P3NK-3992-07Z0

FUJITSU Network Si-R
Si-Rシリーズ

コマンドリファレンス-構成定義編-
V35

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。

2009年11月初版
2010 年 7月第2版
2012 年11月第3版
2013 年11月第4版
2014 年 6月第5版
2015 年 1月第6版
2019 年 7月第7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 2009 - 2019

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のうち、構成定義コマンドについて説明しています。
運用管理コマンド、その他のコマンド、および付録情報については、「コマンドリファレンス-運用管理編-」を参照してください。

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

本書の読者と前提知識

本書は、ネットワーク管理を行っている方を対象に記述しています。

本書を利用するにあたって、ネットワークおよびインターネットに関する基本的な知識が必要です。

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

構成定義コマンドを使用する場合は、以下の点にご注意ください。

- コマンドの設定および変更が終了したら、save コマンドを実行してから commit コマンドまたは reset コマンドを実行し、設定を有効にしてください。save コマンドを実行せず reset コマンドまたは電源再投入を行った場合は、コマンドの設定が元の状態に戻ります。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。

本書における商標の表記について

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

AdobeおよびReaderは、Adobe Systems Incorporated（アドビシステムズ社）の米国ならびに他の国における商標または登録商標です。

UNIXは、米国およびその他の国におけるオープン・グループの登録商標です。

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

製品名の略称について

本書で使用している製品名は、以下のように略して表記します。
なお、本文中では®を省略しています。

製品名称	本文中の表記
Microsoft® Windows® XP Professional operating system	Windows XP
Microsoft® Windows® XP Home Edition operating system	
Microsoft® Windows® 2000 Server Network operating system	Windows 2000
Microsoft® Windows® 2000 Professional operating system	
Microsoft® Windows NT® Server network operating system Version 4.0	Windows NT 4.0
Microsoft® Windows NT® Workstation operating system Version 4.0	
Microsoft® Windows Server® 2003, Standard Edition	Windows Server 2003
Microsoft® Windows Server® 2003 R2, Standard Edition	
Microsoft® Windows Server® 2003, Enterprise Edition	
Microsoft® Windows Server® 2003 R2, Enterprise Edition	
Microsoft® Windows Server® 2003, Datacenter Edition	
Microsoft® Windows Server® 2003 R2, Datacenter Edition	
Microsoft® Windows Server® 2003, Web Edition	
Microsoft® Windows Server® 2003, Standard x64 Edition	
Microsoft® Windows Server® 2003 R2, Standard Edition	
Microsoft® Windows Server® 2003, Enterprise x64 Edition	
Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition	
Microsoft® Windows Server® 2003, Enterprise Edition for Itanium-based systems	
Microsoft® Windows Server® 2003, Datacenter x64 Edition	
Microsoft® Windows Server® 2003 R2, Datacenter x64 Edition	
Microsoft® Windows Vista® Ultimate operating system	Windows Vista
Microsoft® Windows Vista® Business operating system	
Microsoft® Windows Vista® Home Premium operating system	
Microsoft® Windows Vista® Home Basic operating system	
Microsoft® Windows Vista® Enterprise operating system	
Microsoft® Windows® 7 64bit Home Premium	Windows 7
Microsoft® Windows® 7 32bit Professional	

本装置のマニュアルの構成

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

マニュアル名称	内容
Si-R 効率化運用ツール使用手引書	Si-R 効率化運用ツールを使用する方法を説明しています。
Si-R180B　ご利用にあたって	Si-R180B の設置方法やソフトウェアのインストール方法を説明しています。
Si-R220C　ご利用にあたって	Si-R220C の設置方法やソフトウェアのインストール方法を説明しています。
Si-R220D　ご利用にあたって	Si-R220D の設置方法やソフトウェアのインストール方法を説明しています。
Si-R240B　ご利用にあたって	Si-R240B の設置方法やソフトウェアのインストール方法を説明しています。
Si-R260B　ご利用にあたって	Si-R260B の設置方法やソフトウェアのインストール方法を説明しています。
Si-R370　ご利用にあたって	Si-R370 の設置方法やソフトウェアのインストール方法を説明しています。
Si-R370B　ご利用にあたって	Si-R370B の設置方法やソフトウェアのインストール方法を説明しています。
Si-R570　ご利用にあたって	Si-R570 の設置方法やソフトウェアのインストール方法を説明しています。
Si-R570B　ご利用にあたって	Si-R570B 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。
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。
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。
コマンドリファレンス - 構成定義編 -（本書）	構成定義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。
コマンドリファレンス - 運用管理編 -	運用管理コマンド、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。
Web ユーザーズガイド	Web 画面を使用して、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。
Web 設定事例集	Web 画面を使用した、基本的な接続形態または機能の活用方法を説明しています。
Web リファレンス	Web 画面の項目の詳細な情報を説明しています。

目次

第 1 章　パスワード情報 27

1.1　パスワード情報 28
1.1.1　password format 28
1.1.2　password admin set 30
1.1.3　password admin aaa 32
1.1.4　password user set 33
1.1.5　password user aaa 35
1.1.6　password aaa 36
1.1.7　password authtype 37

第 2 章　WAN 情報の設定 38

2.1　回線共通情報 39
2.1.1　wan bind 39
2.1.2　wan line 41

2.2　ISDN 回線情報 43
2.2.1　wan isdn global 43
2.2.2　wan isdn number 44
2.2.3　wan isdn numbersend 46
2.2.4　wan isdn limit charge 48
2.2.5　wan isdn limit time 49
2.2.6　wan isdn accept 50
2.2.7　wan isdn autodial 51
2.2.8　wan isdn activation 52

2.3　専用線情報 53
2.3.1　wan hsd flagdetect 53

2.4　フレームリレー回線情報 54
2.4.1　wan fr lmi 54
2.4.2　wan fr fecn 55
2.4.3　wan fr becn 56
2.4.4　wan fr cllm 57

2.5　ATM 回線情報 58
2.5.1　wan atm vpi 58
2.5.2　wan atm rate 59
2.5.3　wan atm oam 60

2.6　データ通信カード情報 61
2.6.1　wan cardmodem pin 61

第 3 章　ATM 情報の設定 62

3.1　ATM 情報 63
3.1.1　atm send clock 63

第 4 章　スイッチ情報の設定 64

4.1　スイッチ共通情報 65
4.1.1　switch use 65
4.1.2　switch tag transparent 66
4.1.3　switch age 67

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

第 5 章　無線 LAN AP 関連情報の設定 75
5.1　無線 LAN AP 関連情報 76
5.1.1　wlan bind 76
5.1.2　wlan mode 77
5.1.3　wlan channel 78
5.1.4　wlan ssid 79
5.1.5　wlan hide 80
5.1.6　wlan sta limit 81
5.1.7　wlan txpower 82
5.1.8　wlan protection mode 84
5.1.9　wlan rts threshold 85
5.1.10　wlan dtim period 86
5.1.11　wlan beacon interval 87
5.1.12　wlan auth 88
5.1.13　wlan wep mode 89
5.1.14　wlan wep key 90
5.1.15　wlan wep send 92
5.1.16　wlan wpa cipher 93
5.1.17　wlan wpa psk 94
5.1.18　wlan wpa rekey 95
5.1.19　wlan wpa countermeasures 96
5.1.20　wlan filter 97
5.1.21　wlan filter move 99
第 6 章　LAN 情報の設定 100
6.1　lan 共通情報 101
6.1.1　lan bind 101
6.1.2　lan mode 103
6.1.3　lan mdi 105
6.1.4　lan flowctl 106
6.1.5　lan type 107
6.1.6　lan mtu 108
6.1.7　lan shaping 109
6.1.8　lan shaping-opt tc 111
6.2　LAN ポートバックアップ関連情報 112
6.2.1　lan backup bind 112
6.2.2　lan backup mode 113
6.3　LAN ポート閉塞関連情報 114
6.3.1　lan recovery 114
6.4　IP 関連情報 116
6.4.1　lan ip address 116
6.4.2　lan ip alias 118
6.4.3　lan ip dhcp service 120
6.4.4　lan ip dhcp info 121
6.4.5　lan ip dhcp macauth use 124
6.4.6　lan ip dhcp macauth db 125
6.4.7　lan ip dhcp macauth aaa 126
6.4.8　lan ip dhcp macauth type 127
6.4.9　lan ip proxyarp 128
6.4.10　lan ip localproxyarp 129
6.4.11　lan ip route 130
6.4.12　lan ip rip use 133
6.4.13　lan ip rip filter act 135
6.4.14　lan ip rip filter move 137
6.4.15　lan ip rip filter route 138
6.4.16　lan ip rip filter set metric 140
6.4.17　lan ip ospf use 141
6.4.18　lan ip ospf cost 143

6.4.19 lan ip ospf hello . . . 144
6.4.20 lan ip ospf dead . . . 145
6.4.21 lan ip ospf retrans . . . 146
6.4.22 lan ip ospf delay . . . 147
6.4.23 lan ip ospf priority . . . 148
6.4.24 lan ip ospf auth type . . . 149
6.4.25 lan ip ospf auth textkey . . . 150
6.4.26 lan ip ospf auth md5key . . . 151
6.4.27 lan ip ospf passive . . . 152
6.4.28 lan ip vrf use . . . 153
6.4.29 lan ip vrf route . . . 154
6.4.30 lan ip nat mode . . . 156
6.4.31 lan ip nat static . . . 158
6.4.32 lan ip nat static default . . . 160
6.4.33 lan ip nat rule . . . 161
6.4.34 lan ip nat wellknown . . . 163
6.4.35 lan ip nat destination . . . 165
6.4.36 lan ip nat appli . . . 167
6.4.37 lan ip filter . . . 169
6.4.38 lan ip filter move . . . 174
6.4.39 lan ip filter default . . . 175
6.4.40 lan ip tos . . . 176
6.4.41 lan ip tos move . . . 179
6.4.42 lan ip priority . . . 180
6.4.43 lan ip in-policy . . . 184
6.4.44 lan ip in-policy move . . . 186
6.4.45 lan ip icmp redirect . . . 187
6.4.46 lan ip multicast mode . . . 188
6.4.47 lan ip multicast ttl threshold . . . 189
6.4.48 lan ip multicast pim preference . . . 190
6.4.49 lan ip multicast pim upstream type . . . 191
6.4.50 lan ip arp cycle . . . 192
6.4.51 lan ip arp static . . . 193
6.4.52 lan ip ids use . . . 194

6.5 IPv6 関連情報 . . . 195
6.5.1 lan ip6 use . . . 195
6.5.2 lan ip6 ifid . . . 196
6.5.3 lan ip6 address . . . 197
6.5.4 lan ip6 ra mode . . . 199
6.5.5 lan ip6 ra interval . . . 200
6.5.6 lan ip6 ra mtu . . . 201
6.5.7 lan ip6 ra reachabletime . . . 202
6.5.8 lan ip6 ra retranstimer . . . 203
6.5.9 lan ip6 ra curhoplimit . . . 204
6.5.10 lan ip6 ra flags . . . 205
6.5.11 lan ip6 route . . . 206
6.5.12 lan ip6 rip use . . . 208
6.5.13 lan ip6 rip site-local . . . 210
6.5.14 lan ip6 rip aggregate . . . 211
6.5.15 lan ip6 rip filter act . . . 212
6.5.16 lan ip6 rip filter move . . . 214
6.5.17 lan ip6 rip filter route . . . 215
6.5.18 lan ip6 rip filter set metric . . . 217
6.5.19 lan ip6 ospf use . . . 218
6.5.20 lan ip6 ospf cost . . . 220
6.5.21 lan ip6 ospf hello . . . 221
6.5.22 lan ip6 ospf dead . . . 222
6.5.23 lan ip6 ospf retrans . . . 223
6.5.24 lan ip6 ospf delay . . . 224

6.5.25 lan ip6 ospf priority . . . 225
6.5.26 lan ip6 ospf passive . . . 226
6.5.27 lan ip6 filter . . . 227
6.5.28 lan ip6 filter move . . . 232
6.5.29 lan ip6 filter default . . . 233
6.5.30 lan ip6 trafficclass . . . 234
6.5.31 lan ip6 trafficclass move . . . 237
6.5.32 lan ip6 priority . . . 238
6.5.33 lan ip6 in-policy . . . 242
6.5.34 lan ip6 in-policy move . . . 244
6.5.35 lan ip6 dhcp service . . . 245
6.5.36 lan ip6 dhcp duid . . . 246
6.5.37 lan ip6 dhcp client option pd . . . 247
6.5.38 lan ip6 dhcp client option dns . . . 248
6.5.39 lan ip6 dhcp client option domain . . . 249
6.5.40 lan ip6 dhcp client option sipserver address . . . 250
6.5.41 lan ip6 dhcp client option sipserver domain . . . 251
6.5.42 lan ip6 dhcp client option sntpserver . . . 252
6.5.43 lan ip6 dhcp client iaid . . . 253
6.5.44 lan ip6 dhcp client route . . . 254
6.5.45 lan ip6 dhcp relay interface . . . 255
6.5.46 lan ip6 dhcp relay server . . . 256
6.5.47 lan ip6 dhcp relay source . . . 257
6.5.48 lan ip6 dhcp server preference . . . 258
6.5.49 lan ip6 dhcp server info address . . . 259
6.5.50 lan ip6 dhcp server info dns . . . 261
6.5.51 lan ip6 dhcp server info domain . . . 262
6.5.52 lan ip6 dhcp server info prefix . . . 263
6.5.53 lan ip6 dhcp server info sipserver address . . . 265
6.5.54 lan ip6 dhcp server info sipserver domain . . . 266
6.5.55 lan ip6 dhcp server info sntpserver . . . 267

6.6 ブリッジ関連情報 . . . 268
6.6.1 lan bridge use . . . 268
6.6.2 lan bridge group . . . 269
6.6.3 lan bridge static . . . 270
6.6.4 lan bridge stp use . . . 271
6.6.5 lan bridge stp cost . . . 272
6.6.6 lan bridge stp priority . . . 274
6.6.7 lan bridge filter . . . 275
6.6.8 lan bridge filter move . . . 278
6.6.9 lan bridge priority . . . 279

6.7 VRRP 関連情報 . . . 281
6.7.1 lan vrrp use . . . 281
6.7.2 lan vrrp auth . . . 282
6.7.3 lan vrrp group id . . . 283
6.7.4 lan vrrp group ad . . . 285
6.7.5 lan vrrp group preempt . . . 286
6.7.6 lan vrrp group trigger ifdown . . . 287
6.7.7 lan vrrp group trigger route . . . 289
6.7.8 lan vrrp group trigger node . . . 291
6.7.9 lan vrrp group action . . . 294
6.7.10 lan vrrp group vaddr icmp . . . 298
6.7.11 lan vrrp group vaddr etherip . . . 299
6.7.12 lan vrrp trap . . . 300

6.8 MPLS 関連情報 . . . 301
6.8.1 lan mpls use . . . 301
6.8.2 lan mpls distribution . . . 302
6.8.3 lan mpls ldp hello-timers . . . 303
6.8.4 lan mpls ldp keepalive-timers . . . 304

6.8.5 lan mpls ldp advertisement . . . 305
6.8.6 lan mpls ldp retention . . . 306
6.8.7 lan mpls ldp interface-label . . . 307
6.8.8 lan mpls ldp ip transport . . . 308
6.8.9 lan mpls l2-circuit vc . . . 309
6.8.10 lan mpls l2-circuit exp . . . 311

6.9 VLAN 関連情報 . . . 312
6.9.1 lan vlan bind . . . 312
6.9.2 lan vlan tag vid . . . 314
6.9.3 lan vlan tag pri . . . 315
6.9.4 lan vlan tag primap . . . 316

6.10 MAC アドレス認証関連情報 . . . 318
6.10.1 lan macauth use . . . 318
6.10.2 lan macauth expire . . . 319
6.10.3 lan macauth aaa . . . 320
6.10.4 lan macauth security . . . 321

6.11 SNMP 関連情報 . . . 322
6.11.1 lan snmp trap linkdown . . . 322
6.11.2 lan snmp trap linkup . . . 323

6.12 LLDP 関連 . . . 324
6.12.1 lan lldp mode . . . 324
6.12.2 lan lldp info . . . 325
6.12.3 lan lldp vlan . . . 328
6.12.4 lan lldp notification . . . 329

6.13 ARP 認証関連情報 . . . 330
6.13.1 lan arpauth use . . . 330
6.13.2 lan arpauth aaa . . . 331
6.13.3 lan arpauth obstruction . . . 332
6.13.4 lan arpauth dummymac . . . 333
6.13.5 lan arpauth expire . . . 334
6.13.6 lan arpauth overflow . . . 335
6.13.7 lan arpauth type . . . 336
6.13.8 lan arpauth authenticated-ip . . . 337

6.14 IEEE802.1X 認証関連情報 . . . 338
6.14.1 lan dot1x use . . . 338
6.14.2 lan dot1x portcontrol . . . 339
6.14.3 lan dot1x quietperiod . . . 340
6.14.4 lan dot1x txperiod . . . 341
6.14.5 lan dot1x supptimeout . . . 342
6.14.6 lan dot1x maxreq . . . 343
6.14.7 lan dot1x reauthperiod . . . 344
6.14.8 lan dot1x aaa . . . 345
6.14.9 lan dot1x mode . . . 346
6.14.10 lan dot1x wol . . . 347

第 7 章　シリアル情報の設定 . . . 348

7.1 シリアル共通情報 . . . 349
7.1.1 serial use . . . 349
7.1.2 serial speed . . . 350

7.2 モデム関連情報 . . . 351
7.2.1 serial modem dial . . . 351
7.2.2 serial modem tonedetect . . . 352
7.2.3 serial modem speaker mode . . . 353
7.2.4 serial modem speaker volume . . . 354

第 8 章　相手情報の設定 . . . 355

8.1 相手共通情報 . . . 356

8.1.1 remote name 356
8.1.2 remote autodial 357
8.1.3 remote mtu 358
8.1.4 remote shaping 359
8.1.5 remote shaping-opt tc 361
8.2 接続先情報 362
8.2.1 remote ap name 362
8.2.2 remote ap move 363
8.2.3 remote ap datalink type 364
8.2.4 remote ap datalink bind 366
8.2.5 remote ap datalink bundle 368
8.2.6 remote ap recovery 369
8.2.7 remote ap ip dns 370
8.2.8 remote ap multiroute pattern 372
8.2.9 remote ap multiroute pattern move 375
8.2.10 remote ap limit charge 376
8.2.11 remote ap limit time 377
8.2.12 remote ap disconnect time 378
8.2.13 remote ap disconnect packet 379
8.2.14 remote ap ppp auth type 380
8.2.15 remote ap ppp auth send 381
8.2.16 remote ap ppp auth receive 382
8.2.17 remote ap ppp mp use 383
8.2.18 remote ap ppp mp bap use 384
8.2.19 remote ap pppoe acname 385
8.2.20 remote ap pppoe svname 386
8.2.21 remote ap dial number 387
8.2.22 remote ap dial speed 388
8.2.23 remote ap called accept 390
8.2.24 remote ap called clid 391
8.2.25 remote ap called number 392
8.2.26 remote ap connect priority 393
8.2.27 remote ap idle 394
8.2.28 remote ap step 395
8.2.29 remote ap step2 396
8.2.30 remote ap step3 397
8.2.31 remote ap keep 398
8.2.32 remote ap fr dlci 399
8.2.33 remote ap fr cir 400
8.2.34 remote ap atm vci 401
8.2.35 remote ap atm rate 403
8.2.36 remote ap atm ast 404
8.2.37 remote ap atm oam 406
8.2.38 remote ap atm vcwatch 407
8.2.39 remote ap ipsec type 409
8.2.40 remote ap ipsec send spi 411
8.2.41 remote ap ipsec send protocol 412
8.2.42 remote ap ipsec send range 414
8.2.43 remote ap ipsec send encrypt 415
8.2.44 remote ap ipsec send auth 417
8.2.45 remote ap ipsec receive spi 419
8.2.46 remote ap ipsec receive protocol 420
8.2.47 remote ap ipsec receive range 421
8.2.48 remote ap ipsec receive encrypt 422
8.2.49 remote ap ipsec receive auth 424
8.2.50 remote ap ipsec ike protocol 426
8.2.51 remote ap ipsec ike encrypt 427
8.2.52 remote ap ipsec ike auth 428
8.2.53 remote ap ipsec ike pfs 429

8.2.54 remote ap ipsec ike lifetime . . . 430
8.2.55 remote ap ipsec ike lifebyte . . . 431
8.2.56 remote ap ipsec ike newsa initiator . . . 432
8.2.57 remote ap ipsec ike newsa responder . . . 433
8.2.58 remote ap ipsec ike range . . . 434
8.2.59 remote ap ipsec ike esn . . . 435
8.2.60 remote ap ipsec extension-range . . . 436
8.2.61 remote ap ike port . . . 438
8.2.62 remote ap ike shared key . . . 439
8.2.63 remote ap ike proposal move . . . 441
8.2.64 remote ap ike proposal auth-method . . . 442
8.2.65 remote ap ike proposal encrypt . . . 443
8.2.66 remote ap ike proposal hash . . . 444
8.2.67 remote ap ike proposal pfs . . . 445
8.2.68 remote ap ike proposal lifetime . . . 446
8.2.69 remote ap ike proposal prf . . . 447
8.2.70 remote ap ike retry . . . 448
8.2.71 remote ap ike idtype . . . 449
8.2.72 remote ap ike name local . . . 450
8.2.73 remote ap ike name remote . . . 451
8.2.74 remote ap ike release . . . 452
8.2.75 remote ap ike initial . . . 453
8.2.76 remote ap ike sessionwatch . . . 454
8.2.77 remote ap ike mode . . . 456
8.2.78 remote ap ike bind . . . 458
8.2.79 remote ap ike nat-traversal use . . . 460
8.2.80 remote ap ike certificate remote . . . 462
8.2.81 remote ap ike certificate local . . . 463
8.2.82 remote ap ike certificate key . . . 464
8.2.83 remote ap ike certificate expired . . . 465
8.2.84 remote ap ike certificate send . . . 466
8.2.85 remote ap ike certificate request . . . 467
8.2.86 remote ap ike local-idtype . . . 468
8.2.87 remote ap ike remote-idtype . . . 469
8.2.88 remote ap ike remote-id-send . . . 470
8.2.89 remote ap ike dpd use . . . 471
8.2.90 remote ap ike dpd idle . . . 472
8.2.91 remote ap ike dpd retry . . . 473
8.2.92 remote ap dvpn client . . . 474
8.2.93 remote ap dvpn remotenet . . . 475
8.2.94 remote ap dvpn remoteid . . . 477
8.2.95 remote ap tunnel local . . . 478
8.2.96 remote ap tunnel remote . . . 480
8.2.97 remote ap overlap to . . . 481
8.2.98 remote ap overlap nexthop . . . 483
8.2.99 remote ap overlap nexthop6 . . . 484
8.2.100 remote ap sessionwatch address . . . 485
8.2.101 remote ap sessionwatch interval . . . 487
8.2.102 remote ap sessionwatch ttl . . . 489
8.2.103 remote ap sessionwatch mode . . . 490
8.2.104 remote ap sessionwatch recovery . . . 491
8.2.105 remote ap sessionwatch error-wait . . . 492
8.2.106 remote ap mpls to . . . 493
8.2.107 remote ap mpls nexthop . . . 495
8.2.108 remote ap snmp trap linkdown . . . 496
8.2.109 remote ap snmp trap linkup . . . 497

8.3 PPP 関連情報 . . . 498
8.3.1 remote ppp compress . . . 498
8.3.2 remote ppp mp start . . . 499

8.3.3 remote ppp mp max . . . 500
8.3.4 remote ppp mp divide . . . 501
8.3.5 remote ppp mp traffic use . . . 502
8.3.6 remote ppp mp traffic increase . . . 503
8.3.7 remote ppp mp traffic decrease . . . 504
8.3.8 remote ppp mp order . . . 505
8.3.9 remote ppp ipcp vjcomp . . . 506
8.3.10 remote ppp ipcp iphc . . . 507
8.3.11 remote ppp ipv6cp iphc . . . 508

8.4 IP 関連情報 . . . 509
8.4.1 remote ip address local . . . 509
8.4.2 remote ip address remote . . . 510
8.4.3 remote ip route . . . 511
8.4.4 remote ip rip use . . . 513
8.4.5 remote ip rip filter act . . . 515
8.4.6 remote ip rip filter move . . . 517
8.4.7 remote ip rip filter route . . . 518
8.4.8 remote ip rip filter set metric . . . 520
8.4.9 remote ip ospf use . . . 521
8.4.10 remote ip ospf cost . . . 523
8.4.11 remote ip ospf hello . . . 524
8.4.12 remote ip ospf dead . . . 525
8.4.13 remote ip ospf retrans . . . 526
8.4.14 remote ip ospf delay . . . 527
8.4.15 remote ip ospf auth type . . . 528
8.4.16 remote ip ospf auth textkey . . . 529
8.4.17 remote ip ospf auth md5key . . . 530
8.4.18 remote ip ospf passive . . . 531
8.4.19 remote ip ospf multicast . . . 532
8.4.20 remote ip ospf checkmtu . . . 533
8.4.21 remote ip nat mode . . . 534
8.4.22 remote ip nat static . . . 536
8.4.23 remote ip nat static default . . . 538
8.4.24 remote ip nat rule . . . 539
8.4.25 remote ip nat wellknown . . . 541
8.4.26 remote ip nat destination . . . 543
8.4.27 remote ip nat appli . . . 545
8.4.28 remote ip filter . . . 547
8.4.29 remote ip filter move . . . 552
8.4.30 remote ip filter default . . . 553
8.4.31 remote ip tos . . . 554
8.4.32 remote ip tos move . . . 557
8.4.33 remote ip priority . . . 558
8.4.34 remote ip clp . . . 562
8.4.35 remote ip clp move . . . 565
8.4.36 remote ip in-policy . . . 566
8.4.37 remote ip in-policy move . . . 568
8.4.38 remote ip msschange . . . 569
8.4.39 remote ip multicast mode . . . 570
8.4.40 remote ip multicast ttl threshold . . . 571
8.4.41 remote ip multicast pim preference . . . 572
8.4.42 remote ip multicast pim upstream type . . . 573
8.4.43 remote ip dvpn . . . 574
8.4.44 remote ip dvpn move . . . 576
8.4.45 remote ip exp . . . 577
8.4.46 remote ip exp move . . . 580
8.4.47 remote ip ids use . . . 581

8.5 IPv6 関連情報 . . . 582
8.5.1 remote ip6 use . . . 582

8.5.2 remote ip6 ifid 583
8.5.3 remote ip6 address 584
8.5.4 remote ip6 ra mode 586
8.5.5 remote ip6 ra interval 587
8.5.6 remote ip6 ra mtu 588
8.5.7 remote ip6 ra reachabletime 589
8.5.8 remote ip6 ra retranstimer 590
8.5.9 remote ip6 ra curhoplimit 591
8.5.10 remote ip6 ra flags 592
8.5.11 remote ip6 route 593
8.5.12 remote ip6 rip use 595
8.5.13 remote ip6 rip site-local 597
8.5.14 remote ip6 rip aggregate 598
8.5.15 remote ip6 rip filter act 599
8.5.16 remote ip6 rip filter move 601
8.5.17 remote ip6 rip filter route 602
8.5.18 remote ip6 rip filter set metric 603
8.5.19 remote ip6 ospf use 604
8.5.20 remote ip6 ospf cost 606
8.5.21 remote ip6 ospf hello 607
8.5.22 remote ip6 ospf dead 608
8.5.23 remote ip6 ospf retrans 609
8.5.24 remote ip6 ospf delay 610
8.5.25 remote ip6 ospf passive 611
8.5.26 remote ip6 ospf checkmtu 612
8.5.27 remote ip6 filter 613
8.5.28 remote ip6 filter move 618
8.5.29 remote ip6 filter default 619
8.5.30 remote ip6 trafficclass 620
8.5.31 remote ip6 trafficclass move 623
8.5.32 remote ip6 priority 624
8.5.33 remote ip6 in-policy 628
8.5.34 remote ip6 in-policy move 630
8.5.35 remote ip6 dhcp service 631
8.5.36 remote ip6 dhcp duid 632
8.5.37 remote ip6 dhcp client option pd 633
8.5.38 remote ip6 dhcp client option dns 634
8.5.39 remote ip6 dhcp client option domain 635
8.5.40 remote ip6 dhcp client option sipserver address 636
8.5.41 remote ip6 dhcp client option sipserver domain 637
8.5.42 remote ip6 dhcp client option sntpserver 638
8.5.43 remote ip6 dhcp client iaid 639
8.5.44 remote ip6 dhcp client route 640
8.5.45 remote ip6 dhcp relay interface 641
8.5.46 remote ip6 dhcp relay server 642
8.5.47 remote ip6 dhcp relay source 643
8.5.48 remote ip6 dhcp server preference 644
8.5.49 remote ip6 dhcp server info dns 645
8.5.50 remote ip6 dhcp server info domain 646
8.5.51 remote ip6 dhcp server info prefix 647
8.5.52 remote ip6 dhcp server info sipserver address 649
8.5.53 remote ip6 dhcp server info sipserver domain 650
8.5.54 remote ip6 dhcp server info sntpserver 651
8.5.55 remote ip6 dvpn 652
8.5.56 remote ip6 dvpn move 654
8.5.57 remote ip6 exp 655
8.5.58 remote ip6 exp move 657
8.5.59 remote ip6 clp 658
8.5.60 remote ip6 clp move 660

8.6 ブリッジ関連情報 661
8.6.1 remote bridge use. 661
8.6.2 remote bridge group 662
8.6.3 remote bridge static 663
8.6.4 remote bridge stp use. 664
8.6.5 remote bridge stp cost 665
8.6.6 remote bridge stp priority 667
8.6.7 remote bridge filter 668
8.6.8 remote bridge filter move. 671
8.6.9 remote bridge priority 672

8.7 MPLS 関連情報 674
8.7.1 remote mpls use 674
8.7.2 remote mpls distribution 675
8.7.3 remote mpls ldp hello-timers 676
8.7.4 remote mpls ldp keepalive-timers 677
8.7.5 remote mpls ldp advertisement. 678
8.7.6 remote mpls ldp retention. 679
8.7.7 remote mpls ldp interface-label 680
8.7.8 remote mpls ldp ip transport 681
8.7.9 remote mpls ldp multicast-hello 682

8.8 SNMP 関連情報 683
8.8.1 remote snmp trap linkdown. 683
8.8.2 remote snmp trap linkup 684

第 9 章 着信デフォルト情報の設定 685

9.1 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 686
9.1.1 answer accept. 686
9.1.2 answer ppp auth type 687
9.1.3 answer ppp auth receive add 688
9.1.4 answer ppp mp use. 689
9.1.5 answer ppp mp bap use. 690

第 10 章 テンプレート情報の設定 691

10.1 テンプレート共通情報. 692
10.1.1 template name 692
10.1.2 template mtu. 693
10.1.3 template idle 694
10.1.4 template interface pool 695
10.1.5 template aaa. 697
10.1.6 template datalink type 698
10.1.7 template datalink bind 699
10.1.8 template combine use. 700
10.1.9 template tunnel local 701
10.1.10 template sessionwatch address 703
10.1.11 template sessionwatch interval 705

10.2 PPP 関連情報 707
10.2.1 template ppp auth type 707
10.2.2 template ppp compress 708
10.2.3 template ppp ipcp vjcomp. 709
10.2.4 template ppp ipcp iphc 710
10.2.5 template ppp ipv6cp iphc. 711

10.3 IP 関連情報. 712
10.3.1 template ip dns 712
10.3.2 template ip address remote-pool 714
10.3.3 template ip nat mode. 715
10.3.4 template ip nat static 717
10.3.5 template ip nat static default 719
10.3.6 template ip nat rule. 720

10.3.7 template ip nat wellknown . . . 722
10.3.8 template ip nat destination . . . 724
10.3.9 template ip nat appli . . . 726
10.3.10 template ip filter . . . 728
10.3.11 template ip filter move . . . 733
10.3.12 template ip filter default . . . 734
10.3.13 template ip tos . . . 735
10.3.14 template ip tos move . . . 738
10.3.15 template ip priority . . . 739
10.3.16 template ip msschange . . . 743
10.3.17 template ip ids use . . . 744
10.3.18 template ip in-policy . . . 745
10.3.19 template ip in-policy move . . . 747

10.4 IPv6 関連情報 . . . 748
10.4.1 template ip6 use . . . 748
10.4.2 template ip6 ifid . . . 749
10.4.3 template ip6 filter . . . 750
10.4.4 template ip6 filter move . . . 755
10.4.5 template ip6 filter default . . . 756
10.4.6 template ip6 trafficclass . . . 757
10.4.7 template ip6 trafficclass move . . . 760
10.4.8 template ip6 priority . . . 761
10.4.9 template ip6 in-policy . . . 765
10.4.10 template ip6 in-policy move . . . 767

10.5 動的 VPN 関連情報 . . . 768
10.5.1 template dvpn client . . . 768
10.5.2 template dvpn server address . . . 769
10.5.3 template dvpn server auth . . . 771
10.5.4 template dvpn expire register . . . 772
10.5.5 template dvpn expire session . . . 773
10.5.6 template dvpn ua . . . 774
10.5.7 template dvpn domain . . . 776
10.5.8 template dvpn localnet . . . 777
10.5.9 template dvpn localid . . . 779
10.5.10 template dvpn interface . . . 780
10.5.11 template dvpn global . . . 782

10.6 IPsec 関連情報 . . . 783
10.6.1 template ipsec ike protocol . . . 783
10.6.2 template ipsec ike encrypt . . . 784
10.6.3 template ipsec ike auth . . . 785
10.6.4 template ipsec ike pfs . . . 786
10.6.5 template ipsec ike lifetime . . . 787
10.6.6 template ipsec ike lifebyte . . . 788
10.6.7 template ipsec ike newsa initiator . . . 789
10.6.8 template ipsec ike newsa responder . . . 790

10.7 IKE 関連情報 . . . 791
10.7.1 template ike shared key . . . 791
10.7.2 template ike proposal move . . . 793
10.7.3 template ike proposal auth-method . . . 794
10.7.4 template ike proposal encrypt . . . 795
10.7.5 template ike proposal hash . . . 796
10.7.6 template ike proposal pfs . . . 797
10.7.7 template ike proposal lifetime . . . 798
10.7.8 template ike retry . . . 799
10.7.9 template ike idtype . . . 800
10.7.10 template ike name local . . . 801
10.7.11 template ike release . . . 802
10.7.12 template ike mode . . . 803

10.7.13 template ike nat-traversal use 804
10.7.14 template ike certificate local 806
10.7.15 template ike certificate key 807
10.7.16 template ike certificate expired 808
10.7.17 template ike certificate send 809
10.7.18 template ike certificate request 810
10.7.19 template ike dpd use 811
10.7.20 template ike dpd idle 812
10.7.21 template ike dpd retry 813

10.8 SNMP 関連情報 814
10.8.1 template snmp trap linkdown 814
10.8.2 template snmp trap linkup 815

第 11 章 IP 関連情報 816

11.1 IP 関連情報 817
11.1.1 ip nat table 817

第 12 章 動的 VPN 情報の設定 818

12.1 動的 VPN サーバ情報 819
12.1.1 dvpn server use 819
12.1.2 dvpn server domain 820
12.1.3 dvpn server auth use 821
12.1.4 dvpn server auth aaa 822

12.2 動的 VPN クライアント情報 823
12.2.1 dvpn client encode 823
12.2.2 dvpn client server address 824
12.2.3 dvpn client server auth 826
12.2.4 dvpn client expire register 827
12.2.5 dvpn client expire session 828
12.2.6 dvpn client ua 829
12.2.7 dvpn client domain 831
12.2.8 dvpn client localnet 832
12.2.9 dvpn client localid 834
12.2.10 dvpn client interface 835
12.2.11 dvpn client global 836
12.2.12 dvpn client priority 837
12.2.13 dvpn client ip route distance 838
12.2.14 dvpn client ip6 route distance 839

第 13 章 ルーティングプロトコル情報の設定 840

13.1 ルーティングマネージャ情報 841
13.1.1 routemanage ip distance 841
13.1.2 routemanage ip redist rip 843
13.1.3 routemanage ip redist bgp 845
13.1.4 routemanage ip redist ospf 847
13.1.5 routemanage ip ecmp mode 849
13.1.6 routemanage ip ecmp ospf 850
13.1.7 routemanage ip redist ldp 851
13.1.8 routemanage interface floating 852
13.1.9 routemanage ip6 distance 854
13.1.10 routemanage ip6 redist rip 856
13.1.11 routemanage ip6 redist bgp 858
13.1.12 routemanage ip6 redist ospf 859

13.2 RIP 情報 861
13.2.1 rip ip timers basic 861
13.2.2 rip ip timers jitter 862
13.2.3 rip ip multipath 863
13.2.4 rip ip redist 864
13.2.5 rip ip redist move 866

13.2.6 rip ip neighbor 867
13.2.7 rip ip gwfilter 868
13.2.8 rip ip gwfilter move 869
13.2.9 rip ip6 timers basic 870
13.2.10 rip ip6 multipath 871
13.2.11 rip ip6 redist 872
13.2.12 rip ip6 redist move 874

13.3 BGP 情報 875
13.3.1 bgp as 875
13.3.2 bgp id 876
13.3.3 bgp ip vrf rd 877
13.3.4 bgp ip mpls-resolution 878
13.3.5 bgp ip full-route 879
13.3.6 bgp ip network route 880
13.3.7 bgp ip network igp 881
13.3.8 bgp ip aggregate 882
13.3.9 bgp ip redist 883
13.3.10 bgp ip redist move 885
13.3.11 bgp ip6 network route 886
13.3.12 bgp ip6 network igp 887
13.3.13 bgp ip6 aggregate 888
13.3.14 bgp ip6 redist 889
13.3.15 bgp ip6 redist move 891

13.4 BGP 相手側情報 892
13.4.1 bgp neighbor address 892
13.4.2 bgp neighbor as 894
13.4.3 bgp neighbor timers 895
13.4.4 bgp neighbor ebgp-multihop 896
13.4.5 bgp neighbor enforce-multihop 897
13.4.6 bgp neighbor family 898
13.4.7 bgp neighbor source 899
13.4.8 bgp neighbor authentication 900
13.4.9 bgp neighbor graceful-restart family 901
13.4.10 bgp neighbor graceful-restart stale-timer 902
13.4.11 bgp neighbor ip medmetric 903
13.4.12 bgp neighbor ip asprepend 904
13.4.13 bgp neighbor ip localpref 905
13.4.14 bgp neighbor ip nexthopself 906
13.4.15 bgp neighbor ip default-originate 907
13.4.16 bgp neighbor ip filter act 908
13.4.17 bgp neighbor ip filter move 910
13.4.18 bgp neighbor ip filter as 911
13.4.19 bgp neighbor ip filter route 913
13.4.20 bgp neighbor ip filter set medmetric 915
13.4.21 bgp neighbor ip filter set asprepend 917
13.4.22 bgp neighbor ip filter set localpref 919
13.4.23 bgp neighbor ip6 medmetric 921
13.4.24 bgp neighbor ip6 asprepend 922
13.4.25 bgp neighbor ip6 localpref 923
13.4.26 bgp neighbor ip6 nexthopself 924
13.4.27 bgp neighbor ip6 default-originate 925
13.4.28 bgp neighbor ip6 filter act 926
13.4.29 bgp neighbor ip6 filter move 928
13.4.30 bgp neighbor ip6 filter as 929
13.4.31 bgp neighbor ip6 filter route 930
13.4.32 bgp neighbor ip6 filter set medmetric 932
13.4.33 bgp neighbor ip6 filter set asprepend 934
13.4.34 bgp neighbor ip6 filter set localpref 936

13.5 OSPF 情報 938

13.5.1 ospf ip id 938
13.5.2 ospf ip6 id 939
13.6 OSPF エリア情報 940
13.6.1 ospf ip area id 940
13.6.2 ospf ip area type 941
13.6.3 ospf ip area defcost 942
13.6.4 ospf ip area range 943
13.6.5 ospf ip area type3-lsa 945
13.6.6 ospf ip area type3-lsa move 947
13.6.7 ospf ip6 area id 948
13.6.8 ospf ip6 area type 949
13.6.9 ospf ip6 area defcost 950
13.6.10 ospf ip6 area range 951
13.6.11 ospf ip6 area inter-area-prefix 953
13.6.12 ospf ip6 area inter-area-prefix move 955
13.7 OSPF バーチャルリンク情報 956
13.7.1 ospf ip area vlink id 956
13.7.2 ospf ip area vlink hello 957
13.7.3 ospf ip area vlink dead 958
13.7.4 ospf ip area vlink retrans 959
13.7.5 ospf ip area vlink delay 960
13.7.6 ospf ip area vlink auth type 961
13.7.7 ospf ip area vlink auth textkey 962
13.7.8 ospf ip area vlink auth md5key 964
13.8 ASBR 情報 966
13.8.1 ospf ip definfo 966
13.8.2 ospf ip summary 968
13.8.3 ospf ip redist 969
13.8.4 ospf ip redist move 971
13.8.5 ospf ip6 definfo 972
13.8.6 ospf ip6 redist 974
13.8.7 ospf ip6 redist move 976

第 14 章 ブリッジ情報の設定 977

14.1 ブリッジ情報 978
14.1.1 bridge age 978
14.1.2 bridge stp priority 979
14.1.3 bridge stp age 980
14.1.4 bridge stp hello 981
14.1.5 bridge stp delay 982
14.1.6 bridge ip routing 983
14.1.7 bridge ip policy 984
14.1.8 bridge ip6 routing 985
14.1.9 bridge ip6 policy 986
14.1.10 bridge vlan tag transmit 987
14.1.11 bridge inter-remote 988
14.1.12 bridge control 989

第 15 章 LLDP 情報の設定 990

15.1 LLDP 情報 991
15.1.1 lldp send interval 991
15.1.2 lldp send hold 992
15.1.3 lldp reinit delay 993
15.1.4 lldp notification interval 994

第 16 章 IEEE802.1X 情報の設定 995

16.1 IEEE802.1X 情報 996
16.1.1 dot1x use 996
16.1.2 dot1x mode 997

第 17 章　MPLS 情報の設定 998
17.1　LDP 情報 999
17.1.1　mpls ldp router-id 999
17.1.2　mpls ldp control 1000
17.1.3　mpls ldp ip transport 1001
17.1.4　mpls ip propagate-ttl 1002
第 18 章　マルチキャスト情報の設定 1003
18.1　マルチキャスト情報 1004
18.1.1　multicast ip igmp report 1004
18.1.2　multicast ip pimsm candrp mode 1005
18.1.3　multicast ip pimsm candrp address 1006
18.1.4　multicast ip pimsm candrp priority 1007
18.1.5　multicast ip pimsm candbsr mode 1008
18.1.6　multicast ip pimsm candbsr address 1009
18.1.7　multicast ip pimsm candbsr priority 1010
18.1.8　multicast ip pimsm staticrp address 1011
18.1.9　multicast ip pimsm spt mode 1012
18.1.10　multicast ip pimsm spt rate 1013
18.1.11　multicast ip pimsm register checksum 1014
18.1.12　multicast ip route static 1015
第 19 章　UPnP 情報の設定 1017
19.1　UPnP 情報 1018
19.1.1　upnp use 1018
19.1.2　upnp portmapping lease 1020
第 20 章　ACL 情報の設定 1021
20.1　ACL 情報 1022
20.1.1　acl mac 1022
20.1.2　acl ip 1024
20.1.3　acl ip6 1026
20.1.4　acl tcp 1028
20.1.5　acl udp 1030
20.1.6　acl icmp 1031
20.1.7　acl description 1033
第 21 章　ポリシーグループ定義情報の設定 1034
21.1　ポリシーグループ定義情報 1035
21.1.1　policy-group pattern 1035
21.1.2　policy-group pattern move 1037
21.1.3　policy-group interface 1038
21.1.4　policy-group nexthop 1039
21.1.5　policy-group nexthop6 1040
21.1.6　policy-group sessionwatch address 1041
21.1.7　policy-group sessionwatch interval 1043
21.1.8　policy-group sessionwatch ttl 1045
21.1.9　policy-group sessionwatch recovery 1046
21.1.10　policy-group sessionwatch error-wait 1047
第 22 章　AAA 情報の設定 1048
22.1　グループ ID 情報 1049
22.1.1　aaa name 1049
22.2　AAA ユーザ情報 1050
22.2.1　aaa user id 1050
22.2.2　aaa user password 1051
22.2.3　aaa user called number 1053
22.2.4　aaa user ip address local 1054
22.2.5　aaa user ip address remote 1055

22.2.6 aaa user ip route . . . 1056
22.2.7 aaa user ip6 ifid . . . 1058
22.2.8 aaa user ip6 route . . . 1059
22.2.9 aaa user sessionwatch . . . 1061
22.2.10 aaa user ipsec ike range . . . 1062
22.2.11 aaa user ipsec extension-range . . . 1064
22.2.12 aaa user ike shared key . . . 1066
22.2.13 aaa user supplicant vid . . . 1068
22.2.14 aaa user supplicant mac . . . 1069
22.2.15 aaa user user-role . . . 1070

22.3 RADIUS 情報 . . . 1071
22.3.1 aaa radius service . . . 1071
22.3.2 aaa radius auth source . . . 1073
22.3.3 aaa radius auth message-authenticator . . . 1074
22.3.4 aaa radius accounting source . . . 1075
22.3.5 aaa radius server client-info secret . . . 1076
22.3.6 aaa radius server client-info address . . . 1077
22.3.7 aaa radius client server-info auth secret . . . 1078
22.3.8 aaa radius client server-info auth address . . . 1079
22.3.9 aaa radius client server-info auth port . . . 1080
22.3.10 aaa radius client server-info auth deadtime . . . 1081
22.3.11 aaa radius client server-info auth priority . . . 1082
22.3.12 aaa radius client server-info auth source . . . 1083
22.3.13 aaa radius client server-info accounting secret . . . 1084
22.3.14 aaa radius client server-info accounting address . . . 1085
22.3.15 aaa radius client server-info accounting port . . . 1086
22.3.16 aaa radius client server-info accounting deadtime . . . 1087
22.3.17 aaa radius client server-info accounting priority . . . 1088
22.3.18 aaa radius client server-info accounting source . . . 1089
22.3.19 aaa radius client retry . . . 1090
22.3.20 aaa radius client nas-identifier . . . 1091

第 23 章 無線 LAN 管理機能の設定 . . . 1092

23.1 無線 LAN 管理機器情報 . . . 1093
23.1.1 nodemanager group name . . . 1093
23.1.2 nodemanager node name . . . 1094
23.1.3 nodemanager node group . . . 1095
23.1.4 nodemanager node address . . . 1096
23.1.5 nodemanager node user . . . 1097
23.1.6 nodemanager node wlan scan . . . 1098
23.1.7 nodemanager node wlan sta . . . 1099
23.1.8 nodemanager node wlan neighbor . . . 1100

23.2 MAC アドレスフィルタ情報 . . . 1101
23.2.1 nodemanager wlan filterset description . . . 1101
23.2.2 nodemanager wlan filterset filter mac . . . 1102
23.2.3 nodemanager wlan filterset filter description . . . 1103

23.3 電波出力自動調整情報 . . . 1104
23.3.1 nodemanager wlan autotxpower rssi . . . 1104

23.4 チャネル自動調整情報 . . . 1105
23.4.1 nodemanager wlan autochannel channel . . . 1105
23.4.2 nodemanager wlan autochannel layout . . . 1106
23.4.3 nodemanager wlan autochannel rssi . . . 1107
23.4.4 nodemanager wlan autochannel bandwidth . . . 1108

23.5 アクセスポイント情報取得情報 . . . 1109
23.5.1 nodemanager collect interval . . . 1109

23.6 管理外無線 LAN アクセスポイント情報 . . . 1110
23.6.1 nodemanager wlan scan unmanaged . . . 1110

23.7 稼動監視パラメタ情報 1111
23.7.1 nodemanager icmpwatch interval 1111
23.7.2 nodemanager icmpwatch threshold 1112
23.8 スキャンレポート取得パラメタ情報 1113
23.8.1 nodemanager wlan scan interval 1113
23.8.2 nodemanager wlan scan error threshold 1115
23.9 監視ログ・パラメタ情報 1116
23.9.1 nodemanager log 1116
23.9.2 nodemanager wlan sta rssi 1117
第 24 章 メモリ予兆監視情報の設定 1118
24.1 メモリ予兆監視情報 1119
24.1.1 sysmemwatch mode 1119
24.1.2 sysmemwatch threshold 1120
24.1.3 sysmemwatch interval 1121
第 25 章 装置情報の設定 1122
25.1 SNMP 情報 1123
25.1.1 snmp service 1123
25.1.2 snmp agent contact 1124
25.1.3 snmp agent sysname 1125
25.1.4 snmp agent location 1126
25.1.5 snmp agent address 1127
25.1.6 snmp agent engineid 1128
25.1.7 snmp manager 1129
25.1.8 snmp trap coldstart 1131
25.1.9 snmp trap linkdown 1132
25.1.10 snmp trap linkup 1133
25.1.11 snmp trap authfail 1134
25.1.12 snmp trap newroot 1135
25.1.13 snmp trap topologychange 1136
25.1.14 snmp trap vrrpnewmaster 1137
25.1.15 snmp trap vrrpauthfail 1138
25.1.16 snmp trap vrrpprotoerror 1139
25.1.17 snmp trap noserror 1140
25.1.18 snmp trap lldpremtableschange 1141
25.1.19 snmp user name 1142
25.1.20 snmp user address 1143
25.1.21 snmp user notification 1144
25.1.22 snmp user auth 1145
25.1.23 snmp user priv 1146
25.1.24 snmp user write 1147
25.1.25 snmp user read 1148
25.1.26 snmp user notify 1149
25.1.27 snmp view subtree 1150
25.2 システムログ情報 1152
25.2.1 syslog server address 1152
25.2.2 syslog server pri 1153
25.2.3 syslog pri 1154
25.2.4 syslog facility 1155
25.2.5 syslog security 1156
25.2.6 syslog dupcut 1157
25.2.7 syslog command-logging 1158
25.2.8 syslog event dot1x 1159
25.2.9 syslog event arpauth 1160
25.2.10 syslog header 1161
25.2.11 syslog source address 1162
25.3 自動時刻設定情報 1163

25.3.1 time auto server . . . 1163
25.3.2 time auto interval . . . 1164
25.3.3 time zone . . . 1165

25.4 ProxyDNS 情報 . . . 1166
25.4.1 proxydns domain . . . 1166
25.4.2 proxydns domain move . . . 1170
25.4.3 proxydns address . . . 1171
25.4.4 proxydns address move . . . 1174
25.4.5 proxydns unicode . . . 1175
25.4.6 proxydns multi-server . . . 1176

25.5 ホストデータベース情報 . . . 1177
25.5.1 host name . . . 1177
25.5.2 host ip address . . . 1178
25.5.3 host ip6 address . . . 1179
25.5.4 host mac . . . 1180
25.5.5 host duid . . . 1181
25.5.6 host rpon . . . 1182

25.6 スケジュール情報 . . . 1183
25.6.1 schedule at . . . 1183
25.6.2 schedule in . . . 1185
25.6.3 schedule syslog . . . 1187

25.7 外部メディアスタート機能の情報 . . . 1188
25.7.1 storage setup mode . . . 1188
25.7.2 storage setup machine . . . 1189

25.8 電話番号変更予約情報 . . . 1190
25.8.1 dnconvinfo date . . . 1190
25.8.2 dnconvinfo dial . . . 1192

25.9 ファームウェア更新情報 . . . 1194
25.9.1 updateinfo . . . 1194

25.10 MAC アドレス認証情報 . . . 1196
25.10.1 macauth password . . . 1196
25.10.2 macauth type . . . 1197

25.11 その他 . . . 1198
25.11.1 addact . . . 1198
25.11.2 watchdog service . . . 1200
25.11.3 consoleinfo . . . 1201
25.11.4 telnetinfo . . . 1202
25.11.5 sysdown harderr fan . . . 1203
25.11.6 sysdown harderr thermal . . . 1204
25.11.7 sysdown harderr other . . . 1205
25.11.8 sysdown power . . . 1206
25.11.9 mflag . . . 1207
25.11.10 sysname . . . 1208
25.11.11 loopback ip address . . . 1209
25.11.12 loopback ip ospf use . . . 1210
25.11.13 loopback mpls ldp interface-label . . . 1211
25.11.14 loopback ip6 address . . . 1212
25.11.15 serverinfo ftp . . . 1213
25.11.16 serverinfo ftp ip6 . . . 1214
25.11.17 serverinfo ftp filter . . . 1215
25.11.18 serverinfo ftp filter move . . . 1217
25.11.19 serverinfo ftp filter default . . . 1218
25.11.20 serverinfo sftp . . . 1219
25.11.21 serverinfo sftp ip6 . . . 1220
25.11.22 serverinfo telnet . . . 1221
25.11.23 serverinfo telnet ip6 . . . 1222
25.11.24 serverinfo telnet filter . . . 1223

25.11.25 serverinfo telnet filter move . . . 1225
25.11.26 serverinfo telnet filter default . . . 1226
25.11.27 serverinfo ssh . . . 1227
25.11.28 serverinfo ssh ip6 . . . 1228
25.11.29 serverinfo ssh filter . . . 1229
25.11.30 serverinfo ssh filter move . . . 1231
25.11.31 serverinfo ssh filter default . . . 1232
25.11.32 serverinfo http . . . 1233
25.11.33 serverinfo http ip6 . . . 1234
25.11.34 serverinfo http filter . . . 1235
25.11.35 serverinfo http filter move . . . 1237
25.11.36 serverinfo http filter default . . . 1238
25.11.37 serverinfo dns . . . 1239
25.11.38 serverinfo dns ip6 . . . 1240
25.11.39 serverinfo dns filter . . . 1241
25.11.40 serverinfo dns filter move . . . 1243
25.11.41 serverinfo dns filter default . . . 1244
25.11.42 serverinfo sntp . . . 1245
25.11.43 serverinfo sntp ip6 . . . 1246
25.11.44 serverinfo sntp filter . . . 1247
25.11.45 serverinfo sntp filter move . . . 1249
25.11.46 serverinfo sntp filter default . . . 1250
25.11.47 serverinfo time ip tcp . . . 1251
25.11.48 serverinfo time ip6 tcp . . . 1252
25.11.49 serverinfo time ip udp . . . 1253
25.11.50 serverinfo time ip6 udp . . . 1254
25.11.51 serverinfo time filter . . . 1255
25.11.52 serverinfo time filter move . . . 1257
25.11.53 serverinfo time filter default . . . 1258

25.12 シェーピング情報 . . . 1259
25.12.1 shaping timer . . . 1259

第 26 章 SIP-SIP ゲートウェイ情報 . . . 1260

26.1 SIP-SIP ゲートウェイ情報 . . . 1261
26.1.1 sipgw use . . . 1261

26.2 サービス関連情報 . . . 1262
26.2.1 sipgw service type . . . 1262
26.2.2 sipgw service user name . . . 1263
26.2.3 sipgw service user auth id . . . 1264
26.2.4 sipgw service user auth password . . . 1265
26.2.5 sipgw service callin username . . . 1266

26.3 Registrar 連携関連情報 . . . 1267
26.3.1 sipgw registrar server address . . . 1267
26.3.2 sipgw registrar server port . . . 1268

26.4 Proxy 連携関連情報 . . . 1269
26.4.1 sipgw proxy server address . . . 1269
26.4.2 sipgw proxy server port . . . 1270

26.5 ユーザエージェント関連情報 . . . 1271
26.5.1 sipgw agent address . . . 1271
26.5.2 sipgw agent domain name . . . 1272

第 27 章 証明書関連情報の設定 . . . 1273

27.1 証明書関連情報 . . . 1274
27.1.1 certificate local name . . . 1274
27.1.2 certificate local line . . . 1275
27.1.3 certificate remote name . . . 1276
27.1.4 certificate remote line . . . 1277
27.1.5 certificate ca name . . . 1278

27.1.6 certificate ca line 1279
27.1.7 certificate request line. 1280
27.1.8 certificate private line. 1281

索引 1282

第１章　パスワード情報

1.1 パスワード情報

1.1.1 password format

[機能]

暗号化パスワード文字列形式の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

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 admin aaa

[機能]

管理者の AAA 情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

password admin 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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ときに参照する、AAA のグループ ID を指定します。
本コマンドで指定した、AAA のグループ ID に設定されているユーザ ID とパスワードでログインすると、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。

[未設定時]

AAA 情報を参照しないものとみなされます。

1.1.4 password user set

[機能]

一般ユーザパスワードの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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]

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。

1.1.5 password user aaa

[機能]

一般ユーザの AAA 情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

password user 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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ときに参照する、AAA のグループ ID を指定します。
本コマンドで指定した、AAA のグループ ID に設定されているユーザ ID とパスワードでログインすると、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。

[未設定時]

AAA 情報を参照しないものとみなされます。

1.1.6 password aaa

[機能]

ログインユーザの AAA 情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

1.1.7 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～131	Si-R570 Si-R570B
0～15	Si-R370 Si-R370B Si-R260B
0～1	Si-R240B
0	Si-R220C Si-R220D

2.1 回線共通情報

2.1.1 wan bind

[機能]

利用する物理回線の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D

[入力形式]

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

[オプション]

<number>

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

<slot>

利用する回線のボードが、どのスロットに挿入されているかを指定します。
Si-R260B Si-R220C Si-R220D では、必ず"mb"(基本ボード)を指定してください。

・ mb
利用する回線が、基本ボード上にある場合に指定します。

・ スロット番号
ボードが挿入されているスロットの番号を、10 進数で指定します。

範囲	機種
0～3	Si-R570 Si-R570B
0～1	Si-R370 Si-R370B Si-R240B

<line>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

・ ATM 以外
一番小さい番号の wan 定義のみ有効

・ ATM
定義可能 VPC 数まで有効

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

[未設定時]

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

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

扱いは装置により以下のようになります。

・ Si-R220C Si-R220D Si-R260B 以外
  WAN 定義は無効とみなされます。
・ Si-R260B
  wan 定義番号 0 の WAN 定義は
  wan 0 bind mb 0
  と同じ扱いになり、有効になります。それ以外の WAN 定義は無効になります。
・ Si-R220C Si-R220D
  WAN 定義は有効とみなされます。

2.1.2 wan line

[機能]

回線インタフェースおよび通信速度の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D

[入力形式]

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

[オプション]

<number>

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

<speed>

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

インタフェース	回線速度(指定範囲)	Si-R570 Si-R570B Si-R370 Si-R370B	Si-R220C Si-R220D
BRI	64k, 128k	○	○
PRI	192k, 256k, 384k, 512k, 768k, 1m, 1.5m	○	-

[動作モード]

構成定義モード(管理者クラス)

[説明]

wan 定義で利用する回線の、回線種別を設定します。

回線種別	Si-R570B Si-R370B	Si-R570 Si-R370	Si-R260B	Si-R220C Si-R220D	Si-R240B
ISDN	○	○	-	○	-
専用線(64Kbps～128Kbps) (192Kbps～1.5Mbps)	○ ○	○ ○	- -	○ -	- -
フレームリレー(64Kbps～128Kbps) (192Kbps～1.5Mbps)	○ ○	○ ○	- -	○ -	- -
ATM	-	○	○	-	-
データ通信カード	-	-	-	-	○

以下を指定した場合、wan 定義は無効となります。

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

[未設定時]

wan 定義を使用しないものとみなされます。

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

2.2 ISDN 回線情報

2.2.1 wan isdn global

[機能]

グローバル着信の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

wan [<number>] isdn global <mode>

[オプション]

<number>

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

<mode>

グローバル着信を受け付けるかどうかを指定します。

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[未設定時]

グローバル着信を受け付けるものとみなされます。

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

2.2.2 wan isdn number

[機能]

自局電話番号の設定

[適用機種]

Si-R570 | Si-R570B | Si-R370 | Si-R370B | | | Si-R220C | Si-R220D | |

[入力形式]

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

[オプション]

<number>

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

<count>

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

・ 0
着信番号チェックの電話番号 1 を設定します。

・ 1
着信番号チェックの電話番号 2 を設定します。

<tel_number>

着信番号チェックを行う電話番号を指定します。

・ 電話番号
着信時にチェックする電話番号を、0～9 の数字と、*、#、-、(、)、\ の文字で構成される 32 桁以内の ASCII 文字列で指定します。

・ any
着信時に電話番号のチェックを行わない場合に指定します。

・ in1
i・ナンバーサービス契約時に、i・ナンバー情報 1(契約者回線番号)の着信を受け付ける場合に指定します。

・ in2
i・ナンバーサービス契約時に、i・ナンバー情報 2(追加の番号)の着信を受け付ける場合に指定します。

・ in3
i・ナンバーサービス契約時に、i・ナンバー情報 3(追加の番号)の着信を受け付ける場合に指定します。

<subaddress>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

着信番号チェックについて設定します。

ダイヤルイン番号、i・ナンバー、サブアドレスを利用して着信機器を識別するかどうかを、<tel_number>と<subaddress>の組み合わせで指定します。着信番号チェックの電話番号は、2 組まで設定できます。

着信時に網から通知される電話番号とサブアドレスが着信番号チェックの電話番号と一致しない場合は、着信を受け付けません。

<tel_number>に any を指定し、かつ<subaddress>を指定した場合は、<subaddress>だけが着信番号チェックの対象となります。また、<tel_number>に any を指定し、<subaddress>が未指定の場合は、サブアドレス通知がないすべての着信を指定したものとみなされます。

i・ナンバーサービス契約時は、<tel_number>に in1、in2、または in3 のどれかを指定してください。

[注意]

任意のサブアドレス通知を着信するように指定することはできません。

[未設定時]

サブアドレス通知のないすべての着信を指定したものとみなされます。

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

2.2.3 wan isdn numbersend

[機能]

発信者番号通知の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

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

[オプション]

<number>

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

<mode>

発信者番号の通知形態を指定します。

・specified
<tel_number>および<subaddress>で指定する電話番号を、発信者番号として通知します。

・default
網契約に従います。回線の加入契約で選択した内容の設定になります。

・off
接続先に発信者の電話番号を通知しません。

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

<tel_number>

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

・通知電話番号
発信者番号として通知する電話番号を、0～9 の数字と、*、#、-、(、)、\ の文字で構成される 32 桁以内の ASCII 文字列で指定します。

・in1
発信者番号として、i・ナンバー情報 1 を通知します。

・in2
発信者番号として、i・ナンバー情報 2 を通知します。

・in3
発信者番号として、i・ナンバー情報 3 を通知します。

<subaddress>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[注意]

Si-R370 Si-R370B Si-R220C Si-R220D は PIAFS 接続に対応しています。PIAFS(64Kbps)発信時には、<subaddress> で設定したサブアドレスは無視され、相手に通知されません。

[未設定時]

網契約に従うとみなされます。

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

2.2.4 wan isdn limit charge

[機能]

上限課金額による(発呼抑止)条件の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

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

[オプション]

<number>

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

<charge>

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

<diallock>

自動発信を制限するかどうかを指定します。

・ yes
上限課金額に達した場合に、以降の自動発信を制限します。
ただし、回線の手動接続は、制限の対象外となります。

・ no
上限課金額に達した場合に、以降の自動発信を制限しません。

省略時は、yes を指定したものとみなされます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[未設定時]

課金額による自動発信制限を行わないとみなされます。

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

2.2.5 wan isdn limit time

[機能]

上限通信時間による(発呼抑止)条件の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

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

[オプション]

<number>

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

<time>

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

<diallock>

自動発信を制限するかどうかを指定します。

・ yes
接続時間の上限に達した場合に、以降の自動発信を制限します。
ただし、回線の手動接続は、制限の対象外となります。

・ no
接続時間の上限に達した場合に、自動発信を制限しません。

省略時は、yes を指定したものとみなされます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[未設定時]

接続時間による自動発信制限を行わないとみなされます。

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

2.2.6 wan isdn accept

[機能]

装置単位の着信可否の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

wan [<number>] isdn accept <mode>

[オプション]

<number>

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

<mode>

データ着信時の動作について指定します。

・ enable
remote ap called accept の設定に従います。

・ disable
着信を禁止します。着信をすべて拒否し、発信専用の装置となります。

[動作モード]

構成定義モード(管理者クラス)

[説明]

外部から本装置に着信したときの動作について設定します。

[未設定時]

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

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

2.2.7 wan isdn autodial

[機能]

装置単位の自動発信可否の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

wan [<number>] isdn autodial <mode>

[オプション]

<number>

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

<mode>

自動的にダイヤルするかどうかについて指定します。

・enable
remote autodial の設定に従います。

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

通信データが発生したときに、自動的にダイヤルするかどうかを設定します。

[未設定時]

remote autodial の設定に従います。

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

2.2.8 wan isdn activation

[機能]

レイヤ 1 起動種別の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

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

[オプション]

<number>

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

<type>

レイヤ 1 起動種別を指定します。

・ always
常時起動動作を指定します。

・ per-call
呼毎起動動作を指定します。

<time>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[注意]

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

[未設定時]

常時起動動作を指定したものとみなされます。

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

2.3 専用線情報

2.3.1 wan hsd flagdetect

[機能]

専用線のフラグ監視の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

wan [<number>] hsd flagdetect <mode>

[オプション]

<number>

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

<mode>

フラグ監視機能の有無を指定します。

・ disable
フラグ監視機能を利用しません。

・ enable
フラグ監視機能を利用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

専用線接続で、フラグ監視機能を利用するかどうかを指定します。

[注意]

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

[未設定時]

フラグ監視機能を利用しません。

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

2.4 フレームリレー回線情報

2.4.1 wan fr lmi

[機能]

フレームリレーの PVC 状態確認手順の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

wan [<number>] fr lmi <type>

[オプション]

<number>

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

<type>

PVC 状態確認の手順を指定します。

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

フレームリレーでの PVC 状態確認手順を、網契約に合わせて設定します。

[注意]

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

[未設定時]

ITU-T Q.933 Annex A に準拠するとみなされます。

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

2.4.2 wan fr fecn

[機能]

FECN による輻輳制御の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

wan [<number>] fr fecn <mode>

[オプション]

<number>

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

<mode>

FECN によって輻輳制御を行うかどうかを指定します。

・ on
輻輳制御を行います。

・ off
輻輳制御を行いません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

FECN による輻輳制御について設定します。

[未設定時]

FECN によって輻輳制御を行うとみなされます。

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

2.4.3 wan fr becn

[機能]

BECN による輻輳制御の設定

[適用機種]

Si-R570 | Si-R570B | Si-R370 | Si-R370B | | | Si-R220C | Si-R220D | |

[入力形式]

wan [<number>] fr becn <mode>

[オプション]

<number>

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

<mode>

BECN によって輻輳制御を行うかどうかを指定します。

・ on
輻輳制御を行います。

・ off
輻輳制御を行いません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

BECN による輻輳制御について設定します。

[未設定時]

BECN によって輻輳制御を行うとみなされます。

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

2.4.4 wan fr cllm

[機能]

CLLM による輻輳制御の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

wan [<number>] fr cllm <mode>

[オプション]

<number>

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

<mode>

CLLM によって輻輳制御を行うかどうかを指定します。

・ on
輻輳制御を行います。

・ off
輻輳制御を行いません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

CLLM による輻輳制御について設定します。

[未設定時]

CLLM によって輻輳制御を行うとみなされます。

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

2.5 ATM 回線情報

2.5.1 wan atm vpi

[機能]

VPC の VPI 値の設定

[適用機種]

Si-R570 Si-R370 Si-R260B

[入力形式]

wan [<number>] atm vpi <vpi_value>

[オプション]

<number>

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

<vpi_value>

・ VPI 値
使用する VPC の VPI 値を以下の範囲で指定します。

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[未設定時]

0 が設定されたとみなされます。

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

2.5.2 wan atm rate

[機能]

VPC の VP 速度の設定

[適用機種]

Si-R570 Si-R370 Si-R260B

[入力形式]

wan [<number>] atm rate <rate>

[オプション]

<number>

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

<rate>

・ VP 速度
VP 速度を以下の範囲で指定します。

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

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[注意]

ATM 拡張モジュール使用時には以下のことに注意してください。

・ VP 速度設定なしの VPC と VP 速度設定ありの VPC は同時に使用することができません。

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

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

[未設定時]

VP 速度を設定しないものとみなされます。

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

2.5.3 wan atm oam

[機能]

VPC の OAM(F4)による制御の設定

[適用機種]

Si-R570 | Si-R370 | Si-R260B

[入力形式]

wan [<number>] atm oam <mode>

[オプション]

<number>

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

<mode>

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

・off
OAM(F4)の受信を受け付けません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[未設定時]

OAM(F4)の受信を受け付けないとみなされます。

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

2.6 データ通信カード情報

2.6.1 wan cardmodem pin

[機能]

PIN コードの設定

[適用機種]

Si-R240B

[入力形式]

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

[オプション]

<number>

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

<pin>

・ PIN コード
PIN コードを、4～8 文字以内の数字で指定します。
show コマンドで表示される暗号化された PIN コードを encrypted とともに指定することもできます。その場合、表示された文字列をそのまま正確に入力してください。文字列は 8 文字を超えていてもかまいません。

encrypted

・ 暗号化認証パスワード指定
<password>に暗号化された PIN コードを設定する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

PIN コードを設定します。

[注意]

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

[未設定時]

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

第 3 章　ATM 情報の設定

3.1 ATM 情報

3.1.1 atm send clock

[機能]

送信クロックの設定

[適用機種]

Si-R570 Si-R370 Si-R260B

[入力形式]

atm [<slot>] send clock <source>

[オプション]

<slot>

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

範囲	機種
0～3	Si-R570
0～1	Si-R370

<source>

データ送信時に使用するクロックの参照元を指定します。

・self
本装置で生成したクロックを送信クロックとして使用します。

・recovery
受信データから再生したクロックを送信クロックとして使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

データ送信時に使用するクロックの参照元を設定します。

[注意]

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

[未設定時]

本装置で生成したクロックを送信クロックとして使用するものとみなされます。

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

第 4 章　スイッチ情報の設定

・ スイッチ定義番号の指定範囲

本章のコマンドの[オプション] に記載されている<number>(スイッチ定義番号) に指定するスイッチ定義の通し番号(10 進数) 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-R180B

・ ポート番号の指定範囲

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

範囲	機種
1～4	Si-R180B

4.1 スイッチ共通情報

4.1.1 switch use

[機能]

スイッチポート(SW1～SW4)切り替えの設定

[適用機種]

Si-R180B

[入力形式]

switch [<number>] use <mode>

[パラメタ]

<number>

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

<mode>

LAN1 ポートをスイッチポートとして利用するかを指定します。

・on
スイッチポートを使用します。
・off
スイッチ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]

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

[注意]

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

[未設定時]

LAN1 ポートでスイッチポートは利用しないものとみなされます。

```
switch <number> use off
```

4.1.2 switch tag transparent

[機能]

スイッチポート(SW1～SW4)の VLAN tag 透過転送の設定

[適用機種]

Si-R180B

[入力形式]

switch [<number>] tag transparent <mode>

[パラメタ]

<number>

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

<mode>

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

・disable
VLAN tag を透過的に転送しません。

・enable
VLAN tag をすべて透過します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[注意]

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

[未設定時]

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

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

4.1.3 switch age

[機能]

スイッチポート(SW1〜SW4)の学習テーブル生存時間の設定

[適用機種]

Si-R180B

[入力形式]

switch [<number>] age <timer>

[パラメタ]

<number>

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

<timer>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

スイッチのブリッジ学習テーブルの生存時間を設定します。

[未設定時]

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

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

4.2 スイッチポート情報

4.2.1 switch port use

[機能]

スイッチポート(SW1～SW4)利用可否の設定

[適用機種]

Si-R180B

[入力形式]

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

[パラメタ]

<number>

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

<port_no>

・スイッチポート番号
スイッチポートの番号を、10 進数で指定します。

<mode>

スイッチポートの利用有無を指定します。

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[未設定時]

スイッチポートを利用するものとみなされます。

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

4.2.2 switch port mode

[機能]

通信速度の設定

[適用機種]

Si-R180B

[入力形式]

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

[パラメタ]

<number>

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

<port_no>

・スイッチポート番号
スイッチポートの番号を、10 進数で指定します。

<speed>

スイッチポートの通信速度を指定します。

・auto
通信速度を接続先とのネゴシエーションによって自動的に設定されます。

・通信速度
速度固定で動作させる場合に、以下の値のどちらかを設定します。

10
10Mbps 固定で動作します。

100
100Mbps 固定で動作します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

スイッチポート(SW1～SW4)の通信速度の設定を行います。

[未設定時]

