca 0 line 3 ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
certificate ca 0 line 4 MDcwNzIwMDIwNzU4WhcNMDcxMjMxMDIwNzU4WjCBnzELMAkGA1UEBhMCS1AxETAP
certificate ca 0 line 5 BgNVBAgTCEthbmFnYXdhMREwDwYDVQQHEwhLYXdhc2FraTEYMBYGA1UEChMPRnVq
certificate ca 0 line 6 aXRzdSBMaW1pdGVkMRIwEAYDVQQLEwlUZWNoIERpdi4xGzAZBgNVBAMTEnNoaXN5
certificate ca 0 line 7 YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
certificate ca 0 line 8 nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAyTsGr0KJrGHXt9giTBtEsjrgQCM/
certificate ca 0 line 9 VGc0sScsn92z0SsihPiw8Fxn1rSa93PSdGUrweY2YMYyjUNG58Fa55K+z1CCXTPK
certificate ca 0 line 10 RC75Hdgo8w0wneAvTq2I2SXpO001QAr44Z1rRussvq3r6MT9TUqyS03tTN0fVqfU
certificate ca 0 line 11 CuguQu2StWpwE+MCAwEAAaNVMFMwCwYDVR0PBAQDAgKEMA8GA1UdEQQIMAaHBMCo
certificate ca 0 line 12 AQEwHwYDVR0RBBgwFoIUc2hpc3lhLWEuZnVqaXRzdS5jb20wEgYDVR0TAQH/BAgw
certificate ca 0 line 13 BgEB/wIBATANBgkqhkiG9w0BAQUFAAOBgQBcPN+UbzX0VYN4RZ6zcbpn7YCwv/y7
certificate ca 0 line 14 oSR5ppTcZZlVCgWNYFQIz1/MCNv1yGk9at8SO1QgM5zi0bXypD0p10B3Ust0mzGx
certificate ca 0 line 15 3i3jsVuKJKbn0qsysUZQEpMFS7JdYHuIRN5nWPBjqH68CqQD8zPeJ2lVcwcsUohF
certificate ca 0 line 16 FKA8mr9msEiVNQ==
(config)#
```

第 73 章 I'm here コマンド

73.1 I'm here コマンド

73.1.1 iamhere

[機能]

POWER ランプと CHECK ランプの交互点滅の操作

[適用機種]

Si-R G110

[入力形式]

iamhere <mode> [<time>]

[オプション]

<mode>

POWER ランプと CHECK ランプの交互点滅、および点滅解除の操作

- on

  POWER ランプと CHECK ランプの交互点滅を開始します。

  [<time>]

  POWER ランプと CHECK ランプの交互点滅させる時間を指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。
  指定可能な範囲は以下のとおりです。

  1s～86400s
  1m～1440m
  1h～24h
  1d

  省略時は、POWER ランプと CHECK ランプの交互点滅は自動的に解除されません。

- off

  POWER ランプと CHECK ランプの交互点滅を解除します。

[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]

装置のランプを指定時間だけ点滅させます。
ランプを点滅させて本装置の設置場所を目視確認できます。
本コマンドを続けて実行した場合、最後に指定した時間だけ点滅します。

[実行例]

```
# iamhere on 30m
#
```

第 74 章 その他のコマンド

74.1 その他

74.1.1 ping

[機能]

ICMP エコー要求パケットの送信

[適用機種]

Si-R G110

[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>の省略時は、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 ICMP データ長を、46～9600 の 10 進数(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。
IPv4 の場合のみ有効です。

ttl <ttl>

・ TTL 値
TTL 値を、0～255 の 10 進数で指定します。
省略時は、IPv4 の場合は 128、IPv6 の場合は 64 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(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 の省略時は 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
#
```

74.1.2 traceroute

[機能]

ネットワーク経路の表示

[適用機種]

Si-R G110

[入力形式]

traceroute <ip_address> [source <src_ip_address>] [size <data_size>]
[timeout <timeout>] [df]
traceroute <host_name> [{v4 | v6}] [source <src_ip_address>] [size <data_size>]
[timeout <timeout>] [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(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 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(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。

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   *  *  *
#
```

74.1.3 telnet

[機能]

telnet サーバへの接続

[適用機種]

Si-R G110

[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 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]

```
# 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
```

74.1.4 pwconv

[機能]

暗号化パスワードの表示

[適用機種]

Si-R G110

[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
#
```

74.1.5 dnconv

[機能]

電話番号変更処理の実施

[適用機種]

Si-R G110

[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
```

74.1.6 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 G110

[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何もしません。

<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
#
```

第 75 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とき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
パスワード情報	password format	(0)
	password admin set	(0)
	password user set	(0)
	password aaa	(1)
	password authtype	(1)
認証情報		
IEEE802.1X 認証情報	dot1x use	(14)
MAC アドレス認証情報	macauth use	(14)
	macauth password	(14)
	macauth type	(14)
ARP 認証情報	arpauth use	(1)
	arpauth password	(1)
WAN 情報	wan	(3)
ether グループ		(3)
共通情報	ethergroup vlan mode	(5)
アクセス制御	ethergroup access-control	(5)
ブリッジグループ	ethergroup bridgegroup	(1)
ポート情報		(3)
ether 共通情報	ether description	(1)
	ether use	(3) ※8
	ether media	(3)
	ether mode	(3)
	ether duplex	(3)
	ether mdi	(3)
	ether flowctl	(3)
	ether type	(3)
STP 関連情報	ether stp	(1) ※7
VLAN 情報	ether vlan	(3) ※9
	ether vlan primap	(1)
シェーピング関連	ether shaping	(3)
	ether shaping-opt tc	(3)
SNMP 関連情報	ether snmp	(1)
WFQ 関連情報	ether priority	(1)
IEEE802.1X 認証情報	ether dot1x use	(3)
	ether dot1x quietperiod	(3)
	ether dot1x txperiod	(3)
	ether dot1x supptimeout	(3)
	ether dot1x maxreq	(3)
	ether dot1x reauthperiod	(3)
	ether dot1x aaa	(3)
	ether dot1x vid	(3)
	ether dot1x vlan assign	(3)
MAC アドレス認証情報	ether macauth use	(3)
	ether macauth aaa	(3)

種別	コマンド名	commit 実行時影響
	ether macauth authenticated-mac	(3)
	ether macauth expire	(3)
	ether macauth vid	(3)
	ether macauth vlan assign	(3)
バックアップポート	backup	(3)
	backup mode	(3)
	backup standby	(3)
STP 情報	stp	(1) ※7
VLAN 情報の設定		
VLAN 共通情報	vlan description	(1)
	vlan forward	(2)
ブリッジグループ	vlan bridgegroup	(2)
ARP 認証	vlan arpauth	(1)
MAC 情報		
MAC 情報	mac age	(1)
pseudo ether 情報		
共通情報	pseudo-ether description	(1)
	pseudo-ether use	(5)
	pseudo-ether bind	(3)
	pseudo-ether startup-delay	(1)
VLAN 情報	pseudo-ether vlan untag	(5)
lan 情報		
lan 共通情報	lan description	(1)
	lan mtu	(2)
	lan shaping	(2)
	lan shaping-opt tc	(2)
IP 関連情報	lan ip address	(1)
	lan ip alias	(1)
	lan ip dhcp	(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 nat	(1)
	lan ip filter	(1)
	lan ip priority	(1)
	lan ip in-policy	(1)
	lan ip msschange	(1)
	lan ip icmp	(1)

種別	コマンド名	commit 実行時影響
	lan ip multicast	(1)
	lan ip arp cycle	(3)
	lan ip arp static	(1)
	lan ip ids	(1)
IPv6 関連情報	lan ipv6 use	(1)
	lan ipv6 ifid	(1)
	lan ipv6 address	(1)
	lan ipv6 ra	(1)
	lan ipv6 route	(1)
	lan ipv6 rip use	(1)-1
	lan ipv6 rip site-local	(1)-1 ※1
	lan ipv6 rip aggregate	(1)-1 ※1
	lan ipv6 rip filter	(1)-1 ※1
	lan ipv6 filter	(1)
	lan ipv6 ospf use	(1)-1
	lan ipv6 ospf cost	(1)
	lan ipv6 ospf hello	(1)
	lan ipv6 ospf dead	(1)
	lan ipv6 ospf retrans	(1)
	lan ipv6 ospf delay	(1)
	lan ipv6 ospf priority	(1)
	lan ipv6 ospf passive	(1)
	lan ipv6 trafficclass	(1)
	lan ipv6 priority	(1)
	lan ipv6 dhcp	(1)
	lan ipv6 in-policy	(1)
VRRP 関連情報	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 vrrp trap	(1)
VLAN 関連情報	lan vlan	(2)
SNMP 関連情報	lan snmp	(1)
相手情報		
相手共通情報	remote description	(1)
	remote name	(2)
	remote autodial	(2)
	remote mtu	(2)
	remote shaping	(2)
	remote shaping-opt tc	(2)
接続先情報	remote ap description	(1)
	remote ap name	(2)
	remote ap move	(2)
	remote ap datalink	(3)
	remote ap ip	(2)
	remote ap multiroute	(2)

種別	コマンド名	commit 実行時影響
	remote ap limit	(2)
	remote ap disconnect	(1)
	remote ap ppp	(2)
	remote ap pppoe	(2)
	remote ap dial	(2)
	remote ap called	(2)
	remote ap connect	(13)
	remote ap idle	(2)
	remote ap keep	(2)
	remote ap ipsec	(2)
	remote ap ike	(2)
	remote ap dvpn	(2)
	remote ap tunnel	(2)
	remote ap overlap	(2)
	remote ap sessionwatch	(1)
SNMP 関連情報	remote ap snmp	(1)
PPP 関連情報	remote ppp	(2)
IP 関連情報	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 dvpn	(7)
	remote ip ids	(1)
	remote ip in-policy	(1)
IPv6 関連情報	remote ipv6 use	(1)
	remote ipv6 ifid	(1)
	remote ipv6 address	(1)
	remote ipv6 ra	(1)
	remote ipv6 route	(1)
	remote ipv6 rip use	(1)-1
	remote ipv6 rip site-local	(1)-1 ※1
	remote ipv6 rip aggregate	(1)-1 ※1
	remote ipv6 rip filter	(1)-1 ※1

種別	コマンド名	commit 実行時影響
	remote ipv6 ospf use	(1)-1
	remote ipv6 ospf cost	(1)
	remote ipv6 ospf hello	(1)
	remote ipv6 ospf dead	(1)
	remote ipv6 ospf retrans	(1)
	remote ipv6 ospf delay	(1)
	remote ipv6 ospf passive	(1)
	remote ipv6 ospf checkmtu	(1)
	remote ipv6 filter	(1)
	remote ipv6 trafficclass	(1)
	remote ipv6 priority	(1)
	remote ipv6 in-policy	(1)
	remote ipv6 dhcp	(1)
	remote ipv6 dvpn	(7)
	remote ipv6 in-policy	(1)
ブリッジグループ	remote bridgegroup	(2)
SNMP 関連情報	remote snmp	(1)
着信デフォルト情報	answer	(2)
テンプレート情報	template description	(1)
	template name	(6)
	template mtu	(7)
	template idle	(7)
	template interface pool	(8)
	template aaa	(9)
	template datalink	(6)
	template ppp	(7)
	template ip dns	(7)
	template ip address remote pool	(8)
	template ip filter	(1)
	template ip tos	(1)
	template ip priority	(1)
	template ip msschange	(1)
	template ip ids	(1)
	template ip in-policy	(1)
	template ipv6 use	(7)
	template ipv6 ifid	(7)
	template ipv6 filter	(1)
	template ipv6 priority	(1)
	template ipv6 trafficclass	(1)
	template ipv6 in-policy	(1)
	template combine	(6)
	template tunnel	(10)
	template sessionwatch	(10)
	template dvpn	(11)
	template ipsec	(10)
	template ike	(10)
	template snmp	(1)
証明書関連情報	certificate	(1) ※6
IP 情報	ip arp	(1)

種別	コマンド名	commit 実行時影響
動的 VPN 情報	dvpn server	(1)
	dvpn client	(12)
ルーティング プロトコル情報	routemanage ip distance	(1) ※1
	routemanage ip redist rip	(1)
	routemanage ip redist bgp	(1)
	routemanage ip redist ospf	(1)
	routemanage ip ecmp	(1)
	routemanage ipv6 distance	(1) ※1
	routemanage ipv6 redist rip	(1)
	routemanage ipv6 redist bgp	(1)
	routemanage ipv6 redist ospf	(1)
	bgp as	(4)
	bgp id	(4)
	bgp ip network route	(1)
	bgp ip network igp	(1)-1 ※2
	bgp ip aggregate	(1)
	bgp ip redist	(1)
	bgp ipv6 network route	(1)
	bgp ipv6 network igp	(1)-1 ※2
	bgp ipv6 aggregate	(1)
	bgp ipv6 redist	(1)
	bgp neighbor address	(1)-1 ※3
	bgp neighbor as	(1)-1 ※3
	bgp neighbor timers	(1)-1 ※3
	bgp neighbor ebgp-multihop	(1)-1 ※3
	bgp neighbor family	(1)-1 ※3
	bgp neighbor source	(1)-1 ※3
	bgp neighbor authentication	(1) ※5
	bgp neighbor graceful-restart	(1)-1 ※3
	bgp neighbor ip medmetric	(1) ※1
	bgp neighbor ip asprepend	(1) ※1
	bgp neighbor ip localpref	(1) ※1
	bgp neighbor ip nexthopself	(1) ※1
	bgp neighbor ip default-originate	(1) ※1
	bgp neighbor ip filter	(1) ※1
	bgp neighbor ipv6 medmetric	(1) ※1
	bgp neighbor ipv6 asprepend	(1) ※1
	bgp neighbor ipv6 localpref	(1) ※1
	bgp neighbor ipv6 nexthopself	(1) ※1
	bgp neighbor ipv6 default-originate	(1) ※1
	bgp neighbor ipv6 filter	(1) ※1
	ospf ip id	(4)
	ospf ip area id	(1)-1 ※4
	ospf ip area type	(1)-1 ※4
	ospf ip area defcost	(1)
	ospf ip area range	(1)-1
	ospf ip area type3-lsa	(1)
	ospf ip definfo	(1)
	ospf ip summary	(1)-1
	ospf ip redist	(1)-1