スイッチポートを通信速度として自動決定するものとみなされます。

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

4.2.3 switch port duplex

[機能]

全二重/半二重の設定

[適用機種]

Si-R180B

[入力形式]

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

[パラメタ]

<number>

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

<port_no>

・スイッチポート番号
スイッチポートの番号を、10 進数で指定します。

<duplex>

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

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

スイッチポート(SW1～SW4)の全二重／半二重を設定します。

[注意]

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

[未設定時]

スイッチポートが全二重モードに設定されたものとみなされます。

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

4.2.4 switch port mdi

[機能]

MDI 機能の設定

[適用機種]

Si-R180B

[入力形式]

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

[パラメタ]

<number>

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

<port_no>

・スイッチポート番号
スイッチポートの番号を、10 進数で指定します。

<mode>

MDI のモードを指定します。

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

スイッチポート(SW1～SW4)の MDI 機能の設定を行います。

[注意]

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

[未設定時]

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

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

4.2.5 switch port flowctl

[機能]

フロー制御機能の設定

[適用機種]

Si-R180B

[入力形式]

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

[パラメタ]

<number>

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

<port_no>

・スイッチポート番号
スイッチポートの番号を、10 進数で指定します。

<mode>

・on
フロー制御を有効にします。
・off
フロー制御を無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[未設定時]

スイッチポートのフロー制御機能を送受信ともに使用するものとみなされます。

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

4.2.6 switch port vlan tag

[機能]

Tag あり VLAN 登録

[適用機種]

Si-R180B

[入力形式]

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

[オプション]

<number>

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

<port_no>

・スイッチポート番号
スイッチポートの番号を、10 進数で指定します。

<vidlist>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

Tagged VLAN ID の設定を行います。

[注意]

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

[未設定時]

Tagged VLAN ID は存在しないものとみなされます。

4.2.7 switch port vlan untag

[機能]

Tag なし VLAN 登録

[適用機種]

Si-R180B

[入力形式]

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

[オプション]

<number>

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

<port_no>

・ スイッチポート番号
スイッチポートの番号を、10 進数で指定します。

<vidlist>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

Untagged VLAN ID の設定を行います。

[注意]

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

[未設定時]

tag なし VLAN-ID として 1 が指定されたものとみなされます。

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

第 5 章　無線 LAN AP 関連情報の設定

・ wlan 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>(wlan 定義番号) に指定する wlan 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	Si-R240B

5.1 無線 LAN AP 関連情報

5.1.1 wlan bind

[機能]

物理回線の設定

[適用機種]

					Si-R240B			

[入力形式]

wlan [<number>] bind <slot>

[オプション]

<number>

・ wlan 定義番号
wlan 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。

<slot>

利用する無線 LAN カードが、どのスロットに挿入されているかを指定します。

・ スロット番号
無線 LAN カードが挿入されているスロットの番号を、10 進数で指定します。

範囲	機種
0～1	Si-R240B

[動作モード]

構成定義モード(管理者クラス)

[説明]

wlan 定義で利用する物理回線を設定します。
複数の wlan 定義で同一の回線を指定した場合、lan 定義からバインドされている wlan 定義だけが有効となり、ほかの wlan 定義は無効となります。

[注意]

本コマンドで wlan 定義と物理回線を関連付けることと併せ、論理インタフェース(lan 定義)と wlan 定義を関連付けておく必要があります。
たとえば、回線設定である wlan 0 定義と論理インタフェースである lan 2 定義を関連付け、スロット 0 に挿入された無線 LAN カードを利用する場合、以下のような設定が必要になります。

```
# lan 2 bind wlan 0
# wlan 0 bind 0
```

[未設定時]

wlan 定義と物理回線は関連付けされていません。

5.1.2 wlan mode

[機能]

無線通信モードの設定

[適用機種]

					Si-R240B			

[入力形式]

wlan [<number>] mode <mode>

[オプション]

<number>

- 無線 LAN 定義番号
  無線 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。

<mode>

- 11b
  IEEE802.11b で通信を行います。
- 11b/g
  IEEE802.11b または 11g で通信を行います。
- 11g
  IEEE802.11g で通信を行います。
- 11a
  IEEE802.11a で通信を行います。

[動作モード]

構成定義モード(管理者クラス)

[説明]

無線通信モードの IEEE802.11a/b/g を設定します。

[注意]

指定された通信モードに合わないチャネルが指定された場合、通信モードは指定どおりとなり、チャネルは any が指定されたものとして動作します。

[未設定時]

無線通信モードは 11b が指定されたものとみなされます。

```
wlan [<number>] mode 11b
```

5.1.3 wlan channel

[機能]

無線 LAN チャネルの設定

[適用機種]

					Si-R240B			

[入力形式]

wlan [<number>] channel <channel>

[オプション]

<number>

・ 無線 LAN 定義番号
無線 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。

<channel>

・ チャネル番号
使用する無線 LAN チャネル番号を 10 進数で指定します。
11b の場合、1～14 の範囲で指定します。
11b/g,11g の場合、1～13 の範囲で指定します。
11a の場合、36、40、44、48 の中から指定します。

・ any
自動で選択されます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

無線 LAN で使用するチャネルを設定します。

[注意]

11a の W53(52，56，60，64)チャネルはサポートしていません。
wlan channel <channel>に指定したチャネルが、通信モードに対応する設定範囲に一致しない場合、通信モードはそのままに、<channel>に any が選択されたものとして動作します。

[未設定時]

無線 LAN チャネルは any とみなされます。

```
wlan [<number>] channel any
```

5.1.4 wlan ssid

[機能]

SSID の設定

[適用機種]

					Si-R240B			

[入力形式]

wlan [<number>] ssid <ssid>

[オプション]

<number>

・ 無線 LAN 定義番号
無線 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。

<ssid>

・ SSID
無線 LAN アクセスポイントを識別する SSID を、32 文字以内の ASCII 文字列で指定します。
文字列は、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、0x20(空白文字)を使用する場合は、文字列をダブルクォーテーション(")で囲う必要があります。

[動作モード]

構成定義モード(管理者クラス)

[説明]

無線 LAN でのネットワーク識別子である SSID を設定します。
ここで設定した SSID は、アクセスポイントの存在を周囲に広報するビーコンフレームに含まれて送信されます。

[注意]

ビーコンフレームは電波が届く範囲の無線 LAN 端末にアクセスポイントの存在を知らせているため、ユーティリティソフトを使えば第三者でも SSID を知ることができます。第三者が SSID を無断で設定し使用してしまう可能性があるため、必要に応じて SSID 非通知機能やセキュリティ機能を併せて使用することを推奨します。

[未設定時]

SSID は未設定とみなされます。

5.1.5 wlan hide

[機能]

SSID 非通知と ANY 接続拒否の設定

[適用機種]

					Si-R240B			

[入力形式]

wlan [<number>] hide <mode>

[オプション]

<number>

・ 無線 LAN 定義番号
無線 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。

<mode>

・ on
SSID 非通知を有効にすると同時に、ANY 接続を拒否します。
・ off
SSID 非通知を無効にすると同時に、ANY 接続を受け入れます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SSID 非通知を有効にすると、アクセスポイントは SSID を隠蔽したビーコンフレームを送信します。
それと同時に、無線 LAN 端末から SSID を指定しない ANY 接続に対して接続拒否します。

[未設定時]

SSID 非通知と ANY 接続拒否は無効とみなされます。

```
wlan <number> hide off
```

5.1.6 wlan sta limit

[機能]

接続可能台数の設定

[適用機種]

					Si-R240B			

[入力形式]

```
wlan [<number>] sta limit <limit>
```

[オプション]

<number>

・ 無線 LAN 定義番号
無線 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。

<limit>

・ 接続可能台数
アクセスポイントに接続できる無線 LAN 端末台数を 1～10 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]

無線 LAN アクセスポイントに接続できる無線 LAN 端末台数の最大数を設定します。
ここで設定した接続可能台数を超えて無線 LAN 端末からの要求を受けると、アクセスポイントは無線 LAN 端末からのアソシエーション要求を失敗させます。

[未設定時]

接続可能台数は 5 とみなされます。

```
wlan [<number>] sta limit 5
```

5.1.7 wlan txpower

[機能]

無線送信出力の設定

[適用機種]

Si-R240B

[入力形式]

wlan [<number>] txpower <power>

[オプション]

<number>

・ 無線 LAN 定義番号
無線 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。

<power>

無線送信出力を 1～36(0.5dBm 単位)の 10 進数で指定します。

設定値	送信出力	設定値	送信出力
1	0.5 [dBm]	19	9.5 [dBm]
2	1.0 [dBm]	20	10.0 [dBm]
3	1.5 [dBm]	21	10.5 [dBm]
4	2.0 [dBm]	22	11.0 [dBm]
5	2.5 [dBm]	23	11.5 [dBm]
6	3.0 [dBm]	24	12.0 [dBm]
7	3.5 [dBm]	25	12.5 [dBm]
8	4.0 [dBm]	26	13.0 [dBm]
9	4.5 [dBm]	27	13.5 [dBm]
10	5.0 [dBm]	28	14.0 [dBm]
11	5.5 [dBm]	29	14.5 [dBm]
12	6.0 [dBm]	30	15.0 [dBm]
13	6.5 [dBm]	31	15.5 [dBm]
14	7.0 [dBm]	32	16.0 [dBm]
15	7.5 [dBm]	33	16.5 [dBm]
16	8.0 [dBm]	34	17.0 [dBm]
17	8.5 [dBm]	35	17.5 [dBm]
18	9.0 [dBm]	36	18.0 [dBm]

[動作モード]

構成定義モード(管理者クラス)

[説明]

フレーム送信で使用する無線送信出力を設定します。

[注意]

無線通信モードが 11a の場合は、無線 LAN カードの最大送信電力が 17.0[dBm]となり、最大値を上回る値が指定された場合は設定にかかわらず 17.0[dBm]として動作します。

[未設定時]

無線送信出力の設定に 36(18dBm)が設定されたものとみなされます。

```
wlan [<number>] txpower 36
```

5.1.8 wlan protection mode

[機能]

プロテクションモードの設定

[適用機種]

Si-R240B

[入力形式]

wlan [<number>] protection mode <mode>

[オプション]

<number>

・無線 LAN 定義番号
無線 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。

<mode>

・cts
CTS 制御フレームを使用して衝突回避します。
・rtscts
RTS/CTS 制御フレームを使用して衝突回避します。
・off
衝突回避は行いません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

11b/11g 混在環境でのプロテクション(衝突回避)の設定を行います。

[注意]

無線通信モードに 11a または 11b を設定したときは無効となります。

[未設定時]

プロテクションモードに off が設定されたものとみなされます。

```
wlan [<number>] protection mode off
```

5.1.9 wlan rts threshold

[機能]

RTS しきい値の設定

[適用機種]

Si-R240B

[入力形式]

wlan [<number>] rts threshold <length>

[オプション]

<number>

・ 無線 LAN 定義番号
無線 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。

<length>

RTS 制御フレームを送信するしきい値を 1～2346(byte)の 10 進数で指定します。
しきい値には FCS(4byte)が含まれます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RTS 制御フレームを送信するしきい値を設定します。パケット長がしきい値を超える場合、
RTS 制御フレームを送信します。

[未設定時]

RTS しきい値に 2346 が設定されたものとみなされます。

```
wlan [<number>] rts threshold 2346
```

5.1.10 wlan dtim period

[機能]

DTIM 間隔の設定

[適用機種]

					Si-R240B			

[入力形式]

wlan [<number>] dtim period <period>

[オプション]

<number>

・ 無線 LAN 定義番号
無線 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。

<period>

DTIM を付加するビーコンを送信する間隔を 1～15 の 10 進数で指定します。
1 を指定した場合、すべてのビーコンに DTIM を付加します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

DTIM を付加するビーコンを送信する間隔を設定します。

[未設定時]

DTIM 間隔に 1 が設定されたものとみなされます。

```
wlan [<number>] dtim period 1
```

5.1.11 wlan beacon interval

[機能]

ビーコン間隔の設定

[適用機種]

					Si-R240B			

[入力形式]

wlan [<number>] beacon interval <interval>

[オプション]

<number>

・ 無線 LAN 定義番号
無線 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。

<interval>

ビーコンの送出間隔を 20～1000(1.024 ミリ秒単位)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]

ビーコンの送出間隔を設定します。

[未設定時]

ビーコン送出間隔に 100 が設定されたものとみなされます。

```
wlan [<number>] beacon interval 100
```

5.1.12 wlan auth

[機能]

IEEE802.11 認証モードの設定

[適用機種]

					Si-R240B			

[入力形式]

wlan [<number>] auth <auth_algo>

[オプション]

<number>

- 無線 LAN 定義番号
  無線 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。

<auth_algo>

- open
  IEEE802.11 のオープン認証を行います。
- shared
  IEEE802.11 の共通鍵認証を行います。
- wpa
  WPA を使った IEEE802.1X 認証を行います。
- wpa-psk
  WPA を使った事前共有キー(PSK)認証を行います。
- wpa2
  WPA2 を使った IEEE802.1X 認証を行います。
- wpa2-psk
  WPA2 を使った事前共有キー(PSK)認証を行います。
- wpa/wpa2
  WPA または WPA2 を自動判別して IEEE802.1X 認証を行います。
- wpa/wpa2-psk
  WPA または WPA2 を自動判別して事前共有キー(PSK)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]

IEEE802.11 の認証モードを設定します。

<auth_algo>に shared を指定する場合は、WEP キーに関する定義が必須となります。

オープン認証は、チャレンジに対するレスポンスを待たずに認証してしまうため実質的には認証を行わないのと同等となります。

wpa-psk，wpa2-psk，wpa/wpa2-psk を使用するときは、事前共有キー(PSK)設定が必須となります。

wpa，wpa2，wpa/wpa2 を使用するときは、バインドする lan 定義に IEEE802.1X 設定が必須となります。

[未設定時]

IEEE802.11 認証モードの設定は open とみなされます。

```
wlan <number> auth open
```

5.1.13 wlan wep mode

[機能]

WEP 使用の設定

[適用機種]

					Si-R240B			

[入力形式]

wlan [<number>] wep mode <mode>

[オプション]

<number>

・ 無線 LAN 定義番号
無線 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。

<mode>

・ off
WEP を使用しない無線 LAN 端末との通信が可能になります。
・ on
WEP を使用した無線 LAN 端末とだけ通信が可能になります。

[動作モード]

構成定義モード(管理者クラス)

[説明]

無線 LAN 端末に無線ネットワークへの接続にあたって WEP を使用させるかどうかを設定します。

[未設定時]

WEP 使用設定は off とみなされます。

```
wlan <number> wep mode off
```

5.1.14 wlan wep key

[機能]

WEP キーの設定

[適用機種]

Si-R240B

[入力形式]

wlan [<number>] wep key <index> <kind> <wep_key> [encrypted]

[オプション]

<number>

・ 無線 LAN 定義番号
無線 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。

<index>

登録する WEP キーの識別番号を、1～4 の 10 進数で指定します。

<kind>

WEP キー種別を指定します。

・ hex
16 進数キーを使用します。

・ text
文字列キーを使用します。

<wep_key>

WEP キーを指定します。

・ 暗号化されていない WEP キー
<kind>の指定によって入力範囲が異なります。入力範囲を以下に示します。

キー種別 WEP キー長(IV 除く)	hex 16 進数キー	text 文字列キー
WEP 64-bit (40-bit)	10 桁	5 文字
WEP 128-bit(104-bit)	26 桁	13 文字
WEP 152-bit(128-bit)	32 桁	16 文字

指定した WEP キーが入力範囲未満の場合は指定した WEP キー長を超えて近い WEP キー長と判断され、満たない部分は 0x0 でパディングされます。
文字列キーの場合、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、0x20(空白文字)を使用する場合は、文字列をダブルクォーテーション(")で囲う必要があります。

・ 暗号化された WEP キー
暗号化された WEP キーを指定します。
show コマンドで表示される暗号化された WEP キーを 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 WEP キー指定
<wep_key>に暗号化された WEP キー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]

WEP 暗号に用いる WEP キーを指定します。

[未設定時]

WEP キーは設定されていないものとみなされます。

5.1.15 wlan wep send

[機能]

使用 WEP キーの設定

[適用機種]

					Si-R240B			

[入力形式]

wlan [<number>] wep send <index>

[オプション]

<number>

・ 無線 LAN 定義番号
無線 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。

<index>

登録した WEP キーの中から実際に使用する WEP キーの識別番号を、1～4 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]

実際に WEP 暗号で使用する WEP キーを選択します。

[注意]

WEP を使用する場合は、指定した認識番号の WEP キー設定が必須となります。

[未設定時]

使用 WEP キーの識別番号に 1 が設定されているものとみなされます。

```
wlan [<number>] wep send 1
```

5.1.16 wlan wpa cipher

[機能]

WPA/WPA2 暗号化モードの設定

[適用機種]

					Si-R240B			

[入力形式]

wlan [<number>] wpa cipher <cipher>

[オプション]

<number>

・無線 LAN 定義番号
無線 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。

<cipher>

・tkip
TKIP 暗号を行います。

・aes
AES(CCMP)暗号を行います。

・auto
TKIP または AES で自動判別し暗号を行います。

[動作モード]

構成定義モード(管理者クラス)

[説明]

WPA/WPA2 で使用する暗号化モードを設定します。
ここで設定した暗号化モードは、wlan auth <auth_algo>に WPA/WPA2 に関する設定がなされているときに意味を持ちます。

[未設定時]

WPA/WPA2 暗号化モードの設定は auto とみなされます。

```
wlan <number> cipher auto
```

5.1.17 wlan wpa psk

[機能]

WPA/WPA2 事前共有キーの設定

[適用機種]

Si-R240B

[入力形式]

wlan [<number>] wpa psk <kind> <key> [encrypted]

[オプション]

<number>

・ 無線 LAN 定義番号
無線 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。

<kind>

キー種別を指定します。

・ hex
16 進数キーを使用します。

・ text
文字列キー(パスフレーズ)を使用します。

<key>

事前共有キー(PSK)を指定します。

・ 暗号化されていない PSK
<kind>の指定によって入力範囲が異なります。入力範囲を以下に示します。

キー種別	hex 16 進数キー	text 文字列キー
事前共有キー	64 桁	8～63 文字

文字列キーの場合、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、0x20(空白文字)を使用する場合は、文字列をダブルクォーテーション(")で囲う必要があります。
16 進数キーの場合、指定したキーの桁数が 64 桁に満たない部分は 0x0 でパディングされます。

・ 暗号化された PSK
暗号化された PSK を指定します。
show コマンドで表示される暗号化された PSK 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 PSK 指定
<psk>に暗号化された PSK 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]

WPA-PSK/WPA2-PSK で用いる事前共有キーを指定します。

[未設定時]

PSK は設定されていないものとみなされます。

5.1.18 wlan wpa rekey

[機能]

WPA/WPA2 のキー更新間隔の設定

[適用機種]

					Si-R240B			

[入力形式]

wlan [<number>] wpa rekey group <period>

[オプション]

<number>

・ 無線 LAN 定義番号
無線 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。

group <period>

グループキー(GTK)の更新間隔を指定します。
更新間隔を 600s(10 分)～86400s(1 日)の範囲で指定します。
単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

WPA/WPA2 で使用するグループキー(GTK)の更新間隔を設定します。

[未設定時]

WPA/WPA2 グループキー更新間隔の設定は 10m とみなされます。

```
wlan <number> rekey group 10m
```

5.1.19 wlan wpa countermeasures

[機能]

MIC エラー検出の設定

[適用機種]

					Si-R240B			

[入力形式]

wlan [<number>] wpa countermeasures <mode>

[オプション]

<number>

・無線 LAN 定義番号
無線 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。

<mode>

・on
MIC エラー検出を有効にします。
・off
MIC エラー検出を無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

TKIP 暗号を使用する際、パケットの改ざんを防ぐために MIC エラーを検出するかどうかを選択します。

[注意]

本機能を有効にした場合、60 秒に 2 回以上の MIC エラーを検出した際に、すべての STA(無線 LAN 端末)を切断します。
さらに、無線 LAN の動作が保留状態となり、一定時間(60 秒)の間、端末接続が行えない状態となります。
保留状態が解除されたあとは、STA(無線 LAN 端末)が接続できる状態に戻ります。

[未設定時]

MIC エラー検出は無効とみなされます。

```
wlan <number> wpa countermeasures off
```

5.1.20 wlan filter

[機能]

無線 LAN MAC フィルタの設定

[適用機種]

					Si-R240B			

[入力形式]

wlan [<number>] filter <count> <action> acl <acl_count>

[オプション]

<number>

・ 無線 LAN 定義番号
無線 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。

<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
0～29	Si-R240B

<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。
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。
無線 LAN MAC フィルタでは、ACL の以下の定義を使用します。

- mac
送信元 MAC アドレスのみを使用します。
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
0～299	Si-R240B

[動作モード]

構成定義モード(管理者クラス)

[説明]

無線 LAN インタフェースでの MAC フィルタを設定します。

指定した ACL の送信元 MAC アドレスと一致した無線 LAN 端末の接続を、指定した<action>に従って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。

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。

MAC フィルタで遮断されたフレーム数は、show wlan statistics コマンドで表示される統計情報の is_rx_acl で参照することができます。

最大定義数	機種
900	Si-R240B

[未設定時]

無線 LAN インタフェースでの MAC フィルタは無効とみなされます。

5.1.21 wlan filter move

[機能]

無線 LAN MAC フィルタの優先順序の変更

[適用機種]

Si-R240B

[入力形式]

wlan [<number>] filter move <count> <new_count>

[オプション]

<number>

・ 無線 LAN 定義番号
無線 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。

<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
0～29	Si-R240B

[動作モード]

構成定義モード(管理者クラス)

[説明]

無線 LAN MAC フィルタの優先順序を変更します。

第 6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～9	Si-R180B

6.1 lan 共通情報

6.1.1 lan bind

[機能]

利用する物理回線の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

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

[オプション]

<number>

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

<slot>

利用する回線のボードが、どのスロットに挿入されているかを指定します。
Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B では、必ず"mb"(基本ボード)を指定してください。
Si-R180B では TAG 透過モードで使用する場合は"switch"(スイッチポート(SW1～SW4))を指定し、[<line>]には使用するスイッチ情報設定の<number>を指定してください。
Si-R240B では無線 LAN を利用する場合に"wlan"を指定し、[<line>]には使用する無線 LAN 回線定義(wlan)の<number>を指定してください。

・ mb
利用する回線が、基本ボード上にある場合に指定します。

・ switch
TAG 透過モードを利用しかつスイッチポートを利用する場合に指定します。

・ wlan
無線 LAN を利用する場合に指定します。

・ スロット番号
ボードが挿入されているスロットの番号を、10 進数で指定します。

範囲	機種
0～3	Si-R570 Si-R570B
0～1	Si-R370 Si-R370B

<line>

・ 回線番号
同一のボードに複数の回線がある場合に、どの回線を利用するか指定します。
Si-R180B では LAN0 ポートを利用する場合は 0、LAN1 ポートを利用する場合は 1 を指定します。
Si-R180B でスイッチポートを利用する場合(<slot>に"switch"を指定した場合)はスイッチ情報定義の<number>を指定します。
Si-R240B では無線 LAN を利用する場合に無線 LAN(wlan)定義の<number>を指定します。
省略時は、0 を指定したものとみなされます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

lan 定義で利用する物理回線を設定します。

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

[注意]

Si-R570 Si-R570B Si-R370 Si-R370B の場合は以下に注意してください。

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

Si-R180B の場合は以下に注意してください。

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

Si-R240B の場合は以下に注意してください。

・ 本コマンドで論理インタフェース(lan 定義)と wlan 定義を関連付けることと併せ、wlan 定義と物理回線を関連付けておく必要があります。

  たとえば、回線設定である wlan 0 定義と論理インタフェースである lan 2 定義を関連付け、スロット 0 に挿入された無線 LAN カードを利用する場合、以下のような設定が必要になります。

  # lan 2 bind wlan 0

  # wlan 0 bind 0

[未設定時]

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

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

6.1.2 lan mode

[機能]

通信速度および通信モードの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

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

[オプション]

<number>

・ lan 定義番号

lan 定義の通し番号を、10 進数で指定します。

省略時は、0 を指定したものとみなされます。

<speed>

通信速度を指定します。

・ auto

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

・ 通信速度

通信速度を固定して動作させる場合に、以下のどれかを指定します。

1000(1Gbps 固定で動作する)の指定は、Si-R570 Si-R570B の基本ボード上の LAN ポートに対してだけ有効です。Si-R570 Si-R570B 以外では指定できません。

10

10Mbps 固定で動作します。

100

100Mbps 固定で動作します。

1000

1Gbps 固定で動作します。

<duplex>

・ 全二重/半二重モード

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

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

full

全二重(Full duplex)固定で動作します。

half

半二重(Half duplex)固定で動作します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

Ethernet インタフェースの動作モードを設定します。

[注意]

Si-R180B の LAN1 ポートをスイッチポートとして利用する場合、本コマンドの設定は無効となります。switch port mode コマンド、switch port duplex コマンドで設定してください。

[未設定時]

通信速度および全二重/半二重モードを自動設定するものとみなされます。

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

6.1.3 lan mdi

[機能]

MDI の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] mdi <mode>

[オプション]

<number>

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

<mode>

MDI のモードを指定します。

・ auto
MDI を自動検出します。
Si-R260B Si-R180B では指定できません。
・ mdi
MDI として動作します。
・ mdix
MDI-X として動作します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

MDI のモードを設定します。

[注意]

MDI の自動検出は、lan mode の設定が auto である場合にのみ有効です。
lan mode の設定が auto でない場合は、MDI の自動検出を指定しても、MDI として動作します。
MDI の設定は、基本ボード上の LAN ポートでのみ有効です。
スロットに挿入してあるボード上では動作しません。
Si-R260B の LAN0 ポートに対する本コマンドの設定は無効です。LAN0 ポートは、装置前面の to HUB to PC スイッチでだけ設定を変更することができます。
Si-R180B の LAN1 ポート(スイッチ機能未使用時)に対する本コマンドの設定は無効です。MDI として動作します。
Si-R180B の LAN1 ポートをスイッチポートとして利用する場合、本コマンドの設定は無効となります。switch port mdi コマンドで設定してください。

[未設定時]

(Si-R570 Si-R570B Si-R370 Si-R370B Si-R240B Si-R220C Si-R220D の場合)MDI を自動検出するものとみなされます。

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

(Si-R260B Si-R180B の場合)MDI として動作します。

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

6.1.4 lan flowctl

[機能]

フロー制御機能の設定

[適用機種]

Si-R570 | Si-R570B | Si-R370 | Si-R370B | | Si-R240B | Si-R220C | Si-R220D |

[入力形式]

lan [<number>] flowctl <mode>

[オプション]

<number>

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

<mode>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[未設定時]

フロー制御機能を使用するものとみなされます。

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

6.1.5 lan type

[機能]

使用ポートの設定

[適用機種]

Si-R570 Si-R570B

[入力形式]

lan [<number>] type <type>

[オプション]

<number>

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

<type>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

Si-R570 Si-R570B では、基本ボード上の LAN0/1 ポートと LAN0/1 ファイバポートを排他利用することができます。
本コマンドでは、どちらのポートを利用するかの設定をします。

[未設定時]

ポートを自動選択するものとみなされます。

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

6.1.6 lan mtu

[機能]

送信パケット最大長(MTU 値)の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

6.1.7 lan shaping

[機能]

シェーピング機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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-R570 Si-R570B
1～100000 1k～100000k 1m～100m	上記以外

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[注意]

シェーピングを使用しない場合、帯域制御は有効に動作しません。

[未設定時]

シェーピングを使用しないものとみなされます。

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

6.1.8 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

6.2 LAN ポートバックアップ関連情報

6.2.1 lan backup bind

[機能]

バックアップとして利用する物理回線の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D

[入力形式]

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

[オプション]

<number>

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

<slot>

利用する回線のボードが、どのスロットに挿入されているかを指定します。
Si-R260B Si-R240B Si-R220C Si-R220D では、必ず"mb"(基本ボード)を指定してください。

・ mb
利用する回線が、基本ボード上にある場合に指定します。

・ スロット番号
ボードが挿入されているスロットの番号を、10 進数で指定します。

範囲	機種
0～3	Si-R570 Si-R570B
0～1	Si-R370 Si-R370B

<line>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[注意]

Si-R570 Si-R570B Si-R370 Si-R370B の場合は以下に注意してください。

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

[未設定時]

LAN ポートバックアップ機能を利用しないものとみなされます。

6.2.2 lan backup mode

[機能]

使用するポートの選択方法の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D

[入力形式]

lan [<number>] backup mode <mode>

[オプション]

<number>

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

<mode>

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

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[未設定時]

master ポートを優先的に使用します。

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

6.3 LAN ポート閉塞関連情報

6.3.1 lan recovery

[機能]

自動復旧モードの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

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

[オプション]

<number>

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

<mode>

・ auto
LAN 障害復旧時に自動復旧します。

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

<startup>

・ up
装置起動時、および動的定義反映時は閉塞していない状態で動作を開始します。

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

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

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

[注意]

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

[未設定時]

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

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

6.4 IP 関連情報

6.4.1 lan ip address

[機能]

IP アドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

6.4.2 lan ip alias

[機能]

セカンダリ IP アドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

6.4.3 lan ip dhcp service

[機能]

DHCP 機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<mode>

DHCP 機能のモードを指定します。

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

<address1>,<address2>

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

1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

[動作モード]

構成定義モード(管理者クラス)

[説明]

LAN インタフェースに対して、DHCP 機能情報を設定します。

[未設定時]

DHCP サーバ機能を使用しないものとみなされます。

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

6.4.4 lan ip dhcp info

[機能]

DHCP 配布情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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)のどれかを指定します。

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

<gateway>

・デフォルトルータ IP アドレス

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

0.0.0.0 を指定した場合は、設定が削除されます。

指定可能な範囲は以下のとおりです。

1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

<domain>

・ドメイン名

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

<timeserver>

・TIME サーバ IP アドレス

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

0.0.0.0 を指定した場合は、設定が削除されます。

指定可能な範囲は以下のとおりです。

1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

<ntpserver>

・NTP サーバ IP アドレス

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

0.0.0.0 を指定した場合は、設定が削除されます。

指定可能な範囲は以下のとおりです。

1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

<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。

[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。

6.4.5 lan ip dhcp macauth use

[機能]

DHCP MAC アドレスチェック機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<mode>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[未設定時]

MAC アドレスチェックを行わないものとみなされます。

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

6.4.6 lan ip dhcp macauth db

[機能]

DHCP MAC アドレスチェック機能の使用するデータベースの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

6.4.7 lan ip dhcp macauth aaa

[機能]

DHCP MAC アドレスチェック機能で使用する AAA グループの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

6.4.8 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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 PAP が指定されたものとみなされます。

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

6.4.9 lan ip proxyarp

[機能]

ProxyARP 機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

6.4.10 lan ip localproxyarp

[機能]

ローカル ProxyARP 機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<mode>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[注意]

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

[未設定時]

ローカル ProxyARP 機能を使用しないものとみなされます。

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

6.4.11 lan ip route

[機能]

IPv4 スタティック経路情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～1999	Si-R570 Si-R570B
0～1249	Si-R370 Si-R370B
0～255	Si-R260B Si-R240B Si-R220C Si-R220D
0～127	Si-R180B

<address>/<mask>

・ IPv4 アドレス/マスクビット数(またはマスク値)
あて先ネットワークを IPv4 アドレスとマスクビット数の組み合わせで指定します。
マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
- IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
- IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)

・ default
あて先ネットワークとしてデフォルトルートを設定する場合に指定します。
0.0.0.0/0(0.0.0.0/0.0.0.0)を指定するのと同じ意味になります。

<next_hop>

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

・ dhcp
DHCP サーバから受け取った router オプションのゲートウェイアドレスを中継ルータとして使用する場合に指定します。
<number>で指定した lan の定義上に、DHCP クライアントの設定がある場合のみ有効となります。

<metric>

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

<distance>

・ 優先度
このスタティック経路情報の優先度を 10 進数で指定します。
優先度は数値の小さい方がより高い優先度を示します。

<next_hop>に中継ルータ IPv4 アドレスを指定した場合は、0〜254 の範囲となり、省略時は、0 を指定したものとみなされます。

<next_hop>に dhcp を指定した場合は、1〜254 の範囲となり、省略時は、1 を指定したものとみなされます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv4 スタティック経路(静的経路)情報を設定します。

RIP メトリック値は、スタティック経路情報を RIP に再配布するときのメトリック値を設定します。

RIP に再配布したときは、設定した RIP メトリック値+1 のメトリック値で RIP テーブルに登録されます。

優先度は、同じあて先への経路情報が複数ある場合、優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。各ダイナミックルーティングプロトコルの優先度については、routemanage ip distance コマンドを参照してください。

優先度に 0 が設定されているときは、routemanage interface floating コマンドでのフローティング設定に応じてフローティング動作が切り替わります。優先度に 1 以上が設定されているときは、常にフローティング動作します。

フローティング動作する場合、<next_hop>で指定した中継ルータと隣接しているインタフェースが通信可能な状態(リンクアップなど)であれば、スタティック経路情報をルーティングテーブルに追加します。通信不可能な状態(リンクダウンなど)であれば、ルーティングテーブルから削除します。

フローティング動作しない場合は、インタフェースの状態にかかわらず常にスタティック経路情報をルーティングテーブルに追加します。

以下に、各設定値とフローティング動作の関係を示します。

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

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

・ IP ルーティングおよびダイナミックルーティングでの広報で、スタティック経路の出口インタフェースで異常が発生した場合、ルーティングテーブルよりスタティック経路を削除します。

・ あて先が同じ経路をダイナミックルーティングで受信した場合、優先度関係により経路を決定します。

複数のスタティック経路情報で ECMP 機能を使用するときは、あて先、RIP メトリック値、優先度がそれぞれ同じとなるようにスタティック経路情報を設定します。また、ECMP 機能を使用する場合は、routemanage ip ecmp mode コマンドで ECMP を使用するように設定します。

ECMP となるスタティック経路情報は、同じあて先への経路情報ごとに装置全体で 4 個まで定義できます。

DHCP クライアント運用を行う場合で、Router オプションでゲートウェイアドレスが通知された場合、通常はこのゲートウェイアドレス向け優先度 0 のデフォルトルートが自動生成されます。ここで、優先度 0 のデフォルトルートではなく、任意のあて先で任意の優先度のスタティック経路として生成したい場合は、<next_hop>に dhcp と指定する IPv4 スタティック経路を設定することで実現できます。この場合、優先度 0 のデフォルトルートは自動生成されません。

この IPv4 スタティック経路は、DHCP クライアントが DHCP サーバから Router オプションを受け取った時点で有効となります。

ゲートウェイアドレスを受け取れるのは、IPv4 スタティック経路と同じ lan 定義番号で動作する DHCP クライアントからのみです。

IPv4 スタティック経路情報は、本装置全体で以下の数まで定義できます。

最大定義数	機種
2000	Si-R570 Si-R570B

最大定義数	機種
1250	Si-R370 Si-R370B
256	Si-R260B Si-R240B Si-R220C Si-R220D
128	Si-R180B

[注意]

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

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

[未設定時]

IPv4 スタティック経路情報を使用しないものとみなされます。

ただし、DHCP クライアントを有効としたインタフェース上の場合、優先度が 0 で<next_hop>に dhcp が指定された default ルートが設定されたものとみなされます。

6.4.12 lan ip rip use

[機能]

RIP 基本情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<send>

RIP の送信について指定します。

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

<receive>

RIP の受信について指定します。

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

<metric>

・ 加算メトリック値
RIP パケット送信時の加算メトリック値を、0〜16 の 10 進数で指定します。

<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
220	Si-R570 Si-R570B
120	Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
50	Si-R180B

[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 と同時に使用できません。

[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
```

6.4.13 lan ip rip filter act

[機能]

RIP フィルタ動作の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～799	Si-R570 Si-R570B
0～399	Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～199	Si-R180B

<action>

フィルタリング条件に一致した場合の動作を指定します。

・ pass
該当する経路情報を透過します。

・ reject
該当する経路情報を遮断します。

<direction>

フィルタリングを行う方向を指定します。

・ in
受信時にフィルタリングを行います。

・ out
送信時にフィルタリングを行います。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RIP での経路情報送受信時に、フィルタリング条件に一致した経路情報を通過(pass)させるか遮断(reject)させるかを設定します。フィルタリング条件は優先度順に検索し、条件に一致した経路情報があった時点でフィルタリングが行われ、それ以降の条件は参照されません。全条件に不一致の経路情報は遮断されます。

フィルタリング条件は、lan ip rip filter route コマンドを使用し経路情報を設定します。

<count>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。

RIP フィルタは、本装置全体で以下の数まで定義できます。

最大定義数	機種
800	Si-R570 Si-R570B
400	Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
200	Si-R180B

[注意]

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

[未設定時]

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

6.4.14 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～799	Si-R570 Si-R570B
0～399	Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～199	Si-R180B

[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。

6.4.15 lan ip rip filter route

[機能]

RIP フィルタの経路情報設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～799	Si-R570 Si-R570B
0～399	Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～199	Si-R180B

<address>/<mask>

・ IPv4 アドレス/マスクビット数(またはマスク値)
フィルタリング対象とする経路情報を、IPv4 アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
- IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
- IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)

・ any
すべての経路情報をフィルタリング対象とする場合に指定します。

・ default
デフォルトルートをフィルタリング対象とする場合に指定します。
0.0.0.0/0(0.0.0.0/0.0.0.0)を指定するのと同じ意味になります。

<prefix_match>

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

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

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

フィルタリング条件として経路情報を設定します。

[未設定時]

フィルタリング条件が設定されていないものとみなされます。

6.4.16 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～799	Si-R570 Si-R570B
0～399	Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～199	Si-R180B

<metric>

・ メトリック値
メトリック値を、0～16 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 1～16 を設定した場合、メトリック値は設定した値に変更されます。また、この場合、lan ip rip use コマンドで設定した加算メトリック値は加算されません。0 を指定した場合、メトリック値の変更は行われません。

[注意]

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

[未設定時]

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

6.4.17 lan ip ospf use

[機能]

OSPF 利用可否の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<mode>

・ off
OSPF を利用しません。
・ on
OSPF を利用します。

<area_number>

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

範囲	機種
0～9	Si-R570 Si-R570B
0～3	Si-R370 Si-R370B
0～2	Si-R260B Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

最大定義数	機種
100	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
50	Si-R180B

[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
```

6.4.18 lan ip ospf cost

[機能]

OSPF 出力コストの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<cost>

・ 出力コスト
出力コストを、1～65535 で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

OSPF 出力コストを設定します。

[未設定時]

OSPF 出力コストに 10 が設定されているものとみなされます。

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

6.4.19 lan ip ospf hello

[機能]

OSPF Helloパケット送信間隔の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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)のどれかを指定します。
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、ルーティングが行えません。

[未設定時]

Helloパケット送信間隔に10秒が設定されているものとみなされます。

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

6.4.20 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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)のどれかを指定します。
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
```

6.4.21 lan ip ospf retrans

[機能]

OSPF パケット再送間隔の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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)のどれかを指定します。
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
```

6.4.22 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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)のどれかを指定します。
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
```

6.4.23 lan ip ospf priority

[機能]

OSPF 指定ルータ優先度の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

6.4.24 lan ip ospf auth type

[機能]

OSPF パケット認証方式の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

6.4.25 lan ip ospf auth textkey

[機能]

OSPF テキスト認証鍵の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

6.4.26 lan ip ospf auth md5key

[機能]

OSPF MD5 認証鍵情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

6.4.27 lan ip ospf passive

[機能]

OSPF パケット送信抑止の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<interface_type>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

OSPF パケット送信の抑止を設定します。

[未設定時]

OSPF パケットの送信は抑止しないものとみなされます。

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

6.4.28 lan ip vrf use

[機能]

BGP/MPLS VPN 利用可否の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

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

[オプション]

<number>

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

<mode>

・ off
VRF を利用しません。
・ on
VRF を利用します。

<vrf_number>

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

範囲	機種
0～3	Si-R570 Si-R570B Si-R370 Si-R370B
0～1	Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[未設定時]

BGP/MPLS VPN を使用しないものとみなされます。

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

6.4.29 lan ip vrf route

[機能]

BGP/MPLS VPN 用 IPv4 スタティック経路情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

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

[オプション]

<number>

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

<count>

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

範囲	機種
0～255	Si-R570 Si-R570B Si-R370 Si-R370B
0～63	Si-R260B Si-R240B Si-R220C Si-R220D
0～31	Si-R180B

<address>/<mask>

・ IPv4 アドレス/マスクビット数(またはマスク値)
あて先ネットワークを IPv4 アドレスとマスクビット数の組み合わせで指定します。
マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
- IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
- IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)

・ default
あて先ネットワークとしてデフォルトルートを設定する場合に指定します。
0.0.0.0/0(0.0.0.0/0.0.0.0)を指定するのと同じ意味になります。

<next_hop>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

最大定義数	機種
256	Si-R570 Si-R570B Si-R370 Si-R370B
64	Si-R260B Si-R240B Si-R220C Si-R220D
32	Si-R180B

[注意]

メトリック、優先度は設定できません。

[未設定時]

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

6.4.30 lan ip nat mode

[機能]

アドレス変換の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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)のどれかを指定します。
0 秒を指定した場合は、変換テーブル解放のための監視を行いません。
省略時は、5 分を指定したものとみなされます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

LAN インタフェースに対するアドレス変換(NAT)の動作を設定します。

[未設定時]

アドレス変換は使用しないものとみなされます。

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

6.4.31 lan ip nat static

[機能]

静的アドレス変換の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～499	Si-R570 Si-R570B
0～299	Si-R370 Si-R370B
0～199	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

<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
500	Si-R570 Si-R570B
300	Si-R370 Si-R370B
200	Si-R260B Si-R240B Si-R220C Si-R220D
64	Si-R180B

[未設定時]

静的アドレス変換は設定されません。

6.4.32 lan ip nat static default

[機能]

テーブルに一致しないパケットの扱いの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<action>

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

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

・ reject
該当するパケットを破棄します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[未設定時]

すべての NAT テーブルにも一致しないパケットは破棄します。

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

6.4.33 lan ip nat rule

[機能]

アドレス変換ルールの設定

[適用機種]

Si-R570 | Si-R570B | Si-R370 | Si-R370B | Si-R260B | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[入力形式]

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

[オプション]

<number>

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

<count>

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

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

変換ルールの対象となるアプリケーションを指定します。

<server_addr>

・ IP アドレス
NAT に割り当てたグローバルアドレス以外のアドレスを指定します。ここで指定したアドレスを変換ルールの対象とします。

・ any
すべての IP アドレスを変換ルールの対象とします。
any を指定した場合は、グローバル側とプライベート側の両方のアプリケーションサーバに対応します。

・ global
NAT に割り当てたグローバルアドレス以外のすべてのアドレスを変換ルールの対象とします。
global を指定した場合は、グローバル側のアプリケーションサーバに対応します。

・ local
NAT に割り当てたグローバルアドレスを変換ルールの対象とします。
local を指定した場合は、プライベート側のアプリケーションサーバに対応します。

・ off
指定したアプリケーションに対する変換ルールを無効にします。

<server_port>

アプリケーションサーバで待ち受けるポート番号を指定します。

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

6.4.34 lan ip nat wellknown

[機能]

ポート番号変換の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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)
```

6.4.35 lan ip nat destination

[機能]

あて先変換の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～499	Si-R570 Si-R570B
0～299	Si-R370 Si-R370B
0～199	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

<private_addr>

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

<global_addr>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

最大定義数	機種
500	Si-R570 Si-R570B
300	Si-R370 Si-R370B
200	Si-R260B Si-R240B Si-R220C Si-R220D
64	Si-R180B

[未設定時]

あて先変換は設定されません。

6.4.36 lan ip nat appli

[機能]

アプリ対応の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<function>

設定する機能を指定します。

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

<mode>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

各アプリケーションに対する特殊対応を有効にするかどうかを設定します。

[注意]

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

[未設定時]

すべてのアプリ対応を有効にするとみなされます。

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

6.4.37 lan ip filter

[機能]

IP フィルタの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～999	Si-R570 Si-R570B Si-R370 Si-R370B
0～199	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

<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
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

<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
1000	Si-R570 Si-R570B Si-R370 Si-R370B
200	Si-R260B Si-R240B Si-R220C Si-R220D
64	Si-R180B

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

最大定義数	機種
9000	Si-R570 Si-R570B
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
450	Si-R180B

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

[注意]

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

[未設定時]

IP フィルタを設定しないものとみなされ、すべてのパケットが透過します。

6.4.38 lan ip filter move

[機能]

IP フィルタの優先順序の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～999	Si-R570 Si-R570B Si-R370 Si-R370B
0～199	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

[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。

6.4.39 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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)のどれかを指定します。
0 秒を指定した場合は、変換テーブル解放のための監視を行いません。
省略時は、5 分を指定したものとみなされます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[未設定時]

どの IP フィルタテーブルにも一致しないパケットは透過します。

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

6.4.40 lan ip tos

[機能]

TOS 値書き換え条件の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～499	Si-R570 Si-R570B Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～31	Si-R180B

<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
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B

範囲	機種
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

<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
500	Si-R570 Si-R570B Si-R370 Si-R370B
100	Si-R260B Si-R240B Si-R220C Si-R220D
32	Si-R180B

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

最大定義数	機種
9000	Si-R570 Si-R570B
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
450	Si-R180B

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

[未設定時]

TOS 値書き換えを行わないものとみなされます。

6.4.41 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～499	Si-R570 Si-R570B Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～31	Si-R180B

[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。

6.4.42 lan ip priority

[機能]

帯域制御の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

<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
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B

範囲	機種
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

<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～100000kbps または 1mbps～100mbps の範囲で指定します。全定義の帯域の合計が回線速度を超えた場合は、それぞれ指定した値の比で帯域を割り当てます。

指定した値の合計値が回線速度に達しない場合、残った帯域は定義に一致しないデータ用の帯域となります。

「"share" + 数字」で指定した場合、数字で指定した帯域制御定義番号で定義された帯域を共有します。この場合、指定する数字は自分自身の帯域制御定義番号より小さい、すでに定義されているものを指定しなければなりません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

帯域制御を設定します。任意のプロトコル、アドレス、ポート、TOS 値を指定して、割り当てる帯域を指定します。

帯域制御の旧定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
1000	Si-R570 Si-R570B
500	Si-R370 Si-R370B
100	Si-R260B Si-R240B Si-R220C Si-R220D
64	Si-R180B

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

最大定義数	機種
9000	Si-R570 Si-R570B

最大定義数	機種
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
450	Si-R180B

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

[注意]

シェーピングを使用しない場合、帯域制御は有効に動作しません。

[未設定時]

帯域制御を行わないものとみなされます。

6.4.43 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<in-policy_number>

・ Ingress ポリシールーティング定義番号
この I/F での Ingress ポリシールーティング定義の通し番号を、10 進数で指定します。
本定義は、ほかのポリシーグループ参照定義を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
2000	Si-R570 Si-R570B
1000	Si-R370 Si-R370B
200	Si-R260B Si-R240B Si-R220C Si-R220D
100	Si-R180B

<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
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R220C Si-R220D

範囲	機種
0～49	Si-R180B

[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。

6.4.44 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

6.4.45 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

6.4.46 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

6.4.47 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

6.4.48 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

6.4.49 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

6.4.50 lan ip arp cycle

[機能]

ARP 定期送信機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

6.4.51 lan ip arp static

[機能]

スタティック ARP の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<count>

・ スタティック ARP テーブル定義番号
指定した定義番号と同じ値を持つ定義がすでに存在する場合は、既存の設定に対する修正とみなされます。

範囲	機種
0～199	Si-R570 Si-R570B Si-R370 Si-R370B
0～ 99	Si-R260B Si-R240B Si-R220C Si-R220D
0～ 49	Si-R180B

<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。

6.4.52 lan ip ids use

[機能]

IDS の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

6.5 IPv6 関連情報

6.5.1 lan ip6 use

[機能]

IPv6 機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 use <mode>

[オプション]

<number>

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

<mode>

IPv6 パケットの送受信を行うかどうか指定します。

・ on
このインタフェースで、IPv6 パケットの送受信を行います。

・ off
このインタフェースで、IPv6 パケットの送受信を行いません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

このインタフェースで、IPv6 機能を利用するかどうかを設定します。

[未設定時]

IPv6 機能を利用しないものとみなされます。

```
lan <number> ip6 use off
```

6.5.2 lan ip6 ifid

[機能]

IPv6 インタフェース ID の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 ifid <interfaceID>

[オプション]

<number>

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

<interfaceID>

このインタフェースで利用する ID を指定します。

・ auto
本装置が持つ MAC アドレスから、EUI-64 形式の ID を自動生成する場合に指定します。

・ インタフェース ID
このインタフェースで利用する ID を、16 進数で指定します。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> ip6 ifid auto
```

6.5.3 lan ip6 address

[機能]

IPv6 アドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 address [<count>] <address>/<prefixlen> <valid> <preferred> [<flags>]
lan [<number>] ip6 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。

<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。
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～rmt999	Si-R570 Si-R570B
lan0～lan19 rmt0～rmt499	Si-R370 Si-R370B
lan0～lan19 rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
lan0～lan9 rmt0～rmt49	Si-R180B

例)
rmt0 で動作する IPv6 DHCP クライアントが取得した IPv6 プレフィックスを使用する場合の設定例

```
dhcp@rmt0::/64
dhcp@rmt0::1:2:3:4/64
```

プレフィックス長には 64 を指定してください。

<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。

<valid>

・ valid lifetime の時間
このインタフェースから RA(Router Advertisement メッセージ)を送信するときに、このプレフィックスに対する valid lifetime を、0 秒～365 日の範囲で指定します。
単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。

<address>/<prefixlen>に IPv6 DHCP クライアントが取得したプレフィックスを使用する指定をした場合は、IPv6 DHCP クライアントが取得した valid lifetime と比較して短い方が有効になります。

・ infinity

このインタフェースから RA を送信するときに、このプレフィックスに対する valid lifetime を無限とする場合に指定します。

<preferred>

・ preferred lifetime の時間

このインタフェースから RA を送信する場合に、このプレフィックスに対する preferred lifetime を、0 秒～365 日の範囲で指定します。

単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。

<preferred>は、<valid>よりも短い時間となるように設定してください。<preferred>が<valid>よりも大きい場合、<valid>と同じ時間として扱われます。

<address>/<prefixlen>に IPv6 DHCP クライアントが取得したプレフィックスを使用する指定をした場合は、IPv6 DHCP クライアントが取得した preferred lifetime と比較して短い方が有効になります。

・ infinity

このインタフェースから RA を送信する場合に、このプレフィックスに対する preferred lifetime を無限とします。

<flags>

・ RA Prefix Information に付与されるフラグ

このインタフェースから RA を送出する場合に、この prefix に対する flags フィールドの値を 0～ff の 16 進数で指定します。

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]

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。

```
<-IPv6 DHCPクライアントが取得したプレフィックス->
                                  <---------------ユーザ設定値(80bit)---------------------->
┌──────────────────────────────┬──────────────┬──────────────────────────────────────┐
│                                │////////////│                                      │
└──────────────────────────────┴──────────────┴──────────────────────────────────────┘
                                  <------------>
                                  設定値が重なる部分
```

例)

IPv6 DHCP クライアントが 2001:db8:1000:5555::/64 を取得した場合

設定内容	利用されるアドレス
dhcp@rmt0:0:100::1/64	2001:db8:1000:5555:100::1/64
dhcp@rmt0:100:200::1/64	無効

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。

6.5.4 lan ip6 ra mode

[機能]

Router Advertisement の動作の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 ra mode <mode>

[オプション]

<number>

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

<mode>

・ off
RA の送信を行いません。
定期送信、および host からの RS に対する RA の送信を行いません。

・ send
RA の送信を行います。
定期送信、および host からの RS に対する RA の送信を行います。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RA(Router Advertisement メッセージ)を送信するかどうかを設定します。

[未設定時]

RA の送信を行わないものとみなされます。

```
lan <number> ip6 ra mode off
```

6.5.5 lan ip6 ra interval

[機能]

Router Advertisement メッセージ送信間隔の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 ra interval <max> <min> <lifetime>

[オプション]

<number>

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

<max>

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

<min>

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

<lifetime>

・ Router Lifetime の値
送信する RA の Router Lifetime の値を、0 または<max>～9000 の 10 進数で指定します。

[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 の値の設定を行います。RA は<min>～<max>でランダムに決定された間隔で定期送信されます。

[未設定時]

最大送信間隔に 600 秒、最小送信間隔に 200 秒、Router Lifetime の値に 1800 が設定されたものとみなされます。

```
lan <number> ip6 ra interval 600 200 1800
```

6.5.6 lan ip6 ra mtu

[機能]

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

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 ra mtu <mtu>

[オプション]

<number>

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

<mtu>

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

[未設定時]

送信する RA に MTU option を含めないものとみなされます。

```
lan <number> ip6 ra mtu 0
```

6.5.7 lan ip6 ra reachabletime

[機能]

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

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 ra reachabletime <reachabletime>

[オプション]

<number>

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

<reachabletime>

・ Reachable Time の値
RA に含める Reachable Time の値(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 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> ip6 ra reachabletime 0
```

6.5.8 lan ip6 ra retranstimer

[機能]

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

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 ra retranstimer <retranstimer>

[オプション]

<number>

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

<retranstimer>

・ Retrans Timer の値
RA に含める Retrans Timer の値(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 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> ip6 ra retranstimer 0
```

6.5.9 lan ip6 ra curhoplimit

[機能]

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

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 ra curhoplimit <curhoplimit>

[オプション]

<number>

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

<curhoplimit>

・ Cur Hop Limit の値
RA に含める Cur Hop Limit の値を、0～255 の 10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RA に含める Cur Hop Limit の値を設定します。

[未設定時]

Cur Hop Limit の値として 64 が設定されたものとみなされます。

```
lan <number> ip6 ra curhoplimit 64
```

6.5.10 lan ip6 ra flags

[機能]

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

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 ra flags <flags>

[オプション]

<number>

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

<flags>

・ flags field の値
RA に含める flags field の値を、00～ff の 16 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RA に含める flags field の値を設定します。

[未設定時]

flags field の値として 00 が設定されたものとみなされます。

```
lan <number> ip6 ra flags 00
```

6.5.11 lan ip6 route

[機能]

IPv6 スタティック経路情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 route <count> <address>/<prefixlen> <next_hop> [<metric> [<distance>]]

[オプション]

<number>

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

<count>

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

範囲	機種
0～1999	Si-R570 Si-R570B
0～1249	Si-R370 Si-R370B
0～255	Si-R260B Si-R240B Si-R220C Si-R220D
0～127	Si-R180B

<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、1～15 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、0～254 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、0 を指定したものとみなされます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 スタティック経路(静的経路)情報を設定します。

RIP メトリック値は、スタティック経路情報を RIP に再配布するときのメトリック値を設定します。

RIP に再配布したときは、設定した RIP メトリック値+1 のメトリック値で RIP テーブルに登録されます。

優先度は、同じあて先への経路情報が複数ある場合、優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。各ダイナミックルーティングプロトコルの優先度については、routemanage ip6 distance コマンドを参照してください。

優先度に 0 が設定されているときは、routemanage interface floating コマンドでのフローティング設定に応じてフローティング動作が切り替わります。優先度に 1 以上が設定されているときは、常にフローティング動作します。

フローティング動作する場合、<next_hop>で指定した中継ルータと隣接しているインタフェースが通信可能な状態(リンクアップなど)であれば、スタティック経路情報をルーティングテーブルに追加します。通信不可能な状態(リンクダウンなど)であれば、ルーティングテーブルから削除します。

フローティング動作しない場合は、インタフェースの状態にかかわらず常にスタティック経路情報をルーティングテーブルに追加します。

以下に、各設定値とフローティング動作の関係を示します。

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

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

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

IPv6 スタティック経路情報は、本装置全体で以下の数まで定義できます。

最大定義数	機種
2000	Si-R570 Si-R570B
1250	Si-R370 Si-R370B
256	Si-R260B Si-R240B Si-R220C Si-R220D
128	Si-R180B

[注意]

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

・ 優先度が 0 のスタティック経路情報と、優先度が 0 または 1 以上のスタティック経路情報は同時に設定できません。
・ 優先度が同じスタティック経路情報は同時に設定できません。

[未設定時]

IPv6 スタティック経路情報を使用しないものとみなされます。

6.5.12 lan ip6 rip use

[機能]

IPv6 RIP 基本情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 rip use <send> <receive> [<metric>]

[オプション]

<number>

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

<send>

RIP(IPv6)パケットを送信するかどうか指定します。

・ on
RIP(IPv6)パケットを送信します。
・ off
RIP(IPv6)パケットを送信しません。

<receive>

RIP(IPv6)パケットを受信するかどうか指定します。

・ on
RIP(IPv6)パケットを受信します。
・ off
RIP(IPv6)パケットを受信しません。

<metric>

・ 加算メトリック値
RIP(IPv6)パケット送信時の加算メトリック値を、0～16 の 10 進数で指定します。
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
220	Si-R570 Si-R570B Si-R370 Si-R370B
120	Si-R260B Si-R240B Si-R220C Si-R220D
58	Si-R180B

[未設定時]

RIP(IPv6)機能を使用しないものとみなされます。

```
lan <number> ip6 rip use off off 0
```

6.5.13 lan ip6 rip site-local

[機能]

IPv6 RIP site-local プレフィックス送受信の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 rip site-local <mode>

[オプション]

<number>

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

<mode>

site-local プレフィックスを送受信するかどうかを指定します。

・ on
site-local プレフィックスを送受信します。
・ off
site-local プレフィックスを送受信しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RIP(IPv6)で site-local プレフィックスを送受信するかどうかを設定します。

[未設定時]

site-local プレフィックスを送受信するものとみなされます。

```
lan <number> ip6 rip site-local on
```

6.5.14 lan ip6 rip aggregate

[機能]

IPv6 RIP の集約経路の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 rip aggregate <count> <address>/<prefixlen> <rejectroute>

[オプション]

<number>

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

<count>

・ 集約経路定義番号
集約経路の定義番号を、0〜3 の 10 進数で指定します。

<address>/<prefixlen>

・ IPv6 アドレス/プレフィックス長
集約経路のあて先ネットワークを IPv6 アドレスとプレフィックス長の組み合わせで指定します。
・ default
集約経路としてデフォルトルートを設定する場合に指定します。
::/0 を指定するのと同じ意味になります。

<rejectroute>

・ on
集約経路に対する reject 経路を設定します。
・ off
集約経路に対する reject 経路を設定しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RIP の集約経路の設定を行います。
集約経路が設定された場合は、設定された集約経路に含まれる個々の経路は広報されず、集約経路だけを広報します。また、集約経路と等しいネットワークに対する経路情報を持たない場合は、実際に持たないあて先に対するパケットを破棄するために、設定された集約経路に対する reject 経路を設定することもできます。

集約経路情報のメトリック値は、集約された経路のメトリック値に関係なく 1 として広報され lan ip6 rip use および lan ip6 rip filter set metric で広報するメトリック値を変更することができます。

同一 lan 定義内に同一の集約経路は設定できません。

[未設定時]

RIP(IPv6)で経路集約しないものとみなされます。

6.5.15 lan ip6 rip filter act

[機能]

IPv6 RIP フィルタ動作の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 rip filter <count> act <action> <direction>

[オプション]

<number>

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

<count>

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

範囲	機種
0～399	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～199	Si-R180B

<action>

フィルタリング条件に一致した場合の動作を指定します。

・ pass
該当する経路情報を透過します。

・ reject
該当する経路情報を遮断します。

<direction>

フィルタリングを行う方向を指定します。

・ in
受信時にフィルタリングを行います。

・ out
送信時にフィルタリングを行います。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RIP(IPv6)での経路情報送受信時に、フィルタリング条件に一致した経路情報を通過(pass)させるか遮断(reject)させるかを設定します。フィルタリング条件は優先度順に検索し、条件に一致した経路情報があった時点でフィルタリングが行われ、それ以降の条件は参照されません。全条件に不一致の経路情報は遮断されます。

フィルタリング条件は、lan ip6 rip filter route コマンドを使用し経路情報を設定します。

<count>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。

RIP フィルタ(IPv6)は、本装置全体で以下の数まで定義できます。

最大定義数	機種
400	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
200	Si-R180B

[注意]

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

[未設定時]

RIP(IPv6)フィルタを使用しないものとみなされ、すべての RIP(IPv6)の経路情報が透過します。

6.5.16 lan ip6 rip filter move

[機能]

IPv6 RIP フィルタの優先順序の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 rip filter move <count> <new_count>

[オプション]

<number>

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

<count>

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

<new_count>

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

範囲	機種
0～399	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～199	Si-R180B

[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。

6.5.17 lan ip6 rip filter route

[機能]

IPv6 RIP フィルタの経路情報設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 rip filter <count> route <address>/<prefixlen> [<prefix_match>]

[オプション]

<number>

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

<count>

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

範囲	機種
0～399	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～199	Si-R180B

<address>/<prefixlen>

・ IPv6 アドレス/プレフィックス長
フィルタリング対象とする経路情報を、IPv6 アドレスとプレフィックス長の組み合わせで指定します。
・ any
すべての経路情報をフィルタリング対象とする場合に指定します。
・ default
デフォルトルートをフィルタリング対象とする場合に指定します。

<prefix_match>

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

・ exact
指定した<address>/<prefixlen>と経路情報の IPv6 アドレス/プレフィックス長を比較し、一致した場合に、フィルタリング対象とします。
・ inexact
指定した<address>と経路情報の IPv6 アドレスを比較し、<prefixlen>まで一致した場合、フィルタリング対象とします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

フィルタリング条件として経路情報を設定します。

[未設定時]

フィルタリング条件が設定されていないものとみなされます。

6.5.18 lan ip6 rip filter set metric

[機能]

IPv6 RIP フィルタのメトリック設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 rip filter <count> set metric <metric>

[オプション]

<number>

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

<count>

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

範囲	機種
0～399	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～199	Si-R180B

<metric>

・ メトリック値
メトリック値を、0～16 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 1～16 を設定した場合、メトリック値は設定した値に変更されます。この場合、lan ip6 rip use コマンドで設定した加算メトリック値は加算されません。0 を指定した場合、メトリック値の変更は行われません。

[注意]

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

[未設定時]

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

6.5.19 lan ip6 ospf use

[機能]

IPv6 OSPF 利用可否の設定

[適用機種]

Si-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 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。

<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
0～3	Si-R570 Si-R570B
0～2	Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

[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
30	Si-R570 Si-R570B
15	Si-R240B Si-R220C Si-R220D Si-R180B

[注意]

OSPF の利用は、"ospf ip6 area id"を設定した場合にだけ有効です。
Si-R570、Si-R570B では、拡張用 512M メモリモジュールが搭載されているときにのみ使用できます。

[未設定時]

OSPF を使用しないものとみなされます。

```
lan <number> ip6 ospf use off
```

6.5.20 lan ip6 ospf cost

[機能]

IPv6 OSPF 出力コストの設定

[適用機種]

Si-R570 | Si-R570B | | | | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[入力形式]

lan [<number>] ip6 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。

<cost>

・ 出力コスト
出力コストを、1～65535 で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

OSPF 出力コストを設定します。

[未設定時]

OSPF 出力コストに 10 が設定されているものとみなされます。

```
lan <number> ip6 ospf cost 10
```

6.5.21 lan ip6 ospf hello

[機能]

IPv6 OSPF Helloパケット送信間隔の設定

[適用機種]

Si-R570 | Si-R570B | | | | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[入力形式]

lan [<number>] ip6 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。

<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)のどれかを指定します。
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> ip6 ospf hello 10s
```

6.5.22 lan ip6 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-R570 | Si-R570B | | | | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[入力形式]

lan [<number>] ip6 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。

<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)のどれかを指定します。
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。

[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> ip6 ospf dead 40s
```

6.5.23 lan ip6 ospf retrans

[機能]

IPv6 OSPF パケット再送間隔の設定

[適用機種]

Si-R570 | Si-R570B | | | | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[入力形式]

lan [<number>] ip6 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。

<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)のどれかを指定します。
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> ip6 ospf retrans 5s
```

6.5.24 lan ip6 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-R570 | Si-R570B | | | | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[入力形式]

lan [<number>] ip6 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。

<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)のどれかを指定します。
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> ip6 ospf delay 1s
```

6.5.25 lan ip6 ospf priority

[機能]

IPv6 OSPF 指定ルータ優先度の設定

[適用機種]

Si-R570 | Si-R570B | | | | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[入力形式]

lan [<number>] ip6 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。

<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> ip6 ospf priority 1
```

6.5.26 lan ip6 ospf passive

[機能]

IPv6 OSPF パケット送信抑止の設定

[適用機種]

Si-R570 | Si-R570B | | | | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[入力形式]

lan [<number>] ip6 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。

<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。

・ on
パケットの送信を抑止します。

・ off
パケットの送信を抑止しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

OSPF 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> ip6 ospf passive off
```

6.5.27 lan ip6 filter

[機能]

IPv6 フィルタの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 filter <count> <action> acl <acl_count> [<direction>]

lan [<number>] ip6 filter <count> <action> <src_addr>/<prefixlen> <src_port><dst_addr>/<prefixlen> <dst_port> <protocol> <tcpconnect>[<trafficclass> [<direction> [<icmptype> [<icmpcode>]]]]

[オプション]

<number>

・ lan 定義番号

lan 定義の通し番号を、10 進数で指定します。

省略時は、0 を指定したものとみなされます。

<count>

・ フィルタリング定義番号

フィルタリングの優先度を表す番号を、10 進数で指定します。

指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つフィルタリング定義がすでに存在する場合は、既存の定義を変更します。

範囲	機種
0～999	Si-R570 Si-R570B Si-R370 Si-R370B
0～199	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

<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。

- ip6

  ip6 値が設定されていない場合、そのフィルタ定義は無効となり、無視されます。

- tcp

  ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip6 の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。

- udp

  ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip6 の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp

  ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。

また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

<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 として扱われます。

<direction>

フィルタリングする方向を指定します。

省略時は、any を指定したものとみなされます。

・ any

入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。

・ in

入力パケットのみをフィルタリング対象とする場合に指定します。

・ out

出力パケットのみをフィルタリング対象とする場合に指定します。

・ reverse

入力パケットと出力パケットの両方をフィルタリング対象とします。

ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。

- 送信元 IP アドレス/プレフィックス長とあて先 IP アドレス/プレフィックス長
- 送信元ポート番号とあて先ポート番号

<icmptype>

フィルタリングする ICMPv6 メッセージタイプ番号を指定します。

・ フィルタリング対象 icmptype 値

フィルタリング対象となる icmptype フィールドの値を 0-255 までの 10 進数、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 として扱われます。

<icmpcode>

フィルタリングする ICMPv6 メッセージコード番号を指定します。

icmpcode 指定時は、icmptype も指定する必要があります。

・ フィルタリング対象 icmpcode 値

フィルタリング対象となる icmpcode フィールドの値を 0-255 までの 10 進数、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 として扱われます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

このインタフェースに対する IPv6 フィルタを設定します。
各パラメタに設定された値によって、動作が変化する場合があります。以下に説明します。

・ <protocol>に指定した値によって、IPv6 拡張ヘッダの扱いが以下のように変化します。
- any を指定した場合は、0 個以上の IPv6 拡張ヘッダを含む、あらゆる upper-layer protocol(upper-layer protocol なしを含む)に一致します。
- 以下の IPv6 拡張ヘッダの値を指定した場合は、その拡張ヘッダが付与されている、あらゆる upper-layer protocol(upper-layerprotocol なしを含む)のパケットが一致します。

0
Hop-by-Hop Options Header

43
Routing Header

44
Fragment Header

60
Destination Options Header

- 以下の値を指定した場合は、0 個以上の IPv6 拡張ヘッダ(AH、ESP、IPComp を除く)を含む、upper-layer protocol ヘッダが付与されていないパケットが一致します。

59
no next header

- その他の値が設定されている場合は、upper-layer protocol ヘッダの protocol 番号に等しい値であるパケットが一致します。この場合、AH、ESP、IPComp を除くすべての IPv6 拡張ヘッダは無視されます。パケット中に AH、ESP が設定されている場合は、それ以降の拡張ヘッダおよび upper-layer protocol ヘッダの解釈は行いません。

・ <src_port>、<dst_port>に指定した値によって、<protocol>の扱いが以下のように変化します。
- <protocol>に any を指定し、かつ<src_port>、<dst_port>のどちらか、または両方を指定している場合、TCP および UDP パケットの該当ポート番号を持つパケットのみが一致します。
- <protocol>に TCP(6)または UDP(17)を指定し、かつ<src_port>、<dst_port>のどちらか、または両方を指定している場合、指定プロトコルの該当ポート番号を持つパケットのみが一致します。
- <protocol>に TCP(6)または UDP(17)以外を指定し、かつ<src_port>、<dst_port>のどちらか、または両方を指定している場合、あらゆるパケットが一致しません。

・ <icmptype>、<icmpcode>に指定した値によって、<protocol>の扱いが以下のように変化します。
- <protocol>に any を指定し、かつ<icmptype>、<icmpcode>を指定している場合、ICMPv6 パケットの該当 type/code 番号を持つパケットのみが一致します。
- <protocol>に ICMPv6(58)を指定し、かつ<icmptype>、<icmpcode>を指定している場合、指定プロトコルの該当 type/code 番号を持つパケットのみが一致します。
- <protocol>に ICMPv6(58)以外を指定し、かつ<icmptype>、<icmpcode>を指定している場合、あらゆるパケットが一致しません。

・ <tcpconnect>の扱いを以下に示します。
- <protocol>に any を指定した場合、TCP パケットのときにこの設定値が適用されます。
- <protocol>に TCP(6)を指定した場合、常にこの設定値が適用されます。
- <protocol>に any または TCP(6)以外を指定した場合、この設定値は適用されません。

IPv6 フィルタリングの旧定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
1000	Si-R570 Si-R570B Si-R370 Si-R370B
200	Si-R260B Si-R240B Si-R220C Si-R220D

最大定義数	機種
64	Si-R180B

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

最大定義数	機種
9000	Si-R570 Si-R570B
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
450	Si-R180B

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。

6.5.28 lan ip6 filter move

[機能]

IPv6 フィルタの優先順序の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 filter move <count> <new_count>

[オプション]

<number>

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

<count>

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

<new_count>

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

範囲	機種
0～999	Si-R570 Si-R570B Si-R370 Si-R370B
0～199	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

[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。

6.5.29 lan ip6 filter default

[機能]

どの IP フィルタテーブルにも不一致時の動作の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 filter default <action> [<time>]

[オプション]

<number>

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

<action>

どの IPv6 フィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

・ pass
該当するパケットを透過します。

・ reject
該当するパケットを遮断します。

・ spi
該当するパケットに対して SPI を動作させます。

<time>

・ 割り当て時間
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)のどれかを指定します。
0 秒を指定した場合は、変換テーブル解放のための監視を行いません。
省略時は、5 分を指定したものとみなされます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

どの IPv6 フィルタテーブルにも一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

どの IPv6 フィルタテーブルにも一致しないパケットは透過します。