種別	コマンド名	commit 実行時影響
	ospf ipv6 id	(4)
	ospf ipv6 area id	(1)-1 ※4
	ospf ipv6 area type	(1)-1 ※4
	ospf ipv6 area defcost	(1)
	ospf ipv6 area range	(1)-1
	ospf ipv6 area inter-area-prefix	(1)
	ospf ipv6 definfo	(1)
	ospf ipv6 redist	(1)-1
	rip ip timers	(1)
	rip ip multipath	(1)
	rip ip redist	(1)-1
	rip ip neighbor	(1)-1
	rip ip gwfilter	(1)-1
	rip ipv6 timers	(1)
	rip ipv6 multipath	(1)
	rip ipv6 redist	(1)-1
ブリッジグループ情報	bridgegroup ip routing	(1)
	bridgegroup ip policy	(1)
	bridgegroup ipv6 routing	(1)
	bridgegroup ipv6 policy	(1)
	bridgegroup vlan	(1)
	bridgegroup inter-remote	(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)
トラッキング情報	tracking	(1)
	node-trigger	(1)
AAA 情報	aaa	(1)
メモリ予兆監視情報	sysmemwatch	(1)
装置情報	snmp	(1)
	syslog	(1)
	time	(1)
	proxydns	(1)
	host	(1)
	schedule	(1)
	storage setup	(5)-1
	dnconvinfo	(1)
	updateinfo	(1)
	lamp	(1)
	addact	(1)
	watchdog service	(5)
	consoleinfo	(1)
	telnetinfo	(1)
	sysdown	(1)
	mflag	(1)
	sysname	(5)
	loopback ip address	(1)
	loopback ip ospf	(1)-1

種別	コマンド名	commit 実行時影響
	loopback ipv6 address	(1)
	serverinfo	(1)
	resource system	(5)
	resource authenticated	(5)

(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。

(3)

該当物理回線が切断されます。

なお、ether ポートのリンクダウン／リンクアップを伴う ether 定義変更時は、同一 VLAN に属する ether ポートもリンクダウン／リンクアップします。

(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。

(5)-1

次回動作時(電源投入時)から有効となります。

(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、該当テンプレートで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。

(13)

該当接続先情報で転送方法が ipsec の場合は、(2) physical の場合は、(7)と同等です。

(14)

(1)に加え、該当機能を使用中の ether ポートがリンクダウン／リンクアップします。

※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。

※6

設定変更時、該当する IPsec 接続が切断されます。

※7

ブリッジネットワーク構成の変更が行われる場合は、登録された学習テーブルの削除や該当インタフェースでの通信が中断される場合があります。

※8

ether 定義と pseudo-ether 定義の vid が重複した状態で use off する場合、装置の再起動(リセット)が必要となります。

※9

ether 定義と pseudo-ether 定義の vid が重複した状態から、ether 定義の vid を変更する場合、装置の再起動(リセット)が必要となります。

索引

記号・数字

!.....1155

A

aaa name.....911
aaa radius accounting source.....937
aaa radius auth message-authenticator.....936
aaa radius auth source.....935
aaa radius client nas-identifier.....953
aaa radius client retry.....952
aaa radius client security.....954
aaa radius client server-info accounting address 947
aaa radius client server-info accounting deadtime. .
.....949
aaa radius client server-info accounting port...948
aaa radius client server-info accounting priority. .
.....950
aaa radius client server-info accounting secret. 946
aaa radius client server-info accounting source. 951
aaa radius client server-info auth address.....941
aaa radius client server-info auth deadtime.....943
aaa radius client server-info auth port.....942
aaa radius client server-info auth priority.....944
aaa radius client server-info auth secret.....940
aaa radius client server-info auth source.....945
aaa radius server client-info address.....939
aaa radius server client-info secret.....938
aaa radius service.....933
aaa user called number.....915
aaa user id.....912
aaa user ike shared key.....928
aaa user ip address local.....916
aaa user ip address remote.....917
aaa user ip route.....918
aaa user ipsec extension-range.....926
aaa user ipsec ike range.....924
aaa user ipv6 ifid.....920
aaa user ipv6 route.....921
aaa user password.....913
aaa user sessionwatch.....923
aaa user supplicant mac.....931
aaa user supplicant vid.....930
aaa user user-role.....932
aaactl mac collect commit.....1623
aaactl mac collect mark.....1621
aaactl mac collect start.....1618
aaactl mac collect stop.....1620
aaactl mac collect unmark.....1622
acl description.....884
acl icmp.....894
acl ip.....887
acl ipv6.....889
acl mac.....885
acl tcp.....891
acl udp.....893
addact.....1055
admin.....1145
alias.....1169
answer accept.....600
answer ppp auth receive add.....602
answer ppp auth type.....601
arpauth password.....961
arpauth use.....960
arpauthctl initialize.....1599