```
lan <number> ip6 filter default pass
```

6.5.30 lan ip6 trafficclass

[機能]

Traffic Class 値書き換え条件の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 trafficclass <count> acl <acl_count> <new_trafficclass>

lan [<number>] ip6 trafficclass <count> <src_addr>/<prefixlen> <src_port><dst_addr>/<prefixlen> <dst_port> <protocol> <trafficclass> <new_trafficclass>

[オプション]

<number>

・ lan 定義番号

lan 定義の通し番号を、10 進数で指定します。

省略時は、0 を指定したものとみなされます。

<count>

・ Traffic Class 値書き換え定義番号

Traffic Class 値書き換え条件の優先度を表す定義番号を、10 進数で指定します。

指定した値は、設定完了時に順方向にソートされてリナンバリングされます。

また、指定した定義番号と同じ値を持つ Traffic Class 値書き換え定義がすでに存在する場合は、既存定義の値を変更します。

範囲	機種
0～499	Si-R570 Si-R570B Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～31	Si-R180B

<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。

- ip6

  ip6 値が設定されていない場合、その定義は無効となり、無視されます。

- tcp

  ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip6 の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。

- udp

  ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip6 の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp

  ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0～2999	Si-R570 Si-R570B

範囲	機種
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

<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
500	Si-R570 Si-R570B Si-R370 Si-R370B
100	Si-R260B Si-R240B Si-R220C Si-R220D
32	Si-R180B

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

最大定義数	機種
9000	Si-R570 Si-R570B
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
450	Si-R180B

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。

6.5.31 lan ip6 trafficclass move

[機能]

Traffic Class 値書き換え条件の優先度の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 trafficclass move <count> <new_count>

[オプション]

<number>

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

<count>

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

<new_count>

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

範囲	機種
0～499	Si-R570 Si-R570B Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～31	Si-R180B

[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。

6.5.32 lan ip6 priority

[機能]

IPv6 プロトコル帯域制御の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 priority <count> acl <acl_count> <width>

lan [<number>] ip6 priority <count> <src_addr>/<prefixlen> <src_port><dst_addr>/<prefixlen> <dst_port> <protocol> <trafficclass> <width>

[オプション]

<number>

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

<count>

・ 帯域制御定義番号
帯域制御定義番号を、10 進数で指定します。

範囲	機種
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

<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。

- ip6
  ip6 値が設定されていない場合、その定義は無効となり、無視されます。
- tcp
  ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。
- udp
  ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。
- icmp
  ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B

範囲	機種
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

<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として扱われます。

<width>

・ express

最優先データとして扱います。

・ besteffort

非優先(ベストエフォート)として扱います。

・ 帯域

1～99の10進数で指定した場合、それぞれ指定した値の比で帯域を割り当てます。たとえば、同じ相手ネットワーク中の定義が3つあり、それぞれ<width>の値が30、30、60であった場合、帯域として25%、25%、50%が割り当てられます。なお、1～99を指定した定義のそれぞれの合計値が100未満の場合、残った帯域は定義に一致しないデータ用の帯域となります。

「数字 + "kbps"(,"mbps")」で指定した場合、指定した帯域をそのまま割り当てます。1kbps～100000kbpsまたは1mbps～100mbpsの範囲で指定します。全定義の帯域の合計が回線速度を超えた場合は、それぞれ指定した値の比で帯域を割り当てます。

指定した値の合計値が回線速度に達しない場合、残った帯域は定義に一致しないデータ用の帯域となります。

「"share" + 数字」で指定した場合、数字で指定した帯域制御定義番号で定義された帯域を共有します。この場合、指定する数字は自分自身の帯域制御定義番号より小さい、すでに定義されているものを指定しなければなりません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6プロトコル帯域制御を設定します。任意のプロトコル、アドレス、ポート、トラフィッククラスを指定して、割り当てる帯域を指定します。

IPv6プロトコル帯域制御の旧定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
1000	Si-R570 Si-R570B
500	Si-R370 Si-R370B
100	Si-R260B Si-R240B Si-R220C Si-R220D
64	Si-R180B

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

最大定義数	機種
9000	Si-R570 Si-R570B
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
450	Si-R180B

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。

6.5.33 lan ip6 in-policy

[機能]

Ingress ポリシールーティングの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 in-policy <in-policy_number> policy-group <policy-group_number>

[オプション]

<number>

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

<in-policy_number>

・ Ingress ポリシールーティング定義番号
この I/F での Ingress ポリシールーティング定義の通し番号を、10 進数で指定します。
本定義は、ほかのポリシーグループ参照定義を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
2000	Si-R570 Si-R570B
1000	Si-R370 Si-R370B
200	Si-R260B Si-R240B Si-R220C Si-R220D
100	Si-R180B

<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。
- ip6 ip6 値が設定されていない場合、その定義は無効となり、無視されます。
- tcp ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。また、ip6 の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。
- udp ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。また、ip6 の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。
- icmp ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R220C Si-R220D
0～49	Si-R180B

[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。

6.5.34 lan ip6 in-policy move

[機能]

Ingress ポリシールーティングの優先順序の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 in-policy move <count> <new_count>

[オプション]

<number>

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

<count>

・ 対象 Ingress ポリシールーティング定義番号
優先順序を変更するフィルタリング定義の番号を指定します。

<new_count>

・ 移動先 Ingress ポリシールーティング定義番号
<count>に対する新しい順序を、10 進数で指定します。
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。

6.5.35 lan ip6 dhcp service

[機能]

IPv6 DHCP 機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 dhcp service <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。

<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。

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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> ip6 dhcp service off
```

6.5.36 lan ip6 dhcp duid

[機能]

IPv6 DHCP の DUID 設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 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。

<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 ip6 dhcp duid 2105afffe66437d
```

[未設定時]

DUID を自動生成するものとみなされます。

6.5.37 lan ip6 dhcp client option pd

[機能]

IPv6 DHCP クライアントのプレフィックス要求の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 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。

<mode>

・ on
プレフィックスを要求します。
・ off
プレフィックスを要求しません。
・ troan
draft-troan-dhcpv6-opt-prefix-delegation-01 に準拠した方式でプレフィックスを要求します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 DHCP クライアント機能を使用する場合に、サーバにプレフィックスを要求するかどうかを設定します。
<mode>に on を設定した場合は、RFC3315、3633 に準拠したオプション番号を使用します。
<mode>に troan に設定した場合は、DNS サーバオプションのオプション番号に 25 番を使用し、PD オプションのオプション番号に 30 番を使用してプレフィックスの要求を行います。

[未設定時]

プレフィックスを要求するものとみなされます。

```
lan <number> ip6 dhcp client option pd on
```

6.5.38 lan ip6 dhcp client option dns

[機能]

IPv6 DHCP クライアントの DNS サーバアドレス要求の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 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。

<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> ip6 dhcp client option dns on
```

6.5.39 lan ip6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 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。

<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> ip6 dhcp client option domain on
```

6.5.40 lan ip6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 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。

<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> ip6 dhcp client option sipserver address on
```

6.5.41 lan ip6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 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。

<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> ip6 dhcp client option sipserver domain on
```

6.5.42 lan ip6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 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。

<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> ip6 dhcp client option sntpserver on
```

6.5.43 lan ip6 dhcp client iaid

[機能]

IPv6 DHCP クライアントの IAID 設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 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。

<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> ip6 dhcp client iaid auto
```

6.5.44 lan ip6 dhcp client route

[機能]

IPv6 DHCP クライアントのリジェクト経路設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 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。

<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> ip6 dhcp client route blackhole
```

6.5.45 lan ip6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 dhcp relay interface <interface>

[オプション]

<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～rmt999	Si-R570 Si-R570B
lan0～lan19 rmt0～rmt499	Si-R370 Si-R370B
lan0～lan19 rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
lan0～lan9 rmt0～rmt49	Si-R180B

[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。

6.5.46 lan ip6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 dhcp relay server <address>

[オプション]

<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。

6.5.47 lan ip6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 dhcp relay source <address>

[オプション]

<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。

6.5.48 lan ip6 dhcp server preference

[機能]

IPv6 DHCP サーバのプリファレンス値設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 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。

<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> ip6 dhcp server preference 0
```

6.5.49 lan ip6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 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。

<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～rmt999	Si-R570 Si-R570B
lan0～lan19 rmt0～rmt499	Si-R370 Si-R370B
lan0～lan19 rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
lan0～lan9 rmt0～rmt49	Si-R180B

例)
rmt0 で動作する IPv6 DHCP クライアントが取得した IPv6 プレフィックスを使用する場合の設定例
dhcp@rmt0::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)のどれかを指定します。

・ infinity

このインタフェースから配布する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)のどれかを指定します。

<preferred>は、<valid>よりも短い時間となるように設定してください。<preferred>が<valid>よりも大きい場合、<valid>と同じ時間として扱われます。

・infinity

このインタフェースから配布する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。

6.5.50 lan ip6 dhcp server info dns

[機能]

IPv6 DHCP サーバの DNS サーバアドレス配布情報設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 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。

<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～rmt999	Si-R570 Si-R570B
lan0～lan19 rmt0～rmt499	Si-R370 Si-R370B
lan0～lan19 rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
lan0～lan9 rmt0～rmt49	Si-R180B

<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。

6.5.51 lan ip6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 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。

<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～rmt999	Si-R570 Si-R570B
lan0～lan19 rmt0～rmt499	Si-R370 Si-R370B
lan0～lan19 rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
lan0～lan9 rmt0～rmt49	Si-R180B

[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。

6.5.52 lan ip6 dhcp server info prefix

[機能]

IPv6 DHCP サーバのプレフィックス配布情報設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 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。

<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、lan または rmt インタフェースを以下の範囲で指定します。

範囲	機種
lan0～lan19 rmt0～rmt999	Si-R570 Si-R570B
lan0～lan19 rmt0～rmt499	Si-R370 Si-R370B
lan0～lan19 rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
lan0～lan9 rmt0～rmt49	Si-R180B

例)

rmt0 で動作する IPv6 DHCP クライアントが取得した IPv6 プレフィックスを使用する場合の設定例
dhcp@rmt0:1234::/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)のどれかを指定します。

・ infinity

このインタフェースから配布するプレフィックスに対する valid lifetime を、無限とする場合に指定します。

<preferred>

・ preferred lifetime

このインタフェースから配布するプレフィックスに対する preferred lifetime を、0 秒～365 日の範囲で指定します。

単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。

<preferred>は、<valid>よりも短い時間となるように設定してください。<preferred>が<valid>よりも大きい場合、<valid>と同じ時間として扱われます。

・ infinity

このインタフェースから配布するプレフィックスに対する preferred lifetime を無限とします。

<routeset>

・ on

配布プレフィックスへの経路を自動登録します。

・ off

配布プレフィックスへの経路を自動登録しません。

<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。

6.5.53 lan ip6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 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。

<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～rmt999	Si-R570 Si-R570B
lan0～lan19 rmt0～rmt499	Si-R370 Si-R370B
lan0～lan19 rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
lan0～lan9 rmt0～rmt49	Si-R180B

<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。
<sip1>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 SIP サーバアドレス情報の設定をします。

6.5.54 lan ip6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 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。

<sip1>

・ SIP 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 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～rmt999	Si-R570 Si-R570B
lan0～lan19 rmt0～rmt499	Si-R370 Si-R370B
lan0～lan19 rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
lan0～lan9 rmt0～rmt49	Si-R180B

<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 ドメイン名を指定します。

<sip1>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 SIP ドメイン名情報の設定をします。

6.5.55 lan ip6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] ip6 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。

<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～rmt999	Si-R570 Si-R570B
lan0～lan19 rmt0～rmt499	Si-R370 Si-R370B
lan0～lan19 rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
lan0～lan9 rmt0～rmt49	Si-R180B

<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。

6.6 ブリッジ関連情報

6.6.1 lan bridge use

[機能]

ブリッジ動作モードの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] bridge use <mode>

[オプション]

<number>

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

<mode>

ブリッジを使用するかどうかを指定します。

・ on
ブリッジを使用する場合に指定します。
・ off
ブリッジを使用しない場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ブリッジを使用するかどうかを設定します。
ブリッジを使用する場合、IP および IPv6 のパケット以外をすべてブリッジします。

[注意]

IP および IPv6 以外のネットワークプロトコル(IPX など)をルーティングしているネットワークでブリッジを使用する場合は、ブリッジによって中継されることでネットワークがダウンすることがあります。ルーティングと同時に使用する場合は、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に設定してください。

[未設定時]

ブリッジを使用しないものとみなされます。

```
lan <number> bridge use off
```

6.6.2 lan bridge group

[機能]

ブリッジグループ識別子の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] bridge group <group_id>

[オプション]

<number>

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

<group_id>

・ グループ識別子
グループ識別子を 10 進数で指定します。

範囲	機種
0～19	Si-R570 Si-R570B Si-R370 Si-R370B Si-R240B Si-R220C Si-R220D
0～7	Si-R260B Si-R180B

[動作モード]

構成定義モード(管理者クラス)

[説明]

ブリッジのグループ識別子を設定します。

[未設定時]

グループ識別子に 0 を指定したものとみなされます。

```
lan <number> bridge group 0
```

6.6.3 lan bridge static

[機能]

静的学習テーブル情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] bridge static <count> <mac>

[オプション]

<number>

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

<count>

・ 静的学習テーブル定義番号
指定した定義番号と同じ値を持つ定義がすでに存在する場合は、既存の設定に対する修正とみなされます。

範囲	機種
0～399	Si-R570 Si-R570B Si-R370 Si-R370B
0～199	Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

<mac>

静的な定義として学習テーブルに追加する MAC アドレスを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

学習テーブルに指定された MAC アドレスを静的な学習テーブル情報として追加します。

6.6.4 lan bridge stp use

[機能]

STP 動作モードの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] bridge stp use <mode>

[オプション]

<number>

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

<mode>

- on
  STP を使用する場合に指定します。
- off
  STP を使用しない場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

スパニングツリーアルゴリズムで経路制御を行うかどうかを設定します。
本コマンドは、ブリッジを使用している場合にだけ有効です。

[注意]

ブリッジグループ 0 以外のブリッジグループでは STP は動作しません。

[未設定時]

STP を使用しないものとみなされます。

```
lan <number>  bridge stp use off
```

6.6.5 lan bridge stp cost

[機能]

パスコストの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] bridge stp cost <path_cost>

[オプション]

<number>

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

<path_cost>

LAN を経由する通信のパスコストを指定します。
通常は auto を指定してください。ただし、ブリッジネットワークを構築するうえで、優先ブリッジ決定のために任意のパスコストを指定することができます。

・ auto
インタフェースの速度に応じて、パスコストが自動決定されます。

以下に、本パラメタ指定時のパスコストを示します。

回線種別	パスコスト	備考
Ethernet(1Gbps)	100	
Ethernet(100Mbps)	100	
Ethernet(10Mbps)	100	
HSD(64kbps)	15620	*：192kbps～1.5Mbps は PRI の場合
HSD(128kbps)	7810	
HSD(192kbps) *	1000	
HSD(256kbps) *	1000	
HSD(384kbps) *	1000	
HSD(512kbps) *	1000	
HSD(768kbps) *	1000	
HSD(1Mbps) *	667	
HSD(1.5Mbps) *	667	
FR(64kbps)	16000	
FR(128kbps)	8500	
FR(256kbps) *	1100	
FR(384kbps) *	1100	
FR(512kbps) *	1100	
FR(768kbps) *	1100	
FR(1Mbps) *	680	
FR(1.5Mbps) *	680	
ISDN	16000	
MODEM	16000	
IP トンネル	16000	
その他		
1Mbps>=速度	1000	

回線種別	パスコスト	備考
1.5Mbps>=速度>1Mbps	667	
4Mbps>=速度>1.5Mbps	250	
6Mbps>=速度>4Mbps	167	
10Mbps>=速度>6Mbps	100	
16Mbps>=速度>10Mbps	62	
20Mbps>=速度>16Mbps	50	
25Mbps>=速度>20Mbps	40	
40Mbps>=速度>25Mbps	25	
80Mbps>=速度>40Mbps	12	
速度>80Mbps	10	

・ パスコスト
パスコストを、1～65535 の 10 進数で指定します。
値が小さいほど、優先度が高くなります。

[動作モード]

構成定義モード(管理者クラス)

[説明]

スパニングツリーアルゴリズムで使用するパスコストを設定します。
本コマンドは、STP を使用する場合にだけ有効です。

[未設定時]

パスコストを自動決定するとみなされます。

```
lan <number> bridge stp cost auto
```

6.6.6 lan bridge stp priority

[機能]

インタフェース優先度の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] bridge stp priority <port_priority>

[オプション]

<number>

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

<port_priority>

・ インタフェース優先度
インタフェースごとの優先度を、0～255 の 10 進数で指定します。
値が小さいほど、優先度が高くなります。

[動作モード]

構成定義モード(管理者クラス)

[説明]

スパニングツリーアルゴリズムで使用する、インタフェースごとの優先度を設定します。

本コマンドは、STP を使用する場合にだけ有効です。

本コマンドを設定しない場合は、<number>で指定したインタフェースが優先となり、remote 定義で定義されたインタフェースが非優先となります。lan 定義内で定義されたインタフェースでは、定義番号のもっとも小さいものが優先されます。

[未設定時]

インタフェース優先度に 128 が設定されたものとみなされます。

```
lan <number> bridge stp priority 128
```

6.6.7 lan bridge filter

[機能]

MAC フィルタの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

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

lan [<number>] bridge filter <count> <action> <src_mac><dst_mac> <format> [<value> [<vlan_analyze>]]

[オプション]

<number>

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

<count>

・ フィルタリング定義番号
フィルタリングの優先度を表す番号を、10 進数で指定します。
指定した値は、設定完了時に順方向にソートされリナンバリングされます。
指定した定義番号と同じ値を持つ定義がすでに存在する場合は、既存の設定に対する修正とみなされます。
指定した値を持つ定義が存在しない場合は、追加とみなされます。

範囲	機種
0～255	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～127	Si-R180B

<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。
指定した<acl_count>の ACL が定義されていない場合、そのフィルタ定義は無効となり、無視されます。
MAC フィルタでは、ACL の以下の定義を使用します。
- mac
mac 値が設定されていない場合、そのフィルタ定義は無効となり、無視されます。

範囲	機種
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～143	Si-R180B

<direction>

フィルタリングする方向を指定します。
ACL を利用した定義でのみ指定可能です。

省略時は、any を指定したものとみなされます。

・ any
入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。

・ in
入力パケットだけをフィルタリング対象とする場合に指定します。

・ out
出力パケットだけをフィルタリング対象とする場合に指定します。

・ reverse
入力パケットと出力パケットの両方をフィルタリング対象とします。
ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。
- 送信元 MAC アドレスとあて先 MAC アドレス

<src_mac>

フィルタリング対象とする送信元 MAC アドレスを指定します。

・ any
すべての MAC アドレスを対象とする場合に指定します。

・ bcast
ブロードキャスト MAC アドレスを対象とする場合に指定します。

・ mcast
マルチキャスト MAC アドレスを対象とする場合に指定します。

・ 上記以外
対象とする MAC アドレスを指定します。フィルタリング対象とする送信元 MAC アドレスを、xx:xx:xx:xx:xx:xx(xx は 2 桁の 16 進数)の形式で指定します。

<dst_mac>

フィルタリング対象とするあて先 MAC アドレスを指定します。

・ any
すべての MAC アドレスを対象とする場合に指定します。

・ bcast
ブロードキャスト MAC アドレスを対象とする場合に指定します。

・ mcast
マルチキャスト MAC アドレスを対象とする場合に指定します。

・ 上記以外
対象とする MAC アドレスを指定します。フィルタリング対象とする送信元 MAC アドレスを、xx:xx:xx:xx:xx:xx(xx は 2 桁の 16 進数)の形式で指定します。

<format> <value>

・ llc
<value>の値と LSAP が一致する LLC 形式フレームを対象とする場合に指定します。<value>には、0～ffff の 16 進数を指定します。

・ ether
<value>の値とタイプが一致する Ethernet 形式フレームを対象とする場合に指定します。<value>には、5dd～ffff の 16 進数を指定します。

・ any
すべてのフレームを対象とする場合に指定します。<value>は、指定不要です。

<vlan_analyze>

VLAN タグ付きフレームに対してタグの解析を行うかどうかを指定します。
<value>を指定したときだけ指定可能です。
省略時は、off を指定したものとみなされます。

・ on
VLAN タグ付きフレームの場合に VLAN タグを解析してフィルタリング処理を行います。VLAN タグ付きフレームの場合は、タグの長さ分ずれた位置にある LLC 形式フレームの LSAP や Ethernet 形式フレームのタイプに対してフィルタリング処理を行います。

・ off

VLAN タグ付きフレームの場合に VLAN タグを解析しないでフィルタリング処理を行います。VLAN タグ付きフレームの場合でもタグの長さ分ずらさずにそのままフィルタリング処理を行うため、VLAN タグの TPID が、<value>との比較対象になります。

[動作モード]

構成定義モード(管理者クラス)

[説明]

MAC フィルタを設定します。

本コマンドは、ブリッジ機能を使用する場合にだけ有効です。

指定した条件に一致するフレームを、指定した<action>に従って遮断または通過させます。

MAC フィルタの旧定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
256	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
128	Si-R180B

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

最大定義数	機種
9000	Si-R570 Si-R570B
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
432	Si-R180B

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

[注意]

IP および IPv6 以外のネットワークプロトコル(IPX など)をルーティングしているネットワークでブリッジを使用する場合は、ブリッジによって中継されることでネットワークがダウンすることがあります。ルーティングと同時に使用する場合は、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に設定してください。

[未設定時]

MAC フィルタを設定しないものとみなされ、すべてのフレームが透過します。

6.6.8 lan bridge filter move

[機能]

MAC フィルタの優先順序の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

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

[オプション]

<number>

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

<count>

・ 対象フィルタリング定義番号
優先順序を変更する前のフィルタリング定義の番号を指定します。

<new_count>

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

範囲	機種
0～255	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～127	Si-R180B

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

6.6.9 lan bridge priority

[機能]

帯域制御の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

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

[オプション]

<number>

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

<count>

・ 帯域制御定義番号
帯域制御定義番号を、10 進数で指定します。

範囲	機種
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

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

範囲	機種
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～143	Si-R180B

<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～100000kbps または 1mbps～100mbps の範囲で指定します。全定義の帯域の合計が回線速度を超えた場合は、それぞれ指定した値の比で帯域を割り当てます。指定した値の合計値が回線速度に達しない場合、残った帯域は定義に一致しないデータ用の帯域となります。

「"share" + 数字」で指定した場合、数字で指定した帯域制御定義番号で定義された帯域を共有します。この場合、指定する数字は自分自身の帯域制御定義番号より小さい、すでに定義されているものを指定しなければなりません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

帯域制御を設定します。任意の ACL 番号を指定して、割り当てる帯域を指定します。

ACL 参照定義は、ほかの ACL 参照定義(IP フィルタ、TOS 書き換えなど)を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570 Si-R570B
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
432	Si-R180B

[注意]

シェーピングを使用しない場合、帯域制御は有効に動作しません。

[未設定時]

帯域制御を行わないものとみなされます。

6.7 VRRP 関連情報

6.7.1 lan vrrp use

[機能]

VRRP 動作モードの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<mode>

VRRP 機能を使用するかどうかを指定します。

・ on
VRRP を使用する場合に指定します。
<number>で指定した LAN インタフェースで VRRP が機能します。

・ off
VRRP を使用しない場合に指定します。
<number>で指定した LAN インタフェースで VRRP は機能しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

この LAN インタフェースで、VRRP 機能を使用するかどうかを設定します。
VRRP 機能を使用しないと設定した場合、<number>で指定した LAN インタフェースでは VRRP 機能が動作しません。

[未設定時]

VRRP 機能を使用しないものとみなされます。

```
lan <number> vrrp use off
```

6.7.2 lan vrrp auth

[機能]

VRRP-AD の認証方法と認証パスワードの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

6.7.3 lan vrrp group id

[機能]

VRRP グループの設定

[適用機種]

Si-R570 | Si-R570B | Si-R370 | Si-R370B | Si-R260B | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[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。

<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 ip6 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 ip6"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。

6.7.4 lan vrrp group ad

[機能]

VRRP-AD の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

6.7.5 lan vrrp group preempt

[機能]

プリエンプトモードの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

6.7.6 lan vrrp group trigger ifdown

[機能]

インタフェースダウントリガの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～49	Si-R180B

<interface>

トリガ対象インタフェースを指定します。

・ インタフェース名
lan または rmt インタフェースを以下の範囲で指定します。

範囲	機種
lan0～lan19 rmt0～rmt999	Si-R570 Si-R570B
lan0～lan19 rmt0～rmt499	Si-R370 Si-R370B
lan0～lan19 rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
lan0～lan9 rmt0～rmt49	Si-R180B

・ 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。

6.7.7 lan vrrp group trigger route

[機能]

ルートダウントリガの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～49	Si-R180B

<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～rmt999	Si-R570 Si-R570B
lan0～lan19 rmt0～rmt499	Si-R370 Si-R370B
lan0～lan19 rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
lan0～lan9 rmt0～rmt49	Si-R180B

・ 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。

6.7.8 lan vrrp group trigger node

[機能]

ノードダウントリガの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～49	Si-R180B

<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。

・ インタフェース名
rmt インタフェースを以下の範囲で指定します。

範囲	機種
rmt0～rmt999	Si-R570 Si-R570B
rmt0～rmt499	Si-R370 Si-R370B

範囲	機種
rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
rmt0～rmt49	Si-R180B

<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。

・ 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。
anyを指定した場合、送出先インタフェースは経路情報に依存します。

<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。

6.7.9 lan vrrp group action

[機能]

VRRP 状態変化に対するアクションの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] vrrp group <vrrp_number> action <action_no> <state>online lan [<lan_number>]

lan [<number>] vrrp group <vrrp_number> action <action_no> <state>online switch [<switch_number> [port <port_number>]]

lan [<number>] vrrp group <vrrp_number> action <action_no> <state>online remote [<remote_number> [ap <ap_number> [id <id> <password>]]]

lan [<number>] vrrp group <vrrp_number> action <action_no> <state>online access-point <ap_name>

lan [<number>] vrrp group <vrrp_number> action <action_no> <state>online template <template_number> uid <user_id>

lan [<number>] vrrp group <vrrp_number> action <action_no> <state>offline lan [<lan_number>]

lan [<number>] vrrp group <vrrp_number> action <action_no> <state>offline switch [<switch_number> [port <port_number>]]

lan [<number>] vrrp group <vrrp_number> action <action_no> <state>offline remote [<remote_number> [ap <ap_number>]]

lan [<number>] vrrp group <vrrp_number> action <action_no> <state>offline access-point <ap_name>

lan [<number>] vrrp group <vrrp_number> action <action_no> <state>offline template interface <interface_name>

lan [<number>] vrrp group <vrrp_number> action <action_no> <state>offline template <template_number> [uid <user_id>]

lan [<number>] vrrp group <vrrp_number> action <action_no> <state>diallock remote [<remote_number>]

lan [<number>] vrrp group <vrrp_number> action <action_no> <state>dialreject remote [<remote_number>]

[オプション]

<number>

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

<vrrp_number>

・ VRRP グループ定義番号
LAN インタフェースに対する VRRP グループ定義の通し番号を、0～1 の 10 進数で指定します。

<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
0～49	Si-R570 Si-R570B
0～29	Si-R370 Si-R370B
0～19	Si-R260B Si-R240B Si-R220C Si-R220D
0～9	Si-R180B

<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、マスタまたはイニシャル状態から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、マスタまたはイニシャル状態から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。

lan, switch, access-point, template interface, template, remote

アクション適用対象の種別を指定します。

・ lan
適用対象を指定された lan とします。
・ switch
適用対象を指定されたスイッチポートとします。
・ access-point
適用対象を接続先名で指定された接続先とします。
・ template interface
適用対象をテンプレート着信で接続している指定されたインタフェースの相手ネットワークとします。
・ template
適用対象を指定されたテンプレート定義によるテンプレートの接続とします。
・ remote
適用対象を指定された相手ネットワークや接続先とします。

<lan_number>

・ lan 定義番号
lan 定義の通し番号を、10 進数で指定します。
複数の lan 定義番号を指定する場合は、", "(カンマ)で区切って指定します。また、範囲指定する場合は、「2-4」のように"-"(ハイフン)を使用して指定します。
lan 定義番号は、","(カンマ)および"-"(ハイフン)を使用して 5 個まで指定できます。
省略時は、すべての lan を指定したものとみなされます。

<switch_number>

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

<port_number>

・ スイッチポート番号
スイッチポートの番号を、10 進数で指定します。
複数のスイッチポートを指定する場合は、", "(カンマ)で区切って指定します。また、範囲指定する場合は、「2-4」のように"-"(ハイフン)を使用して指定します。

<remote_number> ap <ap_number> id <id> <password>

相手定義番号と接続先定義番号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
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～49	Si-R180B

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
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～49	Si-R180B

複数の接続先定義番号を指定する場合は、", "(カンマ)で区切って指定します。また、範囲指定する場合は、「2-4」のように"-"(ハイフン)を使用して指定します。

接続先定義番号は、","(カンマ)および"-"(ハイフン)を使用して 5 個まで指定できます。

id <id>

・ 送信認証 ID

0x21,0x23～0x7e の文字で構成される 64 文字以内の ASCII 文字列を指定します。

<remote_number>、<ap_number>で複数の接続先を指定していない場合に指定できます。

<password>

・ 送信認証パスワード

0x21,0x23～0x7e の文字で構成される 64 文字以内の ASCII 文字列を指定します。

<remote_number>、<ap_number>で複数の接続先を指定していない場合に指定できます。

<ap_name>

・ 接続先名

0x21,0x23～0x7e の文字で構成される 8 文字以内の ASCII 文字列を指定します。

<template_number>

・ テンプレート定義番号

テンプレート定義の通し番号を、10 進数で指定します。

範囲	機種
0～5	Si-R570 Si-R570B Si-R370 Si-R370B
0～2	Si-R240B Si-R220C Si-R220D
0～1	Si-R260B Si-R180B

<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 ISDN(回線交換)/PPPoE 接続であれば offline により回線を切断し、online で発信します。

テンプレートによる接続の場合はアクション適用時に接続があれば offline により回線を切断します。

なお、online および offline の動作は運用コマンドの online および offline と同様です。

[未設定時]

VRRP 状態変化に対するアクションは設定されないものとみなされます。

6.7.10 lan vrrp group vaddr icmp

[機能]

仮想 IP アドレスあて ICMP ECHO パケット受信動作の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

・ accept
仮想 IP アドレスあて ICMP ECHO パケットを受理する場合に指定します。
受理すると指定しても ICMP ECHO 以外の ICMP パケットは破棄します。

・ discard
仮想 IP アドレスあて ICMP ECHO パケットを破棄する場合に指定します。

<src>

仮想 IP アドレスあて ICMP ECHO を受理すると指定した場合に応答パケット送信元 IP アドレスを指定します。
<mode>に discard を指定した場合は、<src>を指定することはできません。
省略時は、virtual を指定したものとみなされます。

・ virtual
応答パケット送信元 IP アドレスに仮想 IP アドレスを使用します。

・ real
応答パケット送信元 IP アドレスにインタフェースアドレスを使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

VRRP の仮想 IP あて ICMP ECHO の受信動作を設定します。
受理すると設定した場合であっても VRRP グループの状態がマスタ状態以外である場合は破棄します。

[未設定時]

仮想 IP アドレスあて ICMP ECHO は受理しないものとみなされます。

```
lan <number> vrrp group <vrrp_number> vaddr icmp discard
```

6.7.11 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。
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。

・ 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。
・ 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。

[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
```

6.7.12 lan vrrp trap

[機能]

IPv4 VRRP が送信する TRAP モードの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

6.8 MPLS 関連情報

6.8.1 lan mpls use

[機能]

MPLS 利用可否の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] mpls use <mode>

[オプション]

<number>

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

<mode>

・ on
MPLS を利用します。
・ off
MPLS を利用しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

MPLS を利用するかどうかを設定します。

[未設定時]

off が選択されたものとして動作します。

```
lan <number> mpls use off
```

6.8.2 lan mpls distribution

[機能]

ラベル配布プロトコルの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] mpls distribution <protocol>

[オプション]

<number>

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

<protocol>

・ ldp
ラベル配布プロトコルに LDP を使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ラベル配布プロトコルを指定します。

[未設定時]

ldp が選択されたものとして動作します。

```
lan <number> mpls distribution ldp
```

6.8.3 lan mpls ldp hello-timers

[機能]

LDP Hello に関するタイマの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] mpls ldp hello-timers <interval> <holdtime>

[オプション]

<number>

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

<interval>

・ Hello 送信間隔のタイマ値
Hello の送信間隔を、1～65535 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のどれかを指定します。

<holdtime>

・ HoldTime のタイマ値
近隣関係の維持を判定するための HoldTime を、1～65534 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のどれかを指定します。
・ infinity
近隣関係の維持を判定するための HoldTime を infinity(0xffff:無限)とします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

LDP 近隣関係の維持に用いられる Hello パケットの送信間隔と HoldTime を設定します。
HoldTime の値は interval の値より小さくすることはできません。
HoldTime の値は interval の値の 3 倍以上を設定することを推奨します。

[注意]

HoldTime は近隣関係にある LDP ルータとネゴシエーションし、値の小さい方が採用されますが、送信間隔はネゴシエーションしないため、相手 LSR のタイマ設定と自装置のタイマ設定を一致させておくことを推奨します。

[未設定時]

interval が 5 秒、HoldTime が 15 秒として動作します。

```
lan <number> mpls ldp hello-timers 5s 15s
```

6.8.4 lan mpls ldp keepalive-timers

[機能]

LDP KeepAlive に関するタイマの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] mpls ldp keepalive-timers <interval> <timeout>

[オプション]

<number>

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

<interval>

・ KeepAlive 送信間隔のタイマ値
KeepAlive の送信間隔を、1～65535 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のどれかを指定します。

<timeout>

・ KeepAlive タイムアウトのタイマ値
LDP セッションの維持を判定するためのタイムアウト時間を、1～65535 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のどれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

LDP セッションの維持に用いられる KeepAlive メッセージの送信間隔とタイムアウトを設定します。
timeout の値は interval の値より小さくすることはできません。
timeout の値は interval の値の 3 倍以上を設定することを推奨します。

[注意]

タイムアウトは近隣関係にある LDP ルータとネゴシエーションし、値の小さい方が採用されますが、送信間隔はタイムアウトのネゴシエーション結果の 3 分の 1 の値とこのコマンドで設定された送信間隔とを比較し、値が小さい方が送信間隔として採用されます。

[未設定時]

interval が 1 分、timeout が 3 分として動作します。

```
lan <number> mpls ldp keepalive-timers 1m 3m
```

6.8.5 lan mpls ldp advertisement

[機能]

LDP ラベル広報方式の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] mpls ldp advertisement <mode>

[オプション]

<number>

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

<mode>

・ dod
Downstream On Demand を使用します。
・ du
Downstream Unsolicited を使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

LDP のラベル広報方式を指定します。

[未設定時]

du が選択されたものとして動作します。

```
lan <number> mpls ldp advertisement du
```

6.8.6 lan mpls ldp retention

[機能]

LDP ラベル保持方式の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] mpls ldp retention <mode>

[オプション]

<number>

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

<mode>

・ liberal
Liberal Label Retention Mode を使用します。
・ conservative
Conservative Label Retention Mode を使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

LDP のラベル保持方式を指定します。

[未設定時]

liberal が選択されたものとして動作します。

```
lan <number> mpls ldp retention liberal
```

6.8.7 lan mpls ldp interface-label

[機能]

PHP の無効化

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] mpls ldp interface-label <mode>

[オプション]

<number>

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

<mode>

・ off
インタフェースの IP アドレスにラベルを割り当てません。

・ on
インタフェースの IP アドレスにラベルを割り当てます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

インタフェースの IP アドレスに対してラベルを割り当てるかどうかを指定します。
割り当てた場合は、インタフェースあての LSP の PHP を無効にすることができます。

[注意]

MPLS トンネル接続機能を使用する場合、自側エンドポイントと IP アドレスが同一のとき、本設定によらず、PHP 機能は無効となります。

[未設定時]

off が選択されたものとして動作します。

```
lan <number> mpls ldp interface-label off
```

6.8.8 lan mpls ldp ip transport

[機能]

IPv4 Transport Address の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] mpls ldp ip transport <address>

[オプション]

<number>

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

<address>

・ LDP セッションの送信元 IPv4 アドレス
IPv4 アドレスを指定します。以下の範囲で指定してください。

0.0.0.0
1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

[動作モード]

構成定義モード(管理者クラス)

[説明]

インタフェース単位で LDP が相手との通信に用いる送信元 IPv4 アドレスを分ける必要がある場合に、本装置に設定された IPv4 アドレスを指定します。
0.0.0.0 を指定した場合は、MPLS 情報の設定の IPv4 Transport Address の設定に従います。

[注意]

インタフェース単位で IPv4 Transport Address を設定する場合は、必ず本装置に存在するアドレスを指定してください。本装置に存在しないアドレスをインタフェースに指定した場合は、そのインタフェースでは LDP を使用できません。

[未設定時]

MPLS 情報の設定の IPv4 Transport Address の設定に従います。

```
lan mpls ldp ip transport 0.0.0.0
```

6.8.9 lan mpls l2-circuit vc

[機能]

EoMPLS の VC 情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] mpls l2-circuit vc <vc_id> <address> [<vc_type>]

[オプション]

<number>

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

<vc_id>

・ VC ID の設定
lan 定義の VC ID を 1～4294967295 の 10 進数で指定します。
VC ID は装置内で一意でなければなりません。

<address>

・ 相手装置の IPv4 アドレス
指定可能な範囲は以下のとおりです。

1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

<vc_type>

・ auto
lan 定義から、ethernet か vlan かを自動的に識別します。
・ ethernet
lan 定義に関係なく VC Type を Ethernet に設定します。
・ vlan
lan 定義に関係なく VC Type を Ethernet VLAN に設定します。

省略時は auto を指定したものとみなされます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

EoMPLS 通信の VC ID、相手装置のアドレス、VC Type の設定をします。

<vc_id>は EoMPLS 通信の相手装置と同じ値を指定します。本装置と相手装置で同じ VC ID を持つインタフェースどうしを VC LSP で接続し、EoMPLS 通信を行います。VC ID 装置内で一意になるように設定する必要があります。

<address>は EoMPLS 通信の相手装置の IPv4 アドレスを指定します。相手装置で指定した IPv4 Transport Address と同じ値を指定してください。EoMPLS 通信を行うためには相手装置のアドレスへの経路情報が必要となります。LDP ラベル広報経路情報の設定で、必要な経路情報を LDP で広報するように設定してください。

<vc_type>は、相手装置で同じ VC ID を持つインタフェースと同じ値を指定します。lan 定義と VC Type の設定の関係、および EoMPLS 通信時のフレームの処理は以下のようになります。

本装置の設定		LDP の動作	EoMPLS 通信時のフレームの処理	
lan 定義	<vc_type>の値	ラベル交換で使用する VC Type の値	lan 定義の I/F 側から	VC LSP 側から

本装置の設定		LDP の動作	EoMPLS 通信時のフレームの処理			
			タグなし受信	タグ付き受信	タグなし受信	タグ付き受信
VLAN 定義していない lan 定義	auto	Ethernet	そのまま転送	そのまま転送	そのまま転送	そのまま転送
	ethernet	Ethernet				
	vlan	Ethernet VLAN				
VLAN 定義している lan 定義	auto	Ethernet VLAN	--	そのまま転送	タグを挿入して転送	タグを上書きして転送
	ethernet	Ethernet				
	vlan	Ethernet VLAN				

そのまま転送 ：

フレームを加工しないで、そのまま同じフレームを転送します。

タグを挿入して転送 ：

VC LSP から受信し lan 定義に出力する際に、VLAN ID の設定、VLAN のプライオリティ情報の設定で指定した VLAN タグをフレームに挿入します。

タグを上書きして転送：

VC LSP から受信し lan 定義に出力する際に、フレームに設定されている VLAN タグを、VLAN ID の設定、VLAN のプライオリティ情報の設定で指定した VLAN タグで上書きします。

[注意]

- 本設定で EoMPLS 通信の設定を行った LAN インタフェースでは、自装置あての通信を含めて、すべての通信が EoMPLS 通信による転送の対象となります。

  このため本設定を行った lan 定義では以下の機能は使用できません。

  - IP 機能
  - IPv6 機能
  - ブリッジ機能(STP、MAC 学習、MAC フィルタ機能を含みます)
  - VRRP 機能
  - MPLS 機能(EoMPLS 機能は除きます)
- EoMPLS 通信の相手装置のアドレスが、MPLS LSP トンネルの REMOTE インタフェース設定のトンネルエンドポイントと同じである場合は、REMOTE インタフェースの設定で、MPLS を使用する、LDP Multicast Hello パケットを送信しない、と設定してください。
- EoMPLS 通信を行う場合は、MAC 学習や STP のサポートを行いため、パケットのループが発生する構成は行わないでください。フレームがループし続け通信不可となります。EoMPLS 通信を用いて冗長構成を行う場合は、LAN インタフェース側に、STP などを使用できるスイッチ装置を設置し、フレームがループしないようにしてください。
- VLAN タグが異なる VLAN インタフェースどうしで EoMPLS 通信を行い、タグを上書きして転送する構成の場合は、STP パケットの VLAN タグも上書きされるため、STP が正常に動作しない可能性があります。VLAN インタフェース側で STP を使用する場合は、VLAN タグを本装置と相手装置で一致させてください。

[未設定時]

EoMPLS を使用しないものとみなされます。

6.8.10 lan mpls l2-circuit exp

[機能]

EoMPLS 通信時の Exp 値書き換えの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] mpls l2-circuit exp {vlan|<exp>}

[オプション]

<number>

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

vlan

・ VLAN タグのプライオリティを使用
VLAN タグのプライオリティフィールドから値を取り出し、MPLS SHIM ヘッダの Exp フィールドにそのまま格納します。EoMPLS 通信で転送するフレームが VLAN でない場合は、Exp フィールドには 0 が格納されます。

<exp>

・ 固定の Exp 値を使用
書き換える Exp 値を、0〜7 の 10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

EoMPLS 通信が用いる Exp 値を設定します。

[注意]

VC LSP と Tunnel LSP の両方で同じ Exp 値が格納されます。

[未設定時]

0 が設定されているものとみなされます。

```
lan mpls l2-circuit exp 0
```

6.9 VLAN 関連情報

6.9.1 lan vlan bind

[機能]

VLAN インタフェースの出力先の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] vlan bind [<master_type>] <master_number>

[オプション]

<number>

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

<master_type>

このオペランドは Si-R180B のみ有効なオペランドです。
バインド先の定義種別を以下の中から選択して指定します。省略時は"lan"が指定されたものと扱われます。

・ lan
  lan 定義にバインドします。
・ switch
  スイッチ定義にバインドします。

<master_number>

出力先の lan 定義番号またはスイッチ定義番号を指定します。

[注意]

・ <master_number>に VLAN インタフェースを指定しても動作しません。
・ VLAN インタフェースの削除は通常の物理 LAN インタフェースと同様に delete lan コマンドによって行います。
・ lan vlan bind が設定されていない LAN インタフェースで VLAN のほかの設定を行っても、無効となります。

Si-R180B の場合は以下に注意してください。

・ スイッチポート(SW1～SW4)を利用する LAN インタフェースは必ず VLAN 指定となり、<master_type>に'switch'を指定してください。
・ lan vlan tag vid で指定された VLAN-ID と同じ ID を持つポートを少なくとも 1 つ設定してください。
・ スイッチポートをすべて同一のネットワークとして利用する場合、VLAN ID の設定は不要です。
  その場合、スイッチ情報定義の"switch port vlan"の定義も不要です。
・ スイッチポートを利用する場合、Ethernet 上に送出されるパケットの tag の有無は switch 定義で設定された内容に従います。lan vlan vid で VLAN-ID が設定されている場合でも、switch 定義で untag として定義された場合は、tag なしパケットとして Ethernet 上に送出されます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

<master_number>で指定した物理 LAN インタフェースを出力先として、VLAN インタフェースとして動作します。lan vlan bind の定義がある LAN インタフェースは VLAN インタフェースとして動作し、lan vlan bind の定義がない LAN インタフェースは通常の物理 LAN インタフェースとして動作します。

VLAN インタフェースの IP アドレスは、lan ip address コマンドによって指定します。また VLAN 上で動作するサービスの定義は、通常の物理 LAN インタフェースと同様に lan コマンドで行います。

[未設定時]

VLAN として動作しないで、通常の物理 LAN インタフェースとして動作します。

6.9.2 lan vlan tag vid

[機能]

VLAN ID の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] vlan tag vid <vid>

[オプション]

<number>

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

<vid>

VLAN ID を、1～4094 の 10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

VLAN ID を設定します。

[未設定時]

<vid>に 1 が設定されたものとみなされます。

```
lan <number> vlan tag vid 1
```

6.9.3 lan vlan tag pri

[機能]

プライオリティ情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] vlan tag pri <priority>

[オプション]

<number>

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

<priority>

プライオリティを、0〜7 の 10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

VLAN インタフェースのフレーム送出時に、VLAN タグのプライオリティフィールドに格納される値を設定します。

[未設定時]

<priority>に 0 が設定されたものとみなされます。

```
lan <number> vlan tag pri 0
```

6.9.4 lan vlan tag primap

[機能]

VLAN プライオリティマッピングの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] vlan tag primap <count> <proto> <tos> <priority>

[オプション]

<number>

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

<count>

・ プライオリティマッピング定義番号
プライオリティマッピング定義の通し番号を、10 進数で指定します。

範囲	機種
0～199	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～99	Si-R180B

<proto>

・ ip
IP パケットのプライオリティマッピングを定義します。
・ ip6
IPv6 パケットのプライオリティマッピングを定義します。

<tos>

マッピング対象とする ToS 値(IP)または Traffic Class 値(IPv6)を、0～ff の 16 進数、または"any"で指定します。複数の値を指定する場合は、","(カンマ)で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン)を使用して指定します。TOS/Traffic Class 値は","(カンマ)および"-"(ハイフン)を使用して 10 個まで指定できます。

以下に、有効な記述形式を示します。

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

<priority>

プライオリティを、0～7 の 10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IP の ToS 値、および IPv6 の Traffic Class 値から VLAN のプライオリティ値へのマッピングの設定をします。
VLAN プライオリティマッピング定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
200	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
100	Si-R180B

[未設定時]

VLAN プライオリティマッピング機能を使用しません。

6.10 MAC アドレス認証関連情報

6.10.1 lan macauth use

[機能]

MAC アドレス認証機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] macauth use <mode>

[オプション]

<number>

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

<mode>

・ on
MAC アドレス認証機能を使用します。
・ off
MAC アドレス認証機能を使用しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

MAC アドレス認証機能について設定します。
<mode>が on の場合、パケット送信元端末の MAC アドレス認証を行い、認められた MAC アドレスである場合に中継を行い、認められていなければパケット破棄します。
<mode>が off の場合、MAC アドレス認証機能は無効です。

[注意]

MAC アドレス認証を行うために、AAA ユーザ情報、RADIUS 情報を設定しておく必要があります。
また、本コマンドと同時に、lan macauth aaa <group_id> で認証先データベースの指定を行ってください。
<group_id>を指定しておかないと MAC アドレス認証が動作しませんので、必ず設定してください。

[未設定時]

MAC アドレス認証機能を使用しないものとみなされます。

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

6.10.2 lan macauth expire

[機能]

MAC アドレス認証結果保持時間の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] macauth expire <success_time> <failure_time>

[オプション]

<number>

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

<success_time>

・ 認証成功保持時間
MAC アドレス認証が成功した場合の保持時間を、60～86400 秒の範囲で指定します。
単位は、s(秒)、m(分)、h(時)、d(日)のどれかを指定します。

<failure_time>

・ 認証失敗保持時間
MAC アドレス認証が失敗した場合の保持時間を、60～86400 秒の範囲で指定します。
単位は、s(秒)、m(分)、h(時)、d(日)のどれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

本コマンドは、MAC アドレス認証機能を使用する場合にだけ有効です。
MAC アドレス認証結果の保持時間を設定します。

[未設定時]

MAC アドレス認証結果保持時間として認証成功保持時間 20 分、失敗保持時間 5 分を定義したものとみなされます。

```
lan <number> macauth expire 20m 5m
```

6.10.3 lan macauth aaa

[機能]

MAC アドレス認証先データベースの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] macauth aaa <group_id>

[オプション]

<number>

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

<group_id>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

MAC アドレス認証先データベースのグループ ID を設定します。

[注意]

MAC アドレス認証を行うために、AAA ユーザ情報、RADIUS 情報を設定しておく必要があります。
また、本コマンドで<group_id>を指定しておかないと MAC アドレス認証が動作しませんので、必ず設定してください。

[未設定時]

MAC アドレス認証先データベースを指定していないものとみなされます。

6.10.4 lan macauth security

[機能]

MAC アドレス認証エラー時のセキュリティレベルの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] macauth security <level>

[オプション]

<number>

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

<level>

・ high
認証エラー時のセキュリティレベルを高くします。
・ normal
認証エラー時のセキュリティレベルを通常とします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

MAC アドレス認証が正常に行えなかった場合(サーバ無応答、内部資源不足など)のセキュリティ動作について設定します。
<level>が high の場合は、パケット通過を遮断します。<level>が normal の場合は、パケットを通過させます。

[未設定時]

認証エラー時のセキュリティレベルとして high を定義したものとみなされます。

```
lan <number> macauth security high
```

6.11 SNMP 関連情報

6.11.1 lan snmp trap linkdown

[機能]

linkDown トラップの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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 service コマンドで旧バージョン互換 MIB モードに設定された場合、および snmp trap linkdown 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
```

6.11.2 lan snmp trap linkup

[機能]

linkUp トラップの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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 service コマンドで旧バージョン互換 MIB モードに設定された場合、および snmp trap linkdown 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
```

6.12 LLDP 関連

6.12.1 lan lldp mode

[機能]

LLDP 機能の動作設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan <number> lldp 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。

<mode>

・ LLDP 機能の動作

disable
LLDP 機能は動作しません。

enable
LLDP 情報の送受信を行います。

send
LLDP 情報の送信だけを行います。

receive
LLDP 情報の受信だけを行います。

[動作モード]

構成定義モード(管理者クラス)

[説明]

指定した lan ポートでの LLDP 機能の動作を指定します。

[注意]

LLDP 機能は物理 LAN ポートに対して動作します。物理 LAN ポートにバインドされていない場合は動作しません。
Si-R180B のスイッチポートでは、単独ポートモードか VLAN タグ透過モードの場合にのみ LLDP 機能が動作します。VLAN タグ透過モードの場合、各ポートのオートネゴシエーション設定や状態が独立していて一意に決まらないため、LLDP 送信情報の MAC/PHY Configuration/Status 情報の status は disabled、type は unknown として広報します。

[未設定時]

LLDP 機能は動作させないものとみなされます。

```
lan <number> lldp mode disable
```

6.12.2 lan lldp info

[機能]

LLDP 送信情報の設定

[適用機種]

Si-R570 | Si-R570B | Si-R370 | Si-R370B | Si-R260B | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[入力形式]

```
lan <number> lldp info port-description <mode>
lan <number> lldp info system-name <mode>
lan <number> lldp info system-description <mode>
lan <number> lldp info system-capabilities <mode>
lan <number> lldp info management-address <mode>
lan <number> lldp info port-vlan-id <mode>
lan <number> lldp info port-and-protocol-vlan-id <mode>
lan <number> lldp info vlan-name <mode>
lan <number> lldp info protocol-identity <mode>
lan <number> lldp info mac-phy-configuration-status <mode>
lan <number> lldp info power-via-mdi <mode>
lan <number> lldp info link-aggregation <mode>
lan <number> lldp info maximum-frame-size <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。

port-description

system-name

system-description

system-capabilities

management-address

port-vlan-id

port-and-protocol-vlan-id

vlan-name

protocol-identity

mac-phy-configuration-status

power-via-mdi

link-aggregation

maximum-frame-size

・ LLDP 情報名
OLLDP 情報名(802.1AB の TLV 名)を指定します。

port-description
ポート解説情報(Port Description TLV)

system-name
システム名情報(System Name TLV)

system-description
システム解説情報(System Description TLV)
system-capabilities
システム機能情報(System Capabilities TLV)
management-address
管理アドレス情報(Management Address TLV)
port-vlan-id
ポート VLAN ID 情報(IEEE802.1 Port VLAN ID TLV)
port-and-protocol-vlan-id
プロトコル VLAN ID 情報(IEEE802.1 Port And Protocol VLAN ID TLV)
vlan-name
VLAN 名情報(IEEE802.1 VLAN Name TLV)
protocol-identity
プロトコル VLAN 識別情報(IEEE802.1 Protocol Identity TLV)
mac-phy-configuration-status
MAC/PHY 定義/状態情報(IEEE802.3 MAC/PHY Configuration/Status TLV)
power-via-mdi
MDI 給電情報(IEEE802.3 Power Via MDI TLV)
link-aggregation
リンクアグリゲーション情報(IEEE802.3 Link Aggregation TLV)
maximum-frame-size
最大フレーム長情報(IEEE802.3 Maximum Frame Size TLV)

<mode>

・送信動作
指定した LLDP 情報を送信するかどうかを指定します。
enable
送信します。
disable
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]

指定した LLDP 情報を送信するかどうかを指定します。

[注意]

・protocol-identity は現状、enable を設定しても情報は送信されません。
・Si-R180B で LAN 定義を switch にバインドしている場合、スイッチのポートごとにオートネゴシエーションを設定できますが、LLDP ではひとつのポートとしてしか扱えないためオートネゴシエーション状態を判断することができず、mac-phy-configuration-status を enable に設定して MAC/PHY 定義/状態情報を送信するようにした場合、status は disabled、type は unknown として広報します。

[未設定時]

それぞれの LLDP 情報を送信するものとみなされます。

```
lan <number> lldp info port-description enable
lan <number> lldp info system-name enable
lan <number> lldp info system-description enable
lan <number> lldp info system-capabilities enable
lan <number> lldp info management-address enable
lan <number> lldp info port-vlan-id  enable
lan <number> lldp info port-and-protocol-vlan-id  enable
lan <number> lldp info vlan-name  enable
lan <number> lldp info protocol-identity enable
lan <number> lldp info mac-phy-configuration-status  enable
lan <number> lldp info power-via-mdi enable
lan <number> lldp info link-aggregation enable
lan <number> lldp info maximum-frame-size enable
```

6.12.3 lan lldp vlan

[機能]

LLDP 送信情報で送信する VLAN の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan <number> lldp vlan <vlanidlist>

[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。

vlan <vlanidlist>

port-and-protocol-vlan-id, vlan-name,protocol-identity 送信で、情報を送信する VLAN ID を指定します。
指定がない場合は、全 VLAN に関する情報を通知します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

port-and-protocol-vlan-id, vlan-name, protocol-identity 送信で、LLDP 情報を送信する VLAN ID を指定します。

[未設定時]

情報送信する VLAN について指定がない場合は、すべての VLAN の情報を送信するものとみなされます。

6.12.4 lan lldp notification

[機能]

SNMP Notification Trap 送信情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan <number> lldp notification <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。

<mode>

・ 送信動作
指定された物理ポートの LLDP 情報変更時に SNMP Notification Trap 送信するかどうかを指定します。

enable
送信します。

disable
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]

指定された物理ポートの LLDP 情報が変更になったときに、SNMP Notification Trap 送信するかどうかを設定します。

[注意]

snmp service コマンドで disable または compatible に設定している場合、および snmp trap lldpremtableschange コマンドで disable に設定している場合は、SNMP Notification Trap(lldpRemTablesChange トラップ)は送信されません。

[未設定時]

どのポートの情報も Trap 送信しません。

```
lan <number> lldp notification disable
```

6.13 ARP 認証関連情報

6.13.1 lan arpauth use

[機能]

ARP 認証機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] arpauth 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。

<mode>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

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。

```
lan <number> arpauth use off
```

6.13.2 lan 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] arpauth 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。

<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。

6.13.3 lan arpauth obstruction

[機能]

ARP 認証機能での通信妨害の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] arpauth obstruction <mode> [<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。

<mode>

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

<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 10～43200 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)のどれかを指定します。
省略時は、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。

```
lan <number> arpauth obstruction disable
```

6.13.4 lan 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] arpauth dummymac <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。

<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)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。

[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。

```
lan <number> arpauth dummymac 02:ff:ff:ff:ff:ff
```

6.13.5 lan 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] arpauth expire <success_time> [<failure_time>]

[オプション]

<number>

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

<success_time>

・ 認証成功保持時間
ARP 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)のどれかを指定します。

<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、60～86400 秒の範囲で指定します。
単位は、s(秒)、m(分)、h(時)、d(日)のどれかを指定します。
省略時は、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。

```
lan <number> arpauth expire 20m 20m
```

6.13.6 lan 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan <number> arpauth overflow <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。

<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。

```
lan <number> arpauth overflow failure
```

6.13.7 lan arpauth type

[機能]

ARP 認証の認証プロトコルの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan <number> arpauth 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。

<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されます。

```
lan <number> arpauth type chap-md5
```

6.13.8 lan 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan <number> arpauth authenticated-ip <count> <ip_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。

<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
0～499	Si-R570 Si-R570B Si-R370 Si-R370B
0～249	Si-R180B Si-R260B Si-R240B Si-R220C Si-R220D

<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されます。

6.14 IEEE802.1X 認証関連情報

6.14.1 lan dot1x use

[機能]

IEEE802.1X 認証の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] dot1x 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。

<mode>

IEEE802.1X 認証モードを指定します。

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

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。

[注意]

・ 本モードが有効と指定された場合、dot1x mode 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。
・ 同一 LAN インタフェースで MAC アドレス認証機能と、同時に使用できません。
・ Si-R180B のスイッチポートでは IEEE802.1X 認証機能を利用できません。
・ 無線 LAN では、IEEE802.11 認証モードが wpa, wpa2, wpa/wpa2 と設定された場合のみ IEEE802.1X 認証機能が必須ですが、その他のモードで IEEE802.1X 認証機能を有効にするとエラーになります。

[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。

```
lan <number> dot1x use off
```

6.14.2 lan dot1x portcontrol

[機能]

IEEE802.1X 認証状態の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] dot1x portcontrol <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。

<mode>

デフォルト認証状態を指定します。

・ auto
認証結果によりポートアクセス制御を行います。
・ force-unauth
常に認証拒否します。
・ force-auth
常に認証許容します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

デフォルト認証状態を設定します。

[注意]

・ デフォルト認証状態として auto 以外を指定した場合、以下のような挙動となります。
- force-unauth が指定された場合
すべての通信が遮断されるため、利用できなくなります。
- force-auth が指定された場合
すべての通信が透過されるため、正規ユーザとして登録されていない端末(Supplicant)でも常に利用が可能となります。

・ 無線 LAN で利用する場合は常に auto が指定されたものとして動作し、本設定は無視されます。

[未設定時]

端末(Supplicant)からの認証情報を元にポートアクセス制御を行うものとみなされます。

```
lan <number> dot1x portcontrol auto
```

6.14.3 lan dot1x quietperiod

[機能]

認証失敗時再認証抑止時間の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] dot1x quietperiod <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。

<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。

[注意]

無線 LAN の場合は、本設定を変更しないでデフォルト値のまま使用してください。

[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)が指定されたものとみなされます。

```
lan [<number>] dot1x quietperiod 1m
```

6.14.4 lan dot1x txperiod

[機能]

認証開始要求送信待ち時間の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] dot1x txperiod <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。

<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。

[注意]

無線 LAN の場合は、本設定を変更しないでデフォルト値のまま使用してください。

[未設定時]

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

```
lan <number> dot1x txperiod 30s
```

6.14.5 lan dot1x supptimeout

[機能]

EAP 応答待ち時間の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] dot1x supptimeout <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。

<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。

[注意]

無線 LAN インタフェースで利用する場合は使用されず本定義は無視され、応答待ち時間は 1 秒、再送回数は 3 回として固定値で動作します。

[未設定時]

EAP 応答待ち時間として 30 秒が指定されたものとみなされます。

```
lan <number> dot1x supptimeout 30s
```

6.14.6 lan dot1x maxreq

[機能]

EAP 再送回数の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] dot1x maxreq <retry>

[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。

<retry>

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。

[注意]

無線 LAN インタフェースで利用する場合は使用されず本定義は無視され、応答待ち時間は 1 秒、再送回数は 3 回として固定値で動作します。

[未設定時]

EAP 再送回数として 2 回が指定されたものとみなされます。

```
lan <number> dot1x maxreq 2
```

6.14.7 lan dot1x reauthperiod

[機能]

再認証間隔の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] dot1x reauthperiod <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。

<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、LAN インタフェースの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)のどれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

端末(Supplicant)の再認証間隔を指定します。

[注意]

・ 短い再認証間隔設定で同時に複数の端末(Supplicant)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。
・ 無線 LAN の場合は、本設定を変更しないでデフォルト値のまま使用してください。

[未設定時]

再認証間隔として 3600 秒(1 時間)が指定されたものとみなされます。

```
lan <number> dot1x reauthperiod 1h
```

6.14.8 lan dot1x aaa

[機能]

参照する AAA 情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] dot1x 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。

<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。

[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。

[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 LAN インタフェースで AAA グループ ID が未設定の場合、その LAN インタフェースでは IEEE802.1X 認証が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。

```
lan <number> dot1x aaa unuse
```

6.14.9 lan dot1x mode

[機能]

IEEE802.1X 認証方式の設定

[適用機種]

Si-R570 | Si-R570B | Si-R370 | Si-R370B | Si-R260B | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[入力形式]

lan [<number>] dot1x mode <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。

<type>

・ default
dot1x mode コマンドで指定された認証方式に従います。
・ mac
MAC アドレスごとの認証を行います。
・ port
ポートごとの認証を行います。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ポートアクセス制御として IEEE802.1X 認証方式を設定します。

[注意]

・ 認証方式としてポートごとの認証を選択し、そのポートに接続される端末(Supplicant)の 1 台が認証許容された場合、同じポートに接続されるほかの端末からのアクセスがすべて透過として扱われます。
・ 本装置の物理ポートにスイッチング HUB などを接続し 1 つの物理ポートで複数の端末を区別して認証する場合は、本コマンドで MAC アドレスごとの認証を行うように設定してください。
・ 無線 LAN で利用する場合は、本コマンドの設定は無効となり、常に MAC アドレスごとの認証を行います。
・ 本コマンドを動的定義変更すると該当ポートの IEEE802.1X 認証状態を初期化します。

[未設定時]

IEEE802.1X 認証方式として dot1x mode コマンドの設定に従うものとみなされます。

```
lan <number> dot1x mode default
```

6.14.10 lan dot1x wol

[機能]

Wake On LAN パケットの転送モードの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lan [<number>] dot1x wol <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。

<mode>

・ on
Wake On LAN パケットの転送を有効にします。
・ off
Wake On LAN パケットの転送を無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

Wake On LAN パケットの転送モードを設定します。

[注意]

無線 LAN インタフェースでは未認証端末あてのパケットは破棄されるため、WOL の利用はできません。

[未設定時]

Wake On LAN パケットの転送が無効と指定されたものとみなされます。

```
lan <number> dot1x wol off
```

第７章　シリアル情報の設定

・ serial 定義番号の指定範囲

本章のコマンドの[オプション] に記載されている<number>(serial 定義番号) に指定する serial 定義の通し番号(10 進数) 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-R220C Si-R220D

7.1 シリアル共通情報

7.1.1 serial use

[機能]

COM ポート動作モードの設定

[適用機種]

Si-R220C Si-R220D

[入力形式]

serial [<number>] use <mode>

[オプション]

<number>

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

<mode>

COM ポートを利用するかどうかを指定します。

・ on
COM ポートを利用する場合に指定します。
・ off
COM ポートを利用しない場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

COM ポートを利用するかどうかを指定します。

[未設定時]

COM ポートを利用しないものとみなされます。

```
serial <number> use off
```

7.1.2 serial speed

[機能]

COM ポート通信速度の設定

[適用機種]

Si-R220C Si-R220D

[入力形式]

serial [<number>] speed <speed>

[オプション]

<number>

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

<speed>

・ 通信速度
9600/19200/38400/57600/115200/230400

[動作モード]

構成定義モード(管理者クラス)

[説明]

COM ポートの通信速度を指定します。

[未設定時]

COM ポートの通信速度が 115200bps とみなされます。

```
serial <number> modem speed 115200
```

7.2 モデム関連情報

7.2.1 serial modem dial

[機能]

ダイヤル方式の設定

[適用機種]

Si-R220C Si-R220D

[入力形式]

serial [<number>] modem dial <type>

[オプション]

<number>

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

<type>

・ tone
トーン式を使用します。
・ pulse
パルス式を使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

モデムでダイヤルするときにトーン式を使用するかパルス式を使用するかを設定します。

[未設定時]

モデムでダイヤルするときにトーン式を使用するものとみなされます。

```
serial <number> modem dial tone
```

7.2.2 serial modem tonedetect

[機能]

ダイヤルトーン検出の設定

[適用機種]

Si-R220C Si-R220D

[入力形式]

serial [<number>] modem tonedetect <mode>

[オプション]

<number>

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

<mode>

・ on
ダイヤルトーンを検出します。
・ off
ダイヤルトーンを検出しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ダイヤルする前にダイヤルトーンを検出するかを設定します。

[未設定時]

ダイヤルする前にダイヤルトーンを検出するものとみなされます。

```
serial <number> modem tonedetect on
```

7.2.3 serial modem speaker mode

[機能]

スピーカモードの設定

[適用機種]

Si-R220C Si-R220D

[入力形式]

serial [<number>] modem speaker mode <mode>

[オプション]

<number>

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

<mode>

・ on
スピーカを ON にします。
・ off
スピーカを OFF にします。
・ dial
スピーカを呼毎に ON にします。
・ setup
スピーカをダイヤル終了からキャリア検出まで ON にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

スピーカをどのタイミングでならすかを定義します。

[未設定時]

スピーカを呼毎に ON にするものとみなされます。

```
serial <number> modem speaker mode dial
```

7.2.4 serial modem speaker volume

[機能]

スピーカ音量の設定

[適用機種]

Si-R220C Si-R220D

[入力形式]

serial [<number>] modem speaker volume <mode>

[オプション]

<number>

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

<mode>

・ high
スピーカ音量を大に設定します。
・ medium
スピーカ音量を中に設定します。
・ low
スピーカ音量を小に設定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

スピーカの音量を設定します。

[未設定時]

スピーカの音量は中とみなされます。

```
serial <number> modem speaker volume medium
```

第 8 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
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～49	Si-R180B

・ 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
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～49	Si-R180B

8.1 相手共通情報

8.1.1 remote name

[機能]

相手ネットワーク名称の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

8.1.2 remote autodial

[機能]

自動ダイヤル可否の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<mode>

自動的にダイヤルするかどうかを指定します。

・enable
送信すべきパケットが発生した場合に、自動ダイヤルを行います。

・disable
送信すべきパケットが発生しても、自動ダイヤルを行いません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

指定した相手に対して、自動的にダイヤルするかどうかを設定します。

[注意]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D の場合は以下に注意してください。
wan isdn autodial で<mode>に disable を指定している場合は、自動ダイヤルを行えません。自動ダイヤルを行う場合は、<mode>に enable を指定しておいてください。

[未設定時]

自動ダイヤルを行うものとみなされます。

```
remote <number> autodial enable
```

8.1.3 remote mtu

[機能]

送信パケット最大長(MTU 値)の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

8.1.4 remote shaping

[機能]

シェーピング機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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-R570 Si-R570B
1～100000 1k～100000k 1m～100m	上記以外

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[注意]

使用する回線が LAN の場合、シェーピングを使用しないと帯域制御機能は有効に動作しません。

[未設定時]

シェーピングを使用しないものとみなされます。

```
remote <number> shaping off
```

8.1.5 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

8.2 接続先情報

8.2.1 remote ap name

[機能]

接続先の名称の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

8.2.2 remote ap move

[機能]

接続先の優先順序の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<ap_number>

・ 対象接続先定義番号
優先順序を変更する接続先定義番号を指定します。

<new_ap_number>

・ 移動先接続先定義番号
対象接続先を移動させる先の接続先定義番号を指定します。
対象接続先は、ここで指定した接続先の前に移動されます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

接続先の順序を変更します。

8.2.3 remote ap datalink type

[機能]

パケット転送方法の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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-R570B Si-R370B	Si-R570 Si-R370	Si-R180B	Si-R260B	Si-R240B	Si-R220C Si-R220D
ISDN	PPP	○	○	-	-	-	○
HSD	PPP	○	○	-	-	-	○
FR	RFC2427 方式	○	○	-	-	-	○
ATM	AAL5(RFC1483)	-	○	-	○	-	-
Ethernet	PPPoE 方式	○	○	○	○	○	○
モデム接続	非同期 PPP	-	-	-	-	-	○
データ通信カード *1)	非同期 PPP	-	-	-	-	○	-

*1) PC カードスロットに挿入したデータ通信カードを利用

・ ip
IP tunnel を使用する場合に指定します。

・ ipsec
IPsec を使用する場合に指定します。

・ overlap
overlap ap として、別 IF からの出力とする場合に指定します。

・ mpls
MPLS LSP を使用する場合に指定します。

・ discard
この接続先利用時にはすべてのパケットが破棄されます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

指定した接続先を利用してパケットを転送する場合の転送方式を設定します。

[未設定時]

転送方式として physical を設定するものとみなされます。

```
remote <number> ap 0 datalink type physical
```

8.2.4 remote ap datalink bind

[機能]

パケット転送回線の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<kind>

・wan
wan 定義によって指定される回線を利用する場合に指定します。
(※Si-R180B では指定できません)

・lan
lan 定義によって指定される回線を利用する場合に指定します。

・serial
serial 定義によって指定される回線を利用する場合に指定します。
(※Si-R220C Si-R220D だけ指定できます)

・any
ISDN を使用するように設定した、すべての wan 定義を指定したものとみなされます。
(※Si-R260B Si-R240B Si-R180B では指定できません)

<conf_number>

wan 定義または lan 定義または serial 定義の定義番号を指定します。

・wan 定義の定義番号
利用する wan 定義の定義番号を、10 進数で指定します。
(※Si-R180B では指定できません)

範囲	機種
0～131	Si-R570 Si-R570B
0～15	Si-R370 Si-R370B Si-R260B
0～1	Si-R240B
0	Si-R220C Si-R220D

・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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～9	Si-R180B

・ serial 定義の定義番号
serial 定義の定義番号を、10 進数で指定します。
(※Si-R220C Si-R220D だけ指定できます)

範囲	機種
0	Si-R220C Si-R220D

[動作モード]

構成定義モード(管理者クラス)

[説明]

指定した接続先定義を利用してパケットを転送する場合の回線を設定します。
本コマンドは、remote ap datalink type の<type>で physical を指定した場合にだけ有効です。

[未設定時]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D の場合は、<kind>に wan を、<conf_number>に 0 を指定するものとみなされます。

```
remote <number> ap 0 datalink bind wan 0
```

Si-R180B の場合は、パケット転送回線を設定しないものとみなされます。

8.2.5 remote ap datalink bundle

[機能]

パケット転送回線のマルチリンク・マスタ回線設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B

[入力形式]

remote [<number>] ap [<ap_number>] datalink bundle <masterap_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。

<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。

<masterap_number>

・ マスタ回線の接続先定義番号
論理リンクを構成する場合、マスタ回線の接続先定義番号を指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

論理リンク構成のバンドル回線として使用する場合、マスタ回線の接続先定義番号を指定します。マスタ回線の接続先定義番号が指定された場合、『remote ap datalink』以外の接続先情報は無視されます。

また、本定義は以下の場合に有効です。

・ マスタ回線が専用線
・ バンドル回線が専用線または ISDN 回線

[注意]

セッション監視が設定されている場合、論理リンクが ISDN 回線だけで維持されている場合でも、セッション監視動作は継続します。ただし、通信負荷によっては ISDN 回線の接続・切断が発生することがります。このような場合は、状況に応じて常時接続設定を行ってください。

また、ダイヤル番号などの接続情報は、マスタ回線 ap 定義に設定してください。

[未設定時]

マスタ回線の接続先定義番号を指定しないものとみなされます。

8.2.6 remote ap recovery

[機能]

接続自動復旧モードの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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>

・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
```

8.2.7 remote ap ip dns

[機能]

DNS サーバアドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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 機能と同時に使用する場合、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
```

8.2.8 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～49	Si-R180B

<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
1000	Si-R570 Si-R570B
500	Si-R370 Si-R370B
100	Si-R260B Si-R240B Si-R220C Si-R220D
50	Si-R180B

[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。

8.2.9 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～49	Si-R180B

[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。

8.2.10 remote ap limit charge

[機能]

課金累計制限の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

remote [<number>] ap [<ap_number>] limit charge <charge>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
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。

<charge>

・課金累計上限
課金累計の上限金額を、0～999999 の 10 進数で指定します。
0 を指定した場合は、上限を設定しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

指定した接続先に対する課金累計の上限値を設定します。
発信時に、接続先に対する課金累計が指定した上限値を超えていた場合は、この接続先に対する自動発信を行いません。次の優先度の接続先に対して処理を移します。

[未設定時]

課金累計の上限値を設定しないものとみなされます。