B

backup mode.....108
backup standby.....109
bgp as.....772
bgp id.....773
bgp ip aggregate.....776
bgp ip network igp.....775
bgp ip network route.....774
bgp ip redist.....777
bgp ip redist move.....779
bgp ipv6 aggregate.....782
bgp ipv6 network igp.....781
bgp ipv6 network route.....780
bgp ipv6 redist.....783
bgp ipv6 redist move.....785
bgp neighbor address.....786
bgp neighbor as.....787
bgp neighbor authentication.....792
bgp neighbor community.....795
bgp neighbor ebgp-multihop.....789
bgp neighbor family.....790
bgp neighbor graceful-restart family.....793
bgp neighbor graceful-restart stale-timer.....794
bgp neighbor ip asprepend.....797
bgp neighbor ip default-originate.....800
bgp neighbor ip filter act.....801
bgp neighbor ip filter as.....804
bgp neighbor ip filter move.....803
bgp neighbor ip filter route.....805
bgp neighbor ip filter set asprepend.....809
bgp neighbor ip filter set community.....813
bgp neighbor ip filter set localpref.....811
bgp neighbor ip filter set medmetric.....807
bgp neighbor ip localpref.....798
bgp neighbor ip medmetric.....796
bgp neighbor ip nexthopself.....799
bgp neighbor ipv6 asprepend.....815
bgp neighbor ipv6 default-originate.....818
bgp neighbor ipv6 filter act.....819
bgp neighbor ipv6 filter as.....822
bgp neighbor ipv6 filter move.....821
bgp neighbor ipv6 filter route.....823
bgp neighbor ipv6 filter set asprepend.....826
bgp neighbor ipv6 filter set community.....830
bgp neighbor ipv6 filter set localpref.....828
bgp neighbor ipv6 filter set medmetric.....825
bgp neighbor ipv6 localpref.....816
bgp neighbor ipv6 medmetric.....814
bgp neighbor ipv6 nexthopself.....817
bgp neighbor source.....791
bgp neighbor timers.....788
bridgegroup inter-remote.....864
bridgegroup ip policy.....860
bridgegroup ip routing.....859
bridgegroup ipv6 policy.....862

bridgegroup ipv6 routing.....861
bridgegroup vlan tag transmit.....863

C

certificate ca line.....1120
certificate ca name.....1119
certificate local line.....1116
certificate local name.....1115
certificate private line.....1122
certificate remote line.....1118
certificate remote name.....1117
certificate request line.....1121
clear aaa mac collect list.....1566
clear alias.....1172
clear arp.....1278
clear arpauth statistics.....1526
clear bridge.....1491
clear bridgegroup statistics.....1510
clear dot1x statistics.....1518
clear dvpn server session.....1464
clear dvpn server user.....1463
clear ether statistics.....1217
clear ike statistics.....1481
clear interface statistics.....1273
clear ip bgp neighbors.....1329
clear ip bgp statistics.....1331
clear ip filter statistics.....1409
clear ip ids statistics.....1419
clear ip multicast interface statistics.....1441
clear ip multicast route kernel statistics.....1442
clear ip multicast statistics.....1443
clear ip nat statistics.....1426
clear ip ospf statistics.....1367
clear ip rip statistics.....1311
clear ip route.....1289
clear ip route kernel ecmp statistics.....1293
clear ip traffic.....1398
clear ipv6 bgp neighbors.....1344
clear ipv6 bgp statistics.....1346
clear ipv6 dhcp server.....1452
clear ipv6 filter statistics.....1414
clear ipv6 ospf statistics.....1393
clear ipv6 route.....1299
clear ipv6 traffic.....1402
clear logging command.....1168
clear logging error.....1187
clear logging syslog.....1189
clear macauth statistics.....1522
clear modemmodule account.....1238
clear modemmodule condition history.....1239
clear modemmodule condition statistics.....1240
clear modemmodule statistics.....1241
clear ndp.....1282
clear nettime statistics.....1542
clear snmp statistics.....1537
clear spanning-tree statistics.....1504
clear statistics.....1190
clear template statistics.....1274
clear trace ssh.....1585
clear tracking statistics.....1532
clear upnp portmapping.....1550
clear upnp statistics.....1549
clear vrrp statistics.....1487
commit.....1133
commit try cancel.....1135
commit try time.....1134
configure.....1150
consoleinfo.....1058
copy.....1139
crypto certificate ca.....1639
crypto certificate generate.....1629
crypto certificate local.....1635
crypto certificate remote.....1637

D

date.....1192
delete.....1129
diff.....1127
dir.....1137
discard.....1136
dnconv.....1652
dnconvinfo date.....1045
dnconvinfo dial.....1046
domainlistinfo.....1049
dot1x use.....956
dot1xctl initialize port ether.....1596
dot1xctl reconfirm port ether.....1597
dvpn client domain.....732
dvpn client encode.....724
dvpn client expire register.....728
dvpn client expire session.....729
dvpn client global.....737
dvpn client interface.....736
dvpn client ip route distance.....739
dvpn client ipv6 route distance.....740
dvpn client localid.....735
dvpn client localnet.....733
dvpn client priority.....738
dvpn client server address.....725
dvpn client server auth.....727
dvpn client ua.....730
dvpn server auth aaa.....723
dvpn server auth use.....722
dvpn server domain.....721
dvpn server use.....720
dvpnserver disable.....1613
dvpnserver enable.....1614

E

end.....1151
ether description.....59
ether dot1x aaa.....98
ether dot1x maxreq.....102
ether dot1x quietperiod.....99
ether dot1x reauthperiod.....103
ether dot1x supptimeout.....101
ether dot1x txperiod.....100
ether dot1x use.....96
ether dot1x vid.....105
ether dot1x vlan assign.....104
ether duplex.....63
ether flowctl.....66
ether macauth aaa.....90
ether macauth authenticated-mac.....91
ether macauth expire.....93
ether macauth use.....88

ether macauth vid....95
ether macauth vlan assign....94
ether mdi....64
ether media....61
ether mode....62
ether priority ip....84
ether priority ipv6....86
ether recovery....79
ether shaping....81
ether shaping-opt tc....83
ether snmp trap linkdown....106
ether snmp trap linkup....107
ether stp domain cost....70
ether stp domain priority....71
ether stp use....69
ether type....67
ether use....60
ether vlan primap mode....75
ether vlan primap rule....77
ether vlan tag....72
ether vlan untag....73
ethergroup access-control mode....54
ethergroup bridgegroup control....57
ethergroup bridgegroup group....56
ethergroup bridgegroup use....55
ethergroup vlan mode....53
exit....1149

F

format....1143

G

getdomainlist....1197
grep....1175

H

host duid....1036
host ip address....1033
host ipv6 address....1034
host mac....1035
host name....1032
host rpon....1037