```
remote <number> ap <ap_number> limit charge 0
```

8.2.11 remote ap limit time

[機能]

接続時間累計制限の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R240B Si-R220C Si-R220D

[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。

<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。

<time>

・接続時間累計上限
接続時間累計の上限時間を、0 秒～999 時間の範囲で指定します。
単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。
0 秒を指定した場合は、上限を設定しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

指定した接続先に対する接続時間累計の上限値を設定します。
発信時に、この接続先に対する接続時間累計が指定した上限値を超えていた場合は、この接続先に対する自動発信を行いません。次の優先度の接続先に対して処理を移します。

[未設定時]

接続時間累計の上限値を設定しないものとみなされます。

```
remote <number> ap <ap_number> limit time 0s
```

8.2.12 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-R240B

[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。

<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。

<time>

・ 強制切断を行う累計接続時間
累計接続時間の上限値を、0 秒～999 時間の範囲で指定します。
単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。
0 秒を指定した場合は、累計接続時間による強制切断を行いません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

指定した接続先に対する強制切断を行う累計接続時間を設定します。
接続中に、この接続先に対する累計接続時間が指定した上限値を超えていた場合は、切断し、以降の手動および自動発信を行いません。

[注意]

本コマンドはデータ通信カード接続時に有効です。

[未設定時]

指定した接続先に対する強制切断を行う累計接続時間を設定しないものとみなされます。

```
remote <number> ap <ap_number> disconnect time 0s
```

8.2.13 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-R240B

[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。

<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。

<packet>

・ 強制切断を行う累計パケット数
累計パケット数の上限値を 0～1000000000 の範囲で指定します。
0 を指定すると累計パケット数による強制切断を行いません。

<algorithm>

累計パケット数の計算方法を指定します。

・ per128
累計送受信バイト数(PPP パケット長)を 128 で割った値を累計パケット数とします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

指定した接続先に対する強制切断を行う累計パケット数を設定します。
接続中に、この接続先に対する累計パケット数が指定した上限値を超えていた場合は、切断し、以降の手動および自動発信を行いません。

[注意]

本コマンドはデータ通信カード接続時に有効です。

[未設定時]

指定した接続先に対する強制切断を行う累計パケット数を設定しないものとみなされます。

```
remote <number> ap <ap_number> disconnect packet 0 per128
```

8.2.14 remote ap ppp auth type

[機能]

認証方法の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[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。

<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。

<authtype>

認証プロトコルのタイプを指定します。

・off
認証を要求しない場合に指定します。

・pap
PAP による認証を要求する場合に指定します。

・chap_md5
MD5-CHAP による認証を要求する場合に指定します。

・any
MD5-CHAP または PAP による認証を要求し、実際に利用する認証プロトコルはネゴシエーションによって決定する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

接続時に要求する認証プロトコルのタイプを設定します。
ここでの設定は、着信し、かつ CLID 相手判定が行われた場合に有効となります。

[未設定時]

着信時の認証プロトコルに MD5-CHAP または PAP を用います。

```
remote <number> ap 0 ppp auth type any
```

8.2.15 remote ap ppp auth send

[機能]

送信認証情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<id>

・認証 ID
認証 ID を、0x21,0x23～0x7e の文字で構成される 64 文字以内の文字列で指定します。

<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 64 文字以内の文字列を指定します。
show コマンドで表示される暗号化された認証パスワード文字列を encrypted とともに指定することもできます。その場合、表示された文字列をそのまま正確に入力してください。文字列は 64 文字を超えていてもかまいません。

・暗号化された認証パスワード
show コマンドで表示される暗号化された認証パスワードを encrypted と共に指定します。
show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

・暗号化認証パスワード指定
<password>に暗号化された認証パスワードを設定する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

指定した接続先に接続するときに送信する認証情報(認証 ID およびパスワード)を設定します。

[注意]

認証 ID およびパスワードが設定されていない場合、接続相手からの認証要求を拒否します。show コマンドでは、暗号化された認証パスワードが encrypted と共に表示されます。

[未設定時]

送信する認証情報を定義しないものとみなされます。

8.2.16 remote ap ppp auth receive

[機能]

受諾認証情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R240B Si-R220C Si-R220D

[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。

<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。

<id>

・認証 ID
認証 ID を、0x21,0x23～0x7e の文字で構成される 64 文字以内の文字列で指定します。

<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 64 文字以内の文字列を指定します。
show コマンドで表示される暗号化された認証パスワードを encrypted と共に指定します。
show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

・暗号化認証パスワード指定
<password>に暗号化された認証パスワードを設定する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

認証プロトコル使用時に受諾する、認証情報(認証 ID および認証パスワード)を設定します。

[注意]

show コマンドでは、暗号化された認証パスワードが encrypted と共に表示されます。

[未設定時]

受諾する認証情報を設定しないものとみなされます。

8.2.17 remote ap ppp mp use

[機能]

発信時の MP 利用の可否の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

remote [<number>] ap [<ap_number>] ppp mp use <mode>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
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>

MP を利用するかどうかを指定します。

・ off
MP を利用しない場合に指定します。

・ on
MP を利用する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

発信時に MP を利用するかどうかを設定します。
着信時は、CLID 相手判定によって指定した接続先への接続が決定された場合に、MP を利用するかどうかを設定します。

[未設定時]

MP を利用しないものとみなされます。

```
remote <number> ap 0 ppp mp use off
```

8.2.18 remote ap ppp mp bap use

[機能]

発信時の BAP/BACP 利用の可否の設定

[適用機種]

Si-R570 | Si-R570B | Si-R370 | Si-R370B | | | Si-R220C | Si-R220D |

[入力形式]

remote [<number>] ap [<ap_number>] ppp mp bap use <mode>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
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>

BAP/BACP を利用するかどうかを指定します。

・ off
BAP/BACP を利用しない場合に指定します。

・ on
BAP/BACP を利用する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

MP を利用する場合に BAP/BACP を利用するかどうかを設定します。
着信時は、CLID 相手判定によってこの接続先への接続が決定された場合に、BAP/BACP を利用するかどうかを設定します。

[未設定時]

BAP/BACP を利用しないものとみなされます。

```
remote <number> ap 0 ppp mp bap use off
```

8.2.19 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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。

8.2.20 remote ap pppoe svname

[機能]

サービスネーム(Service-Name)の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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。

8.2.21 remote ap dial number

[機能]

接続先の電話番号の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R240B Si-R220C Si-R220D

[入力形式]

remote [<number>] ap [<ap_number>] dial <count> number<dial_number> [<subaddress>]

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
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。

<count>

ダイヤル定義番号として、以下のどれかを指定します。

・ 0
・ 1
・ 2

<dial_number>

・ 相手電話番号
相手の電話番号を、0～9 の数字と、*、#、-、(、)、\ の文字で構成される 32 桁以内の ASCII 文字列で指定します。

<subaddress>

・ 相手サブアドレス
相手のサブアドレスを、0x21,0x23～0x7e の文字で構成される 19 桁以内の ASCII 文字列で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

接続先の電話番号を設定します。

[注意]

Si-R370 Si-R370B Si-R220C Si-R220D は PIAFS 接続に対応しています。PIAFS(64Kbps)着信時は、<subaddress>で設定した相手サブアドレスは無視されます。

[未設定時]

接続先の電話番号を設定しないものとみなされます。

8.2.22 remote ap dial speed

[機能]

接続先の通信速度の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

remote [<number>] ap [<ap_number>] dial <count> speed <speed> [<carrier>]

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
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。

<count>

ダイヤル定義番号として、以下のどれかを指定します。

・ 0
・ 1
・ 2

<speed>

通信速度、通信手順を指定します。"PIAFS" および "PIAFS64K" は PIAFS 対応の Si-R370 Si-R370B Si-R220C Si-R220D でだけ指定できます。

・ 64K
同期 PPP 64Kbps の場合に指定します。
・ PIAFS
PIAFS(32Kbps)接続の場合に指定します。
・ PIAFS64K
PIAFS(64Kbps)接続の場合に指定します。

<carrier>

通信速度に "PIAFS64K" を指定した場合に通信事業者を指定します。
省略時は、"docomo" を指定したものとみなされます。
なお、通信速度に "PIAFS64K" 以外を指定した場合は、本パラメタを指定しないでください。

・ docomo
NTT DoCoMo の PIAFS(64Kbps)接続の場合に指定します。
・ ddip
ウィルコム(旧 DDI Pocket)の PIAFS(64Kbps)接続の場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

接続先の通信速度および通信手順を設定します。

[未設定時]

通信速度に 64kbps を指定したものとみなされます。

```
remote <number> ap 0 dial <count> speed 64K
```

8.2.23 remote ap called accept

[機能]

接続先からの着信許可の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R240B Si-R220C Si-R220D

[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。

<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。

<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
```

8.2.24 remote ap called clid

[機能]

CLID 相手判断利用の可否の設定

[適用機種]

Si-R570 | Si-R570B | Si-R370 | Si-R370B | | | Si-R220C | Si-R220D | |

[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。

<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>

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
```

8.2.25 remote ap called number

[機能]

CLID の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[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。

<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。

<called_number>

相手電話番号

・相手電話番号
相手の電話番号を、0〜9 の数字と、*、#、-、(、)、\ の文字で構成される 32 桁以内の ASCII 文字列で指定します。

・any
着信時の CLID 相手判定に、"remote ap dial number"で設定した相手電話番号を使用する場合に指定します。

<subaddress>

・相手サブアドレス
相手のサブアドレスを、0x21,0x23〜0x7e の文字で構成される 19 桁以内の ASCII 文字列で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

CLID 相手判定で、チェックする番号を設定します。

[注意]

Si-R370 Si-R370B Si-R220C Si-R220D は PIAFS 接続に対応しています。PIAFS(64Kbps)着信時には、<subaddress> で設定した相手サブアドレスは無視されます。

[未設定時]

着信時の CLID 相手判定に、"remote ap dial number"で設定された相手電話番号を使用します。

```
remote <number> ap 0 called number any
```

8.2.26 remote ap connect priority

[機能]

接続優先制御の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

ISDN の場合は、自装置からの発信接続と相手装置からの着信接続が競合した場合に、どちらの接続を優先して接続するかを設定します。

off を設定した場合は、両方の接続処理が行われます。

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、ISDN では接続できない場合があり、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
```

8.2.27 remote ap idle

[機能]

無通信監視タイマの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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)のどれかを指定します。
0 秒を指定した場合は、監視を行いません。

<direction>

・省略
送信パケット、および受信パケットを通信監視の対象とします。
・send
送信パケットだけを通信監視の対象とします。受信パケットは監視対象とはなりません。
・receive
受信パケットだけを通信監視の対象とします。送信パケットは監視対象とはなりません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

指定した接続先と接続したときの無通信監視時間を設定します。
<time>で設定された間、監視対象となるパケットがない場合に、無通信として回線を切断します。

[未設定時]

無通信監視を行わないものとみなされます。

```
remote <number> ap <ap_number> idle 0d
```

8.2.28 remote ap step

[機能]

平日昼間時間帯の課金単位時間の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R240B Si-R220C Si-R220D

[入力形式]

remote [<number>] ap [<ap_number>] step <time>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
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。

<time>

・ 課金単位時間
平日昼間時間帯(月～金曜日 8:00～19:00)の課金単位時間(秒)の 10 倍の値を、0～36000 の 10 進数で指定します(例: 180 秒=1800、16.5 秒=165)。
0 を指定した場合は、課金単位に応じた接続保持を行いません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ISDN 回線を利用して通信するときの平日昼間時間帯(月～金曜日 08:00～19:00)の課金単位時間を設定します。
課金単位時間を設定すると、無通信の場合でも接続時間が設定値の整数倍になるまで接続を保持します。

[注意]

課金単位時間を設定する場合、本装置の時刻を正しく設定してください。祝日の料金には対応していません。

[未設定時]

課金単位時間を設定しないものとみなされます。

8.2.29 remote ap step2

[機能]

夜間・休日時間帯の課金単位時間の設定

[適用機種]

Si-R570 | Si-R570B | Si-R370 | Si-R370B | | Si-R240B | Si-R220C | Si-R220D |

[入力形式]

remote [<number>] ap [<ap_number>] step2 <time2>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
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。

<time2>

・ 課金単位時間
夜間・休日時間帯(月～金曜日 19:00～23:00)、土/日曜日(08:00～23:00)の課金単位時間(秒)の 10 倍の値を、0～36000 の 10 進数で指定します(例: 180 秒=1800、16.5 秒=165)。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ISDN 回線を利用して通信するときの夜間・休日時間帯(月～金曜日 19:00～23:00、土/日曜日 08:00～23:00)の課金単位時間を設定します。課金単位時間を設定すると、無通信の場合でも接続時間が設定値の整数倍になるまで接続を保持します。

[注意]

課金単位時間を設定する場合、本装置の時刻を正しく設定してください。
この設定は、"remote ap step"を設定した場合にだけ有効です。祝日の料金には対応していません。

[未設定時]

課金単位時間を設定していないものとみなされ、"remote ap step"で設定した値が使用されます。

8.2.30 remote ap step3

[機能]

深夜時間帯の課金単位時間の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R240B Si-R220C Si-R220D

[入力形式]

remote [<number>] ap [<ap_number>] step3 <time3>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
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。

<time3>

・ 課金単位時間
深夜時間帯(全日 23:00～08:00)の課金単位時間(秒)の 10 倍の値を、0～36000 の 10 進数で指定します(例:180 秒=1800、16.5 秒=165)。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ISDN 回線を利用して通信するときの深夜時間帯(全日 23:00～08:00)の課金単位時間を設定します。課金単位時間を設定すると、無通信の場合でも接続時間が設定値の整数倍になるまで接続を保持します。

[注意]

課金単位時間を設定する場合、本装置の時刻を正しく設定してください。
この設定は、"remote ap step"を設定した場合にだけ有効です。祝日の料金には対応していません。

[未設定時]

課金単位時間を設定していないものとみなされ、"remote ap step2"で設定した値が使用されます。この設定もない場合は、"remote ap step"で設定した値が使用されます。

8.2.31 remote ap keep

[機能]

回線接続保持機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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、remote ap datalink type の<type>で physical または ipsec を指定した場合にだけ有効です。
"connect"のときには回線接続保持の方式として、常時接続機能による制御を行います。

[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。

[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
```

8.2.32 remote ap fr dlci

[機能]

フレームリレーの DLCI の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

remote [<number>] ap <ap_number> fr dlci <dlci_number>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
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。

<dlci_number>

・ DLCI
自局で使用する DLCI を、16～991 の 10 進数で指定します。
なお、設定を削除する場合は、0 を指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

フレームリレーの DLCI(データリンクコネクション識別子)を設定します。
フレームリレーを使用する場合は、本コマンドを必ず実行してください。

[未設定時]

DLCI を設定しないものとみなされます。

8.2.33 remote ap fr cir

[機能]

フレームリレーの CIR の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

remote [<number>] ap <ap_number> fr cir <cir>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
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。

<cir>

・ CIR 値
CIR 値を、0～アクセス速度/2 で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

フレームリレーの、DLCI ごとの CIR 値(認定情報速度)を設定します。

[未設定時]

CIR 値として 0 を指定したものとみなされます。

```
remote <number> ap <ap_number> fr cir 0
```

8.2.34 remote ap atm vci

[機能]

VCC の VCI 値の設定

[適用機種]

Si-R570 Si-R370 Si-R260B

[入力形式]

remote [<number>] ap [<ap_number>] atm vci <vci_value>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
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。

<vci_value>

・ VCI 値
VCC の VCI 値を以下の範囲で指定します。
なお、設定を削除する場合は、0 を指定します。

機種	拡張モジュール	範囲
Si-R570	ATM25M 拡張モジュール L2 ATM155M 拡張モジュール L2	32～4095 32～2047
	ATM25M 拡張モジュール H1 ATM155M 拡張モジュール H1	32～1023
Si-R370	ATM25M 拡張モジュール L2 ATM155M 拡張モジュール L2	32～4095 32～2047
Si-R260B		32～4095

[動作モード]

構成定義モード(管理者クラス)

[説明]

VCC(Virtual Channel Connection)で使用する VCI 値を設定します。
また、拡張モジュール単位で定義可能な VCC 数は以下のとおりです。
装置全体で定義可能な VCC 数は「仕様一覧」のシステム最大値一覧を参照してください。

・ Si-R260B および ATM25M 拡張モジュール L2
20VCC
・ ATM155M 拡張モジュール L2
20VCC
・ ATM25M 拡張モジュール H1
200VCC
・ ATM155M 拡張モジュール H1
200VCC

[未設定時]

VCI 値を設定しないものとみなされます。

8.2.35 remote ap atm rate

[機能]

VCC の VC 速度の設定

[適用機種]

Si-R570 | Si-R370 | Si-R260B

[入力形式]

remote [<number>] ap [<ap_number>] atm rate <rate>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
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。

<rate>

・VC 速度値
VCC の速度を以下の範囲で指定します。

機種	拡張モジュール	範囲
Si-R570	ATM25M 拡張モジュール L2 ATM155M 拡張モジュール L2	64k～ 25m:8k 刻み、または 50k 刻み
	ATM25M 拡張モジュール H1	64k～ 25m:8k 刻み、または 50k 刻み
	ATM155M 拡張モジュール H1	64k～100m:8k 刻み、または 50k 刻み
Si-R370	ATM25M 拡張モジュール L2 ATM155M 拡張モジュール L2	64k～ 25m:8k 刻み、または 50k 刻み
Si-R260B		64k～ 25m:8k 刻み、または 50k 刻み

k と m は単位を表し、k は Kbps を m は Mbps を示します。なお、設定を削除する場合は、0 を指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

VCC(Virtual Channel Connection)の VC 速度を設定します。
VC 速度は VCC が属する VPC の VP 速度を超えないように設定します。

[未設定時]

VC 速度を設定しないものとみなされます。

```
remote <number> ap <ap_number> atm rate 0
```

8.2.36 remote ap atm ast

[機能]

VCC のサービスタイプの設定

[適用機種]

Si-R570 | Si-R370 | Si-R260B

[入力形式]

```
remote [<number>] ap [<ap_number>] atm ast cbr
remote [<number>] ap [<ap_number>] atm ast vbr [<scr> [<mbs>]]
remote [<number>] ap [<ap_number>] atm ast ubrp [<mcr>]
remote [<number>] ap [<ap_number>] atm ast gfrp [<gr>]
```

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
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。

cbr

・ サービスタイプ CBR
サービスタイプとして CBR を指定します。

vbr

・ サービスタイプ VBR
サービスタイプとして VBR を指定します。

ubrp

・ サービスタイプ UBR+
サービスタイプとして UBR+を指定します。
なお、ATM 拡張モジュール H1 では、1-VPC での VP/VC 同時シェーピング時以外に UBR+を指定された場合は、無効となります。

gfrp

・ サービスタイプ GFR+
サービスタイプとして GFR+を指定します。

<scr>

・ 平均速度値
サービスタイプとして VBR を指定したときの平均速度を以下の範囲で指定します。

機種	拡張モジュール	範囲
Si-R570	ATM25M 拡張モジュール L2 ATM155M 拡張モジュール L2	64k～ 25m:8k 刻み、または 50k 刻み
	ATM25M 拡張モジュール H1	64k～ 25m:8k 刻み、または 50k 刻み
	ATM155M 拡張モジュール H1	64k～100m:8k 刻み、または 50k 刻み
Si-R370	ATM25M 拡張モジュール L2 ATM155M 拡張モジュール L2	64k～ 25m:8k 刻み、または 50k 刻み
Si-R260B		64k～ 25m:8k 刻み、または 50k 刻み

k と m は単位を表し、k は Kbps を m は Mbps を示します。0 を指定、または省略時は、装置内部で自動設定されます。

<mbs>

・ 最大バースト長

サービスタイプとして VBR を指定したときの最大バースト長を、1～1400 の 10 進数で指定します。

省略時は、0 を指定したものとみなされ、装置内部で自動設定されます。

<mcr>

・ 最低速度値

サービスタイプとして UBR+を指定したときの最低速度を指定します。

機種	拡張モジュール	範囲
Si-R570	ATM25M 拡張モジュール L2 ATM155M 拡張モジュール L2	64k～ 25m:8k 刻み、または 50k 刻み
	ATM25M 拡張モジュール H1	64k～ 25m:8k 刻み、または 50k 刻み
	ATM155M 拡張モジュール H1	64k～100m:8k 刻み、または 50k 刻み
Si-R370	ATM25M 拡張モジュール L2 ATM155M 拡張モジュール L2	64k～ 25m:8k 刻み、または 50k 刻み
Si-R260B		64k～ 25m:8k 刻み、または 50k 刻み

k と m は単位を表し、k は Kbps を m は Mbps を示します。0 を指定、または省略時は、装置内部で自動設定されます。

<gr>

・ 保証速度値

サービスタイプとして GFR+を指定したときの保証速度を指定します。

機種	拡張モジュール	範囲
Si-R570	ATM25M 拡張モジュール L2 ATM155M 拡張モジュール L2	64k～ 25m:8k 刻み、または 50k 刻み
	ATM25M 拡張モジュール H1	64k～ 25m:8k 刻み、または 50k 刻み
	ATM155M 拡張モジュール H1	64k～100m:8k 刻み、または 50k 刻み
Si-R370	ATM25M 拡張モジュール L2 ATM155M 拡張モジュール L2	64k～ 25m:8k 刻み、または 50k 刻み
Si-R260B		64k～ 25m:8k 刻み、または 50k 刻み

k と m は単位を表し、k は Kbps を m は Mbps を示します。0 を指定、または省略時は、装置内部で VC 速度の 1/10 が自動設定されます。ただし、VC 速度の 1/10 が 64Kbps 未満になる場合は、64Kbps に設定されます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

VCC(Virtual Channel Connection)のサービスタイプ(ATM Service Type)を設定します。

<scr> <mcr> <gr> は VC 速度 を超えないように指定します。

[未設定時]

cbr が設定されたものとみなされます。

```
remote <number> ap <ap_number> atm ast cbr
```

8.2.37 remote ap atm oam

[機能]

VCC の OAM(F5)による制御の設定

[適用機種]

Si-R570 | Si-R370 | Si-R260B

[入力形式]

remote [<number>] ap [<ap_number>] atm oam <mode>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
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>

・on
以下の OAM(F5)の受信を受け付けます。
- OAM(F5)-AIS
- OAM(F5)-RDI
- OAM(F5)-LPB

・off
OAM(F5)の受信を受け付けません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

VCC(Virtual Channel Connection)で OAM(F5)の受信を受け付けるかどうかを設定します。
OAM(F5)の受信を受け付ける場合、OAM(F5)の故障通知による VCC の故障検出が可能です。

[未設定時]

OAM(F5)の受信を受け付けないとみなされます。

```
remote <number> ap <ap_number> atm oam off
```

8.2.38 remote ap atm vcwatch

[機能]

ATM 到達性監視の設定

[適用機種]

Si-R570

[入力形式]

remote [<number>] ap [<ap_number>] atm vcwatch <interval> [<retry>]

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
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。

<interval>

・監視間隔
到達性監視間隔を 3～10 の 10 進数で指定します。単位は秒です。
0 を指定した場合は設定が削除され、監視は行われません。

<retry>

・再確認回数
到達性確認に対する応答がなかった場合の再確認回数を 1～20 の 10 進数で指定します。
省略時は、5 を指定したものとみなされます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ATM レイヤ(レイヤ 2)の到達性確認を行うための動作情報を設定します。

監視間隔ごとに ATM の OAM(F5)を利用して到達性確認を行います。

到達性確認に対して応答がなければ監視間隔後に再確認します。

再確認回数連続して応答がない場合は、システムログに記録するとともに SNMP で異常を通知します。

応答がない間も監視を行い、接続性が再確認できた場合にも、システムログに記録するとともに SNMP で状態変更を通知します。

[注意]

ATM 到達性監視の設定は、ATM25M 拡張モジュール H1、または ATM155M 拡張モジュール H1 に対してだけ有効です。

到達性確認に対して接続先までの中継装置が応答を返すことがあり、接続先までの到達性が確認できない場合があります。

接続先までの到達性を確認したい場合は、レイヤ 3 での到達性を確認する remote ap sessionwatch コマンドを利用することができます。

本機能使用時には、OAM(F5)の受信を受け付けない設定であっても、OAM(F5)の到達性確認に対する応答は行います。

到達性確認の送信には時間がかかり、50 の VCC に対して 1 秒が必要です。ATM 到達性監視を行う VCC が 150 を超える場合は、50 の VCC あたり 1 秒以上になるように監視間隔を設定してください。監視間隔が短い場合は、誤って到達性がないと認識してしまう場合があります。

[未設定時]

ATM 到達性監視をしないものとみなされます。

```
remote <number> ap <ap_number> atm vcwatch 0
```

8.2.39 remote ap ipsec type

[機能]

IPsec 情報のタイプの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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 のみでしか使用できないコマンド一覧
  - remote ap ike port
  - remote ap ike idtype
  - remote ap ike mode
・ IKE Version2 のみでしか使用できないコマンド一覧
  - remote ap ike proposal prf
  - remote ap ike local-idtype
  - remote ap ike remote-idtype
  - remote ap ike remote-id-send
  - remote ap 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
```

8.2.40 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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。

8.2.41 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<protocol>

手動鍵送信用 IPsec SA のセキュリティプロトコルを指定します。

・ none
セキュリティプロトコル未指定

・ esp
暗号

・ ah
認証

[動作モード]

構成定義モード(管理者クラス)

[説明]

手動鍵送信用 IPsec SA の、セキュリティプロトコルの設定を行います。
認証/暗号アルゴリズム定義、セキュリティプロトコル定義と IPsec SA の関係

auth(認証)	encrypt(暗号)	セキュリティプロトコル	IPsec SA
-	-	esp(暗号)	×
-	-	ah(認証)	×
-	-	-	×
○	-	esp(暗号)	×
○	-	ah(認証)	◎
○	-	-	×
-	○	esp(暗号)	◎
-	○	ah(認証)	×
-	○	-	×
○	○	esp(暗号)	◎ESPinAuth(認証付暗号)
○	○	ah(認証)	◎
○	○	-	×

○:定義あり -:定義なし ◎:SA 作成可 ×:SA 作成不可

[未設定時]

手動鍵送信用 IPsec 情報のセキュリティプロトコルは未指定となります。

```
remote <number> ap <ap_number> ipsec send protocol none
```

8.2.42 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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
```

8.2.43 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<enc_algo>

暗号アルゴリズムを指定します。

・ des-cbc
・ 3des-cbc
・ aes-cbc-128
・ aes-cbc-192
・ aes-cbc-256
・ null
・ none

<kind>

鍵種別を指定します。

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

<enc_key>

暗号鍵を指定します。

・ 暗号化されていない暗号鍵
<enc_algo>で指定した暗号アルゴリズムが使用する鍵長未満の鍵を指定した場合は、16 進数鍵では鍵長になるまで 0x0 でパディングされます。
文字列鍵の場合は、0x22(ダブルクォーテーション)を除く[0x20-0x7e]の範囲のコードで構成される ASCII 文字列で指定します。ただし、文字列鍵で 0x20(空白文字)を使用する場合は、文字列鍵を""で囲う必要があります。
以下に、入力範囲を示します。

鍵種別 暗号アルゴリズム	hex 16 進数鍵	text 文字列鍵
des-cbc	1～16 桁	8 文字
3des-cbc	1～48 桁	24 文字
aes-cbc-128	1～32 桁	16 文字
aes-cbc-192	1～48 桁	24 文字

鍵種別 暗号アルゴリズム	hex 16 進数鍵	text 文字列鍵
aes-cbc-256	1～64 桁	32 文字

・ 暗号化された暗号鍵
暗号化された暗号鍵を指定します。
show コマンドで表示される暗号化された暗号鍵を encrypted と共に指定します。
show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

・ 暗号化暗号鍵指定
<enc_key>に暗号化された暗号鍵を指定する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

送信パケットを暗号化するための、暗号アルゴリズムと鍵の設定を行います。
show コマンドでは、暗号化された暗号鍵が encrypted と共に表示されます。
暗号アルゴリズムの"aes-cbc"に続く数字は鍵長を表しています。
数字が大きいほど強固な鍵になりますが、その分処理時間を要します。

・ 手動鍵設定としての暗号アルゴリズム
暗号アルゴリズムが"null"および"none"の場合、暗号鍵は入力できません。

[注意]

・ weak key
手動鍵設定で指定する暗号鍵に、RFC2409 の Appendix A に記載されている weak key を設定した場合、コマンドエラーとなります。
RFC2409 の Appendix A に記載されている weak key(DES, 3DES だけ)

```
0101010101010101, FEFEFEFEFEFEFEFE, 1F1F1F1FE0E0E0E0, E0E0E0E01F1F1F1F,
01FE01FE01FE01FE, FE01FE01FE01FE01, 1FE01FE00EF10EF1, E01FE01FF10EF10E,
01E001E001F101F1, E001E001F101F101, 1FFE1FFE0EFE0EFE, FE1FFE1FFE0EFE0E,
011F011F010E010E, 1F011F010E010E01, E0FEE0FEF1FEF1FE, FEE0FEE0FEF1FEF1
```

3des-cbc の場合は、暗号鍵を 16 桁ごとに 3 つの鍵に分割し、どれかの鍵が weak key となるような指定はできません。

[未設定時]

IPsec によるパケット暗号は行われません。

```
remote <number> ap <ap_number> ipsec send encrypt none
```

8.2.44 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<auth_algo>

認証アルゴリズムを指定します。

・ hmac-md5
・ hmac-sha1
・ none

<kind>

鍵種別を指定します。

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

<auth_key>

認証鍵を指定します。

・ 暗号化されていない認証鍵
<auth_algo>で指定した認証アルゴリズムが使用する鍵長未満の鍵を指定した場合は、16 進数鍵では鍵長になるまで 0x0 でパディングされます。
文字列鍵の場合は、0x22(ダブルクォーテーション)を除く[0x20-0x7e]の範囲のコードで構成される ASCII 文字列で指定します。ただし、文字列鍵で 0x20(空白文字)を使用する場合は、文字列鍵を""で囲う必要があります。
以下に、入力範囲を示します。

鍵種別 認証アルゴリズム	hex 16 進数鍵	text 文字列鍵
hmac-md5	1～32 桁	16 文字
hmac-sha1	1～40 桁	20 文字

・ 暗号化された認証鍵を指定します。
show コマンドで表示される暗号化された認証鍵を encrypted と共に指定します。
show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

・ 暗号化認証鍵指定
<auth_key>に暗号化された認証鍵を指定する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

送信パケットを認証するための、認証アルゴリズムと鍵の設定を行います。
show コマンドでは、暗号化された認証鍵が encrypted と共に表示されます。

・ 手動鍵設定としての認証アルゴリズム
  認証アルゴリズムが"none"の場合、認証鍵は入力できません。

[未設定時]

IPsec によるパケット認証は行われません。

```
remote <number> ap <ap_number> ipsec send auth none
```

8.2.45 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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。

8.2.46 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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
```

8.2.47 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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
```

8.2.48 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<enc_algo>

暗号アルゴリズムを指定します。

・ des-cbc
・ 3des-cbc
・ aes-cbc-128
・ aes-cbc-192
・ aes-cbc-256
・ null
・ none

<kind>

鍵種別を指定します。

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

<enc_key>

暗号鍵を指定します。

・ 暗号化されていない暗号鍵
<enc_algo>で指定した暗号アルゴリズムが使用する鍵長未満の鍵を指定した場合は、16 進数鍵では鍵長になるまで 0x0 でパディングされます。
文字列鍵の場合は、0x22(ダブルクォーテーション)を除く[0x20-0x7e]の範囲のコードで構成される ASCII 文字列で指定します。ただし、文字列鍵で 0x20(空白文字)を使用する場合は、文字列鍵を""で囲う必要があります。
以下に、入力範囲を示します。

鍵種別 暗号アルゴリズム	hex 16 進数鍵	text 文字列鍵
des-cbc	1～16 桁	8 文字
3des-cbc	1～48 桁	24 文字
aes-cbc-128	1～32 桁	16 文字
aes-cbc-192	1～48 桁	24 文字

鍵種別 暗号アルゴリズム	hex 16 進数鍵	text 文字列鍵
aes-cbc-256	1～64 桁	32 文字

・ 暗号化された暗号鍵
暗号化された暗号鍵を指定します。
show コマンドで表示される暗号化された暗号鍵を encrypted と共に指定します。
show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

・ 暗号化暗号鍵指定
<enc_key>に暗号化された暗号鍵を指定する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

受信パケットを暗号化するための、暗号アルゴリズムと鍵の設定を行います。
show コマンドでは、暗号化された暗号鍵が encrypted と共に表示されます。
暗号アルゴリズムの"aes-cbc"に続く数字は鍵長を表しています。
数字が大きいほど強固な鍵になりますが、その分処理時間を要します。

・ 手動鍵設定としての暗号アルゴリズム
暗号アルゴリズムが"null"および"none"の場合、暗号鍵は入力できません。

[注意]

・ weak key
手動鍵設定で指定する暗号鍵に、RFC2409 の Appendix A に記載されている weak key を設定した場合、コマンドエラーとなります。
RFC2409 の Appendix A に記載されている weak key(DES, 3DES だけ)

```
0101010101010101, FEFEFEFEFEFEFEFE, 1F1F1F1FE0E0E0E0, E0E0E0E01F1F1F1F,
01FE01FE01FE01FE, FE01FE01FE01FE01, 1FE01FE00EF10EF1, E01FE01FF10EF10E,
01E001E001F101F1, E001E001F101F101, 1FFE1FFE0EFE0EFE, FE1FFE1FFE0EFE0E,
011F011F010E010E, 1F011F010E010E01, E0FEE0FEF1FEF1FE, FEE0FEE0FEF1FEF1
```

3des-cbc の場合は、暗号鍵を 16 桁ごとに 3 つの鍵に分割し、どれかの鍵が weak key となるような指定はできません。

[未設定時]

IPsec によるパケット暗号は行われません。

```
remote <number> ap <ap_number> ipsec receive encrypt none
```

8.2.49 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<auth_algo>

認証アルゴリズムを指定します。

・ hmac-md5
・ hmac-sha1
・ none

<kind>

鍵種別を指定します。

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

<auth_key>

認証鍵を指定します。

・ 暗号化されていない認証鍵
<auth_algo>で指定した認証アルゴリズムが使用する鍵長未満の鍵を指定した場合は、16 進数鍵では鍵長になるまで 0x0 でパディングされます。
文字列鍵の場合は、0x22(ダブルクォーテーション)を除く[0x20-0x7e]の範囲のコードで構成される ASCII 文字列で指定します。ただし、文字列鍵で 0x20(空白文字)を使用する場合は、文字列鍵を""で囲う必要があります。以下に、入力範囲を示します。

鍵種別 認証アルゴリズム	hex 16 進数鍵	text 文字列鍵
hmac-md5	1～32 桁	16 文字
hmac-sha1	1～40 桁	20 文字

・ 暗号化された認証鍵を指定します。
show コマンドで表示される暗号化された認証鍵を encrypted と共に指定します。
show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

・ 暗号化認証鍵指定
<auth_key>に暗号化された認証鍵を指定する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

送信パケットを認証するための、認証アルゴリズムと鍵の設定を行います。
show コマンドでは、暗号化された認証鍵が encrypted と共に表示されます。

・ 手動鍵設定としての認証アルゴリズム
  認証アルゴリズムが"none"の場合、認証鍵は入力できません。

[未設定時]

IPsec によるパケット認証は行われません。

```
remote <number> ap <ap_number> ipsec receive auth none
```

8.2.50 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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
```

8.2.51 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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。

・ des-cbc
・ 3des-cbc
・ aes-cbc-128
・ aes-cbc-192
・ aes-cbc-256
・ null
・ none

[動作モード]

構成定義モード(管理者クラス)

[説明]

送受信パケットを暗号化/復号化するための、暗号アルゴリズムの設定を行います。
暗号アルゴリズムを複数指定する場合、指定順序にかかわらず以下の優先順位となります。
暗号アルゴリズムの"aes-cbc"に続く数字は鍵長を表しています。
数字が大きいほど強固な鍵になりますが、その分処理時間を要します。

・ aes-cbc-256
・ aes-cbc-192
・ aes-cbc-128
・ 3des-cbc
・ des-cbc
・ null

[未設定時]

IPsec によるパケット暗号は行われません。

```
remote <number> ap <ap_number> ipsec ike encrypt none
```

8.2.52 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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。

・ hmac-md5
・ hmac-sha1
・ none

[動作モード]

構成定義モード(管理者クラス)

[説明]

送受信パケットを認証するための、認証アルゴリズムの設定を行います。
認証アルゴリズムを複数指定する場合、指定順序にかかわらず以下の優先順位となります。

・ hmac-md5
・ hmac-sha1

[未設定時]

IPsec によるパケット認証は行われません。

```
remote <number> ap <ap_number> ipsec ike auth none
```

8.2.53 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<pfs_group>

Diffie-Hellman グループについて指定します。

・ modp768
Diffie-Hellman グループの MODP768(グループ 1)
・ modp1024
Diffie-Hellman グループの MODP1024(グループ 2)
・ modp1536
Diffie-Hellman グループの MODP1536(グループ 5)
・ off
Diffie-Hellman グループを使用しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPsec セッションの鍵素材を保護する、PFS 使用時の DH(Diffie-Hellman)グループの設定を行います。

[未設定時]

PFS による鍵交換データ保護は行いません。セキュア通信を行いたい場合は適切な PFS 使用時の DH グループを設定してください。

```
remote <number> ap <ap_number> ipsec ike pfs off
```

8.2.54 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<lifetime>

・SA 有効時間
SA 有効時間を、600 秒(10 分)～86400 秒(1 日)の範囲で指定します。
単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPsec セッションの通信データを保護する、IPsec SA の SA 有効時間(秒)の設定を行います。

[未設定時]

IPsec SA の有効時間として 8h(8 時間)が設定されたものとして扱います。

```
remote <number> ap <ap_number> ipsec ike lifetime 8h
```

8.2.55 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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
```

8.2.56 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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
```

8.2.57 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-R570 | Si-R570B | Si-R370 | Si-R370B | Si-R260B | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[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。

<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。

<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
```

8.2.58 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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
```

8.2.59 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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
```

8.2.60 remote ap ipsec extension-range

[機能]

拡張 IPsec 対象範囲の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～49	Si-R180B

<src_addr>/<mask>

IPsec 対象となる送信元 IP アドレス、マスクビット数を指定します。

・ IP アドレス/マスクビット数(またはマスク値)
IPsec 対象となる送信元 IP アドレスとマスクビット数の組み合わせを指定します。

・ any4
すべての IPv4 アドレスを IPsec 対象に含めます。
0.0.0.0/0(0.0.0.0/0.0.0.0)と同意。

・ any6
すべての IPv6 アドレスを IPsec 対象に含めます。
::/0 と同意。

<dst_addr>/<mask>

IPsec 対象となるあて先 IP アドレス、マスクビット数を指定します。

・ IP アドレス/マスクビット数(またはマスク値)
IPsec 対象となるあて先 IP アドレスとマスクビット数の組み合わせを指定します。

・ any4
すべての IPv4 アドレスを IPsec 対象に含めます。
0.0.0.0/0(0.0.0.0/0.0.0.0)と同意。

・ any6

すべての IPv6 アドレスを IPsec 対象に含めます。
::/0 と同意。

[動作モード]

構成定義モード(管理者クラス)

[説明]

拡張 IPsec 対象範囲を設定します。
拡張 IPsec 対象範囲定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
1000	Si-R570 Si-R570B
500	Si-R370 Si-R370B
100	Si-R260B Si-R240B Si-R220C Si-R220D
50	Si-R180B

[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。

8.2.61 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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
```

8.2.62 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<kind>

鍵種別を指定します。

・ hex
16 進数鍵を使用します。
・ text
文字列鍵を使用します。
・ dynamic
動的 VPN 機能により配布された共有鍵を使用する場合に指定します。

<shared_key>

共有鍵(事前共有秘密鍵方式)を指定します。

・ 暗号化されていない共有鍵を指定します。
文字列鍵の場合は、0x22(ダブルクォーテーション)を除く[0x20-0x7e]の範囲のコードで構成される ASCII 文字列で指定します。ただし、文字列鍵で 0x20(空白文字)を使用する場合は、文字列鍵をダブルクォーテーション(")で囲う必要があります。
以下に、入力範囲を示します。

鍵種別	16 進数鍵	文字列鍵
共有鍵	1～256 桁	1～128 文字

・ 暗号化された共有鍵を指定します。
show コマンドで表示される暗号化された共有鍵を encrypted と共に指定します。
show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

・ 暗号化共有鍵指定
<shared_key>に暗号化された共有鍵を指定する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SA 確立のネゴシエーションのときに接続相手を認証するための、共有鍵の設定を行います。
show コマンドでは、暗号化された共有鍵が encrypted と共に表示されます。

動的VPN接続を行う場合に限り、<kind>にdynamicを指定することができます。
dynamicを指定した場合は、共有鍵の指定はできません。

[注意]

dynamicは、IPsec情報のタイプの設定でdvpnを指定したときだけ有効となります。

[未設定時]

共有鍵が設定されません。IKEにより鍵交換を行う場合は必ず設定してください。
動的VPN機能を利用してIKEにより鍵交換を行う場合は必ず設定してください。

8.2.63 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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。

8.2.64 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<proposal_number>

・ Proposal 定義番号
Proposal 定義番号として 0-2 の範囲の 10 進数を指定します。
省略時は、0 を指定したものとみなされます。

<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

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
```

8.2.65 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<proposal_number>

・ Proposal 定義番号
Proposal 定義番号として 0-2 の範囲の 10 進数を指定します。
省略時は、0 を指定したものとみなされます。

<enc_algo>

暗号アルゴリズムを指定します。

・ des-cbc
・ 3des-cbc
・ aes-cbc-128
・ aes-cbc-192
・ aes-cbc-256

[動作モード]

構成定義モード(管理者クラス)

[説明]

IKE セッションの送受信パケットを暗号化/復号化するための、暗号アルゴリズムの設定を行います。
コマンドによる定義を行う場合は、必ず設定してください。
IKE セッション用暗号情報設定が未定義ですと IKE が動作しません。

[未設定時]

IKE セッション用暗号情報が設定されません。IKE により鍵交換を行う場合は必ず設定してください。

8.2.66 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<proposal_number>

・ Proposal 定義番号
Proposal 定義番号として 0-2 の範囲の 10 進数を指定します。
省略時は、0 を指定したものとみなされます。

<hash_algo>

認証(ハッシュ)アルゴリズムを指定します。

・ hmac-md5
・ hmac-sha1

[動作モード]

構成定義モード(管理者クラス)

[説明]

IKE セッションのネゴシエーションパケットを認証するための、ハッシュアルゴリズムの設定を行います。

[未設定時]

認証のためのハッシュアルゴリズムに hmac-md5 を指定したものとみなされます。

```
remote <number> ap <ap_number> ike proposal <count> hash hmac-md5
```

8.2.67 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<proposal_number>

・ Proposal 定義番号
Proposal 定義番号として 0-2 の範囲の 10 進数を指定します。
省略時は、0 を指定したものとみなされます。

<pfs_group>

Diffie-Hellman グループについて指定します。

・ modp768
MODP768(グループ 1)の Diffie-Hellman グループ
・ modp1024
MODP1024(グループ 2)の Diffie-Hellman グループ
・ modp1536
MODP1536(グループ 5)の Diffie-Hellman グループ

[動作モード]

構成定義モード(管理者クラス)

[説明]

IKE セッションのネゴシエーションパケットを保護するための、DH(Diffie-Hellman)グループの設定を行います。

[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
```

8.2.68 remote ap ike proposal lifetime

[機能]

IKE 情報の SA 有効時間の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<proposal_number>

・ Proposal 定義番号
Proposal 定義番号として 0-2 の範囲の 10 進数を指定します。
省略時は、0 を指定したものとみなされます。

<lifetime>

・ SA 有効時間
SA 有効時間を、600 秒(10 分)～86400 秒(1 日)の範囲で指定します。
単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IKE セッションのネゴシエーションパケットを保護するための、SA 有効時間(秒)の設定を行います。

[未設定時]

IKE SA の有効時間として 24h(24 時間)が設定されたものとして扱われます。

```
remote <number> ap <ap_number> ike proposal <count> lifetime 24h
```

8.2.69 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<proposal_number>

・ Proposal 定義番号
Proposal 定義番号として 0～2 の範囲の 10 進数を指定します。
省略時は、0 を指定したものとみなされます。

<prf>

Pseudo Random Function について指定します。

・ hmac-md5
・ hmac-sha1

[動作モード]

構成定義モード(管理者クラス)

[説明]

IKE 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。

8.2.70 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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
```

8.2.71 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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
```

8.2.72 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<name>

・自装置識別情報
自装置を識別する名前を指定します。
指定範囲は、1～64 文字です。
識別情報は､0x22(ダブルクォーテーション)を除く[0x21-0x7e]の範囲のコードで構成される ASCII 文字列で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

・IKE 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。

[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。

8.2.73 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<name>

・相手装置識別情報
相手装置を識別する名前を指定します。
指定範囲は、1～64 文字です。
名前は、0x22(ダブルクォーテーション)を除く[0x21-0x7e]の範囲のコードで構成される ASCII 文字列で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

・IKE 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。

[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。

8.2.74 remote ap ike release

[機能]

IPsec/IKE 情報の解放動作の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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>

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。

・ ISDN(回線交換)を使用したときの回線切断時 (※Si-R260B Si-R240B Si-R180B を除く)
・ PPPoE を使用したときの切断時
・ モデムを使用したときの切断時 (※Si-R220C Si-R220D のみ)
・ データ通信カードを使用したときの切断時 (※Si-R240B のみ)

[未設定時]

回線切断時に IKE SA 情報の解放を行うものとみなされます。

```
remote <number> ap <ap_number> ike release on
```

8.2.75 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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>

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。

・ ISDN(回線交換)を使用したとき (※Si-R260B Si-R240B Si-R180B を除く)
・ PPPoE を使用したとき
・ モデムを使用したとき (※Si-R220C Si-R220D のみ)
・ データ通信カードを使用したとき (※Si-R240B のみ)

[未設定時]

IPsec 対象パケットの送信を契機として、IPsec/IKE SA の確立を行うものとみなされます。

```
remote <number> ap <ap_number> ike initial forward
```

8.2.76 remote ap ike sessionwatch

[機能]

IKE セッション監視の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

```
remote [<number>] ap [<ap_number>] ike sessionwatch <address>[<normal_interval>
[<abnormal_interval> [<timeout>]]]
```

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
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。

<address>

・ICMP ECHO パケットのあて先 IP アドレス
ICMP ECHO パケットのあて先 IP アドレスを指定します。
IPsec 対象範囲に含まれる IP アドレスを以下の範囲で指定してください。

1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

また、0.0.0.0 を指定した場合は IKE セッションを監視しないものとみなされます。

<normal_interval>

・ICMP ECHO パケットの正常時送信間隔
ICMP ECHO パケットの正常時送信間隔を、1 秒～60 秒(1 分)の範囲で指定します。
単位は、m(分)、s(秒)のどちらかを指定します。
省略時は、10 秒を指定したものとみなされます。

<abnormal_interval>

・ICMP ECHO パケットの異常時送信間隔
ICMP ECHO パケットの異常時送信間隔を、60 秒～600 秒(10 分)の範囲で指定します。
単位は、m(分)、s(秒)のどちらかを指定します。
省略時は、180 秒(3 分)を指定したものとみなされます。

<timeout>

・ICMP ECHO パケットのタイムアウト時間
ICMP ECHO パケットのタイムアウト時間を、5 秒～180 秒(3 分)の範囲で指定します。単位は、m(分)、s(秒)のどちらかを指定します。
省略時は、5 秒を指定したものとみなされます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IKE セッションの生存確認を行うための動作情報を設定します。
指定したあて先 IP アドレスに対して ICMP ECHO パケットの送受信で生存確認を行います。

あて先 IP アドレスは、IPv4 アドレスのみ指定可能です。

ICMP ECHO パケットの応答が正常に受信できている間は正常時送信間隔で監視を行いますが、ICMP ECHO パケットの応答が受信できなくなると、障害発生とみなし監視先に関連する IPsec/IKE SA を解放し、異常時送信間隔で監視を行います。

ICMP ECHO パケットの応答が受信できたときを復旧とみなし、監視先に関連する IPsec/IKE SA の確立を行い、正常送信間隔での監視に戻ります。

ICMP ECHO パケットのタイムアウト時間は、回線品質が悪いときや高負荷状態により ICMP ECHO パケットの応答が遅延するような状況のときに有効です。

[未設定時]

IKE セッションの生存を監視しないものとみなされます。

```
remote <number> ap <ap_number> ike sessionwatch 0.0.0.0 10s 3m 5s
```

8.2.77 remote ap ike mode

[機能]

IKE Version1 情報の交換モードの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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>

・IKE ネゴシエーションの交換モード
IKE ネゴシエーションの交換モードを指定します。

auto ：
IKE 情報の交換モードを tunnel endpoint address および IKE 情報装置識別情報の設定によって自動判別します。

aggressive ：
IKE 情報の交換モードとして Aggressive Mode を使用します。

main ：
IKE 情報の交換モードとして Main Mode を使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IKE セッションを確立する、IKE ネゴシエーション交換モードの設定を行います。
交換モード、tunnel endpoint address、装置識別情報の設定により、以下の表のように動作します。

tunnel endpoint address の設定	name の設定	mode の設定		
		aggressive	main	auto
tunnel local ○ tunnel remote ○	name local ○ name remote ×	Aggressive (Initiator)	Main	Main
	name local × name remote ○	Aggressive (Responder)	Main	Main
	name local ○ name remote ○	Aggressive*1	Main	Main
	name local × name remote ×	動作しない	Main	Main
tunnel local ×	name local ○	Aggressive	動作しない	Aggressive

tunnel endpoint address の設定	name の設定	mode の設定		
		aggressive	main	auto
tunnel remote ○	name remote ×	(Initiator)		(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
```

8.2.78 remote ap ike bind

[機能]

利用 IKE 情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<kind>

・ 利用する接続先定義番号指定の有無
利用する IKE 情報が設定されている接続先定義番号を指定するかを決定します。

self ：
同一接続先情報の IKE 定義を利用します。

ap ：
<conf_number>で指定された接続先情報の IKE 定義を利用します。

<conf_number>

・ 接続先情報定義番号
利用する IKE 定義がされている接続先情報定義番号として 0 以上の 10 進数を指定します。利用できる接続先情報は同一の相手情報定義内の接続先情報である必要があります。<kind>が self の場合は設定できません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

利用する IKE 定義の接続先情報を設定します。
利用する IKE 定義に指定する接続先情報番号には、有効な IKE 定義が存在する必要があります。
有効な IKE 定義が存在しない場合、<ap_number>の接続先情報は利用できません。
利用する接続先情報の IKE 定義が有効な場合、利用する接続先情報定義は以下のとおりです。

・ 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 sessionwatch
- 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 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 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 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
```

8.2.79 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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>

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、接続先監視機能と同時に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。

[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
```

8.2.80 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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
0～499	Si-R570 Si-R570B
0～249	Si-R370 Si-R370B
0～49	Si-R260B Si-R240B Si-R220C Si-R220D
0～24	Si-R180B

[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。

8.2.81 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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 までの 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。

8.2.82 remote ap ike certificate key

[機能]

IKE セッション用秘密鍵情報

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<key_number>

・ 秘密鍵識別番号
秘密鍵の識別番号を、0～4 までの 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。

8.2.83 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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>

・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
```

8.2.84 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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
```

8.2.85 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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 までの 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
```

8.2.86 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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。

[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。

8.2.87 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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。

[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。

8.2.88 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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
```

8.2.89 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
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
```

8.2.90 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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
```

8.2.91 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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
```

8.2.92 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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
0～5	Si-R570 Si-R570B Si-R370 Si-R370B
0～2	Si-R240B Si-R220C Si-R220D
0～1	Si-R260B Si-R180B

[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。

8.2.93 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<count>

・プレフィックス定義番号

プレフィックスの定義番号を、0から19までの10進数で指定します。

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。

8.2.94 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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。

8.2.95 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ap [<ap_number>] tunnel local <address>

[オプション]

<number>

・相手定義番号

相手ネットワークの通し番号を、10 進数で指定します。

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。

<address>

・自側のトンネルエンドポイントアドレス

自側のトンネルエンドポイントとなる IPv4 アドレスまたは IPv6 アドレスを指定します。本装置に設定されている IP アドレスを指定してください。

指定可能な範囲は以下のとおりです。

IPv4:

1.0.0.1 ～ 126.255.255.254

128.0.0.1 ～ 191.255.255.254

192.0.0.1 ～ 223.255.255.254

IPv6:

::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff

fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

IPv6 DHCP クライアントが取得したプレフィックスを使用する場合は上位を"dhcp@インタフェース名"の形式で指定し、下位 80bit 分を IPv6 アドレス形式で指定します。インタフェース名には、rmt インタフェースを以下の範囲で指定します。

範囲	機種
rmt0～rmt999	Si-R570 Si-R570B
rmt0～rmt499	Si-R370 Si-R370B
rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
rmt0～rmt49	Si-R180B

例)

rmt0 で動作する IPv6 DHCP クライアントが取得した IPv6 プレフィックスを使用する場合の設定例

```
dhcp@rmt0::
dhcp@rmt0::1:2:3:4
```

[動作モード]

構成定義モード(管理者クラス)

[説明]

指定した接続先定義にトンネル利用が設定されている場合に、そのトンネルの自側エンドポイントアドレスを設定します。

トンネルを利用して通信を行う場合は、本コマンドを必ず実行してください。

[注意]

動的VPN機能を利用した構成でIPv6 DHCPクライアントが取得したプレフィックスを使用する場合、プレフィックスが割り当てられるインタフェースと同じ値になるように指定してください。

[未設定時]

自側のトンネルエンドポイントアドレスを設定しないものとみなされます。

8.2.96 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ap [<ap_number>] tunnel remote <address>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
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。

<address>

・相手側のトンネルエンドポイントアドレス
相手側のトンネルエンドポイントとなる IPv4 アドレスまたは IPv6 アドレスを指定します。
指定可能な範囲は以下のとおりです。

IPv4:

1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

IPv6:

::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

[動作モード]

構成定義モード(管理者クラス)

[説明]

指定した接続先定義にトンネル利用が設定されている場合に、そのトンネルの相手側エンドポイントアドレスを設定します。
トンネルを利用して通信を行う場合は、本コマンドを必ず実行してください。

[未設定時]

相手側のトンネルエンドポイントアドレスを設定しないものとみなされます。

8.2.97 remote ap overlap to

[機能]

overlap ap の実際の送出先の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～9	Si-R180B

・ 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
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～49	Si-R180B

[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。

8.2.98 remote ap overlap nexthop

[機能]

overlap ap の転送先 IPv4 ルータの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ap [<ap_number>] overlap nexthop <address>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
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。

<address>

転送先となる IPv4 ルータの IP アドレスを指定します。
以下の範囲で指定してください。

1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

[動作モード]

構成定義モード(管理者クラス)

[説明]

overlap ap 機能を利用して lan にパケットを転送する場合の、転送先 IPv4 ルータの IP アドレスを指定します。
本コマンドは、remote ap datalink type の<type>で overlap を指定し、remote ap overlap to の<kind>で lan を指定した場合にだけ有効です。

[未設定時]

IPv4 転送を行わないものとみなされます。

8.2.99 remote ap overlap nexthop6

[機能]

overlap ap の転送先 IPv6 ルータの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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。

8.2.100 remote ap sessionwatch address

[機能]

接続先監視のアドレス設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<source>

・ICMP ECHO パケットの送信元 IP アドレス
ICMP ECHO パケットの送信元 IP アドレスを指定します。装置に設定されている自側 IPv4/IPv6 アドレスのどれかを指定してください。
指定可能な範囲は以下のとおりです。

IPv4:

1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

IPv6:

::2 ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<destination>

・ICMP ECHO パケットのあて先 IP アドレス
監視対象となる IPv4/IPv6 アドレスを指定します。
<source>と同じプロトコルアドレスで指定してください。
指定可能な範囲は以下のとおりです。

IPv4:

1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

IPv6:

::2 ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

[動作モード]

構成定義モード(管理者クラス)

[説明]

接続先の生存確認を行うための動作情報を設定します。
指定したあて先 IP アドレスに対して ICMP ECHO パケットの送受信で生存確認を行います。

[注意]

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。

・ ISDN 回線を利用する接続先で、常時接続機能を利用していない場合。

・ PPPoE 回線を利用する接続先で、常時接続機能を利用していない場合。

また、IPsec/IKE を利用する接続先で、IKE セッション監視の設定(remote ap ike sessionwatch)が同時に設定されている場合は、IKE セッション監視は動作しないで、接続先監視機能だけが動作します。

[未設定時]

接続先監視機能を利用しないものとみなされます。

8.2.101 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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、正常送信間隔での監視に戻ります。

[注意]

以下の場合では、監視を行いません。

・ ISDN 回線を利用する接続先で、常時接続機能を利用していない場合。
・ PPPoE 回線を利用する接続先で、常時接続機能を利用していない場合。

また、IPsec/IKE を利用する接続先で、IKE セッション監視の設定(remote ap ike sessionwatch)が同時に設定されている場合は、IKE セッション監視は動作しないで、接続先監視機能だけが動作します。

[未設定時]

正常時送信間隔 10 秒、異常時送信間隔 1 分、監視タイムアウト 5 秒、再送間隔 1 秒が指定されたものとして動作します。

```
remote <number> ap <ap_number> sessionwatch interval 10s 1m 5s 1s
```

8.2.102 remote ap sessionwatch ttl

[機能]

接続先監視の TTL/HopLimit 値設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<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。

・ ISDN 回線を利用する接続先で、常時接続機能を利用していない場合。
・ PPPoE 回線を利用する接続先で、常時接続機能を利用していない場合。

また、IPsec/IKE を利用する接続先で、IKE セッション監視の設定(remote ap ike sessionwatch)が同時に設定されている場合は、IKE セッション監視は動作しないで、接続先監視機能だけが動作します。

[未設定時]

送信 TTL/HopLimit 値に 255 が指定されたものとして動作します。

```
remote <number> ap <ap_number> sessionwatch ttl 255
```

8.2.103 remote ap sessionwatch mode

[機能]

接続先監視の動作モード設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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>

監視方式を指定します。

・ always
常時監視を行います。

・ idleonly
無通信状態(送信がない、または受信がない状態)に限り監視を行います。

[動作モード]

構成定義モード(管理者クラス)

[説明]

接続先の生存確認を行うための動作情報を設定します。
ICMP ECHO パケットによる監視を行う期間を指定します。

[注意]

以下の場合では、監視を行いません。

・ ISDN 回線を利用する接続先で、常時接続機能を利用していない場合。
・ PPPoE 回線を利用する接続先で、常時接続機能を利用していない場合。

また、IPsec/IKE を利用する接続先で、IKE セッション監視の設定(remote ap ike sessionwatch)が同時に設定されている場合は、IKE セッション監視は動作しないで、接続先監視機能だけが動作します。

[未設定時]

常時監視が指定されたものとして動作します。

```
remote <number> ap <ap_number> sessionwatch mode always
```

8.2.104 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<count>

・ 応答受信回数
異常状態から正常状態へ復旧するまでの連続応答受信回数を 1～100 の範囲で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

接続先の生存確認を行うための動作情報を設定します。

異常状態から正常状態へ復旧するために必要な連続応答受信回数を設定します。これにより、回線状態が不安定な場合のインタフェースダウン／アップのばたつきを防ぎます。

連続応答待ち状態での ICMP ECHO パケット送信間隔は、正常時送信間隔を使用します。

本装置起動後を含め、回線接続直後に通信可能な状態であっても、必要な回数の応答を受信するまで通信可能にはなりませんので、ご注意ください。

[注意]

以下の場合では、監視を行いません。

・ ISDN 回線を利用する接続先で、常時接続機能を利用していない場合。
・ PPPoE 回線を利用する接続先で、常時接続機能を利用していない場合。

また、IPsec/IKE を利用する接続先で、IKE セッション監視の設定(remote ap ike sessionwatch)が同時に設定されている場合は、IKE セッション監視は動作しないで、接続先監視機能だけが動作します。

[未設定時]

連続応答受信回数に 1 が指定されたものとして動作します。

```
remote <number> ap <ap_number> sessionwatch recovery 1
```

8.2.105 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

<time>

・ 異常時送信開始待ち時間
異常時 ICMP ECHO パケットの送信開始待ち時間を、0 秒～86400 秒(1 日)の範囲で指定します。0 秒が指定された場合は待ち合わせをしません。
単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

接続先の生存確認を行うための動作情報を設定します。
正常状態から異常状態に遷移した場合に、最初の ICMP ECHO パケットを送信するまでの待ち時間を設定します。

[注意]

以下の場合では、監視を行いません。

・ ISDN 回線を利用する接続先で、常時接続機能を利用していない場合。
・ PPPoE 回線を利用する接続先で、常時接続機能を利用していない場合。

また、IPsec/IKE を利用する接続先で、IKE セッション監視の設定(remote ap ike sessionwatch)が同時に設定されている場合は、IKE セッション監視は動作しないで、接続先監視機能だけが動作します。

[未設定時]

異常時の送信開始待ち時間に 0 秒が指定されたものとして動作します。

```
remote <number> ap <ap_number> sessionwatch error-wait 0s
```

8.2.106 remote ap mpls to

[機能]

MPLS LSP の送出先の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ap [<ap_number>] mpls to <kind> <conf_number>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
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。

<kind>

・lan
MPLS LSP の送出先を lan 定義とする場合に指定します。
・remote
MPLS LSP の送出先を remote 定義とする場合に指定します。

<conf_number>

lan 定義、remote 定義の定義番号を指定します。

・lan 定義の定義番号
利用する lan の定義番号を、10 進数で指定します。

範囲	機種
0～19	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～9	Si-R180B

・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
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～49	Si-R180B

[動作モード]

構成定義モード(管理者クラス)

[説明]

指定した接続先定義を利用してパケットを転送する場合の定義を設定します。
本コマンドは、remote ap datalink type の<type>で mpls を指定した場合にだけ有効です。

[未設定時]

MPLS LSP を設定しないものとみなされます。

8.2.107 remote ap mpls nexthop

[機能]

MPLS LSP の次ホップのラベルスイッチルータの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ap [<ap_number>] mpls nexthop <address>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
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。

<address>

次ホップのラベルスイッチルータの IP アドレスを指定します。
以下の範囲で指定してください。

1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

[動作モード]

構成定義モード(管理者クラス)

[説明]

MPLS LSP を利用して lan にパケットを転送する場合の、次ホップのラベルスイッチルータの IP アドレスを指定します。
本コマンドは、remote ap datalink type の<type>で mpls を指定し、remote ap mpls to の<kind>で lan を指定した場合にだけ有効です。

[未設定時]

lan で MPLS LSP を使用しないものとみなされます。

8.2.108 remote ap snmp trap linkdown

[機能]

linkDown トラップの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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>

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 service コマンドで旧バージョン互換 MIB モードに設定された場合、および snmp trap linkdown 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
```

8.2.109 remote ap snmp trap linkup

[機能]

linkUp トラップの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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>

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 service コマンドで旧バージョン互換 MIB モードに設定された場合、および snmp trap linkdown 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
```

8.3 PPP 関連情報

8.3.1 remote ppp compress

[機能]

データ圧縮機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R240B Si-R220C Si-R220D

[入力形式]

remote [<number>] ppp compress <mode>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<mode>

・off
データ圧縮機能を使用しない場合に指定します。

・on
データ圧縮機能を使用する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

データ圧縮機能を使用するかどうか設定します。

[注意]

MP を使用する場合、受信順序制御(remote ppp mp order を参照)を有効にしてください。MP を使用し、かつ受信順序制御を使用しないと定義している場合、ヒストリ機能(高圧縮のための機能)を使用できません。

[未設定時]

データ圧縮機能を使用しないものとみなされます。

```
remote <number> ppp compress off
```

8.3.2 remote ppp mp start

[機能]

MP 利用時の初期接続リンク数の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

remote [<number>] ppp mp start <link>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<link>

・ MP 利用時の初期接続リンク数
MP 利用時の初期接続リンク数を指定します。

範囲	機種
1～23	Si-R570 Si-R570B Si-R370 Si-R370B
1～2	Si-R220C Si-R220D

[動作モード]

構成定義モード(管理者クラス)

[説明]

MP 利用時の初期接続リンク数を設定します。
MP 利用時に自装置から発信する場合、最初から接続を試みるリンク数を設定します。なお、発信に失敗した場合、再試行は行いません。また、最大接続リンク数の設定値を超えて接続は実施しません。

[注意]

以下の条件に一致した場合は、ここで指定したチャネル数まで増加しません。
・ 接続に失敗した場合
・ 最大接続リンク数の設定値より大きい値を設定した場合
・ 論理リンクを構成している場合
また、初期接続のリンク増加時は、最初に接続を行った電話番号に対して発信します。

[未設定時]

初期接続リンク数として 1 を指定したものとみなされます。

```
remote <number> ppp mp start 1
```

8.3.3 remote ppp mp max

[機能]

MP の最大接続リンク数の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B

[入力形式]

remote [<number>] ppp mp max <link>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<link>

・ MP 利用時の最大接続リンク数
MP 利用時の最大接続リンク数を 2～23 の範囲で指定します。

[注意]

接続先回線が複数の場合は、以下のどちらかを行ってください。
・ 自局電話番号の設定および BAP 有効化。
・ 代表取り扱いサービスの契約。
また、以下の場合に最大接続リンク数を超える場合があります。
・ 論理リンク内、最大接続リンク数を超える、専用線が指定されている場合

[動作モード]

構成定義モード(管理者クラス)

[説明]

MP を利用したときの最大接続リンク数を設定します。
また、論理リンクの場合、専用線は 1 リンクとして設定します。

[未設定時]

最大接続リンク数として 2 を指定したものとみなされます。

```
remote <number> ppp mp max 2
```

8.3.4 remote ppp mp divide

[機能]

MP 通信時の最小分割長の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

remote [<number>] ppp mp divide <length>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<length>

・default
最小分割長を 256byte、最小分割単位を 128byte として動作します。
・最小分割長
最小分割長を 1～1524 の範囲で指定します。この値は最小分割単位としても利用されます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

複数チャネルでの MP 通信時の、送信フレームの最小分割長を指定します。
ここで指定した長さ以上の送信フレームは、余り部分を除き、最小分割単位以上となるように均等に分割して送信されます。

[未設定時]

最小分割長として default を指定したものとみなされます。

```
remote <number> ppp mp divide default
```

8.3.5 remote ppp mp traffic use

[機能]

自動チャネル数制御の可否の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

remote [<number>] ppp mp traffic use <mode>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<mode>

・on
スループット BOD の機能を使用します。

・off
スループット BOD の機能を使用しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

スループット BOD 機能を使用するかどうかを設定します。

[未設定時]

スループット BOD 機能を使用しないとみなされます。

```
remote <number> ppp mp traffic use off
```

8.3.6 remote ppp mp traffic increase

[機能]

リンク増加しきい値の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

remote [<number>] ppp mp traffic increase <traffic> <time>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<traffic>

・回線増加しきい値
単位時間当たりのチャネル利用率を、0～100 の 10 進数で指定します。
以下に、回線増加しきい値の計算式を示します。
チャネル利用率(%) = 転送バイト量 ÷ 転送可能バイト数 × 100

<time>

・増加猶予時間
トラフィックが回線増加しきい値を超え続けた場合に、発信するまでの猶予時間を 0～3600 秒の範囲で指定します。
単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

スループット BOD 機能使用時のリンク増加しきい値を設定します。
スループット BOD 機能を使用する場合は、本コマンドを必ず設定してください。

[注意]

指定した増加猶予時間の間、チャネル利用率が回線増加しきい値を超え続けた場合にチャネル増加のための発信が行われます。

[未設定時]

回線増加しきい値および猶予時間を設定しないものとみなされます。

8.3.7 remote ppp mp traffic decrease

[機能]

リンク減少しきい値の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

remote [<number>] ppp mp traffic decrease <traffic> <time>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<traffic>

・回線減少しきい値
単位時間当たりのチャネル利用率を、0～100 の 10 進数で指定します。
以下に、回線減少しきい値の計算式を示します。
チャネル利用率(%) = 転送バイト量 ÷ 転送可能バイト数 × 100

<time>

・減少猶予時間
トラフィックが回線減少しきい値を超え続けた場合に、切断するまでの猶予時間を 0～3600 秒の範囲で指定します。
単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

スループット BOD 利用時のリンク減少しきい値を設定します。
スループット BOD 機能を使用する場合は、本コマンドを必ず設定してください。

[注意]

設定された減少猶予時間の間、チャネル利用率が回線減少しきい値を下回り続けた場合にチャネル減少が行われます。

[未設定時]

回線減少しきい値および猶予時間を設定しないものとみなされます。

8.3.8 remote ppp mp order

[機能]

受信パケット順序制御の有無の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

remote [<number>] ppp mp order <mode>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<mode>

・ off
順序制御をしない場合に指定します。
・ on
順序制御をする場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

MP 受信パケットの順序制御を行うかどうか設定します。

[注意]

以下に、MP 受信パケットの順序制御が無効になっていると動作に影響が出る機能を示します。

・ ブリッジ機能
順序に依存するプロトコルをブリッジによって通信する場合、通信が停止することがあります。
・ VJ ヘッダ圧縮機能
設定にかかわらず、常に VJ ヘッダ圧縮を使用しません。
・ IP ヘッダ圧縮機能
設定にかかわらず、常に IP ヘッダ圧縮を使用しません。
・ データ圧縮機能
LZS アルゴリズムで、ヒストリ機能(高効率圧縮の機能)を使用しません。

[未設定時]

MP 受信パケットの順序制御をしないものとみなされます。

```
remote <number> ppp mp order off
```

8.3.9 remote ppp ipcp vjcomp

[機能]

VJ-Compression の利用の有無の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<mode>

・ enable
VJ ヘッダ圧縮を使用する場合に指定します。
・ disable
VJ ヘッダ圧縮を使用しない場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

VJ ヘッダ圧縮機能(VJCOMP)を使用するかどうかを設定します。VJ ヘッダ圧縮機能は、RFC1144 に準拠しています。

[注意]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D の場合は以下に注意してください。
MP を使用する場合は、remote ppp mp order の<mode>に on を指定して、受信順序制御を使用してください。
MP を使用するにもかかわらず受信順序制御を使用しないと定義している場合、VJ ヘッダ圧縮機能は無条件に無効となります。

[未設定時]

VJ ヘッダ圧縮機能を使用するものとみなされます。

```
remote <number> ppp ipcp vjcomp enable
```

8.3.10 remote ppp ipcp iphc

[機能]

IPv4 の IP ヘッダ圧縮(IPHC)の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<mode>

・enable
IP ヘッダ圧縮を使用する場合に指定します。
・disable
IP ヘッダ圧縮を使用しない場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv4 で、IP ヘッダ圧縮(IPHC)を使用するかどうかを設定します。IP ヘッダ圧縮機能は、圧縮方法が RFC2507/RFC2508 に、ネゴシエーション方法が RFC2509 に準拠しています。

[注意]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D の場合は以下に注意してください。

MP を使用する場合は、remote ppp mp order の<mode>に on を指定して、受信順序制御を使用してください。

MP を使用するにもかかわらず受信順序制御を使用しないと定義している場合、IP ヘッダ圧縮機能は無条件に無効となります。

[未設定時]

IP ヘッダ圧縮機能を使用しないものとみなされます。

```
remote <number> ppp ipcp iphc disable
```

8.3.11 remote ppp ipv6cp iphc

[機能]

IPv6 の IP ヘッダ圧縮(IPHC)の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<mode>

・enable
IP ヘッダ圧縮を使用する場合に指定します。
・disable
IP ヘッダ圧縮を使用しない場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 で、IP ヘッダ圧縮(IPHC)を使用するかどうかを設定します。IP ヘッダ圧縮機能は、圧縮方法が RFC2507/RFC2508 に、ネゴシエーション方法が RFC2509 に準拠しています。

[注意]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D の場合は以下に注意してください。

MP を使用する場合は、remote ppp mp order の<mode>に on を指定して、受信順序制御を使用してください。

MP を使用するにもかかわらず受信順序制御を使用しないと定義している場合、IP ヘッダ圧縮機能は無条件に無効となります。

[未設定時]

IPv6 ヘッダ圧縮機能を使用しないものとみなされます。

```
remote <number> ppp ipv6cp iphc disable
```

8.4 IP 関連情報

8.4.1 remote ip address local

[機能]

自側 IP アドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

8.4.2 remote ip address remote

[機能]

相手側 IP アドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

8.4.3 remote ip route

[機能]