I

iamhere....1642
ip arp age....717
ip arp verify mode....718

L

lamp delay....1052
lamp mode....1051
lan description....143
lan ip address....148
lan ip alias....150
lan ip arp cycle....218
lan ip arp static....219
lan ip dhcp info....153
lan ip dhcp macauth aaa....159
lan ip dhcp macauth db....158
lan ip dhcp macauth type....160
lan ip dhcp macauth use....157
lan ip dhcp service....152
lan ip filter....196
lan ip filter default....201
lan ip filter move....200
lan ip icmp redirect....213
lan ip ids use....220
lan ip in-policy....209
lan ip in-policy move....211
lan ip localproxyarp....162
lan ip msschange....212
lan ip multicast mode....214
lan ip multicast pim preference....216
lan ip multicast pim upstream type....217
lan ip multicast ttl threshold....215
lan ip nat appli....195
lan ip nat destination....193
lan ip nat mode....184
lan ip nat rule....189
lan ip nat static....186
lan ip nat static default....188
lan ip nat wellknown....191
lan ip ospf auth md5key....182
lan ip ospf auth textkey....181
lan ip ospf auth type....180
lan ip ospf cost....174
lan ip ospf dead....176
lan ip ospf delay....178
lan ip ospf hello....175
lan ip ospf passive....183
lan ip ospf priority....179
lan ip ospf retrans....177
lan ip ospf use....173
lan ip priority....206
lan ip proxyarp....161
lan ip rip filter act....167
lan ip rip filter move....169
lan ip rip filter route....170
lan ip rip filter set metric....172
lan ip rip use....165
lan ip route....163
lan ip tos....202
lan ip tos move....205
lan ipv6 address....223
lan ipv6 dhcp client iaid....283
lan ipv6 dhcp client option dns....277
lan ipv6 dhcp client option domain....278
lan ipv6 dhcp client option na....275
lan ipv6 dhcp client option pd....276
lan ipv6 dhcp client option refreshtime....282
lan ipv6 dhcp client option sipserver address....279
lan ipv6 dhcp client option sipserver domain....280
lan ipv6 dhcp client option sntpserver....281
lan ipv6 dhcp client route....284
lan ipv6 dhcp duid....274
lan ipv6 dhcp relay interface....285
lan ipv6 dhcp relay server....286
lan ipv6 dhcp relay source....287
lan ipv6 dhcp server info address....289
lan ipv6 dhcp server info dns....291
lan ipv6 dhcp server info domain....292
lan ipv6 dhcp server info prefix....293
lan ipv6 dhcp server info sipserver address....295
lan ipv6 dhcp server info sipserver domain....296

lan ipv6 dhcp server info sntpserver.....297
lan ipv6 dhcp server preference.....288
lan ipv6 dhcp service.....273
lan ipv6 filter.....256
lan ipv6 filter default.....262
lan ipv6 filter move.....261
lan ipv6 ifid.....222
lan ipv6 in-policy.....270
lan ipv6 in-policy move.....272
lan ipv6 ospf cost.....249
lan ipv6 ospf dead.....251
lan ipv6 ospf delay.....253
lan ipv6 ospf hello.....250
lan ipv6 ospf passive.....255
lan ipv6 ospf priority.....254
lan ipv6 ospf retrans.....252
lan ipv6 ospf use.....248
lan ipv6 priority.....267
lan ipv6 ra curhoplimit.....230
lan ipv6 ra flags.....231
lan ipv6 ra interval.....226
lan ipv6 ra mode.....225
lan ipv6 ra mtu.....227
lan ipv6 ra prefix.....232
lan ipv6 ra reachabletime.....228
lan ipv6 ra recv valid-lifetime.....235
lan ipv6 ra retranstimer.....229
lan ipv6 ra trigger ifdown.....234
lan ipv6 rip aggregate.....241
lan ipv6 rip filter act.....242
lan ipv6 rip filter move.....244
lan ipv6 rip filter route.....245
lan ipv6 rip filter set metric.....247
lan ipv6 rip site-local.....240
lan ipv6 rip use.....238
lan ipv6 route.....236
lan ipv6 trafficclass.....263
lan ipv6 trafficclass move.....266
lan ipv6 use.....221
lan mtu.....144
lan shaping.....145
lan shaping-opt tc.....147
lan snmp trap linkdown.....318
lan snmp trap linkup.....319
lan vlan.....317
lan vrrp auth.....299
lan vrrp group action.....310
lan vrrp group ad.....302
lan vrrp group id.....300
lan vrrp group preempt.....303
lan vrrp group trigger ifdown.....304
lan vrrp group trigger node.....308
lan vrrp group trigger route.....306
lan vrrp group vaddr etherip.....315
lan vrrp group vaddr icmp.....314
lan vrrp trap.....316
lan vrrp use.....298
load.....1130
loopback ip address.....1064
loopback ip ospf use.....1065
loopback ipv6 address.....1066
loopintercept external.....1113
loopintercept internal.....1112

M

mac age.....133
macauth password.....958
macauth type.....959
macauth use.....957
macauthctl initialize port ether.....1598
mflag.....1062
more.....1173
multicast ip igmp report.....866
multicast ip pimsm candbsr address.....871
multicast ip pimsm candbsr mode.....870
multicast ip pimsm candbsr priority.....872
multicast ip pimsm candrp address.....868
multicast ip pimsm candrp mode.....867
multicast ip pimsm candrp priority.....869
multicast ip pimsm register checksum.....876
multicast ip pimsm spt mode.....874
multicast ip pimsm spt rate.....875
multicast ip pimsm staticrp address.....873
multicast ip route static.....877

N

node-trigger address.....965
node-trigger error-mode.....972
node-trigger error-retry.....973
node-trigger error-wait.....970
node-trigger interval.....967
node-trigger recovery.....969
node-trigger tos.....971
node-trigger ttl.....968

O

offline.....1601
online.....1604
ospf ip area defcost.....835
ospf ip area id.....833
ospf ip area range.....836
ospf ip area type.....834
ospf ip area type3-lsa.....838
ospf ip area type3-lsa move.....840
ospf ip definfo.....849
ospf ip id.....831
ospf ip redist.....851
ospf ip redist move.....853
ospf ip summary.....850
ospf ipv6 area defcost.....843
ospf ipv6 area id.....841
ospf ipv6 area inter-area-prefix.....846
ospf ipv6 area inter-area-prefix move.....848
ospf ipv6 area range.....844
ospf ipv6 area type.....842
ospf ipv6 definfo.....854
ospf ipv6 id.....832
ospf ipv6 redist.....855
ospf ipv6 redist move.....857

P

password aaa.....38
password admin set.....34
password authtype.....39
password format.....32

password user set.....36
ping.....1644
policy-group interface.....900
policy-group nexthop.....901
policy-group nexthop6.....902
policy-group pattern.....897
policy-group pattern move.....899
policy-group sessionwatch address.....903
policy-group sessionwatch error-wait.....909
policy-group sessionwatch interval.....905
policy-group sessionwatch recovery.....908
policy-group sessionwatch ttl.....907
proxydns address.....1024
proxydns address move.....1027
proxydns agetime.....1029
proxydns domain.....1019
proxydns domain move.....1023
proxydns source-port.....1031
proxydns ttl.....1030
proxydns unicode.....1028
pseudo-ether bind.....137
pseudo-ether description.....135
pseudo-ether snmp trap linkdown.....140
pseudo-ether snmp trap linkup.....141
pseudo-ether startup-delay.....138
pseudo-ether use.....136
pseudo-ether vlan untag.....139
pwconv.....1651