IPv4 スタティック経路情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～1999	Si-R570 Si-R570B
0～1249	Si-R370 Si-R370B
0～255	Si-R260B Si-R240B Si-R220C Si-R220D
0～127	Si-R180B

<address>/<mask>

・IPv4 アドレス/マスクビット数(またはマスク値)
あて先ネットワークを IPv4 アドレスとマスクビット数の組み合わせで指定します。
マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
- IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
- IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)

・default
あて先ネットワークとしてデフォルトルートを設定する場合に指定します。
0.0.0.0/0(0.0.0.0/0.0.0.0)を指定するのと同じ意味になります。

<metric>

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

<distance>

・優先度
このスタティック経路情報の優先度を、0～254 の 10 進数で指定します。
優先度は数値の小さい方がより高い優先度を示します。
省略時は、0 を指定したものとみなされます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv4 スタティック経路(静的経路)情報を設定します。

RIP メトリック値は、スタティック経路情報を RIP に再配布するときのメトリック値を設定します。RIP に再配布したときは、設定した RIP メトリック値+1 のメトリック値で RIP テーブルに登録されます。

優先度は、同じあて先への経路情報が複数ある場合、優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。各ダイナミックルーティングプロトコルの優先度については、routemanage ip distance コマンドを参照してください。

優先度に 0 が設定されているときは、routemanage interface floating コマンドでのフローティング設定に応じてフローティング動作が切り替わります。優先度に 1 以上が設定されているときは、常にフローティング動作します。

フローティング動作する場合、remote インタフェースが通信可能な状態(リンクアップなど)であれば、スタティック経路情報をルーティングテーブルに追加します。通信不可能な状態(リンクダウンなど)であれば、ルーティングテーブルから削除します。

フローティング動作しない場合は、インタフェースの状態にかかわらず常にスタティック経路情報をルーティングテーブルに追加します。

以下に、各設定値とフローティング動作の関係を示します。

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

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

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

複数のスタティック経路情報で ECMP 機能を使用するときは、あて先、RIP メトリック値、優先度がそれぞれ同じとなるようにスタティック経路情報を設定します。また、ECMP 機能を使用する場合は、routemanage ip ecmp mode コマンドで ECMP を使用するように設定します。

ECMP となるスタティック経路情報は、同じあて先への経路情報ごとに装置全体で 4 個まで定義できます。

IPv4 スタティック経路情報は、本装置全体で以下の数まで定義できます。

最大定義数	機種
2000	Si-R570 Si-R570B
1250	Si-R370 Si-R370B
256	Si-R260B Si-R240B Si-R220C Si-R220D
128	Si-R180B

[注意]

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

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

[未設定時]

IPv4 スタティック経路情報を使用しないものとみなされます。

8.4.4 remote ip rip use

[機能]

RIP 基本情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<send>

RIP の送信について指定します。

・v1
RIPv1(Unicast または Broadcast)を送信します。
自側 IP アドレスが設定されている場合は Unicast で送信します。
設定されていない場合(unnumbered)は Broadcast で送信します。

・v2
RIPv2(Unicast または Broadcast)を送信します。
自側 IP アドレスが設定されている場合は Unicast で送信します。
設定されていない場合(unnumbered)は Broadcast で送信します。

・v2m
RIPv2(Multicast)を送信します。

・off
RIP を送信しません。

<receive>

RIP の受信について指定します。

・v1
RIPv1 を受信します。

・v2
RIPv1, RIPv2 を受信します。

・off
RIP を受信しません。

<metric>

・加算メトリック値
RIP パケット送信時の加算メトリック値を、0〜16 の 10 進数で指定します。

<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
220	Si-R570 Si-R570B
120	Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
50	Si-R180B

[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 と同時に使用できません。

Si-R570 Si-R570B Si-R370 Si-R370B Si-R240B Si-R220C Si-R220D の場合は以下に注意してください。

ISDN またはフレームリレー(従量課金)の場合、RIP 情報を送信すると、思わぬ課金(定期発信または長時間接続)が発生します。

[未設定時]

RIP 機能を使用しないものとみなされます。

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

8.4.5 remote ip rip filter act

[機能]

RIP フィルタ動作の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～799	Si-R570 Si-R570B
0～399	Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～199	Si-R180B

<action>

フィルタリング条件に一致した場合の動作を指定します。

・pass
該当する経路情報を透過します。

・reject
該当する経路情報を遮断します。

<direction>

フィルタリングを行う方向を指定します。

・in
受信時にフィルタリングを行います。

・out
送信時にフィルタリングを行います。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RIP での経路情報送受信時に、フィルタリング条件に一致した経路情報を通過(pass)させるか遮断(reject)させるかを設定します。フィルタリング条件は優先度順に検索し、条件に一致した経路情報があった時点でフィルタリングが行われ、それ以降の条件は参照されません。全条件に不一致の経路情報は遮断されます。

フィルタリング条件は、remote ip rip filter route コマンドを使用し経路情報を設定します。

<count>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。

RIP フィルタは、本装置全体で以下の数まで定義できます。

最大定義数	機種
800	Si-R570 Si-R570B
400	Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
200	Si-R180B

[注意]

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

[未設定時]

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

8.4.6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～799	Si-R570 Si-R570B
0～399	Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～199	Si-R180B

[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。

8.4.7 remote ip rip filter route

[機能]

RIP フィルタの経路情報設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～799	Si-R570 Si-R570B
0～399	Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～199	Si-R180B

<address>/<mask>

・ IPv4 アドレス/マスクビット数(またはマスク値)
フィルタリング対象とする経路情報を、IPv4 アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
- IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
- IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)

・ any
すべての経路情報をフィルタリング対象とする場合に指定します。

・ default
デフォルトルートをフィルタリング対象とする場合に指定します。
0.0.0.0/0(0.0.0.0/0.0.0.0)を指定するのと同じ意味になります。

<prefix_match>

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

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

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

フィルタリング条件として経路情報を設定します。

[未設定時]

フィルタリング条件が設定されていないものとみなされます。

8.4.8 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～799	Si-R570 Si-R570B
0～399	Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～199	Si-R180B

<metric>

・メトリック値
メトリック値を、0～16 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 1～16 を設定した場合、メトリック値は設定した値に変更されます。また、この場合、remote ip rip use コマンドで設定した加算メトリック値は加算されません。0 を指定した場合、メトリック値の変更は行われません。

[注意]

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

[未設定時]

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

8.4.9 remote ip ospf use

[機能]

OSPF 利用可否の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<mode>

・off
OSPF を利用しません。
・on
OSPF を利用します。

<area_number>

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

範囲	機種
0～9	Si-R570 Si-R570B
0～3	Si-R370 Si-R370B
0～2	Si-R260B Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

最大定義数	機種
100	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
50	Si-R180B

[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
```

8.4.10 remote ip ospf cost

[機能]

OSPF 出力コストの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<cost>

・ 出力コスト
出力コストを、1～65535 で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

OSPF 出力コストを設定します。

[未設定時]

OSPF 出力コストに 10 が設定されているものとみなされます。

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

8.4.11 remote ip ospf hello

[機能]

OSPF Helloパケット送信間隔の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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)のどれかを指定します。
各単位での設定可能範囲は、1s～65535s、1m～1092m、1h～18hです。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[注意]

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

[未設定時]

Helloパケット送信間隔に10秒が設定されているものとみなされます。

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

8.4.12 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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)のどれかを指定します。
各単位での設定可能範囲は、1s～65535s、1m～1092m、1h～18h です。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[注意]

OSPF 隣接ルータ間で異なる隣接ルータ停止確認間隔を設定した場合、ルーティングが行えません。

[未設定時]

隣接ルータ停止確認間隔に 40 秒が設定されているものとみなされます。

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

8.4.13 remote ip ospf retrans

[機能]

OSPF パケット再送間隔の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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)のどれかを指定します。
各単位での設定可能範囲は、3s～65535s、1m～1092m、1h～18h です。

[動作モード]

構成定義モード(管理者クラス)

[説明]

OSPF パケットを再送する間隔を設定します。

[未設定時]

OSPF パケットの再送間隔に 5 秒が設定されているものとみなされます。

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

8.4.14 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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)のどれかを指定します。
各単位での設定可能範囲は、1s～65535s、1m～1092m、1h～18h です。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[注意]

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

[未設定時]

LSU パケット送信遅延時間に 1 秒が設定されているものとみなされます。

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

8.4.15 remote ip ospf auth type

[機能]

OSPF パケット認証方式の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

8.4.16 remote ip ospf auth textkey

[機能]

OSPF テキスト認証鍵の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

8.4.17 remote ip ospf auth md5key

[機能]

OSPF MD5 認証鍵情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

8.4.18 remote ip ospf passive

[機能]

OSPF パケット送信抑止の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<interface_type>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

OSPF パケット送信の抑止を設定します。

[未設定時]

OSPF パケットの送信は抑止しないものとみなされます。

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

8.4.19 remote ip ospf multicast

[機能]

OSPF 送信方法の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

8.4.20 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

8.4.21 remote ip nat mode

[機能]

アドレス変換の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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)のどれかを指定します。
0 秒を指定した場合は、変換テーブル解放のための監視を行いません。
省略時は、5 分を指定したものとみなされます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

相手ネットワークに対するアドレス変換(NAT)の動作を設定します。

[未設定時]

アドレス変換は使用しないものとみなされます。

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

8.4.22 remote ip nat static

[機能]

静的アドレス変換の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～499	Si-R570 Si-R570B
0～299	Si-R370 Si-R370B
0～199	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

<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
500	Si-R570 Si-R570B
300	Si-R370 Si-R370B
200	Si-R260B Si-R240B Si-R220C Si-R220D
64	Si-R180B

[未設定時]

静的アドレス変換は設定されません。

8.4.23 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<action>

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

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

・reject
該当するパケットを破棄します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[未設定時]

すべての NAT テーブルにも一致しないパケットは破棄します。

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

8.4.24 remote ip nat rule

[機能]

アドレス変換ルールの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

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

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

・変換ルール番号
変換ルール番号を、0～31 の 10 進数で指定します。

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

変換ルールの対象となるアプリケーションを指定します。

<server_addr>

・IP アドレス
NAT に割り当てたグローバルアドレス以外のアドレスを指定します。ここで指定したアドレスを変換ルールの対象とします。

・any
すべての IP アドレスを変換ルールの対象とします。
any を指定した場合は、グローバル側とプライベート側の両方のアプリケーションサーバに対応します。

・global
NAT に割り当てたグローバルアドレス以外のすべてのアドレスを変換ルールの対象とします。
global を指定した場合は、グローバル側のアプリケーションサーバに対応します。

・local
NAT に割り当てたグローバルアドレスを変換ルールの対象とします。
local を指定した場合は、プライベート側のアプリケーションサーバに対応します。

・off
指定したアプリケーションに対する変換ルールを無効にします。

<server_port>

アプリケーションサーバで待ち受けるポート番号を指定します。

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

8.4.25 remote ip nat wellknown

[機能]

ポート番号変換の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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)
```

8.4.26 remote ip nat destination

[機能]

あて先変換の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～499	Si-R570 Si-R570B
0～299	Si-R370 Si-R370B
0～199	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

<private_addr>

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

<global_addr>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

最大定義数	機種
500	Si-R570 Si-R570B
300	Si-R370 Si-R370B
200	Si-R260B Si-R240B Si-R220C Si-R220D
64	Si-R180B

[未設定時]

あて先変換は設定されません。

8.4.27 remote ip nat appli

[機能]

アプリ対応の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<function>

設定する機能を指定します。

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

<mode>

・on
アプリ対応を有効にします。
・off
アプリ対応を無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

各アプリケーションに対する特殊対応を有効にするかどうかを設定します。

[注意]

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

[未設定時]

すべてのアプリ対応を有効にするとみなされます。

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

8.4.28 remote ip filter

[機能]

IP フィルタの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～999	Si-R570 Si-R570B Si-R370 Si-R370B
0～199	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

<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
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

<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
1000	Si-R570 Si-R570B Si-R370 Si-R370B
200	Si-R260B Si-R240B Si-R220C Si-R220D
64	Si-R180B

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

最大定義数	機種
9000	Si-R570 Si-R570B
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
450	Si-R180B

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

[注意]

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

[未設定時]

IP フィルタを設定しないものとみなされ、すべてのパケットが透過します。

8.4.29 remote ip filter move

[機能]

IP フィルタの優先順序の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～999	Si-R570 Si-R570B Si-R370 Si-R370B
0～199	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

[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。

8.4.30 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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)のどれかを指定します。
0 秒を指定した場合は、変換テーブル解放のための監視を行いません。
省略時は、5 分を指定したものとみなされます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

どの IP フィルタテーブルに一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

どの IP フィルタテーブルにも一致しないパケットは透過します。

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

8.4.31 remote ip tos

[機能]

TOS 値書き換え条件の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～499	Si-R570 Si-R570B Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～31	Si-R180B

<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
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

<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
500	Si-R570 Si-R570B Si-R370 Si-R370B
100	Si-R260B Si-R240B Si-R220C Si-R220D
32	Si-R180B

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

最大定義数	機種
9000	Si-R570 Si-R570B
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
450	Si-R180B

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

[未設定時]

TOS値書き換えを行わないものとみなされます。

8.4.32 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～499	Si-R570 Si-R570B Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～31	Si-R180B

[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。

8.4.33 remote ip priority

[機能]

帯域制御の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

<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、ip6 の<protocol>値が 1 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B

範囲	機種
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

<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～100000kbps または 1mbps～100mbps の範囲で指定します。全定義の帯域の合計が回線速度を超えた場合は、それぞれ指定した値の比で帯域を割り当てます。

指定した値の合計値が回線速度に達しない場合、残った帯域は定義に一致しないデータ用の帯域となります。

「"share" + 数字」で指定した場合、数字で指定した帯域制御定義番号で定義された帯域を共有します。この場合、指定する数字は自分自身の帯域制御定義番号より小さい、すでに定義されてあるもの指定しなければなりません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

帯域制御を設定します。任意のプロトコル、アドレス、ポート、TOS 値を指定して、割り当てる帯域を指定します。

帯域制御の旧定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
1000	Si-R570 Si-R570B
500	Si-R370 Si-R370B
100	Si-R260B Si-R240B Si-R220C Si-R220D
64	Si-R180B

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

最大定義数	機種
9000	Si-R570 Si-R570B

最大定義数	機種
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
450	Si-R180B

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

[注意]

使用する回線が LAN の場合、シェーピングを使用しないと帯域制御機能は有効に動作しません。
使用する回線が ATM の場合、適切な VC 速度を設定しないと帯域制御機能は有効に動作しません。

[未設定時]

帯域制御を行わないものとみなされます。

8.4.34 remote ip clp

[機能]

IPv4 CLP 値の設定

[適用機種]

Si-R570 Si-R370 Si-R260B

[入力形式]

remote [<number>] ip clp <count> <mode> acl <acl_count>

remote [<number>] ip clp <count> <mode> <src_addr>/<mask> <src_port> <dst_addr>/<mask><dst_port> <protocol> [<tos>]

[オプション]

<number>

・相手定義番号

相手ネットワークの通し番号を、10 進数で指定します。

省略時は、0 を指定したものとみなされます。

<count>

・CLP 値設定条件定義番号

CLP 値設定の優先度を表す番号を、10 進数で指定します。

指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つ CLP 値設定条件定義がすでに存在する場合は、既存の定義を変更します。

範囲	機種
0～1999	Si-R570
0～99	Si-R370 Si-R260B

<mode>

・on

条件と一致する場合に、CLP 値を 1 に設定します。

・off

条件と一致する場合に、CLP 値を 0 に設定します。

<acl_count>

・ACL 定義番号

使用する ACL 定義の番号を、10 進数で指定します。指定した<acl_count>の ACL が定義されていない場合、その CLP 値設定定義は無効となり、無視されます。

CLP 値設定では、ACL の以下の定義を使用します。

- ip

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

- tcp

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

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

- udp

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

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

- icmp

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

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

範囲	機種
0～2999	Si-R570
0～1499	Si-R370
0～299	Si-R260B

<src_addr>/<mask>

CLP 値設定対象となる送信元 IP アドレス、マスクビット数を指定します。

・ IP アドレス/マスクビット数(またはマスク値)

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

以下に、有効な記述形式を示します。

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

・ any

すべての IP アドレスを対象とする場合に指定します。

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

<src_port>

CLP 値設定対象となる送信元ポート番号を指定します。

・ ポート番号

CLP 値設定対象となる送信元ポート番号を、1～65535 の 10 進数で指定します。

複数のポート番号を指定する場合は、","(カンマ)で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン)を使用して指定します。ポート番号は、","(カンマ)および"-"(ハイフン)を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。

以下に、有効な記述形式を示します。

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

・ any

すべてのポート番号を対象とする場合に指定します。

<dst_addr>/<mask>

CLP 値設定対象となる送信先 IP アドレス、マスクビット数を指定します。

・ IP アドレス/マスクビット数(またはマスク値)

CLP 値設定対象となる送信先 IP アドレスとマスクビット数の組み合わせを指定します。

記述形式は、<src_addr>/<mask>と同様です。

・ any

すべての IP アドレスを対象とする場合に指定します。

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

<dst_port>

CLP 値設定対象となる送信先ポート番号を指定します。

・ ポート番号

CLP 値設定対象となる送信先ポート番号を、1～65535 の 10 進数で指定します。

記述形式は、<src_port>と同様です。

・ any

すべてのポート番号を対象とする場合に指定します。

<protocol>

CLP 値設定対象となるプロトコル番号を指定します。

・ プロトコル番号

CLP 値設定対象となるプロトコル番号を、1～255 の 10 進数で指定します(例: ICMP:1、TCP:6、UDP:17 など)。

・ any

すべてのプロトコル番号を CLP 値設定対象とする場合に指定します。

<tos>

CLP 値書き換え対象となる TOS 値を指定します。
省略時は、any を指定したものとみなされます。

・ TOS 値
CLP 値設定対象の TOS 値を、0～ff の 16 進数で指定します。
複数の TOS 値を指定する場合は、","(カンマ)で区切って指定します。また、範囲指定する場合は、"-"(ハイフン)を使用して指定します。
TOS 値は、","(カンマ)および"-"(ハイフン)を使用して 10 個まで指定できます。
以下に、有効な記述形式を示します。
- 00～ff の 16 進数値 (例: ff = ff の TOS 値)
- TOS 値-TOS 値 (例: 32-64 = 32 から 64 までの TOS 値)
- TOS 値- (例: 80- = 80 から ff までの TOS 値)
- -TOS 値 (例: -7f = 0 から 7f までの TOS 値)
- TOS 値,TOS 値,… (例: 10,20,30- = 10 と 20 と 30 以降の TOS 値)

・ any
すべての TOS 値を対象とする場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

相手ネットワークに対する CLP 値設定条件を設定します。
CLP 値設定条件は、IPv4 の旧定義は本装置全体で以下の数まで定義できます。

最大定義数	機種
2000	Si-R570
100	Si-R370 Si-R260B

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

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B

[注意]

ATM にだけ有効です。
また、従来定義と ACL 定義が混在した場合は、ACL 定義から並べ替えられます。

[未設定時]

IPv4 CLP 値設定は行わないとみなされます。
また、CLP 値設定を行わない場合は、常に CLP 値は 0 となります。

8.4.35 remote ip clp move

[機能]

IPv4 CLP 値設定条件優先順序の変更

[適用機種]

Si-R570 Si-R370 Si-R260B

[入力形式]

remote [<number>] ip clp move <count> <new_count>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

・ 対象 CLP 値設定条件定義番号
優先順序を変更する CLP 値設定条件定義の番号を指定します。

<new_count>

・ 移動先 CLP 値設定条件定義番号
<count>に対する新しい順序を、10 進数で指定します。
すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0～1999	Si-R570
0～99	Si-R370 Si-R260B

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv4 CLP 値設定条件優先順序を変更します。
また、従来定義と ACL 定義が混在した場合は、ACL 定義から並べ替えられます。

8.4.36 remote ip in-policy

[機能]

Ingress ポリシールーティングの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<in-policy_number>

・Ingress ポリシールーティング定義番号
この I/F での Ingress ポリシールーティング定義の通し番号を、10 進数で指定します。
本定義は、ほかのポリシーグループ参照定義を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
2000	Si-R570 Si-R570B
1000	Si-R370 Si-R370B
200	Si-R260B Si-R240B Si-R220C Si-R220D
100	Si-R180B

<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
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R220C Si-R220D

範囲	機種
0～49	Si-R180B

[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。

8.4.37 remote ip in-policy move

[機能]

Ingress ポリシールーティングの優先順序の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

8.4.38 remote ip msschange

[機能]

MSS 書き換えの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

8.4.39 remote ip multicast mode

[機能]

マルチキャストインタフェースの定義

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

8.4.40 remote ip multicast ttl threshold

[機能]

マルチキャストインタフェースの TTL しきい値の定義

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

8.4.41 remote ip multicast pim preference

[機能]

マルチキャストインタフェースの PIM プリファレンス値の定義

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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には、プリファレンス値の小さい経路で配送されます。

[注意]

PIM Assert 発行時には Assert 対象となるパケットの発信元へのユニキャスト経路を参照し、発信元へ向かうインタフェースのプリファレンス値を Assert メッセージに格納します。Assert メッセージが出力されるインタフェースのプリファレンス値が格納されるわけではありません。

[未設定時]

1024 になります。

```
remote <number> ip multicast pim preference 1024
```

8.4.42 remote ip multicast pim upstream type

[機能]

上流ルータの種類によるマルチキャストパケット転送許可設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

8.4.43 remote ip dvpn

[機能]

動的 VPN の接続契機となる IPv4 パケットの検出条件の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～9000	Si-R570 Si-R570B
0～4500	Si-R370 Si-R370B
0～900	Si-R260B Si-R240B Si-R220C Si-R220D
0～450	Si-R180B

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
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

<invite_mask>

接続要求を発行する際の相手ネットワークマスクビット数を、0～32 の 10 数数値で指定します。

<template_number>

動的 VPN 接続に利用するテンプレート定義の定義番号を指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

動的VPN接続を利用する場合の、接続契機IPv4パケットの検出条件を設定します。

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。

[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。

8.4.44 remote ip dvpn move

[機能]

動的 VPN の接続契機検出条件の優先順序の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～9000	Si-R570 Si-R570B
0～4500	Si-R370 Si-R370B
0～900	Si-R260B Si-R240B Si-R220C Si-R220D
0～450	Si-R180B

[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。

8.4.45 remote ip exp

[機能]

Exp 値書き換え条件の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip exp <count> acl <acl_count> <exp>

remote [<number>] ip exp <count> <src_addr>/<mask> <src_port> <dst_addr>/<mask><dst_port> <protocol> <tos> <exp>

[オプション]

<number>

・ 相手定義番号

相手ネットワークの通し番号を、10 進数で指定します。

省略時は、0 を指定したものとみなされます。

<count>

・ Exp 書き換え条件定義番号

Exp 書き換えの優先度を表す番号を、10 進数で指定します。

指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つ Exp 書き換え条件定義がすでに存在する場合は、既存の定義を変更します。

範囲	機種
0～499	Si-R570 Si-R570B Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～31	Si-R180B

<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。

範囲	機種
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

<src_addr>/<mask>

Exp 値書き換え対象となる送信元 IP アドレス、マスクビット数を指定します。

・ IP アドレス/マスクビット数(またはマスク値)

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

以下に、有効な記述形式を示します。

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

・ any

すべての IP アドレスを対象とする場合に指定します。

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

<src_port>

Exp 値書き換え対象となる送信元ポート番号を指定します。

・ ポート番号

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

複数のポート番号を指定する場合は、","(カンマ)で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン)を使用して指定します。ポート番号は、","(カンマ)および"-"(ハイフン)を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。

以下に、有効な記述形式を示します。

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

・ any

すべてのポート番号を対象とする場合に指定します。

<dst_addr>/<mask>

Exp 値書き換え対象となる送信先 IP アドレス、マスクビット数を指定します。

・ IP アドレス/マスクビット数(またはマスク値)

Exp 値書き換え対象となる送信先 IP アドレスとマスクビット数の組み合わせを指定します。

記述形式は、<src_addr>/<mask>と同様です。

・ any

すべての IP アドレスを対象とする場合に指定します。

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

<dst_port>

Exp 値書き換え対象となる送信先ポート番号を指定します。

・ ポート番号

Exp 値書き換え対象となる送信先ポート番号を、1～65535 の 10 進数で指定します。

記述形式は、<src_port>と同様です。

・ any

すべてのポート番号を対象とする場合に指定します。

<protocol>

Exp 値書き換え対象となるプロトコル番号を指定します。

・ プロトコル番号

Exp 値書き換え対象となるプロトコル番号を、1～255 の 10 進数で指定します(例: ICMP:1、TCP:6、UDP:17 など)。

・ any

すべてのプロトコル番号を Exp 値書き換え対象とする場合に指定します。

<tos>

Exp 値書き換え対象となる TOS 値を指定します。

・ TOS 値

Exp 値書き換え対象の TOS 値を、0～ff の 16 進数で指定します。

複数の TOS 値を指定する場合は、","(カンマ)で区切って指定します。また、範囲指定する場合は、"-"(ハイフン)を使用して指定します。

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

以下に、有効な記述形式を示します。

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

・ any

すべての TOS 値を対象とする場合に指定します。

<exp>

・ Exp 値

書き換えるExp値を、0〜7の10進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

相手ネットワークに対するExp書き換え条件を設定します。
Exp書き換え条件の旧定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
500	Si-R570 Si-R570B Si-R370 Si-R370B
100	Si-R260B Si-R240B Si-R220C Si-R220D
32	Si-R180B

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

最大定義数	機種
9000	Si-R570 Si-R570B
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
450	Si-R180B

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

[注意]

remote ap datalink type mpls の ap を使用する場合にだけ有効です。

[未設定時]

Exp値書き換えは行わないとみなされます。

8.4.46 remote ip exp move

[機能]

Exp 値書き換え条件優先順序の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip exp move <count> <new_count>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

・ 対象 Exp 書き換え条件定義番号
優先順序を変更する Exp 書き換え条件定義の番号を指定します。

<new_count>

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

範囲	機種
0～499	Si-R570 Si-R570B Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～31	Si-R180B

[動作モード]

構成定義モード(管理者クラス)

[説明]

Exp 値を書き換えの条件優先順序を変更します。
旧定義と ACL 参照定義が混在した場合は、ACL 参照定義から並べ替えられます。

8.4.47 remote ip ids use

[機能]

IDS の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

8.5 IPv6 関連情報

8.5.1 remote ip6 use

[機能]

IPv6 機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

```
remote [<number>] ip6 use <mode>
```

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<mode>

IPv6 パケットの送受信を行うかどうか指定します。

・ on
このインタフェースで、IPv6 パケットの送受信を行います。

・ off
このインタフェースで、IPv6 パケットの送受信を行いません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

このインタフェースで、IPv6 機能を利用するかどうかを設定します。

[未設定時]

IPv6 機能を利用しないものとみなされます。

```
remote <number> ip6 use off
```

8.5.2 remote ip6 ifid

[機能]

IPv6 インタフェース ID の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 ifid <interfaceID>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<interfaceID>

このインタフェースで利用する ID を指定します。

・ auto
本装置が持つ MAC アドレスから、EUI-64 形式の ID を自動生成する場合に指定します。

・ インタフェース ID
このインタフェースで利用する ID を、16 進数で指定します。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> ip6 ifid auto
```

8.5.3 remote ip6 address

[機能]

IPv6 アドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 address [<count>] <address>/<prefixlen> <valid> <preferred> [<flags>]
remote [<number>] ip6 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。

<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。
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～rmt999	Si-R570 Si-R570B
lan0～lan19 rmt0～rmt499	Si-R370 Si-R370B
lan0～lan19 rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
lan0～lan9 rmt0～rmt49	Si-R180B

例)

rmt0 で動作する IPv6 DHCP クライアントが取得した IPv6 プレフィックスを使用する場合の設定例

```
dhcp@rmt0::/64
dhcp@rmt0::1:2:3:4/64
```

プレフィックス長には 64 を指定してください。

<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。

<valid>

・valid lifetime の時間
このインタフェースから RA(Router Advertisement メッセージ)を送信するときに、このプレフィックスに対する valid lifetime を、0 秒～365 日の範囲で指定します。
単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。

<address>/<prefixlen>に IPv6 DHCP クライアントが取得したプレフィックスを使用する指定をした場合は、IPv6 DHCP クライアントが取得した valid lifetime と比較して短い方が有効になります。

・ infinity

このインタフェースから RA を送信するときに、このプレフィックスに対する valid lifetime を無限とする場合に指定します。

<preferred>

・ preferred lifetime の時間

このインタフェースから RA を送信する場合に、このプレフィックスに対する preferred lifetime を、0 秒～365 日の範囲で指定します。

単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。

<preferred>は、<valid>よりも短い時間となるように設定してください。<preferred>が<valid>よりも大きい場合、<valid>と同じ時間として扱われます。

<address>/<prefixlen>に IPv6 DHCP クライアントが取得したプレフィックスを使用する指定をした場合は、IPv6 DHCP クライアントが取得した preferred lifetime と比較して短い方が有効になります。

・ infinity

このインタフェースから RA を送信する場合に、このプレフィックスに対する preferred lifetime を無限とします。

<flags>

・ RA Prefix Information に付与されるフラグ

このインタフェースから RA を送出する場合に、この prefix に対する flags フィールドの値を 16 進数で指定します。

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]

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。

```
<-IPv6 DHCPクライアントが取得したプレフィックス->
                                  <---------------ユーザ設定値(80bit)---------------------->
┌──────────────────────────────┬──────────────┬──────────────────────────────────────┐
│                                │////////////│                                      │
└──────────────────────────────┴──────────────┴──────────────────────────────────────┘
                                  <------------>
                                  設定値が重なる部分
```

例)

IPv6 DHCP クライアントが 2001:db8:1000:5555::/64 を取得した場合

設定内容	利用されるアドレス
dhcp@rmt0:0:100::1/64	2001:db8:1000:5555:100::1/64
dhcp@rmt0:100:200::1/64	無効

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。

8.5.4 remote ip6 ra mode

[機能]

Router Advertisement の動作の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 ra mode <mode>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<mode>

・off
RA の送信を行いません。
定期送信、および host からの RS に対する RA の送信を行いません。

・send
RA の送信を行います。
定期送信、および host からの RS に対する RA の送信を行います。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RA(Router Advertisement メッセージ)を送信するかどうかを設定します。

[未設定時]

RA の送信を行わないものとみなされます。

```
remote <number> ip6 ra mode off
```

8.5.5 remote ip6 ra interval

[機能]

Router Advertisement メッセージ送信間隔の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 ra interval <max> <min> <lifetime>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<max>

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

<min>

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

<lifetime>

・Router Lifetime の値
送信する RA の Router Lifetime の値を、0 または<max>～9000 の 10 進数で指定します。

[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 の値の設定を行います。RA は<min>～<max>でランダムに決定された間隔で定期送信されます。

[未設定時]

最大送信間隔に 600 秒、最小送信間隔に 200 秒、Router Lifetime の値に 1800 が設定されたものとみなされます。

```
remote <number> ip6 ra interval 600 200 1800
```

8.5.6 remote ip6 ra mtu

[機能]

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

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 ra mtu <mtu>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<mtu>

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

[未設定時]

送信する RA に MTU option を含めないものとみなされます。

```
remote <number> ip6 ra mtu 0
```

8.5.7 remote ip6 ra reachabletime

[機能]

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

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 ra reachabletime <time>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<time>

・Reachable Time の値
RA に含める Reachable Time の値(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 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> ip6 ra reachabletime 0
```

8.5.8 remote ip6 ra retranstimer

[機能]

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

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 ra retranstimer <time>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<time>

・ Retrans Timer の値
RA に含める Retrans Timer の値(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 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> ip6 ra retranstimer 0
```

8.5.9 remote ip6 ra curhoplimit

[機能]

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

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 ra curhoplimit <CurHopLimit>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<CurHopLimit>

・Cur Hop Limit の値
RA に含める Cur Hop Limit の値を、0～255 の 10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RA に含める Cur Hop Limit の値を設定します。

[未設定時]

Cur Hop Limit の値として 64 が設定されたものとみなされます。

```
remote <number> ip6 ra curhoplimit 64
```

8.5.10 remote ip6 ra flags

[機能]

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

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 ra flags <flags>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<flags>

・ flags field の値
RA に含める flags field の値を、00～ff の 16 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RA に含める flags field の値を設定します。

[未設定時]

flags field の値として 00 が設定されたものとみなされます。

```
remote <number> ip6 ra flags 00
```

8.5.11 remote ip6 route

[機能]

IPv6 スタティック経路情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 route <count> <address>/<prefixlen> [<metric> [<distance>]]

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

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

範囲	機種
0～1999	Si-R570 Si-R570B
0～1249	Si-R370 Si-R370B
0～255	Si-R260B Si-R240B Si-R220C Si-R220D
0～127	Si-R180B

<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、1～15 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、0～254 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、0 を指定したものとみなされます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 スタティック経路(静的経路)情報を設定します。
RIP メトリック値は、スタティック経路情報を RIP に再配布するときのメトリック値を設定します。RIP に再配布したときは、設定した RIP メトリック値+1 のメトリック値で RIP テーブルに登録されます。

優先度は、同じあて先への経路情報が複数ある場合、優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。各ダイナミックルーティングプロトコルの優先度については、routemanage ip6 distance コマンドを参照してください。

優先度に 0 が設定されているときは、routemanage interface floating コマンドでのフローティング設定に応じてフローティング動作が切り替わります。優先度に 1 以上が設定されているときは、常にフローティング動作します。

フローティング動作する場合、remote インタフェースが通信可能な状態(リンクアップなど)であれば、スタティック経路情報をルーティングテーブルに追加します。通信不可能な状態(リンクダウンなど)であれば、ルーティングテーブルから削除します。

フローティング動作しない場合は、インタフェースの状態にかかわらず常にスタティック経路情報をルーティングテーブルに追加します。

以下に、各設定値とフローティング動作の関係を示します。

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

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

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

IPv6 スタティック経路情報は、本装置全体で以下の数まで定義できます。

最大定義数	機種
2000	Si-R570 Si-R570B
1250	Si-R370 Si-R370B
256	Si-R260B Si-R240B Si-R220C Si-R220D
128	Si-R180B

[注意]

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

- 優先度が 0 のスタティック経路情報と、優先度が 0 または 1 以上のスタティック経路情報は同時に設定できません。
- 優先度が同じスタティック経路情報は同時に設定できません。

[未設定時]

IPv6 スタティック経路情報を使用しないものとみなされます。

8.5.12 remote ip6 rip use

[機能]

IPv6 RIP 基本情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 rip use <send> <receive> [<metric>]

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<send>

RIP(IPv6)パケットを送信するかどうか指定します。

・on
RIP(IPv6)パケットを送信します。

・off
RIP(IPv6)パケットを送信しません。

<receive>

RIP(IPv6)パケットを受信するかどうか指定します。

・on
RIP(IPv6)パケットを受信します。

・off
RIP(IPv6)パケットを受信しません。

<metric>

・加算メトリック値
RIP(IPv6)パケット送信時の加算メトリック値を、0～16 の 10 進数で指定します。
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
220	Si-R570 Si-R570B Si-R370 Si-R370B
120	Si-R260B Si-R240B Si-R220C Si-R220D
58	Si-R180B

[注意]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R240B Si-R220C Si-R220D の場合は以下に注意してください。
ISDN またはフレームリレー(従量課金)の場合、RIP 情報を送信すると、思わぬ課金(定期発信または長時間接続)が発生します。

[未設定時]

RIP(IPv6)機能を使用しないものとみなされます。

```
remote <number> ip6 rip use off off 0
```

8.5.13 remote ip6 rip site-local

[機能]

IPv6 RIP site-local プレフィックス送受信の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 rip site-local <mode>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<mode>

site-local プレフィックスを送受信するかどうかを指定します。

・on
site-local プレフィックスを送受信します。

・off
site-local プレフィックスを送受信しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RIP(IPv6)で site-local プレフィックスを送受信するかどうかを設定します。

[未設定時]

site-local プレフィックスを送受信するものとみなされます。

```
remote <number> ip6 rip site-local on
```

8.5.14 remote ip6 rip aggregate

[機能]

IPv6 RIP の集約経路の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 rip aggregate <count> <address>/<prefixlen> <rejectroute>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

・集約経路定義番号
集約経路の定義番号を、0〜3 の 10 進数で指定します。

<address>/<prefixlen>

・IPv6 アドレス/プレフィックス長
集約経路のあて先ネットワークを IPv6 アドレスとプレフィックス長の組み合わせで指定します。
・default
集約経路としてデフォルトルートを設定する場合に指定します。
::/0 を指定するのと同じ意味になります。

<rejectroute>

・on
集約経路に対する reject 経路を設定します。
・off
集約経路に対する reject 経路を設定しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RIP(IPv6)の集約経路の設定を行います。
集約経路が設定された場合は、設定された集約経路に含まれる個々の経路は広報されず、集約経路だけを広報します。また、集約経路と等しいネットワークに対する経路情報を持たない場合は、実際に持たないあて先に対するパケットを破棄するために、設定された集約経路に対する reject 経路を設定することもできます。

集約経路情報のメトリック値は、集約された経路のメトリック値に関係なく 1 として広報され、remote ip6 rip use および remote ip6 rip filter set metric で広報するメトリック値を変更することができます。

同一 remote 定義内に同一の集約経路は設定できません。

[未設定時]

RIP(IPv6)で経路集約しないものとみなされます。

8.5.15 remote ip6 rip filter act

[機能]

IPv6 RIP フィルタ動作の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 rip filter <count> act <action> <direction>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

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

範囲	機種
0～399	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～199	Si-R180B

<action>

フィルタリング条件に一致した場合の動作を指定します。

・pass
該当する経路情報を透過します。

・reject
該当する経路情報を遮断します。

<direction>

フィルタリングを行う方向を指定します。

・in
受信時にフィルタリングを行います。

・out
送信時にフィルタリングを行います。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RIP(IPv6)での経路情報送受信時に、フィルタリング条件に一致した経路情報を通過(pass)させるか遮断(reject)させるかを設定します。フィルタリング条件は優先度順に検索し、条件に一致した経路情報があった時点でフィルタリングが行われ、それ以降の条件は参照されません。全条件に不一致の経路情報は遮断されます。

フィルタリング条件は、remote ip6 rip filter route コマンドを使用し経路情報を設定します。

<count>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。

RIP フィルタ(IPv6)は、本装置全体で以下の数まで定義できます。

最大定義数	機種
400	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
200	Si-R180B

[注意]

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

[未設定時]

RIP(IPv6)フィルタを使用しないものとみなされ、すべてのRIP(IPv6)の経路情報が透過します。

8.5.16 remote ip6 rip filter move

[機能]

IPv6 RIP フィルタの優先順序の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 rip filter move <count> <new_count>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

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

<new_count>

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

範囲	機種
0～399	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～199	Si-R180B

[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。

8.5.17 remote ip6 rip filter route

[機能]

IPv6 RIP フィルタの経路情報設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 rip filter <count> route <address>/<prefixlen> [<prefix_match>]

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

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

範囲	機種
0～399	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～199	Si-R180B

<address>/<prefixlen>

・IPv6 アドレス/プレフィックス長
フィルタリング対象とする経路情報を、IPv6 アドレスとプレフィックス長の組み合わせで指定します。
・any
すべての経路情報をフィルタリング対象とする場合に指定します。
・default
デフォルトルートをフィルタリング対象とする場合に指定します。

<prefix_match>

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

・exact
指定した<address>/<prefixlen>と経路情報の IPv6 アドレス/プレフィックス長を比較し、一致した場合に、フィルタリング対象とします。
・inexact
指定した<address>と経路情報の IPv6 アドレスを比較し、<prefixlen>まで一致した場合、フィルタリング対象とします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

フィルタリング条件として経路情報を設定します。

[未設定時]

フィルタリング条件が設定されていないものとみなされます。

8.5.18 remote ip6 rip filter set metric

[機能]

IPv6 RIP フィルタのメトリック設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 rip filter <count> set metric <metric>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

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

範囲	機種
0～399	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～199	Si-R180B

<metric>

・メトリック値
メトリック値を、0～16 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 1～16 を設定した場合、メトリック値は設定した値に変更されます。この場合、remote ip6 rip use コマンドで設定した加算メトリック値は加算されません。0 を指定した場合、メトリック値の変更は行われません。

[注意]

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

[未設定時]

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

8.5.19 remote ip6 ospf use

[機能]

IPv6 OSPF 利用可否の設定

[適用機種]

Si-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 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。

<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
0～3	Si-R570 Si-R570B
0～2	Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

[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
30	Si-R570 Si-R570B
15	Si-R240B Si-R220C Si-R220D Si-R180B

[注意]

OSPF の利用は、"ospf ip6 area id"を設定した場合にだけ有効です。
Si-R570、Si-R570B では、拡張用 512M メモリモジュールが搭載されているときにのみ使用できます。

[未設定時]

OSPF を使用しないものとみなされます。

```
remote <number> ip6 ospf use off
```

8.5.20 remote ip6 ospf cost

[機能]

IPv6 OSPF 出力コストの設定

[適用機種]

Si-R570 | Si-R570B | | | | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[入力形式]

remote [<number>] ip6 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。

<cost>

・ 出力コスト
出力コストを、1～65535 で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

OSPF 出力コストを設定します。

[未設定時]

OSPF 出力コストに 10 が設定されているものとみなされます。

```
remote <number> ip6 ospf cost 10
```

8.5.21 remote ip6 ospf hello

[機能]

IPv6 OSPF Helloパケット送信間隔の設定

[適用機種]

Si-R570 | Si-R570B | | | | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[入力形式]

remote [<number>] ip6 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。

<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)のどれかを指定します。
各単位での設定可能範囲は、1s～65535s、1m～1092m、1h～18hです。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[注意]

OSPF隣接ルータ間で異なるHelloパケットの送信間隔を設定した場合、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> ip6 ospf hello 10s
```

8.5.22 remote ip6 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-R570 | Si-R570B | | | | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[入力形式]

remote [<number>] ip6 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。

<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)のどれかを指定します。
各単位での設定可能範囲は、1s～65535s、1m～1092m、1h～18h です。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[注意]

OSPF 隣接ルータ間で異なる隣接ルータ停止確認間隔を設定した場合、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> ip6 ospf dead 40s
```

8.5.23 remote ip6 ospf retrans

[機能]

IPv6 OSPF パケット再送間隔の設定

[適用機種]

Si-R570 | Si-R570B | | | | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[入力形式]

remote [<number>] ip6 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。

<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)のどれかを指定します。
各単位での設定可能範囲は、3s～65535s、1m～1092m、1h～18h です。

[動作モード]

構成定義モード(管理者クラス)

[説明]

OSPF パケット(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> ip6 ospf retrans 5s
```

8.5.24 remote ip6 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-R570 | Si-R570B | | | | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[入力形式]

remote [<number>] ip6 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。

<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)のどれかを指定します。
各単位での設定可能範囲は、1s～65535s、1m～1092m、1h～18h です。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[注意]

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> ip6 ospf delay 1s
```

8.5.25 remote ip6 ospf passive

[機能]

IPv6 OSPF パケット送信抑止の設定

[適用機種]

Si-R570 | Si-R570B | | | | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[入力形式]

remote [<number>] ip6 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。

<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。

・ on
パケットの送信を抑止します。

・ off
パケットの送信を抑止しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

OSPF 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> ip6 ospf passive off
```

8.5.26 remote ip6 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-R570 | Si-R570B | | | | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[入力形式]

remote [<number>] ip6 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。

<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> ip6 ospf checkmtu on
```

8.5.27 remote ip6 filter

[機能]

IPv6 フィルタの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 filter <count> <action> acl <acl_count> [<direction>]

remote [<number>] ip6 filter <count> <action> <src_addr>/<prefixlen> <src_port><dst_addr>/<prefixlen> <dst_port> <protocol> <tcpconnect>[<trafficclass> [<direction> [<icmptype> [<icmpcode>]]]]

[オプション]

<number>

・ 相手定義番号

相手ネットワークの通し番号を、10 進数で指定します。

省略時は、0 を指定したものとみなされます。

<count>

・ フィルタリング定義番号

フィルタリングの優先度を表す番号を、10 進数で指定します。

指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つフィルタリング定義がすでに存在する場合は、既存の定義を変更します。

範囲	機種
0～999	Si-R570 Si-R570B Si-R370 Si-R370B
0～199	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

<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。

- ip6

ip6 値が設定されていない場合、そのフィルタ定義は無効となり、無視されます。

- tcp

ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。

また、ip6 の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。

- udp

ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。

また、ip6 の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp

ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。

また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

<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 として扱われます。

<direction>

フィルタリングする方向を指定します。

省略時は、any を指定したものとみなされます。

・ any

入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。

・ in

入力パケットのみをフィルタリング対象とする場合に指定します。

・ out

出力パケットのみをフィルタリング対象とする場合に指定します。

・ reverse

入力パケットと出力パケットの両方をフィルタリング対象とします。

ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。

- 送信元 IP アドレス/プレフィックス長とあて先 IP アドレス/プレフィックス長
- 送信元ポート番号とあて先ポート番号

<icmptype>

フィルタリングする ICMPv6 メッセージタイプ番号を指定します。

・ フィルタリング対象 icmptype 値

フィルタリング対象となる icmptype フィールドの値を 0-255 までの 10 進数、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 として扱われます。

<icmpcode>

フィルタリングする ICMPv6 メッセージコード番号を指定します。

icmpcode 指定時は、icmptype も指定する必要があります。

・ フィルタリング対象 icmpcode 値

フィルタリング対象となる icmpcode フィールドの値を 0-255 までの 10 進数、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 として扱われます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

相手ネットワークに対する IPv6 フィルタを設定します。

各パラメタに設定された値によって、動作が変化する場合があります。以下に説明します。

・ <protocol>に指定した値によって、IPv6 拡張ヘッダの扱いが以下のように変化します。

- any を指定した場合は、0 個以上の IPv6 拡張ヘッダを含む、あらゆる upper-layer protocol(upper-layer protocol なしを含む)に一致します。
- 以下の IPv6 拡張ヘッダの値を指定した場合は、その拡張ヘッダが付与されている、あらゆる upper-layer protocol(upper-layerprotocol なしを含む)のパケットが一致します。

0

Hop-by-Hop Options Header

43

Routing Header

44

Fragment Header

60

Destination Options Header

- 以下の値を指定した場合は、0 個以上の IPv6 拡張ヘッダ(AH、ESP、IPComp を除く)を含む、upper-layer protocol ヘッダが付与されていないパケットが一致します。

59

no next header

- その他の値が設定されている場合は、upper-layer protocol ヘッダの protocol 番号に等しい値であるパケットが一致します。この場合、AH、ESP、IPComp を除くすべての IPv6 拡張ヘッダは無視されます。パケット中に AH、ESP が設定されている場合は、それ以降の拡張ヘッダおよび upper-layer protocol ヘッダの解釈は行いません。

・ <src_port>、<dst_port>に指定した値によって、<protocol>の扱いが以下のように変化します。

- <protocol>に any を指定し、かつ<src_port>、<dst_port>のどちらか、または両方を指定している場合、TCP および UDP パケットの該当ポート番号を持つパケットのみが一致します。
- <protocol>に TCP(6)または UDP(17)を指定し、かつ<src_port>、<dst_port>のどちらか、または両方を指定している場合、指定プロトコルの該当ポート番号を持つパケットのみが一致します。
- <protocol>に TCP(6)または UDP(17)以外を指定し、かつ<src_port>、<dst_port>のどちらか、または両方を指定している場合、あらゆるパケットが一致しません。

・ <icmptype>、<icmpcode>に指定した値によって、<protocol>の扱いが以下のように変化します。

- <protocol>に any を指定し、かつ<icmptype>、<icmpcode>を指定している場合、ICMPv6 パケットの該当 type/code 番号を持つパケットのみが一致します。
- <protocol>に ICMPv6(58)を指定し、かつ<icmptype>、<icmpcode>を指定している場合、指定プロトコルの該当 type/code 番号を持つパケットのみが一致します。
- <protocol>に ICMPv6(58)以外を指定し、かつ<icmptype>、<icmpcode>を指定している場合、あらゆるパケットが一致しません。

・ <tcpconnect>の扱いを以下に示します。

- <protocol>に any を指定した場合、TCP パケットのときにこの設定値が適用されます。
- <protocol>に TCP(6)を指定した場合、常にこの設定値が適用されます。
- <protocol>に any または TCP(6)以外を指定した場合、この設定値は適用されません。

IPv6 フィルタリングの旧定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
1000	Si-R570 Si-R570B Si-R370 Si-R370B
200	Si-R260B Si-R240B Si-R220C Si-R220D
64	Si-R180B

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

最大定義数	機種
9000	Si-R570 Si-R570B
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
450	Si-R180B

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。

8.5.28 remote ip6 filter move

[機能]

IPv6 フィルタの優先順序の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 filter move <count> <new_count>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

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

<new_count>

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

範囲	機種
0～999	Si-R570 Si-R570B Si-R370 Si-R370B
0～199	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

[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。

8.5.29 remote ip6 filter default

[機能]

どの IP フィルタテーブルにも不一致時の動作の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 filter default <action> [<time>]

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<action>

どの IPv6 フィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

・pass
該当するパケットを透過します。

・reject
該当するパケットを遮断します。

・restrict
該当するパケットを、回線が接続されていれば透過し、切断されていれば遮断します。

・spi
該当するパケットに対して SPI を動作させます。

<time>

・割り当て時間
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)のどれかを指定します。
0 秒を指定した場合は、変換テーブル解放のための監視を行いません。
省略時は、5 分を指定したものとみなされます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

どの IPv6 フィルタテーブルにも一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

どの IPv6 フィルタテーブルにも一致しないパケットは透過します。

```
remote <number> ip6 filter default pass
```

8.5.30 remote ip6 trafficclass

[機能]

Traffic Class 値書き換え条件の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 trafficclass <count> acl <acl_count> <new_trafficclass>

remote [<number>] ip6 trafficclass <count> <src_addr>/<prefixlen> <src_port><dst_addr>/<prefixlen> <dst_port> <protocol> <trafficclass> <new_trafficclass>

[オプション]

<number>

・相手定義番号

相手ネットワークの通し番号を、10 進数で指定します。

省略時は、0 を指定したものとみなされます。

<count>

・Traffic Class 値書き換え定義番号

Traffic Class 値書き換え条件の優先度を表す定義番号を、10 進数で指定します。

指定した値は、設定完了時に順方向にソートされてリナンバリングされます。

また、指定した定義番号と同じ値を持つ Traffic Class 値書き換え定義がすでに存在する場合は、既存定義の値を変更します。

範囲	機種
0～499	Si-R570 Si-R570B Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～31	Si-R180B

<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。

- ip6

  ip6 値が設定されていない場合、その定義は無効となり、無視されます。

- tcp

  ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip6 の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。

- udp

  ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip6 の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp

  ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0～2999	Si-R570 Si-R570B

範囲	機種
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

<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
500	Si-R570 Si-R570B Si-R370 Si-R370B
100	Si-R260B Si-R240B Si-R220C Si-R220D
32	Si-R180B

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

最大定義数	機種
9000	Si-R570 Si-R570B
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
450	Si-R180B

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。

8.5.31 remote ip6 trafficclass move

[機能]

Traffic Class 値書き換え条件の優先度の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 trafficclass move <count> <new_count>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

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

<new_count>

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

範囲	機種
0～499	Si-R570 Si-R570B Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～31	Si-R180B

[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。

8.5.32 remote ip6 priority

[機能]

IPv6 プロトコル帯域制御の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 priority <count> acl <acl_count> <width>

remote [<number>] ip6 priority <count> <src_addr>/<prefixlen> <src_port><dst_addr>/<prefixlen> <dst_port> <protocol> <trafficclass> <width>

[オプション]

<number>

・ 相手定義番号

相手ネットワークの通し番号を、10 進数で指定します。

省略時は、0 を指定したものとみなされます。

<count>

・ 帯域制御定義番号

帯域制御定義番号を、10 進数で指定します。

範囲	機種
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

<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。

- ip6

  ip6 値が設定されていない場合、その定義は無効となり、無視されます。

- tcp

  ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip6 の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。

- udp

  ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip6 の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp

  ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B

範囲	機種
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

<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 として扱われます。

<width>

・ express

最優先データとして扱います。

・ besteffort

非優先(ベストエフォート)として扱います。

・ 帯域

1～99 の 10 進数で指定した場合、それぞれ指定した値の比で帯域を割り当てます。たとえば、同じ相手ネットワーク中の定義が 3 つあり、それぞれ<width>の値が 30、30、60 であった場合、帯域として 25%、25%、50%が割り当てられます。なお、1～99 を指定した定義のそれぞれの合計値が 100 未満の場合、残った帯域は定義に一致しないデータ用の帯域となります。

「数字 + "kbps"(,"mbps")」で指定した場合、指定した帯域をそのまま割り当てます。1kbps～100000kbps または 1mbps～100mbps の範囲で指定します。全定義の帯域の合計が回線速度を超えた場合は、それぞれ指定した値の比で帯域を割り当てます。

指定した値の合計値が回線速度に達しない場合、残った帯域は定義に一致しないデータ用の帯域となります。

「"share" + 数字」で指定した場合、数字で指定した帯域制御定義番号で定義された帯域を共有します。この場合、指定する数字は自分自身の帯域制御定義番号より小さい、すでに定義されてあるもの指定しなければなりません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 プロトコル帯域制御を設定します。任意のプロトコル、アドレス、ポート、トラフィッククラスを指定して、割り当てる帯域を指定します。

IPv6 プロトコル帯域制御の旧定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
1000	Si-R570 Si-R570B
500	Si-R370 Si-R370B
100	Si-R260B Si-R240B Si-R220C Si-R220D
64	Si-R180B

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

最大定義数	機種
9000	Si-R570 Si-R570B
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
450	Si-R180B

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

[注意]

使用する回線が LAN の場合、シェーピングを使用しないと帯域制御機能は有効に動作しません。
使用する回線が ATM の場合、適切な VC 速度を設定しないと帯域制御機能は有効に動作しません。

[未設定時]

IPv6 プロトコル帯域制御を行わないものとみなされます。

8.5.33 remote ip6 in-policy

[機能]

Ingress ポリシールーティングの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 in-policy <in-policy_number> policy-group <policy-group_number>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<in-policy_number>

・Ingress ポリシールーティング定義番号
この I/F での Ingress ポリシールーティング定義の通し番号を、10 進数で指定します。
本定義は、ほかのポリシーグループ参照定義を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
2000	Si-R570 Si-R570B
1000	Si-R370 Si-R370B
200	Si-R260B Si-R240B Si-R220C Si-R220D
100	Si-R180B

<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。

- ip6
  ip6 値が設定されていない場合、その定義は無効となり、無視されます。
- tcp
  ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。
- udp
  ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。
- icmp
  ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R220C Si-R220D

範囲	機種
0～49	Si-R180B

[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。

8.5.34 remote ip6 in-policy move

[機能]

Ingress ポリシールーティングの優先順序の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 in-policy move <count> <new_count>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

・ 対象 Ingress ポリシールーティング定義番号
優先順序を変更するフィルタリング定義の番号を指定します。

<new_count>

・ 移動先 Ingress ポリシールーティング定義番号
<count>に対する新しい順序を、10 進数で指定します。
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。

8.5.35 remote ip6 dhcp service

[機能]

IPv6 DHCP 機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 dhcp service <mode>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<mode>

IPv6 DHCP 機能のモードを指定します。

・ off
IPv6 DHCP 機能を使用しません。
・ client
IPv6 DHCP クライアント機能を使用します。
・ 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。

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[未設定時]

IPv6 DHCP 機能を使用しないものとみなされます。

```
remote <number> ip6 dhcp service off
```

8.5.36 remote ip6 dhcp duid

[機能]

IPv6 DHCP の DUID 設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 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。

<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 ip6 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。

8.5.37 remote ip6 dhcp client option pd

[機能]

IPv6 DHCP クライアントのプレフィックス要求の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 dhcp client option pd <mode>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<mode>

・on
プレフィックスを要求します。
・off
プレフィックスを要求しません。
・troan
draft-troan-dhcpv6-opt-prefix-delegation-01 に準拠した方式でプレフィックスを要求します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 DHCP クライアント機能を使用する場合に、サーバにプレフィックスを要求するかどうかを設定します。
<mode>に on を設定した場合は、RFC3315、3633 に準拠したオプション番号を使用します。
<mode>に troan に設定した場合は、DNS サーバオプションのオプション番号に 25 番を使用し、PD オプションのオプション番号に 30 番を使用してプレフィックスの要求を行います。

[未設定時]

プレフィックスを要求するものとみなされます。

```
remote <number> ip6 dhcp client option pd on
```

8.5.38 remote ip6 dhcp client option dns

[機能]

IPv6 DHCP クライアントの DNS サーバアドレス要求の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 dhcp client option dns <mode>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<mode>

・on
DNS サーバアドレスを要求します。
・off
DNS サーバアドレスを要求しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 DHCP クライアント機能を使用する場合に、サーバに DNS サーバアドレスを要求するかどうかを設定します。

[未設定時]

DNS サーバアドレスを要求するものとみなされます。

```
remote <number> ip6 dhcp client option dns on
```

8.5.39 remote ip6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 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。

<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> ip6 dhcp client option domain on
```

8.5.40 remote ip6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 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。

<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> ip6 dhcp client option sipserver address on
```

8.5.41 remote ip6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

```
remote [<number>] ip6 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。

<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> ip6 dhcp client option sipserver domain on
```

8.5.42 remote ip6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 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。

<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> ip6 dhcp client option sntpserver on
```

8.5.43 remote ip6 dhcp client iaid

[機能]

IPv6 DHCP クライアントの IAID 設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 dhcp client iaid <iaid>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<iaid>

・auto
IAID を自動生成する場合に指定します。
・IAID を指定
IAID を指定する場合の設定可能範囲は、1～4294967295 です。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 DHCP クライアントの IAID を指定します。
auto を指定した場合は、インタフェース番号が IAID として使用されます。

[未設定時]

IAID を自動生成するものとみなされます。

```
remote <number> ip6 dhcp client iaid auto
```

8.5.44 remote ip6 dhcp client route

[機能]

IPv6 DHCP クライアントのリジェクト経路設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 dhcp client route <mode>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<mode>

・blackhole
DHCP クライアントで取得したプレフィックスを、リジェクト経路として登録します。
リジェクト経路あての送信者に対して、応答しません。

・reject
DHCP クライアントで取得したプレフィックスを、リジェクト経路として登録します。
リジェクト経路あての送信者に対して、ICMP の unreach でエラー報告を行います。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 DHCP クライアントで取得したプレフィックスをリジェクト経路として登録します。
<mode>が reject の場合は、リジェクト経路あての送信者に対して、ICMP の unreach でエラー報告を行います。
blackhole の場合は、応答しません。

[未設定時]

blackhole を設定するものとみなされます。

```
remote <number> ip6 dhcp client route blackhole
```

8.5.45 remote ip6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 dhcp relay interface <interface>

[オプション]

<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～rmt999	Si-R570 Si-R570B
lan0～lan19 rmt0～rmt499	Si-R370 Si-R370B
lan0～lan19 rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
lan0～lan9 rmt0～rmt49	Si-R180B

[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。

8.5.46 remote ip6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 dhcp relay server <address>

[オプション]

<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。

8.5.47 remote ip6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 dhcp relay source <address>

[オプション]

<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。

8.5.48 remote ip6 dhcp server preference

[機能]

IPv6 DHCP サーバのプリファレンス値設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 dhcp server preference <preference>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<preference>

・プリファレンス値
IPv6 DHCP サーバの優先度を、0～255 の 10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 DHCP サーバのプリファレンス値を指定します。
プリファレンス値は、Advertise メッセージの Preference オプションで使用され、255 が最優先の値になります。

[未設定時]

プリファレンス値 0 を設定するものとみなされます。

```
remote <number> ip6 dhcp server preference 0
```

8.5.49 remote ip6 dhcp server info dns

[機能]

IPv6 DHCP サーバの DNS サーバアドレス配布情報設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 dhcp server info dns <dns1> [<dns2>]

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<dns1>

・DNS サーバ IPv6 アドレス
IPv6 DHCP クライアントに配布する、DNS サーバの IPv6 アドレスを指定します。
指定可能な範囲は以下のとおりです。

::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

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～rmt999	Si-R570 Si-R570B
lan0～lan19 rmt0～rmt499	Si-R370 Si-R370B
lan0～lan19 rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
lan0～lan9 rmt0～rmt49	Si-R180B

<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。

8.5.50 remote ip6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 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。

<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～rmt999	Si-R570 Si-R570B
lan0～lan19 rmt0～rmt499	Si-R370 Si-R370B
lan0～lan19 rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
lan0～lan9 rmt0～rmt49	Si-R180B

[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。

8.5.51 remote ip6 dhcp server info prefix

[機能]

IPv6 DHCP サーバのプレフィックス配布情報設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 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。

<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、lan または rmt インタフェースを以下の範囲で指定します。

範囲	機種
lan0～lan19 rmt0～rmt999	Si-R570 Si-R570B
lan0～lan19 rmt0～rmt499	Si-R370 Si-R370B
lan0～lan19 rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
lan0～lan9 rmt0～rmt49	Si-R180B

例)

rmt0 で動作する IPv6 DHCP クライアントが取得した IPv6 プレフィックスを使用する場合の設定例

dhcp@rmt0:1234::/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)のどれかを指定します。

・infinity

このインタフェースから配布するプレフィックスに対する valid lifetime を、無限とする場合に指定します。

<preferred>

・ preferred lifetime

このインタフェースから配布するプレフィックスに対する preferred lifetime を、0 秒～365 日の範囲で指定します。

単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。

<preferred>は、<valid>よりも短い時間となるように設定してください。<preferred>が<valid>よりも大きい場合、<valid>と同じ時間として扱われます。

・ infinity

このインタフェースから配布するプレフィックスに対する preferred lifetime を無限とします。

<routeset>

・ on

配布プレフィックスへの経路を自動登録します。

・ off

配布プレフィックスへの経路を自動登録しません。

<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。

8.5.52 remote ip6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 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。

<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～rmt999	Si-R570 Si-R570B
lan0～lan19 rmt0～rmt499	Si-R370 Si-R370B
lan0～lan19 rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
lan0～lan9 rmt0～rmt49	Si-R180B

<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。
<sip1>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 SIP サーバアドレス情報の設定をします。

8.5.53 remote ip6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 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。

<sip1>

・SIP 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 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～rmt999	Si-R570 Si-R570B
lan0～lan19 rmt0～rmt499	Si-R370 Si-R370B
lan0～lan19 rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
lan0～lan9 rmt0～rmt49	Si-R180B

<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 ドメイン名を指定します。

<sip1>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 SIP ドメイン名情報の設定をします。

8.5.54 remote ip6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 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。

<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～rmt999	Si-R570 Si-R570B
lan0～lan19 rmt0～rmt499	Si-R370 Si-R370B
lan0～lan19 rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
lan0～lan9 rmt0～rmt49	Si-R180B

<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。

8.5.55 remote ip6 dvpn

[機能]

動的 VPN の接続契機となる IPv6 パケットの検出条件の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

```
remote [<number>] ip6 dvpn <count> invite acl <acl_count> <invite_mask> <template_number>
remote [<number>] ip6 dvpn <count> ignore acl <acl_count>
remote [<number>] ip6 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。

<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
0～9000	Si-R570 Si-R570B
0～4500	Si-R370 Si-R370B
0～900	Si-R260B Si-R240B Si-R220C Si-R220D
0～450	Si-R180B

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
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

<invite_mask>

接続要求を発行する際の相手ネットワークマスクビット数を、0～128 の 10 数数値で指定します。

<template_number>

動的 VPN 接続に利用するテンプレート定義の定義番号を指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

動的VPN接続を利用する場合の、接続契機IPv6パケットの検出条件を設定します。

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。

8.5.56 remote ip6 dvpn move

[機能]

動的 VPN の接続契機検出条件の優先順序の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 dvpn move <count> <new_count>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

・ 接続契機条件定義番号
優先順序を変更する接続契機条件定義の番号を指定します。

<new_count>

・ 移動先接続契機条件定義番号
<count>に対する新しい順序を 10 進数で指定します。
すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0～9000	Si-R570 Si-R570B
0～4500	Si-R370 Si-R370B
0～900	Si-R260B Si-R240B Si-R220C Si-R220D
0～450	Si-R180B

[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。

8.5.57 remote ip6 exp

[機能]

Exp 値書き換え条件の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 exp <count> acl <acl_count> <exp>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

・ Exp 書き換え条件定義番号
Exp 書き換えの優先度を表す番号を、10 進数で指定します。
指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つ Exp 書き換え条件定義がすでに存在する場合は、既存の定義を変更します。

範囲	機種
0～499	Si-R570 Si-R570B Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～31	Si-R180B

<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。

範囲	機種
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

<exp>

・ Exp 値
書き換える Exp 値を、0～7 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]

相手ネットワークに対する Exp 書き換え条件を設定します。
ACL 参照定義は、ほかの ACL 参照定義(IP フィルタ、帯域制御(WFQ)など)を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570 Si-R570B

最大定義数	機種
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
450	Si-R180B

[注意]

remote ap datalink type mpls の ap を使用する場合にだけ有効です。

[未設定時]

Exp 値書き換えは行わないとみなされます。

8.5.58 remote ip6 exp move

[機能]

Exp 値書き換え条件優先順序の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] ip6 exp move <count> <new_count>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

・ 対象 Exp 書き換え条件定義番号
優先順序を変更する Exp 書き換え条件定義の番号を指定します。

<new_count>

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

範囲	機種
0～499	Si-R570 Si-R570B Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～31	Si-R180B

[動作モード]

構成定義モード(管理者クラス)

[説明]

Exp 値を書き換えの条件優先順序を変更します。

8.5.59 remote ip6 clp

[機能]

IPv6 CLP の設定

[適用機種]

Si-R570 Si-R370 Si-R260B

[入力形式]

remote [<number>] ip6 clp <count> <mode> acl <acl_count>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

・CLP 値設定条件定義番号
CLP 値設定の優先度を表す番号を、10 進数で指定します。
指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つ CLP 値設定条件定義がすでに存在する場合は、既存の定義を変更します。

範囲	機種
0～1999	Si-R570
0～99	Si-R370 Si-R260B

<mode>

・on
条件と一致する場合に、CLP 値を 1 に設定します。
・off
条件と一致する場合に、CLP 値を 0 に設定します。

<acl_count>

・ACL 定義番号
使用する ACL 定義の番号を、10 進数で指定します。
指定した<acl_count>の ACL が定義されていない場合、その CLP 設定定義は無効となり、無視されます。
IPv6 CLP 設定では、ACL の以下の定義を使用します。
- ip6
ip6 値が設定されていない場合、そのフィルタ定義は無効となり、無視されます。
- tcp
ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。
また、ip の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。
- udp
ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。
また、ip の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。
- icmp
ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。
また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0～2999	Si-R570
0～1499	Si-R370
0～299	Si-R260B

[動作モード]

構成定義モード(管理者クラス)

[説明]

相手ネットワークに対する CLP 値設定条件を設定します。
ACL 参照定義はほかの ACL 参照定義(IP フィルタなど)を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
9000	Si-R570
4500	Si-R370
900	Si-R260B

[注意]

ATM にだけ有効です。

[未設定時]

IPv6 CLP 値設定は行わないとみなされます。
また、CLP 値設定を行わない場合は、常に CLP 値は 0 となります。

8.5.60 remote ip6 clp move

[機能]

IPv6 CLP 値設定条件優先順序の変更

[適用機種]

Si-R570 Si-R370 Si-R260B

[入力形式]

remote [<number>] ip clp move <count> <new_count>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

・ 対象 CLP 値設定条件定義番号
優先順序を変更する CLP 値設定条件定義の番号を指定します。

<new_count>

・ 移動先 CLP 値設定条件定義番号
<count>に対する新しい順序を、10 進数で指定します。
すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0～1999	Si-R570
0～99	Si-R370 Si-R260B

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 CLP 値設定条件優先順序を変更します。

8.6 ブリッジ関連情報

8.6.1 remote bridge use

[機能]

ブリッジ機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] bridge use <mode>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<mode>

ブリッジを使用するかどうかを指定します。

・on
ブリッジを使用する場合に指定します。

・off
ブリッジを使用しない場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ブリッジを使用するかどうかを設定します。
ブリッジを使用する場合、IP および IPv6 のパケット以外をすべてブリッジします。
ただし、接続先との接続時に BCP のネゴシエーションを行い、ネゴシエーションが成功した場合にブリッジデータの送受信が可能となります。

[注意]

IP および IPv6 以外のネットワークプロトコル(IPX など)をルーティングしているネットワークでブリッジを使用する場合は、ブリッジによって中継されることでネットワークがダウンすることがあります。ルーティングと同時に使用する場合は、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]

ブリッジを使用しないものとみなされます。

```
remote <number> bridge use off
```

8.6.2 remote bridge group

[機能]

ブリッジグループ識別子の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] bridge group <group_id>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<group_id>

・ グループ識別子
グループ識別子を 10 進数で指定します。

範囲	機種
0～19	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～7	Si-R180B

[動作モード]

構成定義モード(管理者クラス)

[説明]

ブリッジのグループ識別子を設定します。

[未設定時]

グループ識別子に 0 を指定したものとみなされます。

```
remote <number> bridge group 0
```

8.6.3 remote bridge static

[機能]

静的学習テーブル情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] bridge static <count> <mac>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

・ 静的学習テーブル定義番号
指定した定義番号と同じ値を持つ定義がすでに存在する場合は、既存の設定に対する修正をみなされます。

範囲	機種
0～399	Si-R570 Si-R570B Si-R370 Si-R370B
0～199	Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

<mac>

静的な定義として学習テーブルに追加する MAC アドレスを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

学習テーブルに指定された MAC アドレスを静的な学習テーブル情報として追加します。

8.6.4 remote bridge stp use

[機能]

STP モードの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] bridge stp use <mode>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<mode>

・ on
STP を使用する場合に指定します。
・ off
STP を使用しない場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

スパニングツリーアルゴリズムで経路制御を行うかどうかを設定します。
本コマンドは、ブリッジを使用している場合にだけ有効です。

[注意]

ブリッジグループ 0 以外のブリッジグループでは STP は動作しません。

[未設定時]

STP を使用しないものとみなされます。

```
remote <number> bridge stp use off
```

8.6.5 remote bridge stp cost

[機能]

パスコストの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] bridge stp cost <path_cost>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<path_cost>

接続先と通信する場合のパスコストを指定します。
通常は auto を指定してください。ただし、ブリッジネットワークを構築するうえで、優先ブリッジ決定のために任意のパスコストを指定することができます。

・auto
インタフェースの速度に応じて、パスコストが自動決定されます。
以下に、本パラメタ指定時のパスコストを示します。

回線種別	パスコスト	備考
Ethernet(1Gbps)	100	
Ethernet(100Mbps)	100	
Ethernet(10Mbps)	100	
HSD(64kbps)	15620	*：192kbps～1.5Mbps は PRI の場合
HSD(128kbps)	7810	
HSD(192kbps) *	1000	
HSD(256kbps) *	1000	
HSD(384kbps) *	1000	
HSD(512kbps) *	1000	
HSD(768kbps) *	1000	
HSD(1Mbps) *	667	
HSD(1.5Mbps) *	667	
FR(64kbps)	16000	
FR(128kbps)	8500	
FR(256kbps) *	1100	
FR(384kbps) *	1100	
FR(512kbps) *	1100	
FR(768kbps) *	1100	
FR(1Mbps) *	680	
FR(1.5Mbps) *	680	
ISDN	16000	
MODEM	16000	
IP トンネル	16000	
その他 1Mbps>=速度	 1000	

回線種別	パスコスト	備考
1.5Mbps>=速度>1Mbps	667	
4Mbps>=速度>1.5Mbps	250	
6Mbps>=速度>4Mbps	167	
10Mbps>=速度>6Mbps	100	
16Mbps>=速度>10Mbps	62	
20Mbps>=速度>16Mbps	50	
25Mbps>=速度>20Mbps	40	
40Mbps>=速度>25Mbps	25	
80Mbps>=速度>40Mbps	12	
速度>80Mbps	10	

・ パスコスト
パスコストを、1～65535 の 10 進数で指定します。
値が小さいほど、優先度が高くなります。

[動作モード]

構成定義モード(管理者クラス)

[説明]

スパニングツリーアルゴリズムで使用するパスコストを設定します。
本コマンドは、STP を使用する場合にだけ有効です。

[未設定時]

パスコストを自動決定するとみなされます。