Q

quit.....1152

R

radius recovery.....1616
rdate.....1193
remote ap called accept.....349
remote ap called clid.....350
remote ap called number.....351
remote ap connect priority.....352
remote ap datalink bind.....332
remote ap datalink type.....331
remote ap description.....328
remote ap dial number.....348
remote ap disconnect packet.....342
remote ap disconnect time.....341
remote ap dvpn client.....429
remote ap dvpn remoteid.....432
remote ap dvpn remotenet.....430
remote ap idle.....353
remote ap ike bind.....412
remote ap ike certificate expired.....419
remote ap ike certificate key.....418
remote ap ike certificate local.....417
remote ap ike certificate remote.....416
remote ap ike certificate request.....421
remote ap ike certificate send.....420
remote ap ike dpd anti-replay.....428
remote ap ike dpd idle.....426
remote ap ike dpd retry.....427
remote ap ike dpd use.....425
remote ap ike eap auth send.....403
remote ap ike idtype.....402
remote ap ike initial.....409
remote ap ike local-idtype.....422
remote ap ike mode.....410
remote ap ike name local.....405
remote ap ike name remote.....407
remote ap ike nat-traversal use.....414
remote ap ike port.....389
remote ap ike proposal auth-method.....394
remote ap ike proposal encrypt.....396
remote ap ike proposal hash.....397
remote ap ike proposal lifetime.....399
remote ap ike proposal move.....392
remote ap ike proposal pfs.....398
remote ap ike proposal prf.....400
remote ap ike release.....408
remote ap ike remote-id-send.....424
remote ap ike remote-idtype.....423
remote ap ike retry.....401
remote ap ike shared key.....390
remote ap ike ts multi.....404
remote ap ip dns.....334
remote ap ipsec extension-range.....387
remote ap ipsec ike anti-replay.....383
remote ap ipsec ike auth.....375
remote ap ipsec ike encrypt.....373
remote ap ipsec ike esn.....384
remote ap ipsec ike exchange-sa initiator.....385
remote ap ipsec ike exchange-sa responder.....386
remote ap ipsec ike lifebyte.....378
remote ap ipsec ike lifetime.....377
remote ap ipsec ike newsa initiator.....379
remote ap ipsec ike newsa responder.....380
remote ap ipsec ike pfs.....376
remote ap ipsec ike protocol.....372
remote ap ipsec ike range.....381
remote ap ipsec receive auth.....370
remote ap ipsec receive encrypt.....368
remote ap ipsec receive protocol.....366
remote ap ipsec receive range.....367
remote ap ipsec receive spi.....365
remote ap ipsec send auth.....363
remote ap ipsec send encrypt.....361
remote ap ipsec send protocol.....358
remote ap ipsec send range.....360
remote ap ipsec send spi.....357
remote ap ipsec type.....355
remote ap keep.....354
remote ap limit time.....340
remote ap move.....330
remote ap multiroute pattern.....336
remote ap multiroute pattern move.....339
remote ap name.....329
remote ap overlap nexthop.....439
remote ap overlap nexthop6.....440
remote ap overlap to.....438
remote ap ppp auth receive.....345
remote ap ppp auth send.....344
remote ap ppp auth type.....343
remote ap pppoe acname.....346
remote ap pppoe svname.....347
remote ap recovery.....333
remote ap sessionwatch address.....441
remote ap sessionwatch error-wait.....448
remote ap sessionwatch interval.....443
remote ap sessionwatch mode.....446

remote ap sessionwatch recovery.....447
remote ap sessionwatch ttl.....445
remote ap snmp trap linkdown.....449
remote ap snmp trap linkup.....450
remote ap tunnel local.....433
remote ap tunnel mtu.....437
remote ap tunnel remote.....435
remote autodial.....323
remote bridgegroup group.....593
remote bridgegroup macfilter.....594
remote bridgegroup macfilter move.....596
remote bridgegroup use.....592
remote description.....321
remote ip address local.....454
remote ip address remote.....455
remote ip dvpn.....510
remote ip dvpn move.....512
remote ip filter.....489
remote ip filter default.....494
remote ip filter move.....493
remote ip ids use.....513
remote ip in-policy.....502
remote ip in-policy move.....504
remote ip msschange.....505
remote ip multicast mode.....506
remote ip multicast pim preference.....508
remote ip multicast pim upstream type.....509
remote ip multicast ttl threshold.....507
remote ip nat appli.....488
remote ip nat destination.....487
remote ip nat mode.....478
remote ip nat rule.....483
remote ip nat static.....480
remote ip nat static default.....482
remote ip nat wellknown.....485
remote ip ospf auth md5key.....474
remote ip ospf auth textkey.....473
remote ip ospf auth type.....472
remote ip ospf checkmtu.....477
remote ip ospf cost.....467
remote ip ospf dead.....469
remote ip ospf delay.....471
remote ip ospf hello.....468
remote ip ospf multicast.....476
remote ip ospf passive.....475
remote ip ospf retrans.....470
remote ip ospf use.....466
remote ip priority.....499
remote ip rip filter act.....460
remote ip rip filter move.....462
remote ip rip filter route.....463
remote ip rip filter set metric.....465
remote ip rip use.....458
remote ip route.....456
remote ip tos.....495
remote ip tos move.....498
remote ipv6 address.....516
remote ipv6 dhcp client iaid.....576
remote ipv6 dhcp client option dns.....570
remote ipv6 dhcp client option domain.....571
remote ipv6 dhcp client option na.....568
remote ipv6 dhcp client option pd.....569
remote ipv6 dhcp client option refreshtime.....575
remote ipv6 dhcp client option sipserver address 572
remote ipv6 dhcp client option sipserver domain. 573
remote ipv6 dhcp client option sntpserver.....574
remote ipv6 dhcp client route.....577
remote ipv6 dhcp duid.....567
remote ipv6 dhcp relay interface.....578
remote ipv6 dhcp relay server.....579
remote ipv6 dhcp relay source.....580
remote ipv6 dhcp server info dns.....582
remote ipv6 dhcp server info domain.....583
remote ipv6 dhcp server info prefix.....584
remote ipv6 dhcp server info sipserver address. .586
remote ipv6 dhcp server info sipserver domain...587
remote ipv6 dhcp server info sntpserver.....588
remote ipv6 dhcp server preference.....581
remote ipv6 dhcp service.....566
remote ipv6 dvpn.....589
remote ipv6 dvpn move.....591
remote ipv6 filter.....549
remote ipv6 filter default.....555
remote ipv6 filter move.....554
remote ipv6 ifid.....515
remote ipv6 in-policy.....563
remote ipv6 in-policy move.....565
remote ipv6 ospf checkmtu.....548
remote ipv6 ospf cost.....542
remote ipv6 ospf dead.....544
remote ipv6 ospf delay.....546
remote ipv6 ospf hello.....543
remote ipv6 ospf passive.....547
remote ipv6 ospf retrans.....545
remote ipv6 ospf use.....541
remote ipv6 priority.....560
remote ipv6 ra curhoplimit.....523
remote ipv6 ra flags.....524
remote ipv6 ra interval.....519
remote ipv6 ra mode.....518
remote ipv6 ra mtu.....520
remote ipv6 ra prefix.....525
remote ipv6 ra reachabletime.....521
remote ipv6 ra recv valid-lifetime.....528
remote ipv6 ra retranstimer.....522
remote ipv6 ra trigger ifdown.....527
remote ipv6 rip aggregate.....534
remote ipv6 rip filter act.....535
remote ipv6 rip filter move.....537
remote ipv6 rip filter route.....538
remote ipv6 rip filter set metric.....540
remote ipv6 rip site-local.....533
remote ipv6 rip use.....531
remote ipv6 route.....529
remote ipv6 trafficclass.....556
remote ipv6 trafficclass move.....559
remote ipv6 use.....514
remote mtu.....324
remote name.....322
remote ppp ipcp iphc.....452
remote ppp ipcp vjcomp.....451
remote ppp ipv6cp iphc.....453
remote shaping.....325
remote shaping-opt tc.....327
remote snmp trap linkdown.....597
remote snmp trap linkup.....598
remove.....1141
rename.....1142