```
remote <number> bridge stp cost auto
```

8.6.6 remote bridge stp priority

[機能]

インタフェース優先度の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] bridge stp priority <port_priority>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<port_priority>

・インタフェース優先度
インタフェースごとの優先度を、0～255 の 10 進数で指定します。
値が小さいほど、優先度が高くなります。

[動作モード]

構成定義モード(管理者クラス)

[説明]

スパニングツリーアルゴリズムで使用する、インタフェースごとの優先度を設定します。
通常、設定する必要はありません。
本コマンドは、STP を使用する場合にだけ有効です。
本コマンドを設定しない場合は、<number>で指定したインタフェースが優先となり、remote 定義で定義されたインタフェースが非優先となります。lan 定義内で定義されたインタフェースでは、定義番号のもっとも小さいものが優先されます。

[未設定時]

インタフェース優先度に 128 が設定されたものとみなされます。

```
remote <number> bridge stp priority 128
```

8.6.7 remote bridge filter

[機能]

MAC フィルタの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] bridge filter <count> <action> acl <acl_count> [direction]

remote [<number>] bridge filter <count> <action> <src_mac> <dst_mac> <format> [<value> [<vlan_analyze>]]

[オプション]

<number>

・ 相手定義番号

相手ネットワークの通し番号を、10 進数で指定します。

省略時は、0 を指定したものとみなされます。

<count>

・ フィルタリング定義番号

フィルタリングの優先度を表す番号を、10 進数で指定します。

指定した値は、設定完了時に順方向にソートされリナンバリングされます。

指定した定義番号と同じ値を持つ定義がすでに存在する場合は、既存の設定に対する修正とみなされます。指定した値を持つ定義が存在しない場合は、追加とみなされます。

範囲	機種
0～255	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～127	Si-R180B

<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
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～143	Si-R180B

<direction>

フィルタリングする方向を指定します。

ACL を利用した定義でのみ指定可能です。

省略時は、any を指定したものとみなされます。

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

<src_mac>

フィルタリング対象とする送信元 MAC アドレスを指定します。

- any
  すべての MAC アドレスを対象とする場合に指定します。
- bcast
  ブロードキャスト MAC アドレスを対象とする場合に指定します。
- mcast
  マルチキャスト MAC アドレスを対象とする場合に指定します。
- 上記以外
  対象とする MAC アドレスを指定します。フィルタリング対象とする送信元 MAC アドレスを、xx:xx:xx:xx:xx:xx(xx は 2 桁の 16 進数)の形式で指定します。

<dst_mac>

フィルタリング対象とするあて先 MAC アドレスを指定します。

- any
  すべての MAC アドレスを対象とする場合に指定します。
- bcast
  ブロードキャスト MAC アドレスを対象とする場合に指定します。
- mcast
  マルチキャスト MAC アドレスを対象とする場合に指定します。
- 上記以外
  対象とする MAC アドレスを指定します。フィルタリング対象とする送信元 MAC アドレスを、xx:xx:xx:xx:xx:xx(xx は 2 桁の 16 進数)の形式で指定します。

<format> <value>

- llc
  <value>の値と LSAP が一致する LLC 形式フレームを対象とする場合に指定します。<value>には、0～ffff の 16 進数を指定します。
- ether
  <value>の値とタイプが一致する Ethernet 形式フレームを対象とする場合に指定します。<value>には、5dd～ffff の 16 進数を指定します。
- any
  すべてのフレームを対象とする場合に指定します。<value>は、指定不要です。

<vlan_analyze>

VLAN タグ付きフレームに対してタグの解析を行うかどうかを指定します。

<value>を指定したときだけ指定可能です。

省略時は、off を指定したものとみなされます。

- on
  VLAN タグ付きフレームの場合に VLAN タグを解析してフィルタリング処理を行います。VLAN タグ付きフレームの場合は、タグの長さ分ずれた位置にある LLC 形式フレームの LSAP や Ethernet 形式フレームのタイプに対してフィルタリング処理を行います。

・off

VLANタグ付きフレームの場合にVLANタグを解析しないでフィルタリング処理を行います。VLANタグ付きフレームの場合でもタグの長さ分ずらさずにそのままフィルタリング処理を行うため、VLANタグのTPIDが、<value>との比較対象になります。

[動作モード]

構成定義モード(管理者クラス)

[説明]

MACフィルタを設定します。

本コマンドは、ブリッジ機能を使用する場合にだけ有効です。

指定した条件に一致するフレームを、指定した<action>に従って遮断または通過させます。MACフィルタは、本装置全体で以下の数まで定義できます。

最大定義数	機種
256	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
128	Si-R180B

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

最大定義数	機種
9000	Si-R570 Si-R570B
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
432	Si-R180B

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

[注意]

IPおよびIPv6以外のネットワークプロトコル(IPXなど)をルーティングしているネットワークでブリッジを使用する場合は、ブリッジによって中継されることでネットワークがダウンすることがあります。ルーティングと併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。

8.6.8 remote bridge filter move

[機能]

MAC フィルタの優先順序の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] bridge filter move <count> <new_count>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

・ 対象フィルタリング定義番号
優先順序を変更する前のフィルタリング定義の番号を指定します。

<new_count>

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

範囲	機種
0～255	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～127	Si-R180B

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

8.6.9 remote bridge priority

[機能]

帯域制御の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] bridge priority <count> acl <acl_count> <width>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

・ 帯域制御定義番号
帯域制御定義番号を、10 進数で指定します。

範囲	機種
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

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

範囲	機種
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～143	Si-R180B

<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～100000kbps または 1mbps～100mbps の範囲で指定します。全定義の帯域の合計が回線速度を超えた場合は、それぞれ指定した値の比で帯域を割り当てます。指定した値の合計値が回線速度に達しない場合、残った帯域は定義に一致しないデータ用の帯域となります。

「"share" + 数字」で指定した場合、数字で指定した帯域制御定義番号で定義された帯域を共有します。この場合、指定する数字は自分自身の帯域制御定義番号より小さい、すでに定義されているものを指定しなければなりません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

帯域制御を設定します。任意の ACL 番号を指定して、割り当てる帯域を指定します。

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

最大定義数	機種
9000	Si-R570 Si-R570B
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
432	Si-R180B

[注意]

使用する回線が LAN の場合、シェーピングを使用しないと帯域制御機能は有効に動作しません。

使用する回線が ATM の場合、適切な VC 速度を設定しないと帯域制御機能は有効に動作しません。

[未設定時]

帯域制御を行わないものとみなされます。

8.7 MPLS 関連情報

8.7.1 remote mpls use

[機能]

MPLS 機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] mpls use <mode>

[オプション]

<number>

・ 相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<mode>

・ on
MPLS を利用します。
・ off
MPLS を利用しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

MPLS を利用するかどうかを設定します。

[未設定時]

off が選択されたものとして動作します。

```
remote <number> mpls use off
```

8.7.2 remote mpls distribution

[機能]

ラベル配布プロトコルの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] mpls distribution <protocol>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<protocol>

・ldp
ラベル配布プロトコルに LDP を使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ラベル配布プロトコルを指定します。

[未設定時]

ldp が選択されたものとして動作します。

```
remote <number> mpls distribution ldp
```

8.7.3 remote mpls ldp hello-timers

[機能]

LDP Hello に関するタイマの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] mpls ldp hello-timers <interval> <holdtime>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<interval>

・Hello 送信間隔のタイマ値
Hello の送信間隔を、1～65535 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のどれかを指定します。

<holdtime>

・HoldTime のタイマ値
近隣関係の維持を判定するための HoldTime を、1～65534 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のどれかを指定します。
・infinity
近隣関係の維持を判定するための HoldTime を infinity(0xffff:無限)とします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

LDP 近隣関係の維持に用いられる Hello パケットの送信間隔と HoldTime を設定します。
HoldTime の値は interval の値より小さくすることはできません。
HoldTime の値は interval の値の 3 倍以上を設定することを推奨します。

[注意]

HoldTime は近隣関係にある LDP ルータとネゴシエーションし、値の小さい方が採用されますが、送信間隔はネゴシエーションしないため、相手 LSR のタイマ設定と自装置のタイマ設定を一致させておくことを推奨します。

[未設定時]

interval が 5 秒、HoldTime が 15 秒として動作します。

```
remote <number> mpls ldp hello-timers 5s 15s
```

8.7.4 remote mpls ldp keepalive-timers

[機能]

LDP KeepAlive に関するタイマの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] mpls ldp keepalive-timers <interval> <timeout>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<interval>

・KeepAlive 送信間隔のタイマ値
KeepAlive の送信間隔を、1～65535 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のどれかを指定します。

<timeout>

・KeepAlive タイムアウトのタイマ値
LDP セッションの維持を判定するためのタイムアウト時間を、1～65535 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のどれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

LDP セッションの維持に用いられる KeepAlive メッセージの送信間隔とタイムアウトを設定します。
timeout の値は interval の値より小さくすることはできません。
timeout の値は interval の値の 3 倍以上を設定することを推奨します。

[注意]

タイムアウトは近隣関係にある LDP ルータとネゴシエーションし、値の小さい方が採用されますが、送信間隔はタイムアウトのネゴシエーション結果の 3 分の 1 の値とこのコマンドで設定された送信間隔とを比較し、値が小さい方が送信間隔として採用されます。

[未設定時]

interval が 1 分、timeout が 3 分として動作します。

```
remote <number> mpls ldp keepalive-timers 1m 3m
```

8.7.5 remote mpls ldp advertisement

[機能]

LDP ラベル広報方式の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] mpls ldp advertisement <mode>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<mode>

・dod
Downstream On Demand を使用します。
・du
Downstream Unsolicited を使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

LDP のラベル広報方式を指定します。

[未設定時]

du が選択されたものとして動作します。

```
remote <number> mpls ldp advertisement du
```

8.7.6 remote mpls ldp retention

[機能]

LDP ラベル保持方式の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] mpls ldp retention <mode>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<mode>

・liberal
Liberal Label Retention Mode を使用します。
・conservative
Conservative Label Retention Mode を使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

LDP のラベル保持方式を指定します。

[未設定時]

liberal が選択されたものとして動作します。

```
remote <number> mpls ldp retention liberal
```

8.7.7 remote mpls ldp interface-label

[機能]

PHP の無効化

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] mpls ldp interface-label <mode>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<mode>

・off
インタフェースの IP アドレスにラベルを割り当てません。

・on
インタフェースの IP アドレスにラベルを割り当てます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

インタフェースの IP アドレスに対してラベルを割り当てるかどうかを指定します。
割り当てた場合は、インタフェースあての LSP の PHP を無効にすることができます。

[注意]

MPLS トンネル接続機能を使用する場合、自側エンドポイントと IP アドレスが同一のとき、本設定によらず、PHP 機能は無効となります。

[未設定時]

off が選択されたものとして動作します。

```
remote <number> mpls ldp interface-label off
```

8.7.8 remote mpls ldp ip transport

[機能]

IPv4 Transport Address の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] mpls ldp ip transport <address>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<address>

・LDP セッションの送信元 IPv4 アドレス
IPv4 アドレスを指定します。以下の範囲で指定してください。

0.0.0.0
1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

[動作モード]

構成定義モード(管理者クラス)

[説明]

インタフェース単位で LDP が相手装置との通信に用いる送信元 IPv4 アドレスを分ける必要がある場合に、本装置に設定された IPv4 アドレスを指定します。
0.0.0.0 を指定した場合は、MPLS 情報の設定の IPv4 Transport Address の設定に従います。

[注意]

インタフェース単位で IPv4 Transport Address を設定する場合は、必ず本装置に存在するアドレスを指定してください。本装置に存在しないアドレスをインタフェースに指定した場合は、そのインタフェースでは LDP を使用できません。

[未設定時]

MPLS 情報の設定の IPv4 Transport Address の設定に従います。

```
remote mpls ldp ip transport 0.0.0.0
```

8.7.9 remote mpls ldp multicast-hello

[機能]

Multicast Helloの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

remote [<number>] mpls ldp multicast-hello <mode>

[オプション]

<number>

・相手定義番号
相手ネットワークの通し番号を、10進数で指定します。
省略時は、0を指定したものとみなされます。

<mode>

・off
LDP Multicast Helloパケットを送信しません。

・on
LDP Multicast Helloパケットを送信します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

LDP Multicast Helloを送出するかしないかを設定します。offに設定すると、Multicast Helloを送出しません。
本設定は、MPLS LSP トンネルを使用するREMOTEインタフェースの設定で、トンネルエンドポイントに指定した装置がEoMPLS通信の相手装置となる場合にoffに設定します。

[注意]

MPLS LSPトンネルを使用するREMOTEインタフェースのトンネルエンドポイントに指定した装置がEoMPLS通信の相手装置となる場合は、本設定を必ずoffに設定してください。
offに指定しない場合は、VCラベルを交換できない通常のLDPセッションが確立してしまうため、EoMPLS通信で用いるVC LSPができず、EoMPLS通信を行うことができません。
それ以外の場合では必ずonに設定してください。offに設定した場合はLDPの隣接関係が構築できず、LDPのセッションが確立できなくなります。

[未設定時]

on が設定されているものとみなされます。

```
remote mpls ldp multicast-hello on
```

8.8 SNMP 関連情報

8.8.1 remote snmp trap linkdown

[機能]

linkDown トラップの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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 service コマンドで旧バージョン互換 MIB モードに設定された場合、および snmp trap linkdown 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
```

8.8.2 remote snmp trap linkup

[機能]

linkUp トラップの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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 service コマンドで旧バージョン互換 MIB モードに設定された場合、および snmp trap linkdown 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 9 章　着信デフォルト情報の設定

9.1 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

9.1.1 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-R570 Si-R570B Si-R370 Si-R370B Si-R240B Si-R220C Si-R220D

[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
```

9.1.2 answer ppp auth type

[機能]

着信認証方式の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R240B Si-R220C Si-R220D

[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
```

9.1.3 answer ppp auth receive add

[機能]

受諾認証情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

answer ppp auth receive add <id> <password> [encrypted]

[オプション]

<id>

・受諾認証 ID
受諾認証 ID を、0x21,0x23～0x7e のコードで構成される 64 文字以内の ASCII 文字列で指定します。

<password>

・受諾認証パスワード
受諾認証パスワードを、0x21,0x23～0x7e のコードで構成される 64 文字以内の文字列で指定します。

・暗号化された受諾認証パスワード
show コマンドで表示される暗号化された受諾認証パスワードを encrypted と共に指定します。
show コマンドで表示される文字列をそのまま正確に指定してください。

<encrypted>

・暗号化受諾認証パスワード
<password>に暗号化された受諾認証パスワードを設定する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

相手情報の設定に受諾認証情報の設定がない場合に利用される受諾認証情報を設定します。
この情報は、発信者番号(CLID)で相手が判別できた場合に利用されます。

[注意]

発信者番号(CLID)で相手が判別できなかった場合は、この情報は利用されません。
show コマンドでは、暗号化された受諾認証パスワードが encrypted と共に表示されます。

[未設定時]

受諾認証 ID は定義されません。

9.1.4 answer ppp mp use

[機能]

着信時の MP 利用可否の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

answer ppp mp use <mode>

[オプション]

<mode>

MP を利用するかどうかを指定します。

- off
  MP を利用しない場合に指定します。
- on
  MP を利用する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

発信者番号(CLID)で相手が判別できない着信について、MP を利用するかどうかを設定します。

[未設定時]

MP を利用しないものとみなされます。

```
answer ppp mp use off
```

9.1.5 answer ppp mp bap use

[機能]

着信時の BAP/BACP 利用可否の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

answer ppp mp bap use <mode>

[オプション]

<mode>

BAP/BACP を利用するかどうかを指定します。

- off
  BAP/BACP を利用しない場合に指定します。
- on
  BAP/BACP を利用する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

発信者番号(CLID)で相手が判別できない着信について、BAP/BACP を利用するかどうかを設定します。

[未設定時]

BAP/BACP を利用しないものとみなされます。

```
answer ppp mp bap use off
```

第 10 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
0～5	Si-R570 Si-R570B Si-R370 Si-R370B
0～2	Si-R220C Si-R220D
0～1	Si-R260B Si-R240B Si-R180B

10.1 テンプレート共通情報

10.1.1 template name

[機能]

テンプレート名称の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

10.1.2 template mtu

[機能]

送信パケット最大長(MTU 値)の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

10.1.3 template idle

[機能]

無通信監視タイマの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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)のどれかを指定します。
0 秒を指定した場合は、監視を行いません。

<direction>

・省略
送信パケット、および受信パケットを通信監視の対象とします。
・send
送信パケットのみを通信監視の対象とします。受信パケットは監視対象とはなりません。
・receive
受信パケットのみを通信監視の対象とします。送信パケットは監視対象とはなりません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

指定した接続先と接続したときの無通信監視時間を設定します。
<time>で設定された間、監視対象となるパケットがない場合に、無通信として回線を切断します。

[注意]

パケット転送方法に ipsec を指定した場合、無通信監視時間に 1 秒以上 10 秒未満の範囲で指定したときに 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
```

10.1.4 template interface pool

[機能]

テンプレート着信で使用する rmt インタフェースの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～49	Si-R180B

<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
1000	Si-R570 Si-R570B
500	Si-R370 Si-R370B
100	Si-R260B Si-R240B Si-R220C Si-R220D
50	Si-R180B

[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。)

10.1.5 template aaa

[機能]

参照する AAA 情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

10.1.6 template datalink type

[機能]

パケット転送方法の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<type>

パケットの転送方式を指定します。

・physical
bind 命令(template ap datalink bind を参照)によって決定された利用回線のデフォルトの転送方式を提供する場合に指定します。以下に各回線のデフォルトの転送方式を示します。
(※Si-R260B Si-R240B Si-R180B では指定できません)

回線種別	転送方式	Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D	Si-R260B Si-R240B Si-R180B
ISDN	PPP	○	-

・ipsec
IPsec を使用する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

テンプレート着信で使用する rmt インタフェースを利用してパケットを転送する場合の転送方式を設定します。

[未設定時]

転送方式として physical を設定するものとみなされます。

```
template <number> datalink type physical
```

Si-R260B Si-R240B Si-R180B の場合は、パケット転送方式を設定しないものとみなされます。

10.1.7 template datalink bind

[機能]

テンプレート着信で使用する回線の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

template [<number>] datalink bind <kind> [<conf_number>]

[オプション]

<number>

・ テンプレート定義番号
テンプレート定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<kind>

・ wan
wan 定義によって指定される回線を利用する場合に指定します。
・ any
ISDN を使用するように設定した、すべての wan 定義を指定したものとみなされます。

<conf_number>

wan 定義の定義番号を指定します。

・ wan 定義の定義番号
利用する wan 定義の定義番号を、10 進数で指定します。

範囲	機種
0～131	Si-R570 Si-R570B
0～15	Si-R370 Si-R370B
0	Si-R220C Si-R220D

[動作モード]

構成定義モード(管理者クラス)

[説明]

テンプレート着信で使用する回線を設定します。

[未設定時]

<kind>に wan を、<conf_number>に 0 を指定するものとみなされます。

```
template <number> datalink bind wan 0
```

10.1.8 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<function>

テンプレートが利用する機能を指定します。

・ dvpn
動的 VPN 機能を利用する場合に指定します。

・ aaa
不特定相手着信機能を利用する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

テンプレートが利用する機能を指定します。

[未設定時]

不特定相手着信機能の利用を指定したものとみなされます。

```
template <number> combine use aaa
```

10.1.9 template tunnel local

[機能]

トンネル利用時の自側のトンネルエンドポイントアドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<address>

・自側のトンネルエンドポイントアドレス

自側のトンネルエンドポイントとなる IPv4 アドレスまたは IPv6 アドレスを指定します。本装置に設定されている IP アドレスを指定してください。

指定可能な範囲は以下のとおりです。

IPv4:

1.0.0.1 ～ 126.255.255.254

128.0.0.1 ～ 191.255.255.254

192.0.0.1 ～ 223.255.255.254

IPv6:

::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff

fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

IPv6 DHCP クライアントが取得したプレフィックスを使用する場合は上位を"dhcp@インタフェース名"の形式で指定し、下位 80bit 分を IPv6 アドレス形式で指定します。インタフェース名には、rmt インタフェースを以下の範囲で指定します。

範囲	機種
rmt0～rmt999	Si-R570 Si-R570B
rmt0～rmt499	Si-R370 Si-R370B
rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
rmt0～rmt49	Si-R180B

例)

rmt0 で動作する IPv6 DHCP クライアントが取得した IPv6 プレフィックスを使用する場合の設定例

```
dhcp@rmt0::
dhcp@rmt0::1:2:3:4
```

[動作モード]

構成定義モード(管理者クラス)

[説明]

指定したテンプレート着信定義にトンネル利用が設定されている場合に、そのトンネルの自側エンドポイントアドレスを設定します。

IPsec を利用して通信を行う場合は、本コマンドを必ず実行してください。

[注意]

IPsec/IKE の AAA または RADIUS を利用した構成の場合では、IPv6 DHCP クライアントが取得したプレフィックスは使用できません。

また、トンネルの自側エンドポイントアドレスは一意になるように指定してください。

動的 VPN 機能を利用した構成で IPv6 DHCP クライアントが取得したプレフィックスを使用する場合、プレフィックスが割り当てられるインタフェースと同じ値になるように指定してください。

[未設定時]

自側のトンネルエンドポイントアドレスを設定しないものとみなされます。

10.1.10 template sessionwatch address

[機能]

接続先監視アドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<source>

・ICMP ECHO パケットの送信元 IP アドレス

ICMP ECHO パケットの送信元 IP アドレスを指定します。装置に設定されている自側 IPv4/IPv6 アドレスのどれかを指定してください。

指定可能な範囲は以下のとおりです。

IPv4:

1.0.0.1 ～ 126.255.255.254

128.0.0.1 ～ 191.255.255.254

192.0.0.1 ～ 223.255.255.254

IPv6:

::2 ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

IPv6 DHCP クライアントが取得したプレフィックスを使用する場合は上位を"dhcp@インタフェース名"の形式で指定し、下位 80bit 分を IPv6 アドレス形式で指定します。インタフェース名には、rmt インタフェースを以下の範囲で指定します。

範囲	機種
rmt0～rmt999	Si-R570 Si-R570B
rmt0～rmt499	Si-R370 Si-R370B
rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
rmt0～rmt49	Si-R180B

例)

rmt0 で動作する IPv6 DHCP クライアントが取得した IPv6 プレフィックスを使用する場合の設定例

```
dhcp@rmt0::
dhcp@rmt0::1:2:3:4
```

[動作モード]

構成定義モード(管理者クラス)

[説明]

テンプレートを利用した機能で接続先の生存確認を行うための接続先監視アドレスを設定します。

ICMP ECHO パケットの送受信で生存確認を行う際に指定した送信元 IP アドレスを使用します。

ICMP ECHO パケットのあて先 IP アドレスについては以下のアドレスを使用します。

パケットの転送方式(template datalink type)

・ipsec

テンプレートが利用する機能(template combine use)
- dvpn
  動的VPN情報交換で通知された接続先監視アドレス
- aaa
  AAAまたはRADIUSに設定された接続先監視アドレス

・ physical
監視を行いません。

[注意]

以下の場合では、監視を行いません。

・ RADIUSサーバに接続先監視アドレスを登録していない場合。
・ AAA情報に接続先監視アドレスを設定していない場合。
・ 動的VPN接続で接続相手と双方の接続先監視アドレスが交換できない場合。

また、IPsec/IKEのAAAまたはRADIUSを利用した構成の場合では、IPv6 DHCPクライアントが取得したプレフィックスは使用できません。

動的VPN機能を利用した構成でIPv6 DHCPクライアントが取得したプレフィックスを使用する場合、プレフィックスが割り当てられるインタフェースと同じ値になるように指定してください。

[未設定時]

接続先監視アドレスを設定しないものとみなされます。

10.1.11 template sessionwatch interval

[機能]

接続先監視のインターバル設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

	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	
無通信監視タイマあり	動的 VPN	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	無通信監視タイマの設定値で動作する	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
	RADIUS または AAA			
無通信監視タイマなし	動的 VPN	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が動作する	無通信監視タイマが 10 秒で設定されたものとみなし無通信監視タイマのみ動作する
	RADIUS または AAA	正常時送信間隔は設定値でその他は無通	無通信監視タイマが 10 秒で設定されたも	動作しない

	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	
		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	のとみなし接続先監視のみ動作する	

[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。

10.2 PPP 関連情報

10.2.1 template ppp auth type

[機能]

認証方法の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

```
template [<number>] ppp auth type <authtype>
```

[オプション]

<number>

・テンプレート定義番号
テンプレート定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<authtype>

認証プロトコルのタイプを指定します。

・pap
PAP による認証を要求する場合に指定します。

・chap_md5
MD5-CHAP による認証を要求する場合に指定します。

・any
MD5-CHAP または PAP による認証を要求し、実際に利用する認証プロトコルはネゴシエーションによって決定する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

着信時の認証方式を設定します。

[未設定時]

着信時の認証プロトコルに MD5-CHAP または PAP を用います。

```
template <number> ppp auth type any
```

10.2.2 template ppp compress

[機能]

データ圧縮機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

template [<number>] ppp compress <mode>

[オプション]

<number>

・テンプレート定義番号
テンプレート定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<mode>

・off
データ圧縮機能を使用しない場合に指定します。

・on
データ圧縮機能を使用する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

データ圧縮機能を使用するかどうか設定します。

[未設定時]

データ圧縮機能を使用しないものとみなされます。

```
template <number> ppp compress off
```

10.2.3 template ppp ipcp vjcomp

[機能]

VJ-Compression の利用の有無の設定

[適用機種]

Si-R570 | Si-R570B | Si-R370 | Si-R370B | | | Si-R220C | Si-R220D | |

[入力形式]

```
template [<number>] ppp ipcp vjcomp <mode>
```

[オプション]

<number>

・テンプレート定義番号
テンプレート定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<mode>

・enable
VJ ヘッダ圧縮を使用する場合に指定します。

・disable
VJ ヘッダ圧縮を使用しない場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

VJ ヘッダ圧縮機能(VJCOMP)を使用するかどうかを設定します。VJ ヘッダ圧縮機能は、RFC1144 に準拠しています。

[未設定時]

VJ ヘッダ圧縮機能を使用するものとみなされます。

```
template <number> ppp ipcp vjcomp enable
```

10.2.4 template ppp ipcp iphc

[機能]

IPv4 の IP ヘッダ圧縮(IPHC)の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

```
template [<number>] ppp ipcp iphc <mode>
```

[オプション]

<number>

・テンプレート定義番号
テンプレート定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<mode>

・enable
IP ヘッダ圧縮を使用する場合に指定します。
・disable
IP ヘッダ圧縮を使用しない場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv4 で、IP ヘッダ圧縮(IPHC)を使用するかどうかを設定します。IP ヘッダ圧縮機能は、圧縮方法が RFC2507/RFC2508 に、ネゴシエーション方法が RFC2509 に準拠しています。

[未設定時]

IP ヘッダ圧縮機能を使用しないものとみなされます。

```
template <number> ppp ipcp iphc disable
```

10.2.5 template ppp ipv6cp iphc

[機能]

IPv6 の IP ヘッダ圧縮(IPHC)の設定

[適用機種]

Si-R570 | Si-R570B | Si-R370 | Si-R370B | | | Si-R220C | Si-R220D |

[入力形式]

```
template [<number>] ppp ipv6cp iphc <mode>
```

[オプション]

<number>

・テンプレート定義番号
テンプレート定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<mode>

・enable
IP ヘッダ圧縮を使用する場合に指定します。
・disable
IP ヘッダ圧縮を使用しない場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6 で、IP ヘッダ圧縮(IPHC)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。

```
template <number> ppp ipv6cp iphc disable
```

10.3 IP 関連情報

10.3.1 template ip dns

[機能]

DNS サーバアドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

10.3.2 template ip address remote-pool

[機能]

相手に割り当てる IP アドレス範囲の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[入力形式]

template [<number>] ip address remote-pool <start> <num>

[オプション]

<number>

・テンプレート定義番号
テンプレート定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<start>

・割り当て先頭アドレス
割り当てる IP アドレスの先頭アドレスを指定します。
指定可能な範囲は以下のとおりです。

1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

<num>

・割り当てアドレス数
&templatepooladdrmax

最大アドレス数	機種
50	Si-R570 Si-R570B Si-R370 Si-R370B Si-R220C Si-R220D

[動作モード]

構成定義モード(管理者クラス)

[説明]

着信相手に対して、割り当てる IP アドレスの範囲を指定します。

[未設定時]

割り当てる IP アドレス範囲を設定しないものとみなされます。

10.3.3 template ip nat mode

[機能]

アドレス変換の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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)のどれかを指定します。
0 秒を指定した場合は、変換テーブル解放のための監視を行いません。
省略時は、5 分を指定したものとみなされます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

相手ネットワークに対するアドレス変換(NAT)の動作を設定します。

[未設定時]

アドレス変換は使用しないものとみなされます。

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

10.3.4 template ip nat static

[機能]

静的アドレス変換の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～499	Si-R570 Si-R570B
0～299	Si-R370 Si-R370B
0～199	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

<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
500	Si-R570 Si-R570B
300	Si-R370 Si-R370B
200	Si-R260B Si-R240B Si-R220C Si-R220D
64	Si-R180B

[未設定時]

静的アドレス変換は設定されません。

10.3.5 template ip nat static default

[機能]

テーブルに一致しないパケットの扱いの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

```
template [<number>] ip nat static default <action>
```

[オプション]

<number>

・テンプレート定義番号
テンプレート定義の通番として 0 以上の 10 進数を指定します。省略時は 0 と認識します。

<action>

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

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

・reject
該当するパケットを破棄します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[未設定時]

すべての NAT テーブルにも一致しないパケットは破棄します。

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

10.3.6 template ip nat rule

[機能]

アドレス変換ルールの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

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

[オプション]

<number>

・テンプレート定義番号
テンプレート定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

・変換ルール番号
変換ルール番号を、0～31 の 10 進数で指定します。

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

変換ルールの対象となるアプリケーションを指定します。

<server_addr>

・IP アドレス
NAT に割り当てたグローバルアドレス以外のアドレスを指定します。ここで指定したアドレスを変換ルールの対象とします。

・any
すべての IP アドレスを変換ルールの対象とします。
any を指定した場合は、グローバル側とプライベート側の両方のアプリケーションサーバに対応します。

・global
NAT に割り当てたグローバルアドレス以外のすべてのアドレスを変換ルールの対象とします。
global を指定した場合は、グローバル側のアプリケーションサーバに対応します。

・local
NAT に割り当てたグローバルアドレスを変換ルールの対象とします。
local を指定した場合は、プライベート側のアプリケーションサーバに対応します。

・off
指定したアプリケーションに対する変換ルールを無効にします。

<server_port>

アプリケーションサーバで待ち受けるポート番号を指定します。

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

10.3.7 template ip nat wellknown

[機能]

ポート番号変換の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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)
```

10.3.8 template ip nat destination

[機能]

あて先変換の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～499	Si-R570 Si-R570B
0～299	Si-R370 Si-R370B
0～199	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

<private_addr>

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

<global_addr>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

最大定義数	機種
500	Si-R570 Si-R570B
300	Si-R370 Si-R370B
200	Si-R260B Si-R240B Si-R220C Si-R220D
64	Si-R180B

[未設定時]

あて先変換は設定されません。

10.3.9 template ip nat appli

[機能]

アプリ対応の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<function>

設定する機能を指定します。

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

<mode>

・on
アプリ対応を有効にします。
・off
アプリ対応を無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

各アプリケーションに対する特殊対応を有効にするかどうかを設定します。

[注意]

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

[未設定時]

すべてのアプリ対応を有効にするとみなされます。

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

10.3.10 template ip filter

[機能]

IP フィルタの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～999	Si-R570 Si-R570B Si-R370 Si-R370B
0～199	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

<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
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

<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
1000	Si-R570 Si-R570B Si-R370 Si-R370B
200	Si-R260B Si-R240B Si-R220C Si-R220D
64	Si-R180B

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

最大定義数	機種
9000	Si-R570 Si-R570B
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
450	Si-R180B

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

[注意]

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

定義数の計算は「テンプレート情報で設定した定義数 x テンプレートで使用する rmt インタフェース数」で計算されますので、それを含めて装置最大定義数の範囲に収まるように定義してください。

装置最大定義数を超えた場合は資源不足により、該当機能が動作しない場合があります。

[未設定時]

IP フィルタを設定しないものとみなされます。

10.3.11 template ip filter move

[機能]

IP フィルタの優先順序の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～999	Si-R570 Si-R570B Si-R370 Si-R370B
0～199	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

[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。

10.3.12 template ip filter default

[機能]

どの IP フィルタテーブルにも不一致時の動作の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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)のどれかを指定します。
0 秒を指定した場合は、変換テーブル解放のための監視を行いません。
省略時は、5 分を指定したものとみなされます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

どの IP フィルタテーブルに一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

どの IP フィルタテーブルにも一致しないパケットは透過します。

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

10.3.13 template ip tos

[機能]

TOS 値書き換え条件の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～499	Si-R570 Si-R570B Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～31	Si-R180B

<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
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

<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
500	Si-R570 Si-R570B Si-R370 Si-R370B
100	Si-R260B Si-R240B Si-R220C Si-R220D
32	Si-R180B

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

最大定義数	機種
9000	Si-R570 Si-R570B
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
450	Si-R180B

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

[注意]

定義数の計算は「テンプレート情報で設定した定義数 x テンプレートで使用するrmtインタフェース数」で計算されますので、それを含めて装置最大定義数の範囲に収まるように定義してください。
装置最大定義数を超えた場合は資源不足により、該当機能が動作しない場合があります。

[未設定時]

TOS値書き換えを行わないものとみなされます。

10.3.14 template ip tos move

[機能]

TOS 値書き換え条件の優先度の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～499	Si-R570 Si-R570B Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～31	Si-R180B

[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。

10.3.15 template ip priority

[機能]

帯域制御の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

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

[オプション]

<number>

・テンプレート定義番号
テンプレート定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

・帯域制御定義番号
帯域制御定義番号を、10 進数で指定します。

範囲	機種
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

<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、ip6 の<protocol>値が 1 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B

範囲	機種
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

<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～100000kbps または 1mbps～100mbps の範囲で指定します。全定義の帯域の合計が回線速度を超えた場合は、それぞれ指定した値の比で帯域を割り当てます。

指定した値の合計値が回線速度に達しない場合、残った帯域は定義に一致しないデータ用の帯域となります。

「"share" + 数字」で指定した場合、数字で指定した帯域制御定義番号で定義された帯域を共有します。この場合、指定する数字は自分自身の帯域制御定義番号より小さい、すでに定義されてあるもの指定しなければなりません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

帯域制御を設定します。任意のプロトコル、アドレス、ポート、TOS 値を指定して、割り当てる帯域を指定します。

帯域制御の旧定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
1000	Si-R570 Si-R570B
500	Si-R370 Si-R370B
100	Si-R260B Si-R240B Si-R220C Si-R220D
64	Si-R180B

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

最大定義数	機種
9000	Si-R570 Si-R570B

最大定義数	機種
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
450	Si-R180B

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]

帯域制御を行わないものとみなされます。

10.3.16 template ip msschange

[機能]

MSS 書き換えの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

10.3.17 template ip ids use

[機能]

IDS の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

10.3.18 template ip in-policy

[機能]

Ingress ポリシールーティングの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<in-policy_number>

・Ingress ポリシールーティング定義番号
この I/F での Ingress ポリシールーティング定義の通し番号を、10 進数で指定します。
本定義は、ほかのポリシーグループ参照定義を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
2000	Si-R570 Si-R570B
1000	Si-R370 Si-R370B
200	Si-R260B Si-R240B Si-R220C Si-R220D
100	Si-R180B

<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
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R220C Si-R220D

範囲	機種
0～49	Si-R180B

[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。

10.3.19 template ip in-policy move

[機能]

Ingress ポリシールーティングの優先順序の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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 IPv6 関連情報

10.4.1 template ip6 use

[機能]

IPv6 機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

```
template [<number>] ip6 use <mode>
```

[オプション]

<number>

・ テンプレート定義番号
テンプレート定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<mode>

IPv6 パケットの送受信を行うかどうか指定します。

・ on
テンプレート着信で使用する rmt インタフェースで、IPv6 パケットの送受信を行います。

・ off
テンプレート着信で使用する rmt インタフェースで、IPv6 パケットの送受信を行いません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

テンプレート着信で使用する rmt インタフェースで、IPv6 機能を利用するかどうかを設定します。

[未設定時]

IPv6 機能を利用しないものとみなされます。

```
template <number> ip6 use off
```

10.4.2 template ip6 ifid

[機能]

IPv6 インタフェース ID の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

```
template [<number>] ip6 ifid <interfaceID>
```

[オプション]

<number>

・テンプレート定義番号
テンプレート定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<interfaceID>

テンプレート着信で使用する rmt インタフェースで利用する ID を指定します。

・auto
本装置が持つ MAC アドレスから、EUI-64 形式の ID を自動生成する場合に指定します。

・インタフェース ID
rmt インタフェースで利用する ID を、16 進数で指定します。4 桁ずつ":"(コロン)で区切ってください。なお、各フィールドの先頭の 0 は省略できます(例: 2a0:c9ff:fe84:759)。

通常は auto を指定してください。特定のインタフェース ID を指定する場合は、同一の link 上でホストと衝突しない値を指定してください。

[動作モード]

構成定義モード(管理者クラス)

[説明]

テンプレート着信で使用する rmt インタフェースで利用する、インタフェース ID を設定します。

[未設定時]

インタフェース ID を自動生成するものとみなされます。

```
template <number> ip6 ifid auto
```

10.4.3 template ip6 filter

[機能]

IPv6 フィルタの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

```
template [<number>] ip6 filter <count> <action> acl <acl_count> [<direction>]
template [<number>] ip6 filter <count> <action> <src_addr>/<prefixlen> <src_port><dst_addr>/
<prefixlen> <dst_port> <protocol> <tcpconnect>[<trafficclass> [<direction> [<icmptype>
[<icmpcode>]]]]
```

[オプション]

<number>

・テンプレート定義番号

テンプレート定義の通し番号を、10 進数で指定します。

省略時は、0 を指定したものとみなされます。

<count>

・フィルタリング定義番号

フィルタリングの優先度を表す番号を、10 進数で指定します。

指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つフィルタリング定義がすでに存在する場合は、既存の定義を変更します。

範囲	機種
0～999	Si-R570 Si-R570B Si-R370 Si-R370B
0～199	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

<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。

- ip6

  ip6 値が設定されていない場合、そのフィルタ定義は無効となり、無視されます。

- tcp

  ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip6 の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。

- udp

  ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip6 の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp

ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。
また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

<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 として扱われます。

<direction>

フィルタリングする方向を指定します。

省略時は、any を指定したものとみなされます。

・ any

入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。

・ in

入力パケットのみをフィルタリング対象とする場合に指定します。

・ out

出力パケットのみをフィルタリング対象とする場合に指定します。

・ reverse

入力パケットと出力パケットの両方をフィルタリング対象とします。

ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。

- 送信元 IP アドレス/プレフィックス長とあて先 IP アドレス/プレフィックス長
- 送信元ポート番号とあて先ポート番号

<icmptype>

フィルタリングする ICMPv6 メッセージタイプ番号を指定します。

・ フィルタリング対象 icmptype 値

フィルタリング対象となる icmptype フィールドの値を 0-255 までの 10 進数、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 として扱われます。

<icmpcode>

フィルタリングする ICMPv6 メッセージコード番号を指定します。

icmpcode 指定時は、icmptype も指定する必要があります。

・ フィルタリング対象 icmpcode 値

フィルタリング対象となる icmpcode フィールドの値を 0-255 までの 10 進数、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 として扱われます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

相手ネットワークに対する IPv6 フィルタを設定します。

各パラメタに設定された値によって、動作が変化する場合があります。以下に説明します。

・ <protocol>に指定した値によって、IPv6 拡張ヘッダの扱いが以下のように変化します。
  - any を指定した場合は、0 個以上の IPv6 拡張ヘッダを含む、あらゆる upper-layer protocol(upper-layer protocol なしを含む)に一致します。
  - 以下の IPv6 拡張ヘッダの値を指定した場合は、その拡張ヘッダが付与されている、あらゆる upper-layer protocol(upper-layerprotocol なしを含む)のパケットが一致します。

  0
  Hop-by-Hop Options Header

  43
  Routing Header

  44
  Fragment Header

  60
  Destination Options Header

  - 以下の値を指定した場合は、0 個以上の IPv6 拡張ヘッダ(AH、ESP、IPComp を除く)を含む、upper-layer protocol ヘッダが付与されていないパケットが一致します。

  59
  no next header

  - その他の値が設定されている場合は、upper-layer protocol ヘッダの protocol 番号に等しい値であるパケットが一致します。この場合、AH、ESP、IPComp を除くすべての IPv6 拡張ヘッダは無視されます。パケット中に AH、ESP が設定されている場合は、それ以降の拡張ヘッダおよび upper-layer protocol ヘッダの解釈は行いません。

・ <src_port>、<dst_port>に指定した値によって、<protocol>の扱いが以下のように変化します。
  - <protocol>に any を指定し、かつ<src_port>、<dst_port>のどちらか、または両方を指定している場合、TCP および UDP パケットの該当ポート番号を持つパケットのみが一致します。
  - <protocol>に TCP(6)または UDP(17)を指定し、かつ<src_port>、<dst_port>のどちらか、または両方を指定している場合、指定プロトコルの該当ポート番号を持つパケットのみが一致します。
  - <protocol>に TCP(6)または UDP(17)以外を指定し、かつ<src_port>、<dst_port>のどちらか、または両方を指定している場合、あらゆるパケットが一致しません。

・ <icmptype>、<icmpcode>に指定した値によって、<protocol>の扱いが以下のように変化します。
  - <protocol>に any を指定し、かつ<icmptype>、<icmpcode>を指定している場合、ICMPv6 パケットの該当 type/code 番号を持つパケットのみが一致します。
  - <protocol>に ICMPv6(58)を指定し、かつ<icmptype>、<icmpcode>を指定している場合、指定プロトコルの該当 type/code 番号を持つパケットのみが一致します。
  - <protocol>に ICMPv6(58)以外を指定し、かつ<icmptype>、<icmpcode>を指定している場合、あらゆるパケットが一致しません。

・ <tcpconnect>の扱いを以下に示します。
  - <protocol>に any を指定した場合、TCP パケットのときにこの設定値が適用されます。
  - <protocol>に TCP(6)を指定した場合、常にこの設定値が適用されます。
  - <protocol>に any または TCP(6)以外を指定した場合、この設定値は適用されません。

IPv6 フィルタリングの旧定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
1000	Si-R570 Si-R570B Si-R370 Si-R370B
200	Si-R260B Si-R240B Si-R220C Si-R220D
64	Si-R180B

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

最大定義数	機種
9000	Si-R570 Si-R570B
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
450	Si-R180B

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。

10.4.4 template ip6 filter move

[機能]

IPv6 フィルタの優先順序の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

```
template [<number>] ip6 filter move <count> <new_count>
```

[オプション]

<number>

・ テンプレート定義番号
テンプレート定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

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

<new_count>

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

範囲	機種
0～999	Si-R570 Si-R570B Si-R370 Si-R370B
0～199	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

[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。

10.4.5 template ip6 filter default

[機能]

どの IP フィルタテーブルにも不一致時の動作の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

```
template [<number>] ip6 filter default <action> [<time>]
```

[オプション]

<number>

・テンプレート定義番号
テンプレート定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<action>

どの IPv6 フィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

・pass
該当するパケットを透過します。

・reject
該当するパケットを遮断します。

・spi
該当するパケットに対して SPI を動作させます。

<time>

・割り当て時間
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)のどれかを指定します。
0 秒を指定した場合は、変換テーブル解放のための監視を行いません。
省略時は、5 分を指定したものとみなされます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

どの IPv6 フィルタテーブルにも一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

どの IPv6 フィルタテーブルにも一致しないパケットは透過します。

```
template <number> ip6 filter default pass
```

10.4.6 template ip6 trafficclass

[機能]

トラフィッククラス値書き換え条件の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

```
template [<number>] ip6 trafficclass <count> acl <acl_count> <new_trafficclass>
template [<number>] ip6 trafficclass <count> <src_addr>/<prefixlen> <src_port><dst_addr>/
<prefixlen> <dst_port> <protocol> <trafficclass> <new_trafficclass>
```

[オプション]

<number>

・テンプレート定義番号

テンプレート定義の通し番号を、10 進数で指定します。

省略時は、0 を指定したものとみなされます。

<count>

・Traffic Class 値書き換え定義番号

Traffic Class 値書き換え条件の優先度を表す定義番号を、10 進数で指定します。

指定した値は、設定完了時に順方向にソートされてリナンバリングされます。

また、指定した定義番号と同じ値を持つ Traffic Class 値書き換え定義がすでに存在する場合は、既存定義の値を変更します。

範囲	機種
0～499	Si-R570 Si-R570B Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～31	Si-R180B

<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。

- ip6

  ip6 値が設定されていない場合、その定義は無効となり、無視されます。

- tcp

  ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip6 の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。

- udp

  ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip6 の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp

  ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0～2999	Si-R570 Si-R570B

範囲	機種
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

<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
500	Si-R570 Si-R570B Si-R370 Si-R370B
100	Si-R260B Si-R240B Si-R220C Si-R220D
32	Si-R180B

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

最大定義数	機種
9000	Si-R570 Si-R570B
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
450	Si-R180B

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。

10.4.7 template ip6 trafficclass move

[機能]

Traffic Class 値書き換え条件の優先度の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

template [<number>] ip6 trafficclass move <count> <new_count>

[オプション]

<number>

・ テンプレート定義番号
テンプレート定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

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

<new_count>

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

範囲	機種
0～499	Si-R570 Si-R570B Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～31	Si-R180B

[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。

10.4.8 template ip6 priority

[機能]

IPv6 プロトコル帯域制御の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

```
template [<number>] ip6 priority <count> acl <acl_count> <width>
template [<number>] ip6 priority <count> <src_addr>/<prefixlen> <src_port><dst_addr>/<prefixlen>
<dst_port> <protocol> <trafficclass> <width>
```

[オプション]

<number>

・テンプレート定義番号

テンプレート定義の通し番号を、10 進数で指定します。

省略時は、0 を指定したものとみなされます。

<count>

・帯域制御定義番号

帯域制御定義番号を、10 進数で指定します。

範囲	機種
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～63	Si-R180B

<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。

- ip6

  ip6 値が設定されていない場合、その定義は無効となり、無視されます。

- tcp

  ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip6 の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。

- udp

  ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip6 の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。

- icmp

  ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。

  また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B

範囲	機種
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

<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として扱われます。

<width>

・ express

最優先データとして扱います。

・ besteffort

非優先(ベストエフォート)として扱います。

・ 帯域

1～99の10進数で指定した場合、それぞれ指定した値の比で帯域を割り当てます。たとえば、同じ相手ネットワーク中の定義が3つあり、それぞれ<width>の値が30、30、60であった場合、帯域として25%、25%、50%が割り当てられます。なお、1～99を指定した定義のそれぞれの合計値が100未満の場合、残った帯域は定義に一致しないデータ用の帯域となります。

「数字 + "kbps"(,"mbps")」で指定した場合、指定した帯域をそのまま割り当てます。1kbps～100000kbpsまたは1mbps～100mbpsの範囲で指定します。全定義の帯域の合計が回線速度を超えた場合は、それぞれ指定した値の比で帯域を割り当てます。

指定した値の合計値が回線速度に達しない場合、残った帯域は定義に一致しないデータ用の帯域となります。

「"share" + 数字」で指定した場合、数字で指定した帯域制御定義番号で定義された帯域を共有します。この場合、指定する数字は自分自身の帯域制御定義番号より小さい、すでに定義されてあるもの指定しなければなりません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv6プロトコル帯域制御を設定します。任意のプロトコル、アドレス、ポート、トラフィッククラスを指定して、割り当てる帯域を指定します。

IPv6プロトコル帯域制御の旧定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
1000	Si-R570 Si-R570B
500	Si-R370 Si-R370B
100	Si-R260B Si-R240B Si-R220C Si-R220D
64	Si-R180B

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

最大定義数	機種
9000	Si-R570 Si-R570B
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
450	Si-R180B

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

[注意]

ISDN、専用線、フレームリレー以外の回線上で帯域制御機能を使用する場合は、シェーピングを使用しないと帯域制御は有効に動作しません。

定義数の計算は「テンプレート情報で設定した定義数 x テンプレートで使用する rmt インタフェース数」で計算されますので、それを含めて装置最大定義数の範囲に収まるように定義してください。

装置最大定義数を超えた場合は資源不足により、該当機能が動作しない場合があります。

[未設定時]

IPv6 プロトコル帯域制御を行わないものとみなされます。

10.4.9 template ip6 in-policy

[機能]

Ingress ポリシールーティングの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

template [<number>] ip6 in-policy <in-policy_number> policy-group <policy-group_number>

[オプション]

<number>

・テンプレート定義番号
テンプレート定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<in-policy_number>

・Ingress ポリシールーティング定義番号
この I/F での Ingress ポリシールーティング定義の通し番号を、10 進数で指定します。
本定義は、ほかのポリシーグループ参照定義を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
2000	Si-R570 Si-R570B
1000	Si-R370 Si-R370B
200	Si-R260B Si-R240B Si-R220C Si-R220D
100	Si-R180B

<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。

- ip6
  ip6 値が設定されていない場合、その定義は無効となり、無視されます。
- tcp
  ip6 の<protocol>値が 6 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 6 のときに tcp 値が設定されていない場合、tcp の各値は any とみなされます。
- udp
  ip6 の<protocol>値が 17 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 17 のときに udp 値が設定されていない場合、udp の各値は any とみなされます。
- icmp
  ip6 の<protocol>値が 58 のときだけ有効となります。それ以外のとき、設定値は無視されます。
  また、ip6 の<protocol>値が 58 のときに icmp 値が設定されていない場合、icmp の各値は any とみなされます。

範囲	機種
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R220C Si-R220D

範囲	機種
0～49	Si-R180B

[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。

10.4.10 template ip6 in-policy move

[機能]

Ingress ポリシールーティングの優先順序の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

```
template [<number>] ip6 in-policy move <count> <new_count>
```

[オプション]

<number>

・テンプレート定義番号
テンプレート定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<count>

・対象 Ingress ポリシールーティング定義番号
優先順序を変更するフィルタリング定義の番号を指定します。

<new_count>

・移動先 Ingress ポリシールーティング定義番号
<count>に対する新しい順序を、10 進数で指定します。
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 動的 VPN 関連情報

10.5.1 template dvpn client

[機能]

動的 VPN 接続で使用するクライアント情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
0～5	Si-R570 Si-R570B Si-R370 Si-R370B
0～2	Si-R240B Si-R220C Si-R220D
0～1	Si-R260B Si-R180B

[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。

10.5.2 template dvpn server address

[機能]

動的VPNサーバのアドレス、ポート番号の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<count>

・動的VPNサーバ定義番号
動的VPNサーバの定義番号を、0から1までの10進数で指定します。

<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。

[未設定時]

動的VPNサーバのアドレス、ポート番号を設定しないものとみなされます。

10.5.3 template dvpn server auth

[機能]

動的 VPN サーバの認証情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<count>

・動的 VPN サーバ定義番号
動的 VPN サーバの定義番号を、0 から 1 までの 10 進数で指定します。

<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。

10.5.4 template dvpn expire register

[機能]

動的 VPN の情報有効期間の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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)のどれかを指定します。
省略時は 1h が指定されたものとみなします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

動的 VPN サーバに登録する自装置情報の有効期間を設定します。

[未設定時]

情報有効期間に 1h を指定したものとみなされます。

```
template <number> dvpn expire register 1h
```

10.5.5 template dvpn expire session

[機能]

動的 VPN のセッション更新間隔の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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)のどれかを指定します。
省略時は 5m が指定されたものとみなします。

・off
確立した動的 VPN セッションの更新は行いません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

確立した動的 VPN セッションの更新間隔を設定します。

[未設定時]

セッション更新間隔に 5m を指定したものとみなされます。

```
template <number> dvpn expire session 5m
```

10.5.6 template dvpn ua

[機能]

動的VPNクライアントのアドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<address>

・動的VPNクライアントのIPアドレス
動的VPNクライアントとなるIPv4アドレスまたはIPv6アドレスを指定します。
指定可能な範囲は以下のとおりです。

IPv4:

1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

IPv6:

::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

IPv6 DHCPクライアントが取得したプレフィックスを使用する場合は上位を"dhcp@インタフェース名"の形式で指定し、下位80bit分をIPv6アドレス形式で指定します。インタフェース名には、rmtインタフェースを以下の範囲で指定します。

範囲	機種
rmt0～rmt999	Si-R570 Si-R570B
rmt0～rmt499	Si-R370 Si-R370B
rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
rmt0～rmt49	Si-R180B

例)

rmt0で動作するIPv6 DHCPクライアントが取得したIPv6プレフィックスを使用する場合の設定例

```
dhcp@rmt0::
dhcp@rmt0::1:2:3:4
```

[動作モード]

構成定義モード(管理者クラス)

[説明]

動的VPNクライアントのアドレスを設定します。
動的VPN接続で使用するクライアント情報を参照しないで動的VPN機能を利用する場合は、本コマンドを必ず実行してください。

[注意]

動的VPNクライアントのアドレスにIPv6 DHCPクライアントが取得したプレフィックスを使用する場合、プレフィックスが割り当てられるインタフェースと同じ値になるように指定してください。

[未設定時]

動的VPNクライアントのアドレスを設定しないものとみなされます。

10.5.7 template dvpn domain

[機能]

動的VPNドメイン名の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

10.5.8 template dvpn localnet

[機能]

動的VPNで接続する自側ネットワークの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<count>

・プレフィックス定義番号

プレフィックスの定義番号を、0から19までの10進数で指定します。

指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つプレフィックス定義がすでに存在する場合は、既存の定義を変更します。

<address>/<mask>

・自側ネットワーク

自側ネットワークをIPv4アドレス/マスクビット数(またはマスク値)またはIPv6アドレスとプレフィックス長で指定します。

IPv4:

IPv4アドレスとマスクビット数の組み合わせで指定します。

マスク値は、最上位ビットから1で連続した値にしてください。

デフォルトルートを設定する場合は、0.0.0.0/0(0.0.0.0/0.0.0.0)を指定します。

IPv6:

IPv6アドレスとプレフィックスの組み合わせで指定します。

リンクローカルアドレスは指定できません。

デフォルトルートを設定する場合は、::/0を指定します。

IPv6 DHCPクライアントが取得したプレフィックスを使用する場合は上位を"dhcp@インタフェース名"の形式で指定し、下位80bit分をIPv6アドレス形式で指定します。インタフェース名には、rmtインタフェースを以下の範囲で指定します。

範囲	機種
rmt0～rmt999	Si-R570 Si-R570B
rmt0～rmt499	Si-R370 Si-R370B
rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
rmt0～rmt49	Si-R180B

rmt0で動作するIPv6 DHCPクライアントが取得したIPv6プレフィックスを使用する場合の設定例

```
dhcp@rmt0::/64
dhcp@rmt0::1:2:3:4/64
```

プレフィックス長には64を指定してください。

<register>

・on

自側ユーザIDを生成して動的VPNサーバに登録します。

・off

自側ユーザ ID を生成せず動的 VPN サーバに登録しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

動的 VPN で接続する自側ネットワークを IPv4 アドレス/マスクビット数(またはマスク値)または IPv6 アドレスとプレフィックス長と自側ユーザ ID を生成して動的 VPN サーバに登録するかどうかを指定します。

自側ユーザ ID を生成して動的 VPN サーバに登録すると指定した場合、通信パケット契機で動的 VPN 接続をすることができます。通常は、動的 VPN サーバに登録するにしてください。

自側ユーザ ID は、自側ネットワークとドメイン名を結合して以下のように生成されます。

例)

自側ネットワークに 192.168.1.0/24(2001:db8:1111:1::/64)、ドメイン名に example.com を指定した場合

```
IPsecIKE)c0a80100/24@example.com
IPsecIKE)20010db81111000100000000000000000/64@example.com
```

動的 VPN 接続で使用するクライアント情報を参照しないで動的 VPN 機能を利用する場合は、本コマンドを必ず実行してください。

[注意]

自側ネットワーク設定の 0 番目の定義は、IKE ネゴシエーションに使用します。よって、相手装置の自側ネットワーク設定の 0 番目定義のアドレスファミリと一致するように設定してください。

動的 VPN で接続する自側ネットワークを異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。

拡張 IPsec 対象範囲機能未対応版数(V30)の装置と動的 VPN 接続を行う場合、動的 VPN で接続する自側ネットワークに異なるアドレスファミリの設定を行わないでください。

自側ネットワークに IPv6 DHCP クライアントが取得したプレフィックスを使用する場合、プレフィックスが割り当てられるインタフェースと同じ値になるように指定してください。

自側ネットワークは、本コマンドおよび dvpn client localnet コマンドで重複しないように指定してください。

[未設定時]

動的 VPN で接続する自側ネットワークを設定しないものとみなされます。

10.5.9 template dvpn localid

[機能]

動的VPNサーバに登録する自側ユーザIDの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

10.5.10 template dvpn interface

[機能]

VPN 通信で利用するインタフェースの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～9	Si-R180B

・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
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～49	Si-R180B

<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。

10.5.11 template dvpn global

[機能]

VPN 通信の終端グローバルアドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

10.6 IPsec 関連情報

10.6.1 template ipsec ike protocol

[機能]

自動鍵交換用 IPsec 情報のセキュリティプロトコルの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

10.6.2 template ipsec ike encrypt

[機能]

自動鍵交換用 IPsec 情報の暗号情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

・ des-cbc
・ 3des-cbc
・ aes-cbc-128
・ aes-cbc-192
・ aes-cbc-256
・ null
・ none

[動作モード]

構成定義モード(管理者クラス)

[説明]

送受信パケットを暗号化/復号化するための、暗号アルゴリズムの設定を行います。
暗号アルゴリズムを複数指定する場合、指定順序にかかわらず以下の優先順位となります。
暗号アルゴリズムの"aes-cbc"に続く数字は鍵長を表しています。
数字が大きいほど強固な鍵になりますが、その分処理時間を要します。

・ aes-cbc-256
・ aes-cbc-192
・ aes-cbc-128
・ 3des-cbc
・ des-cbc
・ null

[未設定時]

IPsec によるパケット暗号は行われません。

```
template <number> ipsec ike encrypt none
```

10.6.3 template ipsec ike auth

[機能]

自動鍵交換用 IPsec 情報の認証情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

・ hmac-md5
・ hmac-sha1
・ none

[動作モード]

構成定義モード(管理者クラス)

[説明]

送受信パケットを認証するための、認証アルゴリズムの設定を行います。
認証アルゴリズムを複数指定する場合、指定順序にかかわらず以下の優先順位となります。

・ hmac-md5
・ hmac-sha1

[未設定時]

IPsec によるパケット認証は行われません。

```
template <number> ipsec ike auth none
```

10.6.4 template ipsec ike pfs

[機能]

自動鍵交換用 IPsec 情報の PFS 使用時の DH(Diffie-Hellman)グループの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<pfs_group>

Diffie-Hellman グループについて指定します。

・ modp768
Diffie-Hellman グループの MODP768(グループ 1)
・ modp1024
Diffie-Hellman グループの MODP1024(グループ 2)
・ modp1536
Diffie-Hellman グループの MODP1536(グループ 5)
・ off
Diffie-Hellman グループを使用しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPsec セッションの鍵素材を保護する、PFS 使用時の DH(Diffie-Hellman)グループの設定を行います。

[未設定時]

PFS による鍵交換データ保護は行いません。セキュア通信を行いたい場合は適切な PFS 使用時の DH グループを設定してください。

```
template <number> ipsec ike pfs off
```

10.6.5 template ipsec ike lifetime

[機能]

自動鍵交換用 IPsec 情報の SA 有効時間の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<lifetime>

・SA 有効時間
SA 有効時間を、600 秒(10 分)～86400 秒(1 日)の範囲で指定します。
単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPsec セッションの通信データを保護する、IPsec SA の SA 有効時間(秒)の設定を行います。

[未設定時]

IPsec SA の有効時間として 8h(8 時間)が設定されたものとして扱います。

```
template <number> ipsec ike lifetime 8h
```

10.6.6 template ipsec ike lifebyte

[機能]

自動鍵交換用 IPsec 情報の SA 有効パケット量の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

10.6.7 template ipsec ike newsa initiator

[機能]

自動鍵交換用 IPsec 情報の New SA Initiator(更新時間/更新データ量)の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

10.6.8 template ipsec ike newsa responder

[機能]

自動鍵交換用 IPsec 情報の New SA Responder(更新時間／更新データ量)の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

10.7 IKE 関連情報

10.7.1 template ike shared key

[機能]

IKE セッション確立時の共有鍵(Pre-shared key)の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

10.7.2 template ike proposal move

[機能]

IKE セッション用 Proposal 定義優先順序の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

10.7.3 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-R570 | Si-R570B | Si-R370 | Si-R370B | Si-R260B | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[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。

<proposal_number>

・ Proposal 定義番号
Proposal 定義番号として 0-2 の範囲の 10 進数を指定します。
省略時は、0 を指定したものとみなされます。

<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
```

10.7.4 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<proposal_number>

・ Proposal 定義番号
Proposal 定義番号として 0-2 の範囲の 10 進数を指定します。
省略時は、0 を指定したものとみなされます。

<enc_algo>

暗号アルゴリズムを指定します。

・ des-cbc
・ 3des-cbc
・ aes-cbc-128
・ aes-cbc-192
・ aes-cbc-256

[動作モード]

構成定義モード(管理者クラス)

[説明]

IKE セッションの送受信パケットを暗号化/復号化するための、暗号アルゴリズムの設定を行います。
コマンドによる定義を行う場合は、必ず設定してください。
IKE セッション用暗号情報設定が未定義ですと IKE が動作しません。

[未設定時]

IKE セッション用暗号情報が設定されません。IKE により鍵交換を行う場合は必ず設定してください。

10.7.5 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<proposal_number>

・ Proposal 定義番号
Proposal 定義番号として 0-2 の範囲の 10 進数を指定します。
省略時は、0 を指定したものとみなされます。

<hash_algo>

認証(ハッシュ)アルゴリズムを指定します。

・ hmac-md5
・ hmac-sha1

[動作モード]

構成定義モード(管理者クラス)

[説明]

IKE セッションのネゴシエーションパケットを認証するための、ハッシュアルゴリズムの設定を行います。

[未設定時]

認証のためのハッシュアルゴリズムに hmac-md5 を指定したものとみなされます。

```
template <number> ike proposal <proposal_number> hash hmac-md5
```

10.7.6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<proposal_number>

・Proposal 定義番号
Proposal 定義番号として 0-2 の範囲の 10 進数を指定します。
省略時は、0 を指定したものとみなされます。

<pfs_group>

Diffie-Hellman グループについて指定します。

・modp768
MODP768(グループ 1)の Diffie-Hellman グループ
・modp1024
MODP1024(グループ 2)の Diffie-Hellman グループ
・modp1536
MODP1536(グループ 5)の Diffie-Hellman グループ

[動作モード]

構成定義モード(管理者クラス)

[説明]

IKE セッションのネゴシエーションパケットを保護するための、DH(Diffie-Hellman)グループの設定を行います。

[未設定時]

DH グループに modp768 を指定したものとみなされます。

```
template <number> ike proposal <proposal_number> pfs modp768
```

10.7.7 template ike proposal lifetime

[機能]

IKE 情報の SA 有効時間の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<proposal_number>

・Proposal 定義番号
Proposal 定義番号として 0-2 の範囲の 10 進数を指定します。
省略時は、0 を指定したものとみなされます。

<lifetime>

・SA 有効時間
SA 有効時間を、600 秒(10 分)～86400 秒(1 日)の範囲で指定します。
単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IKE セッションのネゴシエーションパケットを保護するための、SA 有効時間(秒)の設定を行います。

[未設定時]

IKE SA の有効時間として 24h(24 時間)が設定されたものとして扱われます。

```
template <number> ike proposal <proposal_number> lifetime 24h
```

10.7.8 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

10.7.9 template ike idtype

[機能]

IKE 情報の送信 ID タイプの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

10.7.10 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<name>

・ 自装置識別情報
自装置を識別する名前を指定します。
指定範囲は、1～64 文字です。
識別情報は、0x22(ダブルクォーテーション)を除く[0x21-0x7e]の範囲のコードで構成される ASCII 文字列で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IKE セッションを確立する、自装置の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。

10.7.11 template ike release

[機能]

IPsec/IKE 情報の解放動作の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<mode>

IPsec/IKE の SA 情報の解放動作設定を指定します。

・ on
回線切断時に解放処理を行います。

・ off
解放処理は行いません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

自動鍵設定で作成された SA 情報の解放動作設定を行います。
on を指定した場合は、回線切断時に自動鍵設定が使用している SA 情報の解放動作を行います。
off を指定した場合は、回線切断時に自動鍵設定が使用している SA 情報の解放動作を行いません。

[注意]

本コマンドは、以下の回線切断動作時に有効です。
ただし、動的 VPN 接続で使用している回線が常時接続で切断された場合、動的 VPN 機能により追加された経路情報が削除されることにより本コマンドの設定にかかわらず IKE SA 情報および動的 VPN 接続が切断されます。

・ ISDN(回線交換)を使用したときの回線切断時 (※Si-R260B Si-R240B Si-R180B を除く)
・ PPPoE を使用したときの切断時
・ モデムを使用したときの切断時 (※Si-R220C Si-R220D のみ)
・ データ通信カードを使用したときの切断時 (※Si-R240B のみ)

[未設定時]

回線切断時に IKE SA 情報の解放を行うものとみなされます。

```
template <number> ike release on
```

10.7.12 template ike mode

[機能]

IKE 情報の交換モードの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

10.7.13 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

10.7.14 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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 までの 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。

10.7.15 template ike certificate key

[機能]

IKE セッション用秘密鍵情報

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<key_number>

・ 秘密鍵識別番号
秘密鍵の識別番号を、0〜4 までの 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。

10.7.16 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

10.7.17 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

10.7.18 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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 までの 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
```

10.7.19 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

10.7.20 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

10.7.21 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

10.8 SNMP 関連情報

10.8.1 template snmp trap linkdown

[機能]

linkDown トラップの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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 service コマンドで旧バージョン互換 MIB モードに設定された場合、および snmp trap linkdown 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
```

10.8.2 template snmp trap linkup

[機能]

linkUp トラップの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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 service コマンドで旧バージョン互換 MIB モードに設定された場合、および snmp trap linkdown 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 11 章 IP 関連情報

11.1 IP 関連情報

11.1.1 ip nat table

[機能]

NAT 変換テーブル数の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

ip nat table <mode>

[オプション]

<mode>

- extension
  NAT 変換テーブル数を拡張します。
- normal
  NAT 変換テーブル数を通常とします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

NAT 変換テーブル数を拡張するかどうかを設定します。
装置全体で使用可能な NAT 変換テーブル数は「仕様一覧」のシステム最大値一覧を参照してください。

[注意]

OSPF または BGP を使用する場合、本設定は無効であり NAT 変換テーブル数は通常とみなされます。
OSPF または BGP を使用していたが、使用しない設定に変更したあと、NAT 変換テーブル数を拡張する場合は commit コマンドによる構成定義情報の動的反映は行えません。save コマンドを実行後に reset コマンドを実行して本装置を再起動してください。
NAT 変換テーブル数の設定変更を行った場合、NAT が有効なすべてのインタフェースの NAT 変換テーブルがいったん解放されます。

[未設定時]

NAT 変換テーブル数は通常とみなされます。

```
ip nat table normal
```

第 12 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
0～5	Si-R570 Si-R570B Si-R370 Si-R370B
0～2	Si-R220C Si-R220D
0～1	Si-R260B Si-R240B Si-R180B

12.1 動的 VPN サーバ情報

12.1.1 dvpn server use

[機能]

動的 VPN サーバ利用可否の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

12.1.2 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

12.1.3 dvpn server auth use

[機能]

動的 VPN サーバの認証の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

12.1.4 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

12.2 動的 VPN クライアント情報

12.2.1 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

dvpn client encode <type>

[オプション]

<type>

交換する情報のエンコードタイプを設定します。

- off
  交換する情報をエンコードしません。
- base64
  交換する情報を base64 エンコードします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

情報を交換する際の、エンコードタイプを設定します。
<type>に off を設定した場合は、情報をエンコードしないで交換します。

[注意]

V30 のソフトウェアと情報を交換する場合は、<type>に off を設定する必要があります。

[未設定時]

情報を base64 でエンコードして交換します。

```
dvpn client encode base64
```

12.2.2 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<count>

・動的VPNサーバ定義番号
動的VPNサーバの定義番号を、0から1までの10進数で指定します。

<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。

[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。

12.2.3 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<count>

・動的 VPN サーバ定義番号
動的 VPN サーバの定義番号を、0 から 1 までの 10 進数で指定します。

<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。

12.2.4 dvpn client expire register

[機能]

動的 VPN の情報有効期間の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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)のどれかを指定します。
省略時は 1h が指定されたものとみなします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

動的 VPN サーバに登録する自装置情報の有効期間を設定します。

[未設定時]

情報有効期間に 1h を指定したものとみなされます。

```
dvpn client <number> expire register 1h
```

12.2.5 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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)のどれかを指定します。
省略時は5mが指定されたものとみなします。

・off
確立した動的VPNセッションの更新は行いません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

確立した動的VPNセッションの更新間隔を設定します。

[未設定時]

セッション更新間隔に5mを指定したものとみなされます。

```
dvpn client <number> expire session 5m
```

12.2.6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<address>

・動的VPNクライアントのIPアドレス
動的VPNクライアントとなるIPv4アドレスまたはIPv6アドレスを指定します。
指定可能な範囲は以下のとおりです。

IPv4:

1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

IPv6:

::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

IPv6 DHCPクライアントが取得したプレフィックスを使用する場合は上位を"dhcp@インタフェース名"の形式で指定し、下位80bit分をIPv6アドレス形式で指定します。インタフェース名には、rmtインタフェースを以下の範囲で指定します。

範囲	機種
rmt0～rmt999	Si-R570 Si-R570B
rmt0～rmt499	Si-R370 Si-R370B
rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
rmt0～rmt49	Si-R180B

例)

rmt0で動作するIPv6 DHCPクライアントが取得したIPv6プレフィックスを使用する場合の設定例
dhcp@rmt0::
dhcp@rmt0::1:2:3:4

[動作モード]

構成定義モード(管理者クラス)

[説明]

動的VPNクライアントのアドレスを設定します。
動的VPN機能を利用する場合は、本コマンドを必ず実行してください。

[注意]

動的VPNクライアントのアドレスにIPv6 DHCPクライアントが取得したプレフィックスを使用する場合、プレフィックスが割り当てられるインタフェースと同じ値になるように指定してください。

[未設定時]

動的VPNクライアントのアドレスを設定しないものとみなされます。

12.2.7 dvpn client domain

[機能]

動的VPNドメイン名の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

12.2.8 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<count>

・プレフィックス定義番号

プレフィックスの定義番号を、0から19までの10進数で指定します。

指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つプレフィックス定義がすでに存在する場合は、既存の定義を変更します。

<address>/<mask>

・自側ネットワーク

自側ネットワークをIPv4アドレス/マスクビット数(またはマスク値)またはIPv6アドレスとプレフィックス長で指定します。

IPv4:

IPv4アドレスとマスクビット数の組み合わせで指定します。

マスク値は、最上位ビットから1で連続した値にしてください。

デフォルトルートを設定する場合は、0.0.0.0/0(0.0.0.0/0.0.0.0)を指定します。

IPv6:

IPv6アドレスとプレフィックスの組み合わせで指定します。

リンクローカルアドレスは指定できません。

デフォルトルートを設定する場合は、::/0を指定します。

IPv6 DHCPクライアントが取得したプレフィックスを使用する場合は上位を"dhcp@インタフェース名"の形式で指定し、下位80bit分をIPv6アドレス形式で指定します。インタフェース名には、rmtインタフェースを以下の範囲で指定します。

範囲	機種
rmt0～rmt999	Si-R570 Si-R570B
rmt0～rmt499	Si-R370 Si-R370B
rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
rmt0～rmt49	Si-R180B

例)

rmt0で動作するIPv6 DHCPクライアントが取得したIPv6プレフィックスを使用する場合の設定例

dhcp@rmt0::/64

dhcp@rmt0::1:2:3:4/64

プレフィックス長には64を指定してください。

<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)20010db81111000100000000000000/64@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。

拡張 IPsec 対象範囲機能未対応版数(V30)の装置と動的 VPN 接続を行う場合、動的 VPN で接続する自側ネットワークに異なるアドレスファミリの設定を行わないでください。

自側ネットワークに IPv6 DHCP クライアントが取得したプレフィックスを使用する場合、プレフィックスが割り当てられるインタフェースと同じ値になるように指定してください。

自側ネットワークは、本コマンドおよび template dvpn localnet コマンドで重複しないように指定してください。

[未設定時]

動的 VPN で接続する自側ネットワークを設定しないものとみなされます。

12.2.9 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

12.2.10 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～9	Si-R180B

・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
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～49	Si-R180B

<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。

12.2.11 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

12.2.12 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

12.2.13 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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
```

12.2.14 dvpn client ip6 route distance

[機能]

動的 VPN IPv6 経路情報の優先度の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

dvpn client [<number>] ip6 route distance <distance>

[オプション]

<number>

・動的 VPN クライアント定義番号
動的 VPN クライアントの通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<distance>

・優先度
動的 VPN 情報交換で相手から配布された IPv6 の経路情報の優先度を、1～254 の 10 進数で指定します。
優先度は、同じあて先への経路情報が複数ある場合、優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

動的 VPN 情報交換で相手から配布された IPv6 経路情報に対する優先度を指定します。

[未設定時]

優先度に 1 を指定したものとみなされます。

```
dvpn client <number> ip6 route distance 1
```

第 13 章 ルーティングプロトコル情報の設定

13.1 ルーティングマネージャ情報

13.1.1 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

13.1.2 routemanage ip redist rip

[機能]

RIP 再配布経路の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

routemanage ip redist rip <redist_info> <mode> [<metric>]

[オプション]

<redist_info>

経路種別を指定します。

- static
  スタティック経路情報を示します。
- connected
  インタフェース経路情報を示します。
- bgp
  BGP 経路情報を示します。
- ospf
  OSPF 経路情報を示します。
- dns
  DNS 経路情報を示します。

<mode>

RIP に再配布するかどうかを指定します。

- off
  再配布しません。
- on
  再配布します。

<metric>

- RIP に再配布するメトリック値
  RIP に再配布する際のメトリック値を、0～16 の 10 進数で指定します。
  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
```

13.1.3 routemanage ip redist bgp

[機能]

BGP 再配布経路の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

```
routemanage ip redist bgp <redist_info> <mode>
routemanage ip redist bgp vrf [<vrf_number>] <redist_info> <mode>
```

[オプション]

<redist_info>

経路種別を指定します。

- static
  スタティック経路情報を示します。
- connected
  インタフェース経路情報を示します。
- rip
  RIP 経路情報を示します。
  routemanage ip redist bgp vrf では指定できません。
- ospf
  OSPF 経路情報を示します。
  routemanage ip redist bgp vrf では指定できません。
- dns
  DNS 経路情報を示します。
  routemanage ip redist bgp vrf では指定できません。

<vrf_number>

- VRF 定義番号
  VRF の定義番号を、10 進数で指定します。
  省略時は、0 を指定したものとみなされます。

範囲	機種
0～3	Si-R570 Si-R570B Si-R370 Si-R370B
0～1	Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

<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
```

13.1.4 routemanage ip redist ospf

[機能]

OSPF 再配布経路の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

13.1.5 routemanage ip ecmp mode

[機能]

IPv4 ルーティングの ECMP の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

routemanage ip ecmp mode <mode>

[オプション]

<mode>

- off
  ECMP を使用しません。
- roundrobin
  ECMP を使用し、送出パス選択方式としてラウンドロビン方式を利用します。
- hash
  ECMP を使用し、送出パス選択方式としてハッシュ方式を使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv4 ルーティング機能の ECMP の使用の有無を設定します。なお、ECMP を使用する場合、以下の 2 種類の送出パス選択方式を選択します。

- ラウンドロビン方式
  パケットごとに送出パスを順次切り替える方式です。すべてのトラフィックがほぼ均等に分散される利点がある一方、通信の連続性(個々の通信セッションが同じパスを利用するか)とパケットの到達順は送信時から保証されないという欠点があります。
- ハッシュ方式
  送信元 IP アドレス、あて先 IP アドレスを基にハッシュ値を計算し、その値に従って送出パスを決定する方式です。通信の連続性および到達順はほぼ保証されますが、トラフィックが一部の通信パスにかたよる可能性があります。

[未設定時]

ECMP を利用しないものとみなされます。

```
routemanage ip ecmp mode off
```

13.1.6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

routemanage ip ecmp ospf <max_multipath>

[オプション]

<max_multipath>

・ 最大 ECMP 数
最大 ECMP 数を、1～4 までの 10 進数で指定します。
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
```

13.1.7 routemanage ip redist ldp

[機能]

LDP ラベル広報経路情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

routemanage ip redist ldp <redist_info> <mode>

[オプション]

<redist_info>

- static
  本装置に設定されているスタティックルーティングの経路情報を示します。
- connected
  インタフェースが接続されているネットワークの経路情報を示します。
- rip
  RIP で受信した経路情報を示します。
- ospf
  OSPF で受信した経路情報を示します。
- bgp
  BGP で受信した経路情報を示します。

<mode>

- off
  <redist_info>で指定した経路情報をラベル広報しません。
- on
  <redist_info>で指定した経路情報をラベル広報します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

LDP でラベル広報する経路情報の種別を選択します。

[未設定時]

以下の設定とみなされます。

- LDP で static を広報された経路をラベル広報しない
- LDP で connected の経路をラベル広報する
- LDP で rip で広報された経路をラベル広報する
- LDP で ospf で広報された経路をラベル広報する
- LDP で bgp で広報された経路をラベル広報しない

```
routemanage ip redist ldp static off
routemanage ip redist ldp connected on
routemanage ip redist ldp rip on
routemanage ip redist ldp ospf on
routemanage ip redist ldp bgp off
```

13.1.8 routemanage interface floating

[機能]

インタフェース経路のフローティング設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

routemanage interface floating <mode>

[オプション]

<mode>

・ off
フローティング機能を使用しません。

・ on
フローティング機能を使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

インタフェース経路のフローティング機能を設定します。

<mode>が on の場合、インタフェースが通信可能(リンクアップなど)状態ならば、インタフェース経路をルーティングテーブルに追加します。通信不可能(リンクダウンなど)状態ならば、インタフェース経路をルーティングテーブルから削除します。

<mode>が off の場合、インタフェースの通信状態に関係なく、インタフェース経路をルーティングテーブルに追加します。

本設定は、IPv4 機能、IPv6 機能で共通となります。

[注意]

ルーティングプロトコル優先度<distance>が 0 のスタティックルーティングも、<mode>が on の場合、インタフェースの状態変動によって、ルーティングテーブルへの追加・削除を制御します。

<mode>が on の場合、インタフェースが利用不可能な状態の場合はインタフェース経路がルーティングテーブルから削除されるとともに、インタフェースに設定された IP アドレスが通信に利用できなくなります。常に利用可能な IP アドレスが必要な場合は、loopback インタフェースに追加 IP アドレスを設定してください。

なお、以下のコマンドでは自装置の IP アドレスを指定します。これらのコマンドで常に利用可能な IP アドレスが必要な場合は、loopback インタフェースの追加 IP アドレスを使用してください。

・ snmp agent address
・ remote ap sessionwatch
・ remote ap tunnel local

<mode>が on で自 IP アドレスを指定していない remote インタフェースから送信される場合、送信元 IP アドレスは以下の順番で選ばれます。

1. loopback インタフェース追加アドレス
2. 利用可能な lan の IP アドレス(定義番号の小さいものが優先)
3. 利用可能な remote の IP アドレス(定義番号の小さいものが優先)

常に同じアドレスが選択されるようにするためには、loopback インタフェースに追加 IP アドレスを設定してください。この設定がない場合、インタフェースの状態によって送信元 IP アドレスが変化する場合があります。

<mode>が on でマルチキャストで自装置が RP として動作している場合、RP として動作しているインタフェースの状態の変化により以下の動作になります。

・ RP を自動選択にしている場合
RP として動作しているインタフェースがダウンした場合、利用可能なインタフェースを自動検索し更新します。この場合、ネットワーク上で RP が更新されるため、その RP を利用している通信は RP が更新されるまで

一定時間停止します。また、インタフェース回線が再びアップすることで、RP が切り戻るため、やはりその RP を利用している通信は切り戻るまでの一定時間停止します。

利用可能なインタフェースが検索できなかった場合は、RP としての動作を停止しますが、インタフェースが再びアップすることで復旧します。

・ RP を手動選択にしている場合

選択されているインタフェースがダウンした場合、RP としての動作を停止します。この場合、ネットワーク上で RP が更新されるため、その RP を利用している通信が RP が更新されるまで一定時間停止します。

また、インタフェースが再びアップすることで、RP は切り戻りますが、やはりその RP を利用している通信が切り戻るまでの一定時間停止します。

<mode>が on でマルチキャストで自装置が BSR として動作している場合、BSR として動作しているインタフェースの状態の変化により以下の動作になります。

・ BSR を自動選択にしている場合

RP として動作しているインタフェースがダウンした場合、利用可能なインタフェースを自動検索し更新します。この場合、ネットワーク上で BSR が更新されるため、その BSR を利用している通信は BSR が更新されるまでの一定時間停止します。また、インタフェースが再び UP することで、BSR が切り戻るため、やはりその BSR を利用している通信は BSR が切り戻るまでの一定時間停止します。

なお検索できなかった場合は、BSR としての動作を停止しますが、インタフェース回線が再びアップすることで復旧します。

・ BSR を手動選択にしている場合

選択されているインタフェースがダウンした場合は、BSR としての動作を停止します。この場合、ネットワーク上で BSR が更新されるため、その BSR を利用している通信は BSR が更新されるまでの一定時間停止します。

また、インタフェースが再びアップすることで BSR は切り戻りますが、やはりその BSR を利用している通信は切り戻るまでの一定時間停止します。

[未設定時]

インタフェースの通信状態に関係なく、常にインタフェース経路をルーティングテーブルに追加するものとみなされます。

```
routemanage interface floating off
```

13.1.9 routemanage ip6 distance

[機能]

IPv6 ルーティングプロトコル優先度の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

```
routemanage ip6 distance rip <rip_distance>
routemanage ip6 distance bgp <external_distance> [<internal_distance>]
routemanage ip6 distance ospf <ospf_distance>
routemanage ip6 distance dns <dns_distance>
routemanage ip6 distance dhcp <dhcp_distance>
```

[オプション]

<rip_distance>

・RIP 優先度
RIP の優先度を、1～254 の 10 進数で指定します。

<external_distance>

・EBGP 優先度
EBGP の優先度を、1～254 の 10 進数で指定します。
本オプションは、Si-R570、Si-R570B、Si-R240B、Si-R220C、Si-R220D、Si-R180B で指定可能です。

<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。
本オプションは、Si-R570、Si-R570B、Si-R240B、Si-R220C、Si-R220D、Si-R180B で指定可能です。

<ospf_distance>

・OSPF 優先度
OSPF の優先度を、1～254 の 10 進数で指定します。
本オプションは、Si-R570、Si-R570B、Si-R240B、Si-R220C、Si-R220D、Si-R180B で指定可能です。

<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。

[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 として優先経路選択を行うものとみなされます。

```
routemanage ip6 distance rip 120
routemanage ip6 distance bgp 20 200
routemanage ip6 distance ospf 110
routemanage ip6 distance dns 15
routemanage ip6 distance dhcp 10
```

13.1.10 routemanage ip6 redist rip

[機能]

IPv6 RIP 再配布経路の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

routemanage ip6 redist rip <redist_info> <mode> [<metric>]

[オプション]

<redist_info>

経路種別を指定します。

- static
  スタティック経路情報を示します。
- connected
  インタフェース経路情報を示します。
- bgp
  BGP 経路情報を示します。
  Si-R570、Si-R570B、Si-R240B、Si-R220C、Si-R220D、Si-R180B で指定可能です。
- ospf
  OSPF 経路情報を示します。
  Si-R570、Si-R570B、Si-R240B、Si-R220C、Si-R220D、Si-R180B で指定可能です。
- dns
  DNS 経路情報を示します。
- dhcp
  DHCP 経路情報を示します。

<mode>

RIP に再配布するかどうかを指定します。

- off
  再配布しません。
- on
  再配布します。

<metric>

- RIP に再配布するメトリック値
  RIP に再配布する際のメトリック値を、0～16 の 10 進数で指定します。
  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 ip6 redist rip static on
routemanage ip6 redist rip connected on
routemanage ip6 redist rip bgp off 0
routemanage ip6 redist rip ospf off 0
routemanage ip6 redist rip dns off 0
routemanage ip6 redist rip dhcp off 0
```

13.1.11 routemanage ip6 redist bgp

[機能]

BGP IPv6 再配布経路の設定

[適用機種]

Si-R570 | Si-R570B | | | | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[入力形式]

routemanage ip6 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 ip6 redist bgp static off
routemanage ip6 redist bgp connected off
routemanage ip6 redist bgp rip off
routemanage ip6 redist bgp ospf off
routemanage ip6 redist bgp dns off
routemanage ip6 redist bgp dhcp off
```

13.1.12 routemanage ip6 redist ospf

[機能]

IPv6 OSPF 再配布経路の設定

[適用機種]

Si-R570 | Si-R570B | | | | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[入力形式]

routemanage ip6 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 ip6 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 ip6 redist ospf static off 20 type2
routemanage ip6 redist ospf connected off 20 type2
routemanage ip6 redist ospf rip off 20 type2
routemanage ip6 redist ospf bgp off 20 type2
routemanage ip6 redist ospf dns off 20 type2
routemanage ip6 redist ospf dhcp off 20 type2
```

13.2 RIP 情報

13.2.1 rip ip timers basic

[機能]

RIP タイマの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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)のどれかを指定します。
各単位での設定可能範囲は、10s～3600s、1m～60m、1h です。

<timeout>

・有効期限タイマ値
有効期限タイマ値を、10～3600 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のどれかを指定します。
各単位での設定可能範囲は、10s～3600s、1m～60m、1h です。

<garbage>

・ガーベージタイマ値
ガーベージタイマ値を、10～3600 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のどれかを指定します。
各単位での設定可能範囲は、10s～3600s、1m～60m、1h です。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RIP の基準となる定期広報タイマ値、有効期限タイマ値、ガーベージタイマ値を指定します。

<update>は、定期広報の送信間隔を設定します。なお、次に定期広報を行うまでの時間は、送信間隔に送信間隔の最大±50%のゆらぎ幅の範囲で乱数により求められる値を加算した値が使用されます。ゆらぎ幅は、rip ip timers jitter コマンドで変更することができます。

<timeout>は、隣接ルータから一定時間通知がない場合、その隣接ルータから受信していた経路を無効とするまでの時間を設定します。

<garbage>では、無効となった経路情報を削除するまでの時間を設定します。無効となった経路は削除されるまでの間、定期広報でメトリック 16 として広報されます。

[未設定時]

定期広報タイマ値に 30 秒、有効期限タイマ値に 3 分、ガーベージタイマ値に 2 分が設定されているものとみなされます。

```
rip ip timers basic 30s 3m 2m
```

13.2.2 rip ip timers jitter

[機能]

RIP 定期広報ゆらぎ幅の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

13.2.3 rip ip multipath

[機能]

RIP マルチパスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

rip ip multipath <path_num>

[オプション]

<path_num>

・同一パス数
同一パス数を、1～2 までの 10 進数で指定します。

[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
```

13.2.4 rip ip redist

[機能]

RIP 再配布フィルタの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～499	Si-R570 Si-R570B
0～249	Si-R370 Si-R370B
0～49	上記以外

<action>

フィルタリング条件に一致した場合の動作を指定します。

・pass
該当する経路情報を透過します。

・reject
該当する経路情報を遮断します。

<address>/<mask>

フィルタリング対象とする経路情報を指定します。

・IPv4 アドレス/マスクビット数(またはマスク値)
フィルタリング対象とする経路情報を、IPv4 アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
- IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
- IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)

・any
すべての経路情報をフィルタリング対象とする場合に指定します。

・default
デフォルトルートをフィルタリング対象とする場合に指定します。
0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<prefix_match>

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

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

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

RIP に再配布する経路情報に対するフィルタリング条件と動作を設定します。

フィルタリング条件は優先順位で検索され、条件に一致した場合にフィルタリングの動作が行われ、それ以降の条件は参照されません。

すべてのフィルタリング条件に一致しない経路情報は RIP に再配布されません。

<number>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。

RIP 再配布フィルタは、本装置全体で以下の数まで定義できます。

範囲	機種
500	Si-R570 Si-R570B
250	Si-R370 Si-R370B
50	上記以外

[未設定時]

RIP 再配布フィルタが設定されていないものとみなされます。

13.2.5 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～499	Si-R570 Si-R570B
0～249	Si-R370 Si-R370B
0～49	上記以外

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

13.2.6 rip ip neighbor

[機能]

RIP ユニキャスト送信の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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や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 コマンド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。

13.2.7 rip ip gwfilter

[機能]

RIP 相手フィルタの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

13.2.8 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

13.2.9 rip ip6 timers basic

[機能]

IPv6 RIP タイマの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

rip ip6 timers basic <update> <timeout> <garbage>

[オプション]

<update>

・定期広報タイマ値
定期広報タイマ値を、10～3600 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のどれかを指定します。
各単位での設定可能範囲は、10s～3600s、1m～60m、1h です。

<timeout>

・有効期限タイマ値
有効期限タイマ値を、10～3600 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のどれかを指定します。
各単位での設定可能範囲は、10s～3600s、1m～60m、1h です。

<garbage>

・ガーベージタイマ値
ガーベージタイマ値を、10～3600 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のどれかを指定します。
各単位での設定可能範囲は、10s～3600s、1m～60m、1h です。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RIP(IPv6)の基準となる定期広報タイマ値、有効期限タイマ値、ガーベージタイマ値を指定します。

<update>は、定期広報の送信間隔を設定します。なお、次に定期広報を行うまでの時間は、送信間隔に送信間隔の最大±50%のゆらぎ幅の範囲で乱数により求められる値を加算した値が使用されます。

<timeout>は、隣接ルータから一定時間通知がない場合、その隣接ルータから受信していた経路を無効とするまでの時間を設定します。

<garbage>では、無効となった経路情報を削除するまでの時間を設定します。無効となった経路は削除されるまでの間、定期広報でメトリック 16 として広報されます。

[未設定時]

定期広報タイマ値に 30 秒、有効期限タイマ値に 3 分、ガーベージタイマ値に 2 分が設定されているものとみなされます。

```
rip ip6 timers basic 30s 3m 2m
```

13.2.10 rip ip6 multipath

[機能]

IPv6 RIP マルチパスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

rip ip6 multipath <path_num>

[オプション]

<path_num>

・同一パス数
同一パス数を、1～2 までの 10 進数で指定します。

[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 ip6 multipath 1
```

13.2.11 rip ip6 redist

[機能]

IPv6 RIP 再配布フィルタの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

rip ip6 redist <number> <action> <address>/<prefixlen> [<prefix_match>]

[オプション]

<number>

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

範囲	機種
0～499	Si-R570 Si-R570B
0～249	Si-R370 Si-R370B
0～49	上記以外

<action>

フィルタリング条件に一致した場合の動作を指定します。

・pass
該当する経路情報を透過します。

・reject
該当する経路情報を遮断します。

<address>/<prefixlen>

フィルタリング対象とする経路情報を指定します。

・IPv6 アドレス/プレフィックス長
フィルタリング対象とする経路情報を、IPv6 アドレスとプレフィックス長の組み合わせで指定します。

・any
すべての経路情報をフィルタリング対象とする場合に指定します。

・default
デフォルトルートをフィルタリング対象とする場合に指定します。
::/0 を指定するのと同じ意味になります。

<prefix_match>

経路情報(IPv6 アドレス/プレフィックス長)の検索条件を指定します。
省略時は、exact を指定したものとみなされます。
<address>/<prefixlen>に"any"または"default"を指定した場合は、<prefix_match>は指定できません。

・exact
指定した<address>/<mask>と経路情報の IPv6 アドレス/プレフィックス長を比較し、一致した場合に、フィルタリング対象とします。

・inexact
指定した<address>と経路情報の IPv6 アドレスを比較し、<prefixlen>まで一致した場合、フィルタリング対象とします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RIP(IPv6)に再配布する経路情報に対するフィルタリング条件と動作を設定します。

フィルタリング条件は優先順位で検索され、条件に一致した場合にフィルタリングの動作が行われ、それ以降の条件は参照されません。

すべてのフィルタリング条件に一致しない経路情報はRIP(IPv6)に再配布されません。

<number>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。

RIP(IPv6)再配布フィルタは、本装置全体で以下の数まで定義できます。

範囲	機種
500	Si-R570 Si-R570B
250	Si-R370 Si-R370B
50	上記以外

[未設定時]

RIP(IPv6)再配布フィルタが設定されていないものとみなされます。

13.2.12 rip ip6 redist move

[機能]

IPv6 RIP 再配布フィルタの優先順序の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

rip ip6 redist move <number> <new_number>

[オプション]

<number>

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

<new_number>

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

範囲	機種
0～499	Si-R570 Si-R570B
0～249	Si-R370 Si-R370B
0～49	上記以外

[動作モード]

構成定義モード(管理者クラス)

[説明]

RIP(IPv6)再配布フィルタの優先順序を変更します。

<new_number>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、<new_number>は順番にソートされてリナンバリングされます。

13.3 BGP 情報

13.3.1 bgp as

[機能]

BGP AS 番号の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

13.3.2 bgp id

[機能]

BGP ID の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

13.3.3 bgp ip vrf rd

[機能]

IPv4 BGP/MPLS VPN ルート識別子の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bgp ip vrf [<vrf_number>] rd <as_number> <id>

[オプション]

<vrf_number>

・VRF 定義番号
VRF の定義番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～3	Si-R570 Si-R570B Si-R370 Si-R370B
0～1	Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

<as_number>

・ルート識別用 AS 番号
ルート識別子用の AS 番号を、1～65535 の 10 進数で指定します。

<id>

・ID 番号
VRF の ID 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]

IPv4 BGP/MPLS VPN で使用するルート識別子を AS 番号と ID で設定します。
<as_number>は、自装置の属する AS 番号を設定します。
<id>は、VPN を一意に示す id を設定します。

[未設定時]

ルート識別子が設定されていないものとみなされます。

13.3.4 bgp ip mpls-resolution

[機能]

IPv4 BGP MPLS 解決の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bgp ip mpls-resolution <mode>

[オプション]

<mode>

MPLS 解決を行うかどうかを指定します。

- on
  MPLS 解決を行います。
- off
  MPLS 解決を行いません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

BGP で受信した IPv4 経路情報を MPLS で解決するかどうかを設定します。
<mode>が on の場合は、BGP で受信した IPv4 経路情報を MPLS のラベルパスにマッピングします。
off の場合は、マッピングしません。

[注意]

MPLS トンネル接続上で BGP を使用する場合は、本設定を off にしてください。

[未設定時]

MPLS 解決を行わないものとみなされます。

```
bgp ip mpls-resolution off
```

13.3.5 bgp ip full-route

[機能]

BGP IPv4 フルルートの設定

[適用機種]

Si-R570 Si-R570B

[入力形式]

bgp ip full-route <mode>

[オプション]

<mode>

IPv4 フルルートを使用するかどうかを指定します。

- on
  IPv4 フルルートを使用します。
- off
  IPv4 フルルートを使用しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

BGP で IPv4 フルルート(15 万経路)を使用するかどうかを設定します。

IPv4 フルルートを使用することにより、BGP テーブルエントリ数の最大値が拡張され、15 万経路を扱えるようになります。

IPv4 フルルートを使用しない場合：

エントリの最大値が 6000 エントリ

IPv4 フルルートを使用した場合 ：

エントリの最大値が 150000 エントリ

IPv4 フルルートは、拡張用 512M メモリモジュールが搭載されているときにのみ使用できます。

IPv4 フルルートを使用するときに設定できる BGP セッションは、BGP 相手情報の定義番号 0 に設定された EBGP(マルチホップを除く)の 1 セッションだけです。

IPv4 フルルートは、以下の機能と同時に使用することはできません。

- BGP への再配布、および BGP 経路情報の RIP/OSPF/LDP への再配布機能
- IPv4 BGP/MPLS VPN 機能
- IPv4 BGP MPLS 解決機能
- IPv6 OSPF 機能
- BGP IPv6 機能

[未設定時]

IPv4 フルルートを使用しないものとみなされます。

13.3.6 bgp ip network route

[機能]

BGP IPv4 ネットワークの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～199	Si-R570 Si-R570B
0～15	上記以外

<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。

[注意]

IPv4 BGP/MPLS VPN で使用する IBGP では、本コマンドで設定した経路は広報されません。

[未設定時]

BGP 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。

13.3.7 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

13.3.8 bgp ip aggregate

[機能]

BGP IPv4 集約経路の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～49	Si-R570 Si-R570B
0～15	上記以外

<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。

[注意]

IPv4 BGP/MPLS VPN で使用する IBGP では、本コマンドで経路を集約することはできません。

[未設定時]

BGP IPv4 集約経路が設定されていないものとみなされます。

13.3.9 bgp ip redist

[機能]

BGP IPv4 再配布フィルタの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～499	Si-R570 Si-R570B
0～249	Si-R370 Si-R370B
0～49	上記以外

<action>

フィルタリング条件に一致した場合の動作を指定します。

・ pass
該当する 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
指定した<address>/<mask>と IPv4 経路情報のネットワークアドレスを比較し、ネットワークアドレス部とホストアドレス部がともに完全に一致した場合、フィルタリング対象とします。

・ inexact
指定した<address>/<mask>と IPv4 経路情報のネットワークアドレスを比較し、ネットワークアドレス部まで一致した場合に、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。

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
500	Si-R570 Si-R570B
250	Si-R370 Si-R370B
50	上記以外

[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。

13.3.10 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～499	Si-R570 Si-R570B
0～249	Si-R370 Si-R370B
0～49	上記以外

[動作モード]

構成定義モード(管理者クラス)

[説明]

BGP 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。

13.3.11 bgp ip6 network route

[機能]

BGP IPv6 ネットワークの設定

[適用機種]

Si-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bgp ip6 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
0～199	Si-R570 Si-R570B
0～15	上記以外

<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 ip6 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 ip6 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。

13.3.12 bgp ip6 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-R570 | Si-R570B | | | | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[入力形式]

bgp ip6 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 ip6 network igp on
```

13.3.13 bgp ip6 aggregate

[機能]

BGP IPv6 集約経路の設定

[適用機種]

Si-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bgp ip6 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
0～49	Si-R570 Si-R570B
0～15	上記以外

<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。

13.3.14 bgp ip6 redist

[機能]

BGP IPv6 再配布フィルタの設定

[適用機種]

Si-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bgp ip6 redist <number> <action> <address>/<prefixlen> [<prefix_match>]

[オプション]

<number>

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

範囲	機種
0～499	Si-R570 Si-R570B
0～49	上記以外

<action>

フィルタリング条件に一致した場合の動作を指定します。

・ pass
該当する 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
指定した<address>/<prefixlen>と IPv6 経路情報のネットワークアドレスを比較し、ネットワークアドレス部とホストアドレス部がともに完全に一致した場合、フィルタリング対象とします。

・ inexact
指定した<address>/<prefixlen>と IPv6 経路情報のネットワークアドレスを比較し、ネットワークアドレス部まで一致した場合に、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。

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
500	Si-R570 Si-R570B
50	上記以外

[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。

13.3.15 bgp ip6 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-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bgp ip6 redist move <number> <new_number>

[オプション]

<number>

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

<new_number>

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

範囲	機種
0～499	Si-R570 Si-R570B
0～49	上記以外

[動作モード]

構成定義モード(管理者クラス)

[説明]

BGP 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。

13.4 BGP 相手側情報

13.4.1 bgp neighbor address

[機能]

BGP 相手側アドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～199	Si-R570 Si-R570B
0～49	Si-R370 Si-R370B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B
0～3	Si-R260B

<address>

相手装置のアドレスを指定します。

・ IPv4 アドレス
IPv4 経路情報または IPv4VPN 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。
IPv6 アドレスは Si-R570、Si-R570B、Si-R240B、Si-R220C、Si-R220D、Si-R180B で指定できます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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 BGP/MPLS VPN 運用では、相手装置は 1 つだけ設定できます。
Si-R240B、Si-R220C、Si-R220D、Si-R180B の場合：
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。

13.4.2 bgp neighbor as

[機能]

BGP 相手側 AS 番号の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～199	Si-R570 Si-R570B
0～49	Si-R370 Si-R370B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B
0～3	Si-R260B

<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。
IPv4 BGP/MPLS VPN を使用する場合は、IBGP 接続とするため本装置と同じ AS 番号を設定します。

[注意]

BGP を利用する場合は、必ず設定してください。
IP-VPN 接続と IPv4 BGP/MPLS VPN 接続は同時に使用することはできません。

[未設定時]

相手装置の AS 番号が設定されていないものとみなされます。

13.4.3 bgp neighbor timers

[機能]

BGP 無通信監視タイマの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～199	Si-R570 Si-R570B
0～49	Si-R370 Si-R370B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B
0～3	Si-R260B

<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)のどれかを指定します。
各単位での設定可能範囲は、1s～65535s、1m～1092m、1h～18h です。

<holdtime>

・ HoldTime のタイマ値(秒)
HoldTime のタイマ値を、3～65535 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のどれかを指定します。
各単位での設定可能範囲は、3s～65535s、1m～1092m、1h～18h です。

[動作モード]

構成定義モード(管理者クラス)

[説明]

<keepalive>では、無通信状態で、相手装置との通信可否を確認するために送信する KEEPALIVE メッセージのタイマ値を設定します。相手装置の<holdtime>が自装置の<holdtime>よりも小さな値が設定されている場合、相手装置の<holdtime>の 3 分の 1 の値が使用されます。

<holdtime>では無通信状態で通信異常と判断する時間を設定します。本値は相手装置とネゴシエーションし、より小さな値をお互いの装置で使用します。

<keepalive>には<holdtime>よりも小さな値を指定してください。

<holdtime>と<keepalive>の設定値は、上位単位で表示可能な場合、上位単位で表示されます。

[未設定時]

<keepalive>に 30 秒、<holdtime>に 90 秒が設定されているものとみなされます。

```
bgp neighbor <count> timers 30s 90s
```

13.4.4 bgp neighbor ebgp-multihop

[機能]

EBGP マルチホップの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～199	Si-R570 Si-R570B
0～49	Si-R370 Si-R370B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B
0～3	Si-R260B

<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
```

13.4.5 bgp neighbor enforce-multihop

[機能]

BGP エンフォースマルチホップの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bgp neighbor [<count>] enforce-multihop <mode>

[オプション]

<count>

・ 相手装置の定義番号
相手装置の定義番号を 10 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～199	Si-R570 Si-R570B
0～49	Si-R370 Si-R370B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B
0～3	Si-R260B

<mode>

エンフォースマルチホップとして動作させるかどうかを指定します。

・ on
エンフォースマルチホップとして動作させます。

・ off
エンフォースマルチホップとして動作させません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

エンフォースマルチホップとして動作させるかどうかを設定します。

エンフォースマルチホップは、EBGP のマルチホップ接続で EBGP マルチホップのホップ値に 1 が設定されていても、受信した IPv4 経路情報を破棄しないようにする機能です。

MPLS-IX 接続で EBGP を用いて経路交換を行う場合は、通常、LSP 未確立時には EBGP を確立しないようにするために、ホップ値 1 での EBGP が用いられます。LSP 確立時には、ホップ値の減算なしでフォワーディングされるため、ホップ値 1 での BGP マルチホップでの経路交換が可能となります。

通常のマルチホップ接続では、相手装置からの経路をホップ値 1 で受信した場合は破棄しますが、本設定により受け取ることが可能となります。

[注意]

BGP 相手側アドレスで<address>に IPv6 アドレスを指定した場合に無効となります。

[未設定時]

エンフォースマルチホップとして動作しないものとみなされます。

```
bgp neighbor <count> enforce-multihop off
```

13.4.6 bgp neighbor family

[機能]

BGP アドレスファミリの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～199	Si-R570 Si-R570B
0～49	Si-R370 Si-R370B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B
0～3	Si-R260B

<address_family>

・ ipv4
アドレスファミリとして IPv4 ユニキャストを使用します。
・ vpnv4
アドレスファミリとして VPN IPv4 ユニキャストを使用します。
・ 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。
本オプションは Si-R570、Si-R570B、Si-R240B、Si-R220C、Si-R220D、Si-R180B で指定できます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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。
<address_family>で vpnv4 は、本装置全体で 1 つだけ設定できます。

[未設定時]

アドレスファミリとして IPv4 ユニキャストを使用するものとみなされます。

```
bgp neighbor <count> family ipv4
```

13.4.7 bgp neighbor source

[機能]

BGP 自側アドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～199	Si-R570 Si-R570B
0～49	Si-R370 Si-R370B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B
0～3	Si-R260B

<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。
本オプションは Si-R570、Si-R570B、Si-R240B、Si-R220C、Si-R220D、Si-R180B で指定できます。

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。
IPv4 BGP/MPLS VPN を使用する場合は、loopback インタフェースのアドレスを指定します。

[未設定時]

BGP セッションの自側アドレスを自動的に選択するものとみなされます。

13.4.8 bgp neighbor authentication

[機能]

BGP TCP-MD5 認証鍵の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～199	Si-R570 Si-R570B
0～49	Si-R370 Si-R370B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B
0～3	Si-R260B

<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。

13.4.9 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～199	Si-R570 Si-R570B
0～49	Si-R370 Si-R370B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B
0～3	Si-R260B

<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。

13.4.10 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～199	Si-R570 Si-R570B
0～49	Si-R370 Si-R370B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B
0～3	Si-R260B

<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)のどれかを指定します。各単位での設定可能範囲は、1s～65535s、1m～1092m、1h～18h です。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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
```

13.4.11 bgp neighbor ip medmetric

[機能]

BGP IPv4 MED メトリックの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～199	Si-R570 Si-R570B
0～49	Si-R370 Si-R370B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B
0～3	Si-R260B

<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]

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
```

13.4.12 bgp neighbor ip asprepend

[機能]

BGP IPv4 AS パスプリペンドの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～199	Si-R570 Si-R570B
0～49	Si-R370 Si-R370B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B
0～3	Si-R260B

<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]

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
```

13.4.13 bgp neighbor ip localpref

[機能]

BGP IPv4 ローカル優先度の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～199	Si-R570 Si-R570B
0～49	Si-R370 Si-R370B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B
0～3	Si-R260B

<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、相手装置からすでに受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から経路を受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 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
```

13.4.14 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～199	Si-R570 Si-R570B
0～49	Si-R370 Si-R370B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B
0～3	Si-R260B

<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]

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
```

13.4.15 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～199	Si-R570 Si-R570B
0～49	Si-R370 Si-R370B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B
0～3	Si-R260B

<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]

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
```

13.4.16 bgp neighbor ip filter act

[機能]

BGP IPv4 フィルタの動作設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～199	Si-R570 Si-R570B
0～49	Si-R370 Si-R370B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B
0～3	Si-R260B

<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
0～799	Si-R570 Si-R570B
0～199	上記以外

<action>

フィルタリング条件に一致した場合の動作を指定します。

・ pass
該当する 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
800	Si-R570 Si-R570B
200	上記以外

[注意]

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

BGP 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。

IPv4 BGP/MPLS VPN 運用では、BGP IPv4 フィルタを使用できません。

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、相手装置との間ですでに送受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と経路を送受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 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。

13.4.17 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～199	Si-R570 Si-R570B
0～49	Si-R370 Si-R370B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B
0～3	Si-R260B

<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
0～799	Si-R570 Si-R570B
0～199	上記以外

[動作モード]

構成定義モード(管理者クラス)

[説明]

BGP 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、相手装置との間ですでに送受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と経路を送受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 both

13.4.18 bgp neighbor ip filter as

[機能]

BGP IPv4 フィルタの AS 番号設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～199	Si-R570 Si-R570B
0～49	Si-R370 Si-R370B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B
0～3	Si-R260B

<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
0～799	Si-R570 Si-R570B
0～199	上記以外

<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、相手装置との間ですでに送受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と経路を送受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 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。

13.4.19 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～199	Si-R570 Si-R570B
0～49	Si-R370 Si-R370B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B
0～3	Si-R260B

<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
0～799	Si-R570 Si-R570B
0～199	上記以外

<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
指定した<address>/<mask>とルーティング情報のネットワークアドレスを比較し、ネットワークアドレス部とホストアドレス部がともに完全に一致した場合、フィルタリング対象とします。

・ inexact

指定した<address>/<mask>とルーティング情報のネットワークアドレスを比較し、ネットワークアドレス部まで一致した場合に、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。

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、相手装置との間ですでに送受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と経路を送受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 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。

13.4.20 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～199	Si-R570 Si-R570B
0～49	Si-R370 Si-R370B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B
0～3	Si-R260B

<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
0～799	Si-R570 Si-R570B
0～199	上記以外

<medmetric>

・ MED メトリック値
相手装置に広報する MED メトリック値を、0～4294967295 の範囲で指定します。

[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]

MEDメトリック値を0として広報します。

13.4.21 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～199	Si-R570 Si-R570B
0～49	Si-R370 Si-R370B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B
0～3	Si-R260B

<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
0～799	Si-R570 Si-R570B
0～199	上記以外

<asprepend>

・ AS 番号追加数
相手装置に広報する AS 番号の追加数を、0～4 の 10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

相手装置に広報する 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]

AS番号の追加を行わないものとみなされます。

13.4.22 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～199	Si-R570 Si-R570B
0～49	Si-R370 Si-R370B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B
0～3	Si-R260B

<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
0～799	Si-R570 Si-R570B
0～199	上記以外

<localpref>

・ ローカル優先度
ローカル優先度を、0～4294967295 の 10 進数で指定します。

[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、相手装置からすでに受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から経路を受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 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。

13.4.23 bgp neighbor ip6 medmetric

[機能]

BGP IPv6 MED メトリックの設定

[適用機種]

Si-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bgp neighbor [<count>] ip6 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
0～199	Si-R570 Si-R570B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B

<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]

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> ip6 medmetric 0
```

13.4.24 bgp neighbor ip6 asprepend

[機能]

BGP IPv6 AS パスプリペンドの設定

[適用機種]

Si-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bgp neighbor [<count>] ip6 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
0～199	Si-R570 Si-R570B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B

<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]

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> ip6 asprepend 0
```

13.4.25 bgp neighbor ip6 localpref

[機能]

BGP IPv6 ローカル優先度の設定

[適用機種]

Si-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bgp neighbor [<count>] ip6 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
0～199	Si-R570 Si-R570B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B

<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、相手装置からすでに受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から経路を受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 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> ip6 localpref 100
```

13.4.26 bgp neighbor ip6 nexthopself

[機能]

BGP IPv6 ネクストホップセルフの設定

[適用機種]

Si-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bgp neighbor [<count>] ip6 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
0～199	Si-R570 Si-R570B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B

<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]

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> ip6 nexthopself off
```

13.4.27 bgp neighbor ip6 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-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bgp neighbor [<count>] ip6 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
0～199	Si-R570 Si-R570B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B

<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]

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> ip6 default-originate off
```

13.4.28 bgp neighbor ip6 filter act

[機能]

BGP IPv6 フィルタの動作設定

[適用機種]

Si-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bgp neighbor [<count>] ip6 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
0～199	Si-R570 Si-R570B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B

<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
0～799	Si-R570 Si-R570B
0～199	上記以外

<action>

フィルタリング条件に一致した場合の動作を指定します。

・ pass
該当する 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 ip6 filter as コマンドを使用し AS 番号を、または、bgp neighbor ip6 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
800	Si-R570 Si-R570B
200	上記以外

[注意]

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

BGP 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、相手装置との間ですでに送受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と経路を送受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 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。

13.4.29 bgp neighbor ip6 filter move

[機能]

BGP IPv6 フィルタの優先順序の変更

[適用機種]

Si-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bgp neighbor [<count>] ip6 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
0～199	Si-R570 Si-R570B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B

<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
0～799	Si-R570 Si-R570B
0～199	上記以外

[動作モード]

構成定義モード(管理者クラス)

[説明]

BGP 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、相手装置との間ですでに送受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と経路を送受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 both

13.4.30 bgp neighbor ip6 filter as

[機能]

BGP IPv6 フィルタの AS 番号設定

[適用機種]

Si-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bgp neighbor [<count>] ip6 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
0～199	Si-R570 Si-R570B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B

<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
0～799	Si-R570 Si-R570B
0～199	上記以外

<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、相手装置との間ですでに送受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と経路を送受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 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。

13.4.31 bgp neighbor ip6 filter route

[機能]

BGP IPv6 フィルタの経路情報設定

[適用機種]

Si-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bgp neighbor [<count>] ip6 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
0～199	Si-R570 Si-R570B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B

<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
0～799	Si-R570 Si-R570B
0～199	上記以外

<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
指定した<address>/<prefixlen>とルーティング情報のネットワークアドレスを比較し、ネットワークアドレス部とホストアドレス部がともに完全に一致した場合、フィルタリング対象とします。

・ inexact
指定した<address>/<prefixlen>とルーティング情報のネットワークアドレスを比較し、ネットワークアドレス部まで一致した場合に、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。

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、相手装置との間ですでに送受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と経路を送受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 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。

13.4.32 bgp neighbor ip6 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-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bgp neighbor [<count>] ip6 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
0～199	Si-R570 Si-R570B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B

<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
0～799	Si-R570 Si-R570B
0～199	上記以外

<medmetric>

・ MED メトリック値
相手装置に広報する MED メトリック値を、0～4294967295 の範囲で指定します。

[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]

IPv6 経路情報の MED メトリック値を 0 として広報します。

13.4.33 bgp neighbor ip6 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-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bgp neighbor [<count>] ip6 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
0～199	Si-R570 Si-R570B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B

<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
0～799	Si-R570 Si-R570B
0～199	上記以外

<asprepend>

・ AS 番号追加数
相手装置に広報する AS 番号の追加数を、0～4 の 10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

相手装置に広報する 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]

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。

13.4.34 bgp neighbor ip6 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-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bgp neighbor [<count>] ip6 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
0～199	Si-R570 Si-R570B
0～7	Si-R240B Si-R220C Si-R220D Si-R180B

<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
0～799	Si-R570 Si-R570B
0～199	上記以外

<localpref>

・ ローカル優先度
ローカル優先度を、0～4294967295 の 10 進数で指定します。

[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、相手装置からすでに受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から経路を受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 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。

13.5 OSPF 情報

13.5.1 ospf ip id

[機能]

OSPF ID の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

13.5.2 ospf ip6 id

[機能]

IPv6 OSPF ID の設定

[適用機種]

Si-R570 | Si-R570B | | | | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[入力形式]

ospf ip6 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。

13.6 OSPF エリア情報

13.6.1 ospf ip area id

[機能]

OSPF エリア ID の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

ospf ip area [<area_number>] id <area_id>

[オプション]

<area_number>

・ エリア定義番号
エリアの定義番号を指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～9	Si-R570 Si-R570B
0～3	Si-R370 Si-R370B
0～2	Si-R260B Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

<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。

13.6.2 ospf ip area type

[機能]

OSPF エリアタイプの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

ospf ip area [<area_number>] type <area_type>

[オプション]

<area_number>

・エリア定義番号
エリアの定義番号を指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～9	Si-R570 Si-R570B
0～3	Si-R370 Si-R370B
0～2	Si-R260B Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

<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
```

13.6.3 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

ospf ip area [<area_number>] defcost <cost>

[オプション]

<area_number>

・エリア定義番号
エリアの定義番号を指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～9	Si-R570 Si-R570B
0～3	Si-R370 Si-R370B
0～2	Si-R260B Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

<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
```

13.6.4 ospf ip area range

[機能]

OSPF エリア内部集約経路の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

ospf ip area [<area_number>] range <range_number> <address>/<mask> [<cost>]

[オプション]

<area_number>

・ エリア定義番号
エリアの定義番号を指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～9	Si-R570 Si-R570B
0～3	Si-R370 Si-R370B
0～2	Si-R260B Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

<range_number>

・ 集約経路定義番号
集約経路の定義番号を指定します。

範囲	機種
0～49	Si-R570 Si-R570B
0～29	Si-R370 Si-R370B
0～3	Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

<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。

13.6.5 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

ospf ip area [<area_number>] type3-lsa <count> <action> <address>/<mask> <direction>[<prefix_match>]

[オプション]

<area_number>

・ エリア定義番号
エリアの定義番号を指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～9	Si-R570 Si-R570B
0～3	Si-R370 Si-R370B
0～2	Si-R260B Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

<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
0～49	Si-R570 Si-R570B
0～29	上記以外

<action>

サマリ LSA 入出力可否条件と一致した場合の動作を指定します。

・ pass
該当するサマリ LSA を透過します。
・ reject
該当するサマリ LSA を遮断します。

<address>/<mask>

・ IPv4 アドレス/マスクビット数(またはマスク値)
サマリ LSA 入出力可否の条件とする経路情報を、IPv4 アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。
以下に、有効な記述形式を示します。
- IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
- IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)

・ any
すべての経路情報をサマリ LSA 入出力可否の条件とする場合に指定します。

<direction>

サマリ LSA 入出力の方向を示します。

・ in

ほかのエリアからのサマリ LSA の入力を示します。

・ out

ほかのエリアへのサマリ LSA の出力を示します。

<prefix_match>

経路情報(IPv4 アドレス/マスク)の検索条件を指定します。

省略時は、exact を指定したものとみなされます。

<address>/<mask>に"any"を指定した場合は、<prefix_match>は指定できません。

・ exact

指定した<address>/<mask>と経路情報の IPv4 アドレス/マスクを比較し、一致した場合に、サマリ LSA 入出力可否の対象とします。

・ inexact

指定した<address>と経路情報の IPv4 アドレスを比較し、<mask>まで一致した場合に、サマリ LSA 入出力可否の対象とします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

エリア境界ルータで、エリア間で入出力するサマリ LSA を透過(pass)するか、または遮断(reject)するかを設定します。

ほかのエリアからサマリ LSA の入力があった場合は、優先度順に<direction>に in が設定されているサマリ LSA 入出力可否条件から一致する条件を検索します。一致する条件がない場合は、遮断されます。一致する条件があった場合は、その条件に設定されている<action>により動作が決定されます。

pass が設定されている場合は、透過され、reject が設定されている場合は、遮断されます。<direction>に in が設定されている条件がない場合は、透過されます。

ほかのエリアへサマリ LSA を出力する場合は、優先度順に<direction>に out が設定されているサマリ LSA 入出力可否条件から一致する条件を検索します。一致する条件がない場合は、遮断されます。

一致する条件があった場合は、その条件に設定されている<action>により動作が決定されます。

pass が設定されている場合は、透過され、reject が設定されている場合は、遮断されます。

<direction>に out が設定されている条件がない場合は、透過されます。

LSA 入出力可否条件に一致する条件があった場合、それ以降の条件は参照されません。

<count>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。

サマリ LSA 入出力可否は、本装置全体で以下の数まで定義できます。

範囲	機種
50	Si-R570 Si-R570B
30	上記以外

[注意]

ospf ip area range コマンドを使用し集約経路を設定しているエリアで、集約経路はサマリ LSA 入出力可否の対象となります。集約される経路は対象にならないことに注意してください。

また、以下の経路情報は、サマリ LSA 入出力可否の対象となりません。

・ 各エリアの AS 境界ルータから注入された AS 外部経路

・ スタブエリアおよび準スタブエリアのエリア境界ルータが注入するデフォルト経路

[未設定時]

エリア間でのサマリ LSA すべて透過するものとみなされます。

13.6.6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

ospf ip area [<area_number>] type3-lsa move <count> <new_count>

[オプション]

<area_number>

・エリア定義番号
エリアの定義番号を指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～9	Si-R570 Si-R570B
0～3	Si-R370 Si-R370B
0～2	Si-R260B Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

<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
0～49	Si-R570 Si-R570B
0～29	上記以外

[動作モード]

構成定義モード(管理者クラス)

[説明]

サマリ LSA 入出力可否定義の優先順序を変更します。
<count>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、<new_count>は順番にソートされてリナンバリングされます。

13.6.7 ospf ip6 area id

[機能]

IPv6 OSPF エリア ID の設定

[適用機種]

Si-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

ospf ip6 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
0～3	Si-R570 Si-R570B
0～2	Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

<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。

13.6.8 ospf ip6 area type

[機能]

IPv6 OSPF エリアタイプの設定

[適用機種]

Si-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

ospf ip6 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
0～3	Si-R570 Si-R570B
0～2	Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

<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 ip6 area <area_number> type normal
```

13.6.9 ospf ip6 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-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

ospf ip6 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
0～3	Si-R570 Si-R570B
0～2	Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

<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 ip6 area <area_number> defcost 1
```

13.6.10 ospf ip6 area range

[機能]

IPv6 OSPF エリア内部集約経路の設定

[適用機種]

Si-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

ospf ip6 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
0～3	Si-R570 Si-R570B
0～2	Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

<range_number>

・集約経路定義番号
集約経路の定義番号を指定します。

範囲	機種
0～49	Si-R570 Si-R570B
0～3	Si-R240B Si-R220C Si-R220D Si-R180B

<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。

13.6.11 ospf ip6 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-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

ospf ip6 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
0～3	Si-R570 Si-R570B
0～2	Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

<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
0～49	Si-R570 Si-R570B
0～29	Si-R240B Si-R220C Si-R220D Si-R180B

<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

指定した<address>/<prefixlen>と経路情報の IPv6 アドレス/プレフィックス長を比較し、一致した場合に、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>と経路情報の IPv6 アドレスを比較し、<prefixlen>まで一致した場合に、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。

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
50	Si-R570 Si-R570B
30	Si-R240B Si-R220C Si-R220D Si-R180B

[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同時に使用する場合は、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。

13.6.12 ospf ip6 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-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

ospf ip6 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
0～3	Si-R570 Si-R570B
0～2	Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

<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
0～49	Si-R570 Si-R570B
0～29	Si-R240B Si-R220C Si-R220D Si-R180B

[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。

13.7 OSPF バーチャルリンク情報

13.7.1 ospf ip area vlink id

[機能]

OSPF バーチャルリンク接続先の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

ospf ip area [<area_number>] vlink [<vlink_number>] id <router_id>

[オプション]

<area_number>

・ エリア定義番号
エリアの定義番号を指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～9	Si-R570 Si-R570B
0～3	Si-R370 Si-R370B
0～2	Si-R260B Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

<vlink_number>

・ バーチャルリンク定義番号
バーチャルリンクの定義番号を、0～1 で指定します。
省略時は、0 を指定したものとみなされます。

<router_id>

・ 接続先 OSPF ルータ ID
接続先ルータの OSPF ルータ ID を指定します。
IPv4 アドレスをドット形式で指定します。0.0.0.0 は指定できません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

バーチャルリンクの接続先を OSPF ルータ ID で設定します。
バーチャルリンクは、Si-R570 Si-R570B では、本装置全体で 8 個まで定義できます。

[注意]

バーチャルリンクは、スタブエリア、準スタブエリアでは使用できません。

[未設定時]

バーチャルリンクを使用しないものとみなされます。

13.7.2 ospf ip area vlink hello

[機能]

OSPF バーチャルリンク用 Hello パケット送信間隔の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

ospf ip area [<area_number>] vlink [<vlink_number>] hello <hello_interval>

[オプション]

<area_number>

・エリア定義番号
エリアの定義番号を指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～9	Si-R570 Si-R570B
0～3	Si-R370 Si-R370B
0～2	Si-R260B Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

<vlink_number>

・バーチャルリンク定義番号
バーチャルリンクの定義番号を、0～1 で指定します。
省略時は、0 を指定したものとみなされます。

<hello_interval>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

バーチャルリンク接続先との OSPF 隣接関係の維持に用いられる Hello パケットの送信間隔を設定します。
hello_interval の値はバーチャルリンク接続先と同じ値を設定します。

[注意]

バーチャルリンク接続先と異なる Hello パケット送信間隔を設定した場合、ルーティングが行えません。

[未設定時]

バーチャルリンク用 Hello パケット送信間隔に 10 秒が設定されているものとみなされます。

```
ospf ip area <area_number> vlink <vlink_number> hello 10s
```

13.7.3 ospf ip area vlink dead

[機能]

OSPF バーチャルリンク用隣接ルータ停止確認間隔の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

ospf ip area [<area_number>] vlink [<vlink_number>] dead <dead_interval>

[オプション]

<area_number>

・エリア定義番号
エリアの定義番号を指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～9	Si-R570 Si-R570B
0～3	Si-R370 Si-R370B
0～2	Si-R260B Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

<vlink_number>

・バーチャルリンク定義番号
バーチャルリンクの定義番号を、0～1 で指定します。
省略時は、0 を指定したものとみなされます。

<dead_interval>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[注意]

バーチャルリンク接続先と異なる隣接ルータ停止確認間隔を設定した場合、ルーティングが行えません。

[未設定時]

バーチャルリンク用隣接ルータ停止確認間隔に 40 秒が設定されているものとみなされます。

```
ospf ip area <area_number> vlink <vlink_number> dead 40s
```

13.7.4 ospf ip area vlink retrans

[機能]

OSPF バーチャルリンク用パケット再送間隔の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

ospf ip area [<area_number>] vlink [<vlink_number>] retrans <retransmit_interval>

[オプション]

<area_number>

・エリア定義番号
エリアの定義番号を指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～9	Si-R570 Si-R570B
0～3	Si-R370 Si-R370B
0～2	Si-R260B Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

<vlink_number>

・バーチャルリンク定義番号
バーチャルリンクの定義番号を、0～1 で指定します。
省略時は、0 を指定したものとみなされます。

<retransmit_interval>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

バーチャルリンクで OSPF パケットを再送する間隔を設定します。

[未設定時]

バーチャルリンク用パケット再送間隔に 5 秒が設定されているものとみなされます。

```
ospf ip area <area_number> vlink <vlink_number> retrans 5s
```

13.7.5 ospf ip area vlink delay

[機能]

OSPF バーチャルリンク用 LSU パケット送信遅延時間の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

ospf ip area [<area_number>] vlink [<vlink_number>] delay <transmit_delay>

[オプション]

<area_number>

・エリア定義番号
エリアの定義番号を指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～9	Si-R570 Si-R570B
0～3	Si-R370 Si-R370B
0～2	Si-R260B Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

<vlink_number>

・バーチャルリンク定義番号
バーチャルリンクの定義番号を、0～1 で指定します。
省略時は、0 を指定したものとみなされます。

<transmit_delay>

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[注意]

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

[未設定時]

バーチャルリンク用 LSU パケット送信遅延時間に 1 秒が設定されているものとみなされます。

```
ospf ip area <area_number> vlink <vlink_number> delay 1s
```

13.7.6 ospf ip area vlink auth type

[機能]

OSPF バーチャルリンク用パケット認証方式の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

ospf ip area [<area_number>] vlink [<vlink_number>] auth type <authtype>

[オプション]

<area_number>

・ エリア定義番号
エリアの定義番号を指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～9	Si-R570 Si-R570B
0～3	Si-R370 Si-R370B
0～2	Si-R260B Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

<vlink_number>

・ バーチャルリンク定義番号
バーチャルリンクの定義番号を、0～1 で指定します。
省略時は、0 を指定したものとみなされます。

<authtype>

パケット認証方式を指定します。

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

バーチャルリンクで OSPF パケットに対する認証方式を設定します。

[注意]

authtype で text を設定した場合は、テキスト認証鍵の設定が必要です。md5 を設定した場合は、MD5 認証鍵情報の設定が必要です。

[未設定時]

バーチャルリンクで OSPF パケット認証を使用しないものとみなされます。

```
ospf ip area <area_number> vlink <vlink_number> auth type off
```

13.7.7 ospf ip area vlink auth textkey

[機能]

OSPF バーチャルリンク用テキスト認証鍵の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

ospf ip area [<area_number>] vlink [<vlink_number>] auth textkey <kind> <key> [encrypted]

[オプション]

<area_number>

・ エリア定義番号
エリアの定義番号を指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～9	Si-R570 Si-R570B
0～3	Si-R370 Si-R370B
0～2	Si-R260B Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

<vlink_number>

・ バーチャルリンク定義番号
バーチャルリンクの定義番号を、0～1 で指定します。
省略時は、0 を指定したものとみなされます。

<kind>

鍵種別を指定します。

・ text
文字列鍵を使用します。

・ hex
16 進数鍵を使用します。

<key>

・ テキスト認証鍵
文字列鍵の場合は、0x21,0x23～0x7e のコードで構成される 8 文字以内の ASCII 文字列で指定します。
16 進数鍵の場合は、16 桁以内の 16 進数で指定します。16 桁未満の値を指定したときは左詰めで設定され、残りは 16 桁になるまで 0x0 でパディングされます。

・ 暗号化されたテキスト認証鍵
show コマンドで表示される暗号化されたテキスト認証鍵を encrypted と共に指定します。
show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[未設定時]

バーチャルリンク用テキスト認証鍵が設定されていないものとみなされます。

13.7.8 ospf ip area vlink auth md5key

[機能]

OSPF バーチャルリンク用 MD5 認証鍵情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

ospf ip area [<area_number>] vlink [<vlink_number>] auth md5key <key_id> <key> [encrypted]

[オプション]

<area_number>

・ エリア定義番号
エリアの定義番号を指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～9	Si-R570 Si-R570B
0～3	Si-R370 Si-R370B
0～2	Si-R260B Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

<vlink_number>

・ バーチャルリンク定義番号
バーチャルリンクの定義番号を、0～1 で指定します。
省略時は、0 を指定したものとみなされます。

<key_id>

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

<key>

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

encrypted

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

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

[未設定時]

バーチャルリンク用 MD5 認証鍵情報が設定されていないものとみなされます。

13.8 ASBR 情報

13.8.1 ospf ip definfo

[機能]

OSPF AS 境界ルータのデフォルトルート広報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。
- インタフェースのフローティング機能を使用する設定で、かつ、優先度 0 のデフォルトルートのスタティック経路設定がされている場合、デフォルトルートが IP カーネルのルーティングテーブルで有効な状態であっても、経路共通管理部のルーティングテーブルで無効となる場合があります。この場合、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
```

13.8.2 ospf ip summary

[機能]

OSPF AS 外部経路集約の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

ospf ip summary <summary_number> <address>/<mask>

[オプション]

<summary_number>

・ 集約経路定義番号
集約経路の定義番号を指定します。

範囲	機種
0～49	Si-R570 Si-R570B
0～29	Si-R370 Si-R370B
0～3	Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

<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。

13.8.3 ospf ip redist

[機能]

OSPF 再配布フィルタの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～499	Si-R570 Si-R570B
0～249	Si-R370 Si-R370B
0～49	上記以外

<action>

フィルタリング条件に一致した場合の動作を指定します。

・pass

該当する経路情報を透過します。

・reject

該当する経路情報を遮断します。

<address>/<mask>

フィルタリング対象とする経路情報を指定します。

・IPv4 アドレス/マスクビット数(またはマスク値)

フィルタリング対象とする経路情報を、IPv4 アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。

- IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
- IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)

・any

すべての経路情報をフィルタリング対象とする場合に指定します。

・default

デフォルトルートをフィルタリング対象とする場合に指定します。

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

<prefix_match>

経路情報(IPv4 アドレス/マスク)の検索条件を指定します。

省略時は、exact を指定したものとみなされます。

<address>/<mask>に"any"または"default"を指定した場合は、<prefix_match>は指定できません。

・exact

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

・inexact

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

<metric>

再配布する経路情報のメトリック値を指定します。

省略時は、IPv4ルーティングプロトコル再配布の設定で指定した値となります。

<action>に"reject"を指定した場合は、<metric>は指定できません。

・ 再配布するメトリック値
  設定可能範囲は、0～16777214です。

<metric_type>

再配布する経路情報のメトリックタイプを指定します。

省略時は、IPv4ルーティングプロトコル再配布の設定で指定した値となります。

<action>に"reject"を指定した場合は、<metric_type>は指定できません。

・ type1
  外部経路のメトリックタイプがtype1
・ type2
  外部経路のメトリックタイプがtype2

[動作モード]

構成定義モード(管理者クラス)

[説明]

OSPFに再配布する経路に対するフィルタリング条件と動作を設定します。

フィルタリング条件は優先順位で検索され、条件に一致した場合にフィルタリングの動作が行われそれ以降の条件は参照されません。

すべてのフィルタリング条件に一致しない経路情報は再配布されません。

再配布する経路情報にメトリック値、およびメトリックタイプを指定できます。

<address>/<mask>に"any"を指定した場合、メトリック値、およびメトリックタイプは、IPv4ルーティングプロトコル再配布の設定で指定した値となります。また、"default"を指定した場合は、ospf ip definfoコマンドで指定した値となります。

<number>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。

OSPF再配布フィルタは、本装置全体で以下の数まで定義できます。

範囲	機種
500	Si-R570 Si-R570B
250	Si-R370 Si-R370B
50	上記以外

[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]

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。

13.8.4 ospf ip redist move

[機能]

OSPF 再配布フィルタの優先順序の変更

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～499	Si-R570 Si-R570B
0～249	Si-R370 Si-R370B
0～49	上記以外

[動作モード]

構成定義モード(管理者クラス)

[説明]

OSPF 再配布フィルタの優先順序を変更します。

<new_number>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、<new_number>は順番にソートされてリナンバリングされます。

13.8.5 ospf ip6 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-R570 | Si-R570B | | | | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[入力形式]

ospf ip6 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。
- インタフェースのフローティング機能を使用する設定で、かつ、優先度 0 のデフォルトルートのスタティック経路設定がされている場合、デフォルトルートが IP カーネルのルーティングテーブルで有効な状態であっても、経路共通管理部のルーティングテーブルで無効となる場合があります。この場合、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 ip6 definfo off
```

13.8.6 ospf ip6 redist

[機能]

IPv6 OSPF 再配布フィルタの設定

[適用機種]

Si-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

ospf ip6 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
0～499	Si-R570 Si-R570B
0～49	Si-R240B Si-R220C Si-R220D Si-R180B

<action>

フィルタリング条件に一致した場合の動作を指定します。

・ pass
該当する経路情報を透過します。

・ reject
該当する経路情報を遮断します。

<address>/<prefixlen>

フィルタリング対象とする経路情報を指定します。

・ IPv6 アドレス/プレフィックス長
フィルタリング対象とする経路情報を、IPv6 アドレスとプレフィックス長の組み合わせで指定します。

・ any
すべての経路情報をフィルタリング対象とする場合に指定します。

・ default
デフォルトルートをフィルタリング対象とする場合に指定します。
::/0 を指定するのと同じ意味になります。

<prefix_match>

経路情報(IPv6 アドレス/プレフィックス長)の検索条件を指定します。
省略時は、exact を指定したものとみなされます。
<address>/<prefixlen>に"any"または"default"を指定した場合は、<prefix_match>は指定できません。

・ exact
指定した<address>/<prefixlen>と経路情報の IPv6 アドレス/プレフィックス長を比較し、一致した場合に、フィルタリング対象とします。

・ inexact
指定した<address>と経路情報の IPv6 アドレスを比較し、<prefixlen>まで一致した場合、フィルタリング対象とします。

<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 ip6 definfo コマンドで指定した値となります。

<number>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。

OSPF 再配布フィルタは、本装置全体で以下の数まで定義できます。

最大定義数	機種
500	Si-R570 Si-R570B
50	Si-R240B Si-R220C Si-R220D Si-R180B

[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 ip6 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。

13.8.7 ospf ip6 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-R570 Si-R570B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

ospf ip6 redist move <number> <new_number>

[オプション]

<number>

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

<new_number>

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

範囲	機種
0～499	Si-R570 Si-R570B
0～49	Si-R240B Si-R220C Si-R220D Si-R180B

[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 14 章 ブリッジ情報の設定

14.1 ブリッジ情報

14.1.1 bridge age

[機能]

ブリッジ学習テーブルの生存時間の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bridge [<group_id>] age <age_time>

[オプション]

<group_id>

・ ブリッジグループ識別子
ブリッジグループ識別子を 10 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～19	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～7	Si-R180B

<age_time>

・ 生存時間
MAC アドレス学習によって学習した情報の生存時間を、10～1000000 秒の範囲で指定します。
単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

本コマンドは、ブリッジ機能を使用する場合にだけ有効です。
アドレス学習テーブルの生存時間を設定します。
アドレス学習機能によって学習された MAC アドレステーブルを最後に使用してから削除されるまでの時間を設定します。

[注意]

ブリッジグループ 0 に設定された値がすべてのブリッジグループで使用され、ブリッジグループ 0 以外に設定された値は使用されません。

[未設定時]

アドレス学習テーブルの生存時間として 5 分を定義するものとみなされます。

```
bridge <group_id> age 5m
```

14.1.2 bridge stp priority

[機能]

ブリッジ優先度の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bridge [<group_id>] stp priority <priority>

[オプション]

<group_id>

・ ブリッジグループ識別子
ブリッジグループ識別子を 10 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～19	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～7	Si-R180B

<priority>

・ 優先度
ブリッジネットワーク内での本装置の優先度を、0～65535 の 10 進数で指定します。値が小さいほど、優先度が高くなります。

[動作モード]

構成定義モード(管理者クラス)

[説明]

本コマンドは、STP を使用する場合にだけ有効です。
ルートブリッジ決定アルゴリズムで使用するブリッジの優先度を指定します。一般的なブリッジネットワークではルートブリッジにトラフィックが集中するため、バックボーンに近いブリッジが優先となるように設定してください。ルートブリッジにするブリッジには、最小の値を指定してください。

[注意]

ブリッジグループ 0 以外のブリッジグループでは STP は動作しません。

[未設定時]

優先度として 32768 を定義するものとみなされます。

```
bridge <group_id> stp priority 32768
```

14.1.3 bridge stp age

[機能]

Helloメッセージ待ち時間の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bridge [<group_id>] stp age <max_age>

[オプション]

<group_id>

・ブリッジグループ識別子
ブリッジグループ識別子を10進数で指定します。
省略時は、0を指定したものとみなされます。

範囲	機種
0～19	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～7	Si-R180B

<max_age>

・待ち時間
ルートブリッジから送出される構成情報BPDUの待ち時間を、6～40秒の範囲で指定します。
単位は、s(秒)を指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

本コマンドは、STPを使用する場合にだけ有効です。
ルートブリッジまたは代表ブリッジから送出される構成情報BPDUの待ち時間を指定します。

[注意]

ブリッジグループ0以外のブリッジグループではSTPは動作しません。

[未設定時]

待ち時間に20秒を設定したものとみなされます。

```
bridge <group_id> stp age 20s
```

14.1.4 bridge stp hello

[機能]

Helloメッセージ送出間隔の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bridge [<group_id>] stp hello <time>

[オプション]

<group_id>

・ブリッジグループ識別子
ブリッジグループ識別子を10進数で指定します。
省略時は、0を指定したものとみなされます。

範囲	機種
0～19	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～7	Si-R180B

<time>

・送出間隔
ルートブリッジになったときに定期的に送出する構成情報BPDUの送出間隔の時間を、1～10秒の範囲で指定します。
単位は、s(秒)を指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

本コマンドは、STPを使用する場合にだけ有効です。
本装置がルートブリッジとなったときに送出する構成情報BPDUの送出間隔を指定します。
STPを使用する場合でも、本装置がルートブリッジとならなかった場合は、設定が無効となります。

[注意]

ブリッジグループ0以外のブリッジグループではSTPは動作しません。

[未設定時]

送出間隔に2秒を設定したものとみなされます。

```
bridge <group_id> stp hello 2s
```

14.1.5 bridge stp delay

[機能]

最大中継遅延時間の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bridge [<group_id>] stp delay <delay_time>

[オプション]

<group_id>

・ ブリッジグループ識別子
ブリッジグループ識別子を 10 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～19	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～7	Si-R180B

<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]

本コマンドは、STP を使用する場合にだけ有効です。
最大中継遅延時間を設定します。
STP を使用する場合でも、本装置がルートブリッジとならなかった場合は、設定が無効となります。
STP で Listening 状態から Learning 状態に変化する場合、または Learning 状態から Forwarding 状態に変化するまでの時間(ルートブリッジから広報される時間)を指定します。

[注意]

ブリッジグループ 0 以外のブリッジグループでは STP は動作しません。

[未設定時]

最大中継遅延時間に 15 秒を設定したものとみなされます。

```
bridge <group_id> stp delay 15s
```

14.1.6 bridge ip routing

[機能]

IPv4 ルーティングの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bridge [<group_id>] ip routing <mode>

[オプション]

<group_id>

・ ブリッジグループ識別子
ブリッジグループ識別子を 10 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～19	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～7	Si-R180B

<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 ルーティングの有効/無効を設定します。
IPv4 ルーティングを無効とした場合、IPv4 フレームはブリッジにより制御されます。

[未設定時]

IPv4 をルーティングにより制御するものとみなされます。

```
bridge <group_id> ip routing on
```

14.1.7 bridge ip policy

[機能]

IPv4 転送ポリシの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bridge [<group_id>] ip policy <mode>

[オプション]

<group_id>

・ ブリッジグループ識別子
ブリッジグループ識別子を 10 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～19	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～7	Si-R180B

<mode>

・ strict
IPv4 ブリッジを行う場合に、グループ外からグループ内およびグループ内からグループ外へのルーティングによる転送を行いません。

・ loose
IPv4 ブリッジを行う場合に、グループ外からグループ内およびグループ内からグループ外へのルーティングによる転送を行います。

[動作モード]

構成定義モード(管理者クラス)

[説明]

本コマンドは、IPv4 をブリッジ対象とした場合にだけ有効です。

IPv4 ブリッジを行う場合に、グループ外からグループ内、およびグループ内からグループ外へのルーティングによる転送を行うかどうかを設定します。

IPv4 ブリッジ動作時にグループ内からグループ外へのルーティングによる転送が行われるのは以下の場合です。

・ 受信フレームのあて先 MAC アドレスが受信インタフェースあてであるが、あて先 IP アドレスが受信インタフェースあてでない場合。

IPv4 ブリッジ動作時にグループ外からグループ内へのルーティングによる転送が行われるのは以下の場合です。

・ IPv4 をルーティングするインタフェースで受信したパケットがルーティングにより IPv4 をブリッジするインタフェースへ出力される場合。

<mode>が strict の場合、これらの転送をブロックすることで、ブリッジ転送対象外のパケットに対してもグループ内に閉じた通信を行うことができます。

[未設定時]

グループ外からグループ内、およびグループ内からグループ外へのルーティングによる転送を行わないものとして動作します。

```
bridge <group_id> ip policy strict
```

14.1.8 bridge ip6 routing

[機能]

IPv6 ルーティングの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bridge [<group_id>] ip6 routing <mode>

[オプション]

<group_id>

・ ブリッジグループ識別子
ブリッジグループ識別子を 10 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～19	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～7	Si-R180B

<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]

IPv4 ルーティングの有効/無効を設定します。
IPv6 ルーティングを無効とした場合、IPv6 フレームはブリッジにより制御されます。

[未設定時]

IPv6 をルーティングにより制御するものとみなされます。

```
bridge <group_id> ip6 routing
```

14.1.9 bridge ip6 policy

[機能]

IPv6 転送ポリシの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bridge [<group_id>] ip6 policy <mode>

[オプション]

<group_id>

・ ブリッジグループ識別子
ブリッジグループ識別子を 10 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～19	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～7	Si-R180B

<mode>

・ strict
IPv6 ブリッジを行う場合に、グループ外からグループ内およびグループ内からグループ外へのルーティングによる転送を行いません。

・ loose
IPv6 ブリッジを行う場合に、グループ外からグループ内およびグループ内からグループ外へのルーティングによる転送を行います。

[動作モード]

構成定義モード(管理者クラス)

[説明]

本コマンドは、IPv6 をブリッジ対象とした場合にだけ有効です。

IPv6 ブリッジを行う場合に、グループ外からグループ内、およびグループ内からグループ外へのルーティングによる転送を行うかどうかを設定します。

IPv6 ブリッジ動作時にグループ内からグループ外へのルーティングによる転送が行われるのは以下の場合です。

・ 受信フレームのあて先 MAC アドレスが受信インタフェースあてであるが、あて先 IP アドレスが受信インタフェースあてでない場合。

IPv6 ブリッジ動作時にグループ外からグループ内へのルーティングによる転送が行われるのは以下の場合です。

・ IPv6 をルーティングするインタフェースで受信したパケットがルーティングにより IPv6 をブリッジするインタフェースへ出力される場合。

<mode>が strict の場合、これらの転送をブロックすることで、ブリッジ転送対象外のパケットに対してもグループ内に閉じた通信を行うことができます。

[未設定時]

グループ外からグループ内、およびグループ外からグループ内へのルーティングによる転送を行わないものとして動作します。