reset.....1194
resource authenticated vlan.....1054
resource system vlan.....1053
rip ip gwfilter.....765
rip ip gwfilter move.....766
rip ip multipath.....760
rip ip neighbor.....764
rip ip redist.....761
rip ip redist move.....763
rip ip timers basic.....758
rip ip timers jitter.....759
rip ipv6 multipath.....768
rip ipv6 redist.....769
rip ipv6 redist move.....771
rip ipv6 timers basic.....767
routemanage ip distance.....742
routemanage ip ecmp mode.....749
routemanage ip ecmp ospf.....750
routemanage ip redist bgp.....746
routemanage ip redist ospf.....747
routemanage ip redist rip.....744
routemanage ipv6 distance.....751
routemanage ipv6 redist bgp.....755
routemanage ipv6 redist ospf.....756
routemanage ipv6 redist rip.....753
rpon.....1653

S

save.....1132
schedule at.....1038
schedule in.....1040
schedule syslog.....1042
serverinfo dns.....1092
serverinfo dns filter.....1094
serverinfo dns filter default.....1097
serverinfo dns filter move.....1096
serverinfo dns ipv6.....1093
serverinfo ftp.....1067
serverinfo ftp filter.....1069
serverinfo ftp filter default.....1072
serverinfo ftp filter move.....1071
serverinfo ftp ipv6.....1068
serverinfo http.....1087
serverinfo http filter.....1088
serverinfo http filter default.....1091
serverinfo http filter move.....1090
serverinfo sftp.....1073
serverinfo sftp ipv6.....1074
serverinfo sntp.....1098
serverinfo sntp filter.....1100
serverinfo sntp filter default.....1103
serverinfo sntp filter move.....1102
serverinfo sntp ipv6.....1099
serverinfo ssh.....1081
serverinfo ssh filter.....1083
serverinfo ssh filter default.....1086
serverinfo ssh filter move.....1085
serverinfo ssh ipv6.....1082
serverinfo telnet.....1075
serverinfo telnet filter.....1077
serverinfo telnet filter default.....1080
serverinfo telnet filter move.....1079
serverinfo telnet ipv6.....1076
serverinfo time filter.....1108
serverinfo time filter default.....1111
serverinfo time filter move.....1110
serverinfo time ip tcp.....1104
serverinfo time ip udp.....1106
serverinfo time ipv6 tcp.....1105
serverinfo time ipv6 udp.....1107
show aaa mac collect list.....1565
show aaa mac collect status.....1564
show aaa radius client server-info.....1561
show aaa radius client statistics.....1562
show access-point.....1265
show alias.....1171
show arp.....1276
show arpauth statistics.....1525
show arpauth vlan.....1523
show auth port ether.....1512
show bridge.....1489
show bridgegroup.....1506
show bridgegroup status.....1508
show candidate-config.....1124
show crypto certificate.....1587
show date.....1191
show domainlist.....1555
show dot1x port ether.....1514
show dot1x statistics port ether.....1516
show dvpn client session.....1456
show dvpn client user.....1454
show dvpn server.....1458
show dvpn server session.....1461
show dvpn server user.....1459
show ether.....1199
show ether brief.....1202
show ether media-info.....1215
show ether queue.....1213
show ether statistics.....1204
show ether utilization.....1211
show ike statistics.....1476
show interface.....1254
show interface brief.....1257
show interface detail.....1259
show interface statistics.....1263
show interface summary.....1258
show ip bgp neighbors.....1325
show ip bgp route.....1317
show ip bgp route summary.....1321
show ip bgp status.....1323
show ip dhcp.....1445
show ip filter.....1404
show ip filter statistics.....1407
show ip filter summary.....1408
show ip ids statistics.....1416
show ip multicast group.....1428
show ip multicast interface.....1430
show ip multicast interface statistics.....1432
show ip multicast pimsm rp.....1433
show ip multicast protocol.....1434
show ip multicast route.....1435
show ip multicast route kernel.....1437
show ip multicast route kernel statistics.....1439
show ip multicast statistics.....1440
show ip nat.....1421
show ip nat statistics.....1423
show ip nat summary.....1425