```
bridge <group_id> ip6 policy strict
```

14.1.10 bridge vlan tag transmit

[機能]

VLAN タグの転送方式の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bridge [<group_id>] vlan tag transmit <mode>

[オプション]

<group_id>

・ ブリッジグループ識別子
ブリッジグループ識別子を 10 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～19	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～7	Si-R180B

<mode>

・ on
VLAN タグをつけたまま透過ブリッジします。
・ off
VLAN タグを挿抜してブリッジします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

VLAN インタフェースで受信した VLAN タグ付きフレームのタグを透過転送するかどうかを設定します。
VLAN タグを挿抜する設定の場合、VLAN インタフェースで受信してリモートインタフェースへ出力する際には VLAN タグを除去して転送し、リモートインタフェースで受信して VLAN インタフェースへ出力する際には VLAN タグを挿入して転送します。

[未設定時]

VLAN タグを挿抜してブリッジします。

```
bridge <group_id> vlan tag transmit off
```

14.1.11 bridge inter-remote

[機能]

リモートインタフェース間のブリッジ転送の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bridge [<group_id>] inter-remote <mode>

[オプション]

<group_id>

・ ブリッジグループ識別子
ブリッジグループ識別子を 10 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～19	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～7	Si-R180B

<mode>

・ on
リモートインタフェース間のブリッジ転送を行います。
・ off
リモートインタフェース間のブリッジ転送を行いません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

リモートインタフェース間でブリッジ転送を行うか行わないかを設定します。
リモートインタフェースと LAN インタフェースの間のブリッジだけを許し、あるリモートインタフェースから別のリモートインタフェースへのブリッジ転送をブロックしたい場合に<mode>に off を設定します。

[未設定時]

リモートインタフェース間でブリッジ転送を行います。

```
bridge <group_id> inter-remote on
```

14.1.12 bridge control

[機能]

MAC コントロールフレーム転送設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

bridge [<group_id>] control <protocol>

[オプション]

<group_id>

・ ブリッジグループ識別子
ブリッジグループ識別子を 10 進数で指定します。
省略時は、0 を指定したものとみなされます。

範囲	機種
0～19	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
0～7	Si-R180B

<protocol>

ブリッジ転送する MAC コントロールフレームを、以下の中から指定します。複数指定する場合は、","(カンマ)で区切ります。

・ stp
STP のフレーム(BPDU)をブリッジ転送します。
・ lacp
LACP のフレームをブリッジ転送します。
・ eapol
IEEE 802.1X のフレーム(EAPOL)をブリッジ転送します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

MAC コントロールフレームのブリッジ転送を有効にするかどうかを設定します。
ここで転送を行うと定義されたプロトコルは、本装置では受信しません。そのため、STP を転送すると定義した場合、STP でのループ検出はできなくなります。

[注意]

本コマンドで定義可能なフレームは IEEE 802.1D でブリッジ転送を禁止しているフレームです。
Si-R180B ではスイッチポートを使用しないまたはスイッチポートの VLAN tag 透過転送の設定が有効となっている場合のみ利用が可能です。

[未設定時]

定義なしとして、MAC コントロールフレームの転送をしません。

第 15 章 LLDP 情報の設定

15.1 LLDP 情報

15.1.1 lldp send interval

[機能]

LLDP 送信間隔時間の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

```
lldp send interval <interval> <delay>
```

[オプション]

<interval>

・ LLDP 送信間隔時間
LLDP 情報の定期送信間隔時間を、10 進数と時間単位で指定します。
時間単位には、h(時)、m(分)、s(秒)のどれかを指定します。
指定可能な範囲は、5～32768 秒です。
本設定は、802.1AB の msgTxInterval 変数に相当します。

<delay>

・ LLDP 送信最小間隔時間
LLDP 情報の送信最小間隔時間を、10 進数と時間単位で指定します。
時間単位には、h(時)、m(分)、s(秒)のどれかを指定します。
指定可能な範囲は、1 秒～0.25×<interval>(最大 8192 秒)です。
本設定は、802.1AB の txDelay 変数に相当します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

本装置が LLDP 情報を定期送信する間隔時間と、LLDP 情報を変更したときに送信する際の送信最小間隔時間を指定します。

LLDP 送信動作を有効にした物理ポートでは、LLDP 送信間隔時間ごとに LLDP 情報が定期送信されます。

LLDP 情報を変更したときはそのつど LLDP 情報が送信されますが、送信が連続してネットワーク負荷が上がらないように、LLDP 送信最小間隔時間分空くようにして送信されます。

[未設定時]

LLDP 送信間隔時間には 30 秒、LLDP 送信最小間隔時間には 2 秒が指定されたものとみなされます。

```
lldp send interval 30s 2s
```

15.1.2 lldp send hold

[機能]

LLDP 保持回数の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lldp send hold <count>

[オプション]

<count>

・LLDP 保持回数
隣接装置が本装置の LLDP 情報を保持すべき時間を、LLDP 送信間隔時間の回数で指定します。
指定可能な範囲は 2～10 回で、10 進数で指定します。
「LLDP 送信間隔時間×LLDP 保持回数」で計算される TTL(最大 65535 秒)を隣接装置に通知します。
本設定は、802.1AB の msgTxHold 変数に相当します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

本装置の LLDP 情報を受信した隣接装置が本装置の LLDP 情報を保持すべき時間を、LLDP 送信間隔時間の回数で指定します。
隣接装置には、以下の計算式で示すように、本コマンドで設定した LLDP 保持回数と、lldp send interval コマンドで設定した LLDP 送信間隔時間を積算した TTL(Time To Live)を通知します。

TTL = LLDP 送信間隔時間 × LLDP 保持回数

ただし、TTL の最大値は 65535 秒のため、計算結果が 65535 秒を超えた場合は 65535 秒を通知します。

[未設定時]

4 回が指定されたものとみなされます。
LLDP 送信間隔時間が 30 秒の場合、30 秒×4 回=120 秒を TTL として LLDP クライアントに通知します。

```
lldp send hold 4
```

15.1.3 lldp reinit delay

[機能]

LLDP 送信停止後遅延時間の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lldp reinit delay <delay>

[オプション]

<delay>

・ LLDP 送信停止後遅延時間

LLDP 送信動作を無効にしたときに、TTL が 0 の LLDP 情報を送信してから内部の状態を再初期化するまでの遅延時間を、10 進数と時間単位で指定します。

時間単位には、s(秒)を指定します。

指定可能な範囲は、1～10 秒です。

本設定は、802.1AB の reinitDelay 変数に相当します。

[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 LLDP 送信動作を無効したときには、隣接装置に本装置の LLDP 情報を破棄させるために TTL が 0 の LLDP 情報が送信されます。

その LLDP 情報を送信してから装置の内部状態を再初期化するまでの遅延時間を設定します。

[未設定時]

2 秒が指定されたものとみなされます。

```
lldp reinit delay 2s
```

15.1.4 lldp notification interval

[機能]

SNMP Notification Trap 送信の最小間隔時間の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

lldp notification interval <interval>

[オプション]

<interval>

・Trap 送信の最小間隔時間
SNMP Notification Trap 送信の最小間隔時間を、10 進数と時間単位で指定します。
時間単位には、h(時)、m(分)、s(秒)のどれかを指定します。
指定可能な範囲は、5～3600 秒です。
本設定は、802.1AB の NotificationInterval 変数に相当します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNMP Notification Trap 送信してから、次に SNMP Notification Trap 送信するまでの最小送信間隔時間を指定します。

[注意]

snmp service コマンドで disable または compatible に設定している場合、および snmp trap lldpremtableschange コマンドで disable に設定している場合は、SNMP Notification Trap(lldpRemTablesChange トラップ)は送信されません。

[未設定時]

5 秒が指定されたものとみなされます。

```
lldp notification interval 5s
```

第 16 章 IEEE802.1X 情報の設定

16.1 IEEE802.1X 情報

16.1.1 dot1x use

[機能]

IEEE802.1X 認証モードの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

- on
  IEEE802.1X 認証を有効にします。
- off
  IEEE802.1X 認証を無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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、lan 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。

[未設定時]

IEEE802.1X 認証を利用しないものとみなされます。

```
dot1x use off
```

16.1.2 dot1x mode

[機能]

IEEE802.1X 認証方式の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

dot1x mode <mode>

[オプション]

<mode>

IEEE802.1X 認証方式を指定します。

- mac
  MAC アドレスごとの認証を行います。
- port
  ポートごとの認証を行います。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IEEE802.1X 認証方式を設定します。

[注意]

- IEEE802.1X 認証方式としてポートごとの認証を選択した場合、そのポートに接続される端末(Supplicant)の一台が認証許容された場合、同じポートに接続されるほかの端末からのアクセスがすべて透過として扱われます。
- 無線 LAN で利用する場合は、本コマンドの設定は無効となり、常に MAC アドレスごとの認証を行います。

[未設定時]

IEEE802.1X 認証方式として MAC アドレスごとの認証が指定されたものとみなされます。

```
dot1x mode mac
```

第 17 章 MPLS 情報の設定

17.1 LDP 情報

17.1.1 mpls ldp router-id

[機能]

LDP ROUTER-ID の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

mpls ldp router-id <identifier>

[オプション]

<identifier>

・ LDP を使用するルータを特定するための ID
IPv4 アドレスで指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

自装置を一意に示す ID を設定します。設定する ID はほかのルータと重複しない ID を指定します。通信可能な自装置の IP アドレス(IPv4)を設定します。
0.0.0.0 を指定した場合、自動的にどれかの自装置の IP アドレス(IPv4)を使用します。

[未設定時]

0.0.0.0 が設定されているものとみなされ、router-id は自動的に設定されます。

```
mpls ldp router-id 0.0.0.0
```

17.1.2 mpls ldp control

[機能]

LDP 制御方式の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

mpls ldp control <mode>

[オプション]

<mode>

- ordered
  Ordered Label Distribution Control を使用します。
- independent
  Independent Label Distribution Control を使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

LDP の制御方式を指定します。

[未設定時]

independent が選択されたものとして動作します。

```
mpls ldp control independent
```

17.1.3 mpls ldp ip transport

[機能]

IPv4 Transport Address の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

mpls ldp ip transport <address>

[オプション]

<address>

・ LDP セッションの送信元 IPv4 アドレス
IPv4 アドレスを指定します。以下の範囲で指定してください。

0.0.0.0
1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

[動作モード]

構成定義モード(管理者クラス)

[説明]

LDP がピアとの通信に用いる送信元 IPv4 アドレスを設定します。本装置に設定された IPv4 アドレスを指定します。
インタフェースの設定で IPv4 Transport Address を指定しない場合に、本設定が使用されます。本定義に 0.0.0.0 を指定した場合は、LDP が動作するインタフェースの IPv4 アドレスを IPv4 Transport Address として使用します。

[注意]

IPv4 Transport Address を指定する場合は、必ず本装置に存在するにアドレスを指定する必要があります。本装置に存在しないアドレスを指定した場合は、LDP を使用できません。

[未設定時]

IPv4 Transport Address の設定を行わず、LDP が動作するインタフェースの IPv4 アドレスを送信元として使用します。

```
mpls ldp ip transport 0.0.0.0
```

17.1.4 mpls ip propagate-ttl

[機能]

MPLS TTL 伝達の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

mpls ip propagate-ttl <mode>

[オプション]

<mode>

- on
  MPLS から IP または IP から MPLS にパケットを交換する際に、TTL の情報を伝達します。
- off
  MPLS から IP または IP から MPLS にパケットを交換する際に、TTL の情報を伝達しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

MPLS と IP の間での TTL の伝達方法を指定します。

mode が on の場合は。MPLS ラベル PUSH 時に IP パケットの TTL が伝達され、MPLS ラベル POP 時に IP パケットの TTL に書き戻されるため、MPLS ドメインを転送される IP パケットはドメインの hop 数分だけ TTL が減少します。

mode が off の場合は。MPLS ラベル PUSH 時に IP パケットの TTL が伝達されず、MPLS パケットの TTL は無条件で 255 となり、また MPLS ラベル POP 時にも IP パケットの TTL は書き戻されないため、MPLS ドメインを転送される IP パケットはドメインの hop 数を意識することがなく、ドメインを 1 つの仮想的なルータとして見るようになります。

[注意]

本設定は MPLS ドメイン中のすべてのルータで一致させる必要があります。

[未設定時]

on が選択されたものとして動作します。

```
mpls ip propagate-ttl on
```

第 18 章 マルチキャスト情報の設定

18.1 マルチキャスト情報

18.1.1 multicast ip igmp report

[機能]

IGMP Membership Report パケットの送出の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

18.1.2 multicast ip pimsm candrp mode

[機能]

PIM-SM(IPv4)の RP の動作の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

18.1.3 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

18.1.4 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

18.1.5 multicast ip pimsm candbsr mode

[機能]

PIM-SM(IPv4)の BSR の動作の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

18.1.6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

18.1.7 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

18.1.8 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

18.1.9 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

18.1.10 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B
1～100000 1k～100000k 1m～100m	上記以外

[動作モード]

構成定義モード(管理者クラス)

[説明]

SPT への経路変更のしきい値をデータ転送速度で設定します。

[注意]

経路変更が行われるまで、最大で 5 秒のタイムラグが発生する場合があります。

[未設定時]

即座に SPT への経路変更を行います。

```
multicast ip pimsm spt rate 0
```

18.1.11 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

18.1.12 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
5	Si-R180B

<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～rmt999	Si-R570 Si-R570B
lan0～lan19 rmt0～rmt499	Si-R370 Si-R370B
lan0～lan19 rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
lan0～lan9 rmt0～rmt49	Si-R180B

[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 19 章 UPnP 情報の設定

19.1 UPnP 情報

19.1.1 upnp use

[機能]

VoIP NAT トラバーサル機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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 変換も同時に使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
```

19.1.2 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

upnp portmapping lease <time>

[オプション]

<time>

・ポートマッピング有効期限

UPnP クライアントがポートマッピングを無期限で設定しようとしたときに、強制的に設定する有効期限を指定します。

有効期限は、60 秒(1 分)～86400 秒(1 日)の範囲で、数字と単位をつなげて指定します。

単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

UPnP クライアントがポートマッピングを無期限で設定しようとしたときに、強制的に設定する有効期限を設定します。設定したポートマッピングが使用されなくなってから有効期限を過ぎたとき、そのポートマッピングを強制的に削除します。

本設定がなく、UPnP クライアントがポートマッピングを無期限で登録した場合、UPnP クライアントがポートマッピングを削除するまでポートマッピングが設定されたままになります。

[注意]

本設定によってポートマッピングが強制的に削除された場合、そのポートマッピングを設定した UPnP クライアントが通信できなくなります。その場合、その UPnP クライアントを再起動してください。

[未設定時]

ポートマッピング有効期限を設定しないものとみなされ、ポートマッピングを強制的に削除しません。

第 20 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
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

20.1 ACL 情報

20.1.1 acl mac

[機能]

ACL MAC 定義

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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 進数を指定します。

すべての LLC 形式フレームを対象とする場合は<value>に any を指定します。

snap <value>

<value>の値とタイプフィールドが一致する SNAP 形式フレームを対象とする場合に指定します。<value>には、0～ffff の 16 進数を指定します。

すべての SNAP 形式フレームを対象とする場合は<value>に any を指定します。

ether <value>

<value>の値とタイプフィールドが一致する Ethernet 形式フレームを対象とする場合に指定します。<value>には、5dd～ffff の 16 進数を指定します。

すべての Ethernet 形式フレームを対象とする場合は<value>に any を指定します。

any

すべてのフレームを対象とする場合に指定します。

<vlan_analyze>

VLAN タグ付きフレームに対してタグの解析を行うかどうかを指定します。

省略時は、off を指定したものとみなされます。

- on

  VLAN タグ付きフレームの場合に VLAN タグを解析してフィルタリング処理を行います。VLAN タグ付きフレームの場合は、タグの長さ分ずれた位置にある LLC 形式フレームの LSAP や Ethernet 形式フレームのタイプに対してフィルタリング処理を行います。

- off

  VLAN タグ付きフレームの場合に VLAN タグを解析しないでフィルタリング処理を行います。VLAN タグ付きフレームの場合でもタグの長さ分ずらさずにそのままフィルタリング処理を行うため、VLAN タグの TPID が、<value>との比較対象になります。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ACL 定義で etherframe パターンを指定します。

[未設定時]

ACL 定義でどのような etherframe パターンでも対象とします。

20.1.2 acl ip

[機能]

ACL IPv4 定義

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

```
acl <acl_count> ip <src_addr>/<mask> <dst_addr>/<mask> [<protocol> [any]]
acl <acl_count> ip <src_addr>/<mask> <dst_addr>/<mask> [<protocol> [tos <value>]]
acl <acl_count> ip <src_addr>/<mask> <dst_addr>/<mask> [<protocol> [dscp <value>]]
```

[オプション]

<acl_count>

・ ACL 定義番号

ACL 定義の通し番号を、10 進数で指定します。

<src_addr>/<mask>

ACL 対象とする送信元 IP アドレスとマスクビット数を指定します。

・ IP アドレス/マスクビット数(またはマスク値)

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

以下に、有効な記述形式を示します。

- IP アドレス/マスクビット数 (例: 192.168.1.1/24)

・ any

すべての送信元 IP アドレスを ACL 対象とする場合に指定します。

0.0.0.0/0 を指定するのと同じ意味になります。

<dst_addr>/<mask>

ACL 対象とするあて先 IP アドレスとマスクビット数を指定します。

・ IP アドレス/マスクビット数(またはマスク値)

ACL 対象とするあて先 IP アドレスとマスクビット数の組み合わせを指定します。

記述形式は、<src_addr>/<mask>と同様です。

・ any

すべてのあて先 IP アドレスを ACL 対象とする場合に指定します。

0.0.0.0/0 を指定するのと同じ意味になります。

<protocol>

ACL 対象とするプロトコル番号を指定します。

・ プロトコル番号

ACL 対象とするプロトコル番号を、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。

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、dscp オプション省略時は any を指定したものとみなされ、すべての TOS 値、すべての DSCP 値を ACL 対象とします。

・ TOS 値

ACL 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)

・ 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。

[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)

20.1.3 acl ip6

[機能]

ACL IPv6 定義

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

```
acl <acl_count> ip6 <src_addr>/<prefixlen> <dst_addr>/<prefixlen> [<protocol> [any]]
acl <acl_count> ip6 <src_addr>/<prefixlen> <dst_addr>/<prefixlen> [<protocol> [tc <value>]]
acl <acl_count> ip6 <src_addr>/<prefixlen> <dst_addr>/<prefixlen> [<protocol> [dscp <value>]]
```

[オプション]

<acl_count>

・ ACL 定義番号
ACL 定義の通し番号を、10 進数で指定します。

<src_addr>/<prefixlen>

フィルタリング対象とする送信元 IPv6 アドレスとプレフィックス長を指定します。

・ IPv6 アドレス/プレフィックス長
フィルタリング対象とする送信元 IPv6 アドレスとプレフィックス長の組み合わせを指定します。

・ any
すべての送信元 IPv6 アドレスをフィルタリング対象とする場合に指定します。
::/0 を指定するのと同じ意味になります。

<dst_addr>/<prefixlen>

フィルタリング対象とするあて先 IPv6 アドレスとプレフィックス長を指定します。

・ IPv6 アドレス/プレフィックス長
フィルタリング対象とするあて先 IPv6 アドレスとプレフィックス長の組み合わせを指定します。

・ any
すべてのあて先 IPv6 アドレスをフィルタリング対象とする場合に指定します。
::/0 を指定するのと同じ意味になります。

<protocol>

ACL 対象とするプロトコル番号を指定します。

・ プロトコル番号
ACL 対象とするプロトコル番号を、1～255 の 10 進数で指定します(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。

<value>

ACL 対象とする Traffic Class 値、または DSCP 値を指定します。
tc、dscp オプション省略時は any を指定したものとみなされ、すべての Traffic Class 値、すべての DSP 値を ACL 対象とします。

・ 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 ip6 を定義してください。

[未設定時]

ACL 定義でどのような IPv6 パケットのパターンでも対象とします。
(all any 設定時、未定義では acl 定義は存在しません)

20.1.4 acl tcp

[機能]

ACL TCP 定義

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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/ip6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。

20.1.5 acl udp

[機能]

ACL UDP 定義

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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/ip6 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。

20.1.6 acl icmp

[機能]

ACL ICMP 定義

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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/ip6 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。

20.1.7 acl description

[機能]

ACL description 定義

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

<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。

第 21 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
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～49	Si-R180B

21.1 ポリシーグループ定義情報

21.1.1 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
9000	Si-R570 Si-R570B
4500	Si-R370 Si-R370B
900	Si-R260B Si-R240B Si-R220C Si-R220D
450	Si-R180B

<action>

動作
acl 定義に一致した場合の動作を指定します。

・ match
acl 定義に一致した場合、このポリシーグループのポリシーに従います。
・ unmatch
acl 定義に一致した場合、このポリシーグループのポリシーに従いません。
・ backup
以降の policy-group 定義に一致しなかった場合に、このポリシーグループのポリシーに従います。

<acl_number>

・ 参照 ACL 番号
ポリシーとして参照する ACL 定義の定義番号を指定します。
指定した<acl_count>の ACL が定義されていない場合、その定義は無効となり、無視されます。

範囲	機種
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

[動作モード]

構成定義モード(管理者クラス)

[説明]

ポリシーグループのルールを ACL を利用して指定します。

[注意]

参照すべき ACL 定義が未定義の場合、該当するポリシー定義は無効となりますが、定義あり状態となります。

[未設定時]

ポリシーグループ定義は無効とみなされます。

21.1.2 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

21.1.3 policy-group interface

[機能]

送出先インタフェースの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

21.1.4 policy-group nexthop

[機能]

送出先 IPv4 ルータの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

21.1.5 policy-group nexthop6

[機能]

送出先 IPv6 ルータの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

21.1.6 policy-group sessionwatch address

[機能]

接続先監視のアドレス設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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 アドレスのどれかを指定してください。
指定可能な範囲は以下のとおりです。

IPv4:
1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

IPv6:
::2 ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<destination>

・ICMP ECHO パケットのあて先 IP アドレス
監視対象となる IPv4/IPv6 アドレスを指定します。
<source>と同じプロトコルアドレスで指定してください。
指定可能な範囲は以下のとおりです。

IPv4:
1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

IPv6:
::2 ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

[動作モード]

構成定義モード(管理者クラス)

[説明]

接続先の生存確認を行うための動作情報を設定します。
指定したあて先 IP アドレスに対して ICMP ECHO パケットの送受信で生存確認を行います。

[注意]

以下の場合は、監視を行いません。
・policy-group pattern 定義がない場合。
・policy-group interface 定義がない場合。
・policy-group sessionwatch address 定義がない場合。

- policy-group interface 定義に lan を指定し、policy-group sessionwatch address 定義に IPv4 アドレスを指定したとき、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。
- ISDN 回線を利用する接続先で、常時接続機能を利用していない場合。
- PPPoE 回線を利用する接続先で、常時接続機能を利用していない場合。

[未設定時]

接続先監視機能を利用しないものとみなされます。

21.1.7 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。
- ISDN 回線を利用する接続先で、常時接続機能を利用していない場合。
- PPPoE 回線を利用する接続先で、常時接続機能を利用していない場合。

[未設定時]

```
policy-group <policy-group_number> sessionwatch interval 10s 1m 5s 1s
```

21.1.8 policy-group sessionwatch ttl

[機能]

接続先監視の TTL/HopLimit 値設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。
・ ISDN 回線を利用する接続先で、常時接続機能を利用していない場合。
・ PPPoE 回線を利用する接続先で、常時接続機能を利用していない場合。

[未設定時]

```
policy-group <policy-group_number> sessionwatch ttl 255
```

21.1.9 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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 の範囲で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

接続先の生存確認を行うための動作情報を設定します。

異常状態から正常状態へ復旧するために必要な連続応答受信回数を設定します。これにより、回線状態が不安定な場合のダウン／アップのばたつきを防ぎます。

連続応答待ち状態での ICMP ECHO パケット送信間隔は、正常時送信間隔を使用します。

本装置起動後を含め、回線接続直後に通信可能な状態であっても、必要な回数の応答を受信するまで通信可能とはなりませんので、ご注意ください。

[注意]

以下の場合は、監視を行いません。

・ policy-group pattern 定義がない場合。
・ policy-group interface 定義がない場合。
・ policy-group sessionwatch address 定義がない場合。
・ policy-group interface 定義に lan を指定し、policy-group sessionwatch address 定義に IPv4 アドレスを指定したとき、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。
・ ISDN 回線を利用する接続先で、常時接続機能を利用していない場合。
・ PPPoE 回線を利用する接続先で、常時接続機能を利用していない場合。

[未設定時]

```
policy-group <policy-group_number> sessionwatch recovery 1
```

21.1.10 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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)のどれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

接続先の生存確認を行うための動作情報を設定します。

正常状態から異常状態に遷移した場合に、最初の ICMP ECHO パケットを送信するまでの待ち時間を設定します。

[注意]

以下の場合は、監視を行いません。

・ policy-group pattern 定義がない場合。
・ policy-group interface 定義がない場合。
・ policy-group sessionwatch address 定義がない場合。
・ policy-group interface 定義に lan を指定し、policy-group sessionwatch address 定義に IPv4 アドレスを指定したとき、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。
・ ISDN 回線を利用する接続先で、常時接続機能を利用していない場合。
・ PPPoE 回線を利用する接続先で、常時接続機能を利用していない場合。

[未設定時]

```
policy-group sessionwatch error-wait 0s
```

・ 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

・ 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
0～1999	Si-R570 Si-R570B Si-R370 Si-R370B
0～999	Si-R260B Si-R240B Si-R220C Si-R220D
0～199	Si-R180B

22.1 グループ ID 情報

22.1.1 aaa name

[機能]

グループ名称の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

22.2 AAA ユーザ情報

22.2.1 aaa user id

[機能]

認証情報の設定(ユーザ ID)

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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 64 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。

22.2.2 aaa user password

[機能]

認証情報の設定(パスワード)

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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 64 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。

[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。

22.2.3 aaa user called number

[機能]

CLID の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R240B Si-R220C Si-R220D

[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。

[注意]

Si-R370 Si-R370B Si-R220C Si-R220D は PIAFS 接続に対応しています。PIAFS(64Kbps)着信時には、<subaddress> で設定した相手サブアドレスは無視されますので、設定しないでください。

[未設定時]

CLID 相手判定を行わないものとみなされます。

22.2.4 aaa user ip address local

[機能]

自側 IP アドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

22.2.5 aaa user ip address remote

[機能]

相手側 IP アドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

22.2.6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～1999	Si-R570 Si-R570B
0～1249	Si-R370 Si-R370B
0～255	Si-R260B Si-R240B Si-R220C Si-R220D
0～127	Si-R180B

<address>/<mask>

・ IPv4 アドレス/マスクビット数(またはマスク値)
あて先ネットワークを IPv4 アドレスとマスクビット数の組み合わせで指定します。
マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
- IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
- IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)

・ default
あて先ネットワークとしてデフォルトルートを設定する場合に指定します。
0.0.0.0/0(0.0.0.0/0.0.0.0)を指定するのと同じ意味になります。

<metric>

・ RIP メトリック値
このスタティック経路情報を RIP に再配布するときのメトリック値を、1～15 の 10 進数で指定します。

<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。

優先度の設定値にかかわらず、常にフローティング動作します。

remote インタフェースが通信可能な状態(リンクアップなど)であれば、スタティック経路情報をルーティングテーブルに追加します。通信不可能な状態(リンクダウンなど)であれば、ルーティングテーブルから削除します。

複数のスタティック経路情報で ECMP 機能を使用するときは、あて先、RIP メトリック値、優先度がそれぞれ同じとなるようにスタティック経路情報を設定します。また、ECMP 機能を使用する場合は、routemanage ip ecmp mode コマンドで ECMP を使用するように設定します。

ECMP となるスタティック経路情報は、同じあて先への経路情報ごとに装置全体で 4 個まで定義できます。

IPv4 スタティック経路情報は、本装置全体で以下の数まで定義できます。

最大定義数	機種
2000	Si-R570 Si-R570B
1250	Si-R370 Si-R370B
256	Si-R260B Si-R240B Si-R220C Si-R220D
128	Si-R180B

[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。

22.2.7 aaa user ip6 ifid

[機能]

IPv6 インタフェース ID の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

aaa [<group_id>] user [<number>] ip6 ifid <interfaceID>

[オプション]

<group_id>

・グループ ID
各グループを示す ID を 10 進数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。

22.2.8 aaa user ip6 route

[機能]

IPv6 スタティック経路情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

aaa [<group_id>] user [<number>] ip6 route <count> <address>/<prefixlen> <metric> <distance>

[オプション]

<group_id>

・ グループ ID
各グループを示す ID を 10 進数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
0～1999	Si-R570 Si-R570B
0～1249	Si-R370 Si-R370B
0～255	Si-R260B Si-R240B Si-R220C Si-R220D
0～127	Si-R180B

<address>/<prefixlen>

・ IPv6 アドレス/プレフィックス
あて先ネットワークを IPv6 アドレスとプレフィックスの組み合わせを指定します。
・ default
あて先ネットワークとしてデフォルトルートを設定する場合に指定します。
::/0 を指定するのと同じ意味になります。

<metric>

・ メトリック値
このスタティック経路情報を RIPng で広報する場合のメトリック値を、 1～15 の 10 進数で指定します。
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 ip6 distance コマンドを参照してください。

優先度の設定値にかかわらず、常にフローティング動作します。

remote インタフェースが通信可能な状態(リンクアップなど)であれば、スタティック経路情報をルーティングテーブルに追加します。通信不可能な状態(リンクダウンなど)であれば、ルーティングテーブルから削除します。

IPv6 スタティック経路情報は、本装置全体で以下の数まで定義できます。

最大定義数	機種
2000	Si-R570 Si-R570B
1250	Si-R370 Si-R370B
256	Si-R260B Si-R240B Si-R220C Si-R220D
128	Si-R180B

[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。

22.2.9 aaa user sessionwatch

[機能]

接続先監視アドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

22.2.10 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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 <number> ipsec ike range any4 any4
```

22.2.11 aaa user ipsec extension-range

[機能]

拡張 IPsec 対象範囲の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～49	Si-R180B

<src_addr>/<mask>

IPsec 対象となる送信元 IP アドレス、マスクビット数を指定します。

・ IP アドレス/マスクビット数(またはマスク値)
IPsec 対象となる送信元 IP アドレスとマスクビット数の組み合わせを指定します。

・ any4
すべての IPv4 アドレスを IPsec 対象に含めます。
0.0.0.0/0(0.0.0.0/0.0.0.0)と同意。

・ any6
すべての IPv6 アドレスを IPsec 対象に含めます。
::/0 と同意。

<dst_addr>/<mask>

IPsec 対象となるあて先 IP アドレス、マスクビット数を指定します。

・ IP アドレス/マスクビット数(またはマスク値)
IPsec 対象となるあて先 IP アドレスとマスクビット数の組み合わせを指定します。

・ any4
すべての IPv4 アドレスを IPsec 対象に含めます。
0.0.0.0/0(0.0.0.0/0.0.0.0)と同意。

・ any6
すべての IPv6 アドレスを IPsec 対象に含めます。
::/0 と同意。

[動作モード]

構成定義モード(管理者クラス)

[説明]

拡張 IPsec 対象範囲を設定します。
拡張 IPsec 対象範囲定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
1000	Si-R570 Si-R570B
500	Si-R370 Si-R370B
100	Si-R260B Si-R240B Si-R220C Si-R220D
50	Si-R180B

[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。

22.2.12 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

22.2.13 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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を指定します。
指定可能な範囲は、1～4094です。

[動作モード]

構成定義モード(管理者クラス)

[説明]

Supplicant(ユーザ端末)に割り当てるVLAN IDを指定します。

[注意]

本設定で指定したVLAN IDは、RADIUSサーバから送出されるAccess-Accept中の Tunnel-Private-Group-Idアトリビュートで送信されます。また本設定を行った場合は、Tunnel-Private-Group-Id アトリビュートに加えて、Tunnel-Type アトリビュートが値 13 (VLAN) で、Tunnel-Medium-Type アトリビュートが値 6 (IEEE802) が同時に送信されます。
未設定の場合は、これらのアトリビュートは送信されません。

[未設定時]

割り当てるVLAN IDが存在しないものとして扱われます。

22.2.14 aaa user supplicant mac

[機能]

Supplicant MAC アドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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 アドレスを同時に使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。

22.2.15 aaa user user-role

[機能]

権限クラスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

22.3 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
0～3	Si-R570 Si-R570B Si-R370 Si-R370B
0	Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

・ 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
0～3	Si-R570 Si-R570B Si-R370 Si-R370B
0～1	Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

22.3.1 aaa radius service

[機能]

RADIUS サービスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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、同時に使用できません。
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
```

22.3.2 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

22.3.3 aaa radius auth message-authenticator

[機能]

Message-Authenticator の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

22.3.4 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

22.3.5 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

22.3.6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

22.3.7 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

22.3.8 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

22.3.9 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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 radius client server-info auth port 1812
```

22.3.10 aaa radius client server-info auth deadtime

[機能]

復旧待機時間の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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)のどれかを指定します。
指定可能な範囲は以下のとおりです。
0～86400(秒)
0s を指定した場合は、自動的に alive 状態に復旧しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RADIUS サーバから aaa radius client retry コマンドで設定した応答待ち受け時間を経過しても応答が得られなかった場合、その RADIUS サーバは dead 状態となり、優先度は最非優先となります。dead 状態となった RADIUS サーバは、alive 状態のサーバが存在する限り使わなくなります。本設定は、dead 状態になってから、設定した優先度となる alive 状態へ自動的に復旧するための待ち時間を設定します。

dead 状態から alive 状態に復旧するためには、以下のどれかの条件を満たす必要があります。

・ 本設定の時間が経過した場合
・ 利用可能なすべてのサーバが dead 状態となったあと、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 radius client server-info auth deadtime 0s
```

22.3.11 aaa radius client server-info auth priority

[機能]

優先度の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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 radius client server-info auth priority 0
```

22.3.12 aaa radius client server-info auth source

[機能]

自側 IP アドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

22.3.13 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

22.3.14 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

22.3.15 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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 radius client server-info accounting port 1813
```

22.3.16 aaa radius client server-info accounting deadtime

[機能]

復旧待機時間の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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)のどれかを指定します。
指定可能な範囲は以下のとおりです。
0～86400(秒)
0s を指定した場合は、自動的に alive 状態に復旧しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RADIUS サーバから aaa radius client retry コマンドで設定した応答待ち受け時間を経過しても応答が得られなかった場合、その RADIUS サーバは dead 状態となり、優先度は最非優先となります。dead 状態となった RADIUS サーバは、alive 状態のサーバが存在する限り使わなくなります。本設定は、dead 状態になってから、設定した優先度となる alive 状態へ自動的に復旧するための待ち時間を設定します。

dead 状態から alive 状態に復旧するためには、以下のどれかの条件を満たす必要があります。

・ 本設定の時間が経過した場合
・ 利用可能なすべてのサーバが dead 状態となったあと、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 radius client server-info accounting deadtime 0s
```

22.3.17 aaa radius client server-info accounting priority

[機能]

優先度の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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 radius client server-info accounting priority 0
```

22.3.18 aaa radius client server-info accounting source

[機能]

自側 IP アドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

22.3.19 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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指定します。
指定可能な範囲は以下のとおりです。

1～10(秒)

<retry>

・ 再送回数
RADIUS サーバ未応答時のパケット再送回数を指定します。
指定可能な範囲は以下のとおりです。

1～10(回)

[動作モード]

構成定義モード(管理者クラス)

[説明]

RADIUS サーバ未応答時のパケットの再送回数・送信間隔を設定します。
サーバからの応答待ち受け時間は、送信間隔×(再送回数+1)秒となります。

[未設定時]

送信間隔を 1 秒、再送回数を 2 回として動作します。
この場合は、サーバからの応答待ち受け時間はパケットの初回送信後、3 秒となります。

```
aaa 0 client radius retry 1 2
```

22.3.20 aaa radius client nas-identifier

[機能]

NAS 識別子の設定

[適用機種]

Si-R570 | Si-R570B | Si-R370 | Si-R370B | Si-R260B | Si-R240B | Si-R220C | Si-R220D | Si-R180B

[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。

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

範囲	機種
0～39	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

・ 管理機器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>(管理機器定義番号)に指定する管理機器の通し番号(10 進数)は、以下に示す範囲で指定してください。

範囲	機種
0～39	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

・ MAC アドレスフィルタセッ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<set_num>(MAC アドレスフィルタセット定義番号)に指定する MAC アドレスフィルタセットの通し番号(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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

・ MAC アドレスフィルタ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<filter_num>(MAC アドレスフィルタ定義番号)に指定する MAC アドレスフィルタの通し番号(10 進数)は、以下に示す範囲で指定してください。

範囲	機種
0～99	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

・ 管理外無線 LAN アクセスポイ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>(管理外無線 LAN アクセスポイント定義番号)に指定する管理外無線 LAN アクセスポイントの通し番号(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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

23.1 無線 LAN 管理機器情報

23.1.1 nodemanager group name

[機能]

管理グループ名の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

nodemanager group <number> name <name>

[オプション]

<number>

・ グループ定義番号
管理グループの通し番号を 10 進数で指定します。

<name>

・ グループ名
管理グループ名には既存のグループ名と同じ名前は使用できません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

管理グループの名前を設定します。

[未設定時]

管理グループを設定しないものとみなされます。

23.1.2 nodemanager node name

[機能]

管理機器名の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

nodemanager node <number> name <name>

[オプション]

<number>

・ 管理機器定義番号
管理機器の通し番号を 10 進数で指定します。

<name>

・ 管理機器名
管理機器名を、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]

管理機器の名前を設定します。

[注意]

管理機器名が設定されていない管理機器は、無線 LAN 管理機能の対象となりません。

[未設定時]

管理機器を設定しないものとみなされます。

23.1.3 nodemanager node group

[機能]

管理機器の所属グループの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

nodemanager node <number> group <group_number>

[オプション]

<number>

・管理機器定義番号
管理機器の通し番号を 10 進数で指定します。

<group_number>

・グループ定義番号
所属先の管理グループ通し番号を 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]

設定済みの管理機器を管理グループに所属させます。所属先の管理グループが削除された場合は、管理機器は自動的にどのグループにも所属していない状態になります。

[注意]

存在しないグループを指定した場合、設定済みのグループを削除した場合は、管理機器はどのグループにも所属しないものとして動作します。
管理機器に管理機器名が定義されていない場合、このコマンドの設定は無効になります。

[未設定時]

管理機器の所属グループを設定しないものとみなされます。

23.1.4 nodemanager node address

[機能]

管理機器の IP アドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

nodemanager node <number> address <address>

[オプション]

<number>

・管理機器定義番号
管理機器の通し番号を 10 進数で指定します。

<address>

・管理機器 IP アドレス
IP アドレスの設定を変更する場合に指定します。
管理機器の 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。

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

[動作モード]

構成定義モード(管理者クラス)

[説明]

管理機器の IP アドレスを設定します。

[注意]

管理機器に管理機器名が定義されていない場合、このコマンドの設定は無効になります。
管理機器の IP アドレスが設定されていない管理機器は、無線 LAN 管理機能の対象となりません。

[未設定時]

IP アドレスがないものとみなされます。

23.1.5 nodemanager node user

[機能]

リモートログイン時のユーザ名、パスワードの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

nodemanager node <number> user nodemgr <password> [encrypted]

[オプション]

<number>

・管理機器定義番号
管理機器の通し番号を 10 進数で指定します。

<password>

・パスワード
管理機器のパスワードを設定する場合に指定します。
パスワードを、0x21,0x23～0x7e の 64 文字以内の ASCII 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]

管理機器へのリモートログインに使用するユーザ名、パスワードを設定します。
リモートログインに使用されるユーザ名は、常に "nodemgr" です。

[注意]

管理機器に管理機器名が定義されていない場合、このコマンドの設定は無効になります。

[未設定時]

リモートログイン時のユーザ名、パスワードを設定しないものとみなされます。

23.1.6 nodemanager node wlan scan

[機能]

管理機器用のスキャン要求の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

nodemanager node <number> wlan scan {enable|disable}

[オプション]

<number>

・ 管理機器定義番号
管理機器の通し番号を 10 進数で指定します。

enable|disable

・ スキャニングフラグ
管理機器のスキャン要求を設定します。
指定可能な値は以下のとおりです。

disable
:スキャン要求なし

enable
:スキャン要求あり

[動作モード]

構成定義モード(管理者クラス)

[説明]

管理機器の「スキャン要求なし」、「スキャン要求あり」を設定します。

[注意]

管理機器に管理機器名が定義されていない場合、このコマンドの設定は無効になります。
スキャン要求を設定する無線 LAN アクセスポイントは、以下の条件を満たす必要があります。

・ 無線 LAN インタフェースの動作タイプが、無線 LAN アクセスポイント、または、スキャン専用モードであること。
・ 周辺アクセスポイント検出の動作モードが有効であること。

[未設定時]

管理機器のスキャニングフラグに「スキャン要求あり」が設定されたものとみなされます。

```
nodemanager node <number> wlan scan enable
```

23.1.7 nodemanager node wlan sta

[機能]

無線 LAN 端末の情報取得の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

nodemanager node <number> wlan sta {enable|disable}

[オプション]

<number>

・管理機器定義番号
管理機器の通し番号を 10 進数で指定します。

enable|disable

・情報取得フラグ
管理機器の無線 LAN 端末情報取得を設定します。
指定可能な値は以下のとおりです。

disable
:無線 LAN 端末の情報取得なし

enable
:無線 LAN 端末の情報取得あり

[動作モード]

構成定義モード(管理者クラス)

[説明]

管理機器用の「無線 LAN 端末の情報取得なし」、「無線 LAN 端末の情報取得あり」を設定します。

[注意]

管理機器に管理機器名が定義されていない場合、このコマンドの設定は無効になります。

[未設定時]

管理機器の情報取得フラグに「無線 LAN 端末の情報取得あり」が設定されたものとみなされます。

```
nodemanager node <number> wlan sta enable
```

23.1.8 nodemanager node wlan neighbor

[機能]

近隣の管理機器の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

nodemanager node <number> wlan neighbor <node_num1> [<node_num2>[<node_num3> [<node_num4>]]]

[オプション]

<number>

・ 管理機器定義番号
管理機器の通し番号を 10 進数で指定します。

<node_num1>,<node_num2>,<node_num3>,<node_num4>

・ 近隣管理機器定義番号
近隣の管理機器の通し番号を 10 進数で指定します。
<number>と同じ値は指定できません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

近隣の管理機器を設定します。近隣管理機器情報は、管理機器間の関係を調整する場合に使用されます。

[注意]

管理機器に管理機器名が定義されていない場合、このコマンドの設定は無効になります。
近隣管理機器に未定義の近隣管理機器を設定した場合、このコマンドの設定は無効になります。

[未設定時]

近隣管理機器を設定しないものとみなされ、電波出力自動調整の対象から除外されます。

23.2 MAC アドレスフィルタ情報

23.2.1 nodemanager wlan filterset description

[機能]

MAC アドレスフィルタセットのコメントの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

nodemanager wlan filterset <set_num> description <desc>

[オプション]

<set_num>

・ MAC アドレスフィルタセット定義番号
MAC アドレスフィルタセット定義番号を 10 進数で指定します。

<desc>

・ コメント
MAC アドレスフィルタに対するコメントを、0x21,0x23～0x7e の 50 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]

MAC アドレスフィルタセットにコメントを設定します。

[未設定時]

MAC アドレスフィルタセットにコメントを設定しないものとみなされます。

23.2.2 nodemanager wlan filterset filter mac

[機能]

管理機器用の MAC アドレスフィルタの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

nodemanager wlan filterset <set_num> filter <filter_num> mac <mac> <action>

[オプション]

<set_num>

・ MAC アドレスフィルタセット定義番号
MAC アドレスフィルタセット定義番号を 10 進数で指定します。

<filter_num>

・ MAC アドレスフィルタ定義番号
MAC アドレスフィルタセット内の MAC アドレスフィルタ定義番号を 10 進数で指定します。

<mac>

・ 無線 LAN 端末 MAC アドレス
無線 LAN 端末の MAC アドレスを<set_num>,<filter_num>で指定した MAC アドレスフィルタに指定します。
指定可能な値は以下のとおりです。

any

: すべての MAC アドレスが対象

MAC アドレス

: 対象とする無線 LAN 端末の 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。

<action>

・ アクション
MAC アドレスフィルタで設定された MAC アドレスの接続を許可するかどうかを指定します。
指定可能な値は以下のとおりです。

pass

: MAC アドレスの接続を許可(透過)

reject

: MAC アドレスの接続を拒否(遮断)

[動作モード]

構成定義モード(管理者クラス)

[説明]

管理機器用の MAC アドレスフィルタを設定します。
「管理機器への MAC アドレスフィルタ配布」で MAC アドレスフィルタを管理機器に反映すると、管理機器は MAC アドレスフィルタと一致した無線 LAN 端末の接続を<action>に従って許可または拒否します。

[注意]

本コマンドで追加した MAC アドレスの情報を、実際の管理機器に反映させるには nodemanagerctl update wlan filterset コマンドを使用します。

[未設定時]

MAC アドレスフィルタを設定しないものとみなされます。

23.2.3 nodemanager wlan filterset filter description

[機能]

MAC アドレスフィルタへのコメントの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

nodemanager wlan filterset <set_num> filter <filter_num> description <desc>

[オプション]

<set_num>

・ MAC アドレスフィルタセット定義番号
MAC アドレスフィルタセット定義番号を 10 進数で指定します。

<filter_num>

・ MAC アドレスフィルタ定義番号
MAC アドレスフィルタセット内の MAC アドレスフィルタ定義番号を 10 進数で指定します。

<desc>

・ コメント
MAC アドレスフィルタに対するコメントを、0x21,0x23～0x7e の 50 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]

MAC アドレスフィルタに無線 LAN 端末の MAC アドレスコメントを設定します。

[注意]

管理機器用の MAC アドレスフィルタが設定されていない場合、このコマンドの設定は無効になります。

[未設定時]

MAC アドレスフィルタに無線 LAN 端末の MAC アドレスコメントを設定しないものとみなされます。

23.3 電波出力自動調整情報

23.3.1 nodemanager wlan autotxpower rssi

[機能]

電波出力自動調整の RSSI 最低しきい値の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

nodemanager wlan autotxpower rssi <low_rssi>

[オプション]

<low_rssi>

・ 電波出力自動調整用 RSSI 最低しきい値

近隣の無線 LAN アクセスポイントで、設定対象の無線 LAN アクセスポイントの無線送信出力を判定するための RSSI 最低しきい値を 1～255 の範囲の 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]

電波出力自動調整機能は、任意の無線 LAN アクセスポイントの無線送信出力を自動的に調整する機能で、その電波の到達範囲が必要以上に大きくなるのを防止します。

電波出力自動調整用 RSSI 最低しきい値には、電波出力自動調整時に近隣の無線 LAN アクセスポイントで計測される、設定対象の無線 LAN アクセスポイントの RSSI のしきい値を指定します。

RSSI と信号強度 (dBm) 関係は、以下のとおりです。

dBm = (RSSI 値) - 95

[未設定時]

電波出力自動調整用 RSSI 最低しきい値は 20 が設定されたものとみなされます。

```
nodemanager wlan autotxpower rssi 20
```

23.4 チャネル自動調整情報

23.4.1 nodemanager wlan autochannel channel

[機能]

5GHz 帯のチャネル自動調整の割り当て範囲の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

nodemanager wlan autochannel channel <mode>

[オプション]

<mode>

- w52
  5GHz 無線 LAN W52 で規定されたチャネルの中で割り当てを行います。
- w53
  5GHz 無線 LAN W53 で規定されたチャネルの中で割り当てを行います。
- w56
  5GHz 無線 LAN W56 で規定されたチャネルの中で割り当てを行います。
- w52/53
  5GHz 無線 LAN W52 と W53 で規定されたチャネルの中で割り当てを行います。
- w52/53/56
  5GHz 無線 LAN W52、W53 および W56 で規定されたチャネルの中で割り当てを行います。

[動作モード]

構成定義モード(管理者クラス)

[説明]

チャネル自動調整で、5GHz 帯のチャネルの割り当て範囲を設定します。

[未設定時]

5GHz 帯のチャネル自動調整の割り当て範囲は、w52/53/56 が設定されたものとみなされます。

```
nodemanager wlan autochannel channel w52/53/56
```

23.4.2 nodemanager wlan autochannel layout

[機能]

2.4GHz 帯のチャネル自動調整のレイアウトの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

nodemanager wlan autochannel layout <ch_number> <interval>

[オプション]

<ch_number>

・ 2.4GHz 帯の開始チャネル
1～5 の 10 進数で指定します。

<interval>

・ 2.4GHz 帯のチャネル割り当て間隔
3～5 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]

「管理機器のチャネル自動調整」で、2.4GHz 帯のチャネルを割り当てるときのチャネルのレイアウトを設定します。
チャネルレイアウトは、以下の式で求めることができます。

```
<ch_number>, <ch_number> + (1 * <interval>), ..., <ch_number> + (n * <interval>)
```

[未設定時]

2.4GHz 帯の開始チャネルに 1、2.4GHz 帯のチャネル割り当て間隔に 5 が設定されたものとみなされます。

```
nodemanager wlan autochannel layout 1 5
```

23.4.3 nodemanager wlan autochannel rssi

[機能]

2.4GHz 帯のチャネル自動調整の判定用 RSSI しきい値の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

nodemanager wlan autochannel rssi <rssi>

[オプション]

<rssi>

・ 2.4GHz 帯のチャネル自動調整の判定用 RSSI のしきい値

2.4GHz 帯のチャネル自動調整で、使用済みのチャネルを割り当てる場合の RSSI のしきい値を 1～128 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]

チャネル自動調整の判定用 RSSI のしきい値は、2.4GHz 帯で使用済みチャネルを設定する必要が発生した場合の、設定対象である無線 LAN アクセスポイントでの同チャネルの RSSI のしきい値を指定します。

使用済みチャネルを設定する場合、この RSSI のしきい値以下であるチャネルを設定するようにします。

RSSI と信号強度 (dBm) 関係は、以下のとおりです。

dBm = (RSSI 値) - 95

[未設定時]

チャネル自動調整の判定用 RSSI のしきい値は 20 が設定されたものとみなされます。

```
nodemanager wlan autochannel rssi 20
```

23.4.4 nodemanager wlan autochannel bandwidth

[機能]

チャネル自動調整時の通信帯域幅の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

nodemanager wlan autochannel bandwidth <width>

[オプション]

<width>

- 20
  無線 LAN の通信帯域幅を 20MHz に設定します。
- 40
  無線 LAN の通信帯域幅を 40MHz に設定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

40MHz が指定され、管理アクセスポイントが IEEE802.11n で通信可能な場合、チャネルボンディング機能を使用したチャネル調整を行います。

ただし、管理アクセスポイントの周辺のチャネルの利用状況によっては、チャネルボンディング機能を使用できないことがあります。その場合は、20MHz の帯域幅でチャネルの自動割り当てを行います。

[未設定時]

通信帯域幅として 20 が設定されたものとみなされます。

```
nodemanager wlan autochannel bandwidth 20
```

23.5 アクセスポイント情報取得情報

23.5.1 nodemanager collect interval

[機能]

アクセスポイント情報取得の時間パラメタの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

nodemanager collect interval <period> <wait_period> <time_out>

[オプション]

<period>

・情報取得間隔
管理機器から情報取得の間隔を 1～600 秒の範囲の 10 進数で指定します。
単位は、m(分)、s(秒) のどちらかを指定します。

<wait_period>

・情報取得待機間隔
管理機器からの情報取得の待機時間を 1～600 秒の範囲の 10 進数で指定します。
単位は、m(分)、s(秒) のどちらかを指定します。

<time_out>

・情報取得タイムアウト時間
管理機器からの情報取得タイムアウト時間を 1～60 秒の範囲の 10 進数で指定します。
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]

無線 LAN 管理機能が管理機器や無線 LAN 端末の情報取得を行う際の時間パラメタを設定します。

情報取得間隔は、ある管理機器の情報を取得してから次の管理機器の情報を取得するまでの間隔です。

情報取得待機間隔は、すべての情報取得対象の管理機器の情報を取得したあと、次の情報取得を開始するまでの待ち時間です。

情報取得タイムアウト時間は、管理機器との通信時のタイムアウト時間です。タイムアウトが発生したら次の管理機器の情報取得を行います。

情報取得間隔は、10 秒を設定することを推奨します。

情報取得待機間隔は、10 秒を設定することを推奨します。

情報取得タイムアウト時間は、5 秒を設定することを推奨します。

[注意]

情報取得間隔が短いほどリアルタイムに近い情報を得ることができますが、本装置とネットワークの負荷は増大します。システム、ネットワークのパフォーマンスに応じて適切な値を設定してください。

[未設定時]

情報取得間隔、情報取得待機間隔、情報取得タイムアウト時間を設定しないものとみなされ、アクセスポイント情報の取得を行いません。

23.6 管理外無線 LAN アクセスポイント情報

23.6.1 nodemanager wlan scan unmanaged

[機能]

管理外無線 LAN アクセスポイントの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

nodemanager wlan scan unmanaged <number> <name> <mac>

[オプション]

<number>

・ 管理外無線 LAN アクセスポイント定義番号
管理外無線 LAN アクセスポイントの通し番号を 10 進数で指定します。

<name>

・ 管理外無線 LAN アクセスポイント名
管理外無線 LAN アクセスポイント名を、0x21,0x23～0x7e の 8 文字以内の ASCII 文字列で指定します。

<mac>

・ MAC アドレス
管理外無線 LAN アクセスポイントの 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]

指定した MAC アドレスを有する無線 LAN アクセスポイントを、管理外無線 LAN アクセスポイントとして指定した名前で設定します。

無線 LAN 監視が検出した無線 LAN アクセスポイントの MAC アドレスが、管理外無線 LAN アクセスポイントとして設定した MAC アドレスと一致する場合は、検出された無線 LAN アクセスポイントは不明無線 LAN アクセスポイントとみなされません。

使用している場所、目的などが明らかで監視する必要がない無線 LAN アクセスポイントを管理外無線 LAN アクセスポイントとして設定します。

すでに管理外無線 LAN アクセスポイントに設定されている無線 LAN アクセスポイントと同じ MAC アドレスを指定した場合、このコマンドの設定は無効になります。

[注意]

管理無線 LAN アクセスポイントの稼動情報を取得した結果、いったん管理外無線 LAN アクセスポイントとして設定された MAC アドレスが、あとから管理無線 LAN アクセスポイントの MAC アドレスと重複していることが判明する場合があります。この場合、MAC アドレスが重複した管理外無線 LAN アクセスポイントの情報は、システムによって自動的に削除されます。

[未設定時]

管理外無線 LAN アクセスポイントがないものとみなされます。

23.7 稼動監視パラメタ情報

23.7.1 nodemanager icmpwatch interval

[機能]

稼動監視パラメタの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

nodemanager icmpwatch interval <period> <wait_period> <time_out>

[オプション]

<period>

・稼動監視間隔
管理対象の管理機器に ping を送信する間隔時間を 1～600 秒の範囲の 10 進数で指定します。
単位は、m(分)、s(秒) のどちらかを指定します。

<wait_period>

・稼動監視待機間隔
管理対象の管理機器への ping 送信の待機時間を 1～600 秒の範囲の 10 進数で指定します。
単位は、m(分)、s(秒) のどちらかを指定します。

<time_out>

・稼動監視タイムアウト時間
管理対象の管理機器からの ping 応答待ちタイムアウト時間を 1～60 秒の範囲の 10 進数で指定します。
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]

無線 LAN 管理機能が、ping を使って有線 LAN 経由で管理機器の稼動状況を監視する際の待ち時間を設定します。稼動監視間隔は、ある管理機器に ping を送信し応答を得たあと、次の管理機器に ping を送信するまでの間隔です。

稼動監視待機間隔は、すべての監視対象の管理機器に ping を送信したあと、次の ping 送信を開始するまでの待ち時間です。

稼動監視タイムアウト時間は、管理機器からの ping 応答待ち許容時間です。管理機器からの ping 応答がなく稼動監視応答待ちタイムアウトとなった場合は、次の管理機器へ ping を送信します。

稼動監視間隔は、10 秒を設定することを推奨します。

稼動監視待機間隔は、10 秒を設定することを推奨します。

稼動監視応答待ちタイムアウト時間は、5 秒を設定することを推奨します。

[注意]

稼動監視間隔が短いほどリアルタイムに近い情報を得ることができますが、本装置とネットワークの負荷は増大します。システム、ネットワークのパフォーマンスに応じて適切な値を設定してください。

[未設定時]

稼動監視間隔、稼動監視待機間隔、稼動監視応答待ちタイムアウト時間を設定しないものとみなされ、稼動監視を行いません。

23.7.2 nodemanager icmpwatch threshold

[機能]

稼動監視 通信異常判定しきい値の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

nodemanager icmpwatch threshold <count>

[オプション]

<count>

・ 通信異常判定しきい値
稼動監視が通信異常の疑いありとみなすしきい値を 1～11 の範囲の 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]

稼動監視は、管理機器に ping を送り、その応答によって管理機器との通信状態を確認します。
管理機器との通信が確認できない回数が通信異常判定しきい値に達した場合は、「active? (通信異常の疑い)」のステータスになります。通信が確認できない回数が通信異常判定しきい値を超えると「inactive(通信異常)」のステータスになります。

[未設定時]

通信異常判定しきい値は 6 が設定されたものとみなされます。

```
nodemanager icmpwatch threshold 6
```

23.8 スキャンレポート取得パラメタ情報

23.8.1 nodemanager wlan scan interval

[機能]

スキャンレポート取得パラメタの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

nodemanager wlan scan interval <period> <wait_period> <time_out>

[オプション]

<period>

・スキャンレポート取得間隔

監視用無線 LAN アクセスポイントからスキャンレポートを取得する間隔時間を 1～600 秒の範囲の 10 進数で指定します。

単位は、m(分)、s(秒) のどちらかを指定します。

<wait_period>

・スキャンレポート取得待機間隔

監視用無線 LAN アクセスポイントからのスキャンレポート取得の待機時間を 1～600 秒の範囲の 10 進数で指定します。

単位は、m(分)、s(秒) のどちらかを指定します。

<time_out>

・スキャンレポート取得タイムアウト時間

監視用無線 LAN アクセスポイントからスキャンレポート受信待ちタイムアウト時間を 1～60 秒の範囲の 10 進数で指定します。

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]

無線 LAN 管理機能が、スキャン要求設定コマンド(nodemanager node <number> wlan scan)によって設定した監視用無線 LAN アクセスポイントからスキャンレポートを取得する際の待ち時間を設定します。スキャンレポート取得間隔は、ある監視用無線 LAN アクセスポイントのスキャンレポートを取得してから次の監視用無線 LAN アクセスポイントのスキャンレポートを取得するまでの間隔です。

スキャンレポート取得待機間隔は、すべての監視用無線 LAN アクセスポイントからスキャンレポートを取得したあと、次のスキャンレポート取得を開始するまでの待ち時間です。

スキャンレポート取得タイムアウト時間は、監視用無線 LAN アクセスポイントからのスキャンレポート受信待ち許容時間です。監視用無線 LAN アクセスポイントからのスキャンレポート受信がなくスキャンレポート受信待ちタイムアウトとなった場合は、次の監視用無線 LAN アクセスポイントからスキャンレポート取得を行います。

スキャンレポート取得間隔は、10 秒を設定することを推奨します。

スキャンレポート取得待機間隔は、10 秒を設定することを推奨します。

スキャンレポート受信待ちタイムアウト時間は、60 秒を設定することを推奨します。

[注意]

スキャンレポート取得間隔が短いほどリアルタイムに近い情報を得ることができますが、本装置とネットワークの負荷は増大します。システム、ネットワークのパフォーマンスに応じて適切な値を設定してください。

[未設定時]

スキャンレポート取得間隔、スキャンレポート取得待機間隔、スキャンレポート受信待ちタイムアウト時間を設定しないものとみなされ、スキャンレポートの取得を行いません。

23.8.2 nodemanager wlan scan error threshold

[機能]

無線 LAN 監視 通信異常判定しきい値の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

nodemanager wlan scan error threshold <count>

[オプション]

<count>

・ 通信異常判定しきい値
無線 LAN 監視が通信異常の疑いありとみなすしきい値を 1～11 の範囲の 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]

無線 LAN 監視は、監視用無線 LAN アクセスポイントにより無線 LAN アクセスポイントを検出することによって通信状態を確認します。無線 LAN アクセスポイントの未検出が通信異常判定しきい値に達した場合は、「active? (通信異常の疑い)」のステータスになります。連続未検出が通信異常判定しきい値を超えると「inactive (通信異常)」のステータスになります。

[未設定時]

通信異常判定しきい値に 6 が設定されたものとみなされます。

```
nodemanager wlan scan error threshold 6
```

23.9 監視ログ・パラメタ情報

23.9.1 nodemanager log

[機能]

監視ログのパラメタの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

nodemanager log <lines>

[オプション]

<lines>

・ 監視ログ保持件数
監視ログの最大件数を 100～10000 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]

監視ログ保持件数は保持する監視ログの最大件数を設定します。

[未設定時]

監視ログ保持件数に 1000 を設定したものとみなされます。

```
nodemanager log 1000
```

23.9.2 nodemanager wlan sta rssi

[機能]

無線 LAN 端末の RSSI 監視のパラメタの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

nodemanager wlan sta rssi <param> <low_rssi>

[オプション]

<param>

・ RSSI 評価母数
RSSI 評価値を求めるのに必要な RSSI データ数を 1～50 の範囲の 10 進数で指定します。

<low_rssi>

・ RSSI 最低しきい値
RSSI 低下通知の契機となる RSSI の最低しきい値を 1～255 の範囲の 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]

無線 LAN 端末は端末の状態の変化によって RSSI が短期間に増減したり、アソシエーションが突然解除されることが想定されます。そのため RSSI 監視は電波品質の評価のために複数の RSSI データから評価値を求めます。RSSI 評価母数には、評価値を求める際の RSSI のデータ数を設定します。

RSSI と信号強度（dBm）関係は、以下のとおりです。

dBm = (RSSI 値) - 95

得られた RSSI 評価値が、RSSI 最低しきい値を下回るとき、電波品質の低下を通知するメッセージが監視ログに出力されます。

[注意]

無線 LAN 端末の RSSI 監視は、無線 LAN 端末の情報を取得する管理機器に対してのみ実行することができます。

[未設定時]

RSSI 評価母数に 10、RSSI 最低しきい値に 20 が設定されたものとみなされます。

```
nodemanager wlan sta rssi 10 20
```

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-R570 Si-R570B Si-R370 Si-R370B

[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-R570 Si-R570B Si-R370 Si-R370B

[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-R570 Si-R570B Si-R370 Si-R370B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。
- compatible
  旧バージョン互換 MIB モードで、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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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 address

[機能]

SNMP エージェントアドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

snmp agent address <address>

[オプション]

<address>

・エージェントアドレス
本装置のエージェントアドレスを設定します。
0.0.0.0 を指定した場合は、SNMP エージェントアドレスを削除します。
指定可能な範囲は以下のとおりです。

1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNMP エージェントのアドレスを設定します。本設定は TRAP 送信時の自局アドレスにも使用されます。SNMP エージェント機能を使用する場合は必ず設定してください。

[未設定時]

エージェントアドレスを設定しないものとみなされます。その場合、TRAP パケットの自局 IP アドレスは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 engineid

[機能]

SNMP エンジン ID の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

25.1.7 snmp manager

[機能]

SNMP ホスト情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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/トラップ送信アドレス
アクセス許可およびトラップを送信するあて先 IP アドレスを、XXX.XXX.XXX.XXX(XXX は 3 桁の 10 進数)の形式で指定します。
0.0.0.0 を指定すると、すべてのホストからのアクセスを許可し、trap 送信は行いません。
指定可能な範囲は以下のとおりです。

1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

<community>

コミュニティ名を指定します。

・ コミュニティ名
トラップを送信するときのコミュニティ名を、1～32 文字で指定します。

・ public
任意の SNMP マネージャと通信する場合に指定します。

<trap>

トラップ送信するかどうかを指定します。

・ 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。

25.1.8 snmp trap coldstart

[機能]

coldStart トラップの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.1.9 snmp trap linkdown

[機能]

linkDown トラップの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.1.10 snmp trap linkup

[機能]

linkUp トラップの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.1.11 snmp trap authfail

[機能]

authenticationFailure トラップの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.1.12 snmp trap newroot

[機能]

newRoot トラップの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

snmp trap newroot <mode>

[オプション]

<mode>

トラップの動作を指定します。

- enable
  トラップを有効にします。
- disable
  トラップを無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

newRoot トラップを有効または無効にするかを設定します。

[未設定時]

newRoot トラップが有効とみなされます。

```
snmp trap newroot enable
```

25.1.13 snmp trap topologychange

[機能]

topologyChange トラップの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

snmp trap topologychange <mode>

[オプション]

<mode>

トラップの動作を指定します。

- enable
  トラップを有効にします。
- disable
  トラップを無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

topologyChange トラップを有効または無効にするかを設定します。

[未設定時]

topologyChange トラップが有効とみなされます。

```
snmp trap topologychange enable
```

25.1.14 snmp trap vrrpnewmaster

[機能]

vrrpTrapNewMaster トラップの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.1.15 snmp trap vrrpauthfail

[機能]

vrrpTrapAuthFailure トラップの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.1.16 snmp trap vrrpprotoerror

[機能]

vrrpTrapProtoError トラップの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.1.17 snmp trap noserror

[機能]

nosError トラップの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.1.18 snmp trap lldpremtableschange

[機能]

lldpRemTablesChange トラップの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

snmp trap lldpremtableschange <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]

lldpRemTablesChange 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]

lldpRemTablesChange トラップが有効とみなされます。

```
snmp trap lldpremtableschange enable
```

25.1.19 snmp user name

[機能]

SNMP ユーザ名の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

25.1.20 snmp user address

[機能]

SNMP ホストアドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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>

・SNMP ホストアドレス
SNMPv3 アクセスを許可するホストの IP アドレスを、XXX.XXX.XXX.XXX(XXX は最大 3 桁の 10 進数)の形式で指定します。
指定可能な範囲は以下のとおりです。

1.0.0.1 〜 126.255.255.254
128.0.0.1 〜 191.255.255.254
192.0.0.1 〜 223.255.255.254

[動作モード]

構成定義モード(管理者クラス)

[説明]

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。

25.1.21 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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>

・トラップ通知ホストアドレス
トラップを通知するホストの IP アドレスを、XXX.XXX.XXX.XXX(XXX は最大 3 桁の 10 進数)の形式で指定します。
指定可能な範囲は以下のとおりです。

1.0.0.1 〜 126.255.255.254
128.0.0.1 〜 191.255.255.254
192.0.0.1 〜 223.255.255.254

[動作モード]

構成定義モード(管理者クラス)

[説明]

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。

25.1.22 snmp user auth

[機能]

認証プロトコルの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.1.23 snmp user priv

[機能]

暗号プロトコルの設定

[入力形式]

snmp user [<number>] priv <protocol> [<password> [encrypted]]

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.1.24 snmp user write

[機能]

MIB 書き込み許可ビューの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.1.25 snmp user read

[機能]

MIB 読み出し許可ビューの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.1.26 snmp user notify

[機能]

トラップ通知許可ビューの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.1.27 snmp view subtree

[機能]

SNMP MIB ビュー情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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	
	dot1dBridge	1.3.6.1.2.1.17	
	snmpDot3RptrMgt	1.3.6.1.2.1.22	Si-R180B

サブツリー名		オブジェクト ID	備考
	rip2	1.3.6.1.2.1.23	
	ifMIB	1.3.6.1.2.1.31	
	atmMIB	1.3.6.1.2.1.37	Si-R260B Si-R370 Si-R570
	radiusMIB	1.3.6.1.2.1.67	
	vrrpMIB	1.3.6.1.2.1.68	
	enterprises	1.3.6.1.4.1	
	lldpMIB	1.0.8802.1.1.2	
トラップ名	coldstart	1.3.6.1.6.3.1.1.5.1	
	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	
	newroot	1.3.6.1.2.1.17.0.1	
	topologychange	1.3.6.1.2.1.17.0.2	
	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	
	lldpremtableschange	1.0.8802.1.1.2.0.0.1	

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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>

・IP 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

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

syslog security <securetype>

[オプション]

<securetype>

・セキュリティ対象
セキュリティログ情報の出力対象を、以下の中から指定します。
複数指定する場合は、","(カンマ)で区切ります。

ipfilter
IP filter モジュールを対象とする場合に指定します。

nat
NAT モジュールを対象とする場合に指定します。

ids
IDS モジュールを対象とする場合に指定します。

ppp
PPP モジュールを対象とする場合に指定します。

dhcp
DHCP モジュールを対象とする場合に指定します。

proxydns
ProxyDNS モジュールを対象とする場合に指定します。

macauth
MAC アドレス認証モジュールを対象とする場合に指定します。

dot1x
IEEE802.1X 認証モジュールを対象とする場合に指定します。

arpauth
ARP 認証モジュールを対象とする場合に指定します。

none
すべてのモジュールを対象外とする場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

システムログ情報を出力する対象となるセキュリティを指定します。

[未設定時]

すべてを指定したものとみなされます。

```
syslog security ipfilter,nat,ids,ppp,dhcp,proxydns,macauth,dot1x,arpauth
```

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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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 event dot1x

[機能]

システムログ情報の IEEE802.1X 認証出力対象イベントの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

syslog event dot1x <type>

[オプション]

<type>

・対象イベント
システムログ情報の出力対象とするイベントを、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。

- success
  認証成功メッセージを対象とする場合に指定します。
- continue
  再認証による認証成功メッセージを対象とする場合に指定します。
- fail
  認証失敗メッセージを対象とする場合に指定します。
- logout
  認証解除メッセージを対象とする場合に指定します。
- none
  すべてのメッセージ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イベントを指定します。
出力対象とするイベントに該当するメッセージを以下に示します。

対象イベント	対象メッセージ
success	Supplicant is accepted on ether ..
continue	Supplicant is accepted on ether ..
fail	Supplicant is denied on ether ..
logout	Supplicant is logged-off on ether ..

[未設定時]

success,continue,fail,logout が指定されたものとみなされます。

```
syslog event dot1x success,continue,fail,logout
```

25.2.9 syslog event arpauth

[機能]

システムログ情報の ARP 認証出力対象イベントの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

syslog event arpauth <type>

[オプション]

<type>

・対象イベント
システムログ情報の出力対象とするイベントを、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。

- success
  認証成功メッセージを対象とする場合に指定します。
- fail
  認証失敗メッセージを対象とする場合に指定します。
- none
  すべてのメッセージ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イベントを指定します。
出力対象とするイベントに該当するメッセージを以下に示します。

対象イベント	対象メッセージ
success	ARP authentication accepted ..
fail	ARP authentication illegal MAC address detected ..

[未設定時]

success,fail が指定されたものとみなされます。

```
syslog event arpauth success,fail
```

25.2.10 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.2.11 syslog source address

[機能]

システムログ情報の送信元 IP アドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

syslog source address <address>

[オプション]

<address>

・ IP アドレス
送信メッセージの送信元 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]

送信メッセージの送信元 IP アドレスを設定します。

[未設定時]

送信メッセージの送信元 IP アドレスを指定しないものとみなされます。

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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

time auto interval <time>

[オプション]

<time>

時刻情報を設定する間隔を指定します。

- start
  電源投入時またはリセット時に一度だけ、時刻情報を設定する場合に指定します。
- 間隔
  時刻情報を設定する間隔を、0 秒～最大 10 日の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

自動時刻を設定する間隔を設定します。

[未設定時]

時刻提供サーバを使用する場合だけ、電源投入時またはリセット時に一度だけ時刻情報設定するものとみなされます。

```
time auto interval start
```

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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

proxydns domain <count> <qtype> <qname> <address>/<mask> reject
(転送要求の破棄)
proxydns domain <count> <qtype> <qname> <address>/<mask> static <ipaddress>
(固定 DNS サーバ指定)
proxydns domain