show ip ospf database.....1354
show ip ospf interface.....1361
show ip ospf neighbor.....1364
show ip ospf protocol.....1351
show ip ospf route.....1348
show ip rip protocol.....1309
show ip rip route.....1307
show ip route.....1284
show ip route kernel.....1290
show ip route kernel ecmp statistics.....1292
show ip route summary.....1287
show ip traffic.....1395
show ipsec sa.....1466
show ipv6 bgp neighbors.....1340
show ipv6 bgp route.....1332
show ipv6 bgp route summary.....1336
show ipv6 bgp status.....1338
show ipv6 dhcp.....1448
show ipv6 filter.....1410
show ipv6 filter statistics.....1412
show ipv6 filter summary.....1413
show ipv6 ospf database.....1374
show ipv6 ospf interface.....1385
show ipv6 ospf neighbor.....1389
show ipv6 ospf protocol.....1371
show ipv6 ospf route.....1368
show ipv6 ra default-router-list.....1302
show ipv6 ra prefix-list.....1304
show ipv6 rip protocol.....1314
show ipv6 rip route.....1312
show ipv6 route.....1294
show ipv6 route kernel.....1300
show ipv6 route summary.....1297
show ipv6 traffic.....1399
show logging command.....1167
show logging error.....1184
show logging syslog.....1188
show macauth port ether.....1519
show macauth statistics port ether.....1521
show modemmodule.....1222
show modemmodule account.....1225
show modemmodule condition history.....1231
show modemmodule condition statistics.....1234
show modemmodule condition status.....1227
show modemmodule statistics.....1236
show ndp.....1280
show nettime statistics.....1539
show policy-group.....1552
show pseudo-ether.....1249
show pseudo-ether statistics.....1251
show running-config.....1125
show snmp statistics.....1534
show socket.....1568
show spanning-tree.....1492
show ssh server key.....1558
show startup-config.....1126
show system funcswitch.....1182
show system information.....1178
show system status.....1180
show tech-support.....1183
show template.....1270
show template statistics.....1272
show terminal.....1166
show trace ike.....1577
show trace modemmodule.....1581
show trace ppp.....1572
show trace pppoe.....1575
show trace ssh.....1583
show tracking.....1528
show tracking brief.....1531
show upnp.....1544
show upnp portmapping.....1548
show upnp statistics.....1546
show usb hcd status.....1243
show usb storage status.....1244
show vlan.....1219
show vrrp.....1483
snmp agent contact.....980
snmp agent engineid.....985
snmp agent ip address.....983
snmp agent ipv6 address.....984
snmp agent location.....982
snmp agent sysname.....981
snmp manager.....986
snmp service.....979
snmp trap authfail.....991
snmp trap coldstart.....988
snmp trap linkdown.....989
snmp trap linkup.....990
snmp trap noserror.....995
snmp trap vrrpauthfail.....993
snmp trap vrrpnewmaster.....992
snmp trap vrrpprotoerror.....994
snmp user address.....997
snmp user auth.....999
snmp user name.....996
snmp user notification.....998
snmp user notify.....1003
snmp user priv.....1000
snmp user read.....1002
snmp user write.....1001
snmp view subtree.....1004
storage setup machine.....1044
storage setup mode.....1043
stp age.....112
stp delay.....113
stp domain priority.....115
stp hello.....114
stp mode.....111
su.....1147
sysdown harderr other.....1061
sysdown harderr thermal.....1060
syslog command-logging.....1012
syslog dupcut.....1011
syslog facility.....1009
syslog header.....1013
syslog pri.....1008
syslog security.....1010
syslog server address.....1006
syslog server pri.....1007
syslog source ip address.....1014
syslog source ipv6 address.....1015
sysmemwatch interval.....977
sysmemwatch mode.....975
sysmemwatch threshold.....976
sysname.....1063

T

tail.....1174
telnet.....1649
telnetinfo.....1059
template aaa.....609
template combine use.....611
template datalink type.....610
template description.....604
template dvpn client.....659
template dvpn domain.....667
template dvpn expire register.....663
template dvpn expire session.....664
template dvpn global.....672
template dvpn interface.....671
template dvpn localid.....670
template dvpn localnet.....668
template dvpn server address.....660
template dvpn server auth.....662
template dvpn ua.....665
template idle.....607
template ike certificate expired.....701
template ike certificate key.....700
template ike certificate local.....699
template ike certificate request.....703
template ike certificate send.....702
template ike dpd anti-replay.....707
template ike dpd idle.....705
template ike dpd retry.....706
template ike dpd use.....704
template ike idtype.....693
template ike mode.....696
template ike name local.....694
template ike nat-traversal use.....697
template ike proposal auth-method.....687
template ike proposal encrypt.....688
template ike proposal hash.....689
template ike proposal lifetime.....691
template ike proposal move.....686
template ike proposal pfs.....690
template ike release.....695
template ike retry.....692
template ike shared key.....684
template interface pool.....608
template ip dns.....612
template ip filter.....625
template ip filter default.....630
template ip filter move.....629
template ip ids use.....636
template ip in-policy.....637
template ip in-policy move.....639
template ip msschange.....635
template ip nat appli.....624
template ip nat destination.....623
template ip nat mode.....614
template ip nat rule.....619
template ip nat static.....616
template ip nat static default.....618
template ip nat wellknown.....621
template ip tos.....631
template ip tos move.....634
template ipsec ike anti-replay.....681
template ipsec ike auth.....675
template ipsec ike encrypt.....674
template ipsec ike exchange-sa initiator.....682
template ipsec ike exchange-sa responder.....683
template ipsec ike lifebyte.....678
template ipsec ike lifetime.....677
template ipsec ike newsa initiator.....679
template ipsec ike newsa responder.....680
template ipsec ike pfs.....676
template ipsec ike protocol.....673
template ipv6 filter.....642
template ipv6 filter default.....648
template ipv6 filter move.....647
template ipv6 ifid.....641
template ipv6 in-policy.....656
template ipv6 in-policy move.....658
template ipv6 priority.....653
template ipv6 trafficclass.....649
template ipv6 trafficclass move.....652
template ipv6 use.....640
template mtu.....606
template name.....605
template sessionwatch address.....710
template sessionwatch interval.....712
template snmp trap linkdown.....714
template snmp trap linkup.....715
template tunnel local.....708
terminal bell.....1164
terminal charset.....1160
terminal logging.....1165
terminal pager.....1156
terminal prompt.....1161
terminal timestamp.....1163
terminal window.....1159
time auto interval.....1017
time auto server.....1016
time zone.....1018
top.....1153
traceroute.....1646
tracking action.....964
tracking trigger node.....963

U

up.....1154
update.....1195
updateinfo.....1047
upnp portmapping lease.....882
upnp use.....880
usbctl.....1626

V

vlan arpauth aaa.....125
vlan arpauth authenticated-ip.....131
vlan arpauth dummymac.....127
vlan arpauth expire.....128
vlan arpauth obstruction.....126
vlan arpauth overflow.....129
vlan arpauth type.....130
vlan arpauth use.....124
vlan bridgegroup group.....120
vlan bridgegroup macfilter.....121
vlan bridgegroup macfilter move.....123
vlan bridgegroup use.....119
vlan description.....117
vlan forward.....118

vrrp action.....1608
vrrp preempt-permit.....1610

W

wan bind.....43
wan description.....41
wan line.....44
wan modemmodule condition connect mode.....48
wan modemmodule condition history dupcut.....49
wan modemmodule condition level.....46
wan modemmodule condition mode.....45
wan modemmodule condition watch.....47
wan snmp trap linkdown.....50
wan snmp trap linkup.....51
wan use.....42
watchdog service.....1057

Si-R G シリーズ　コマンドリファレンス

P3NK-5322-02Z0

発行日　　2016年7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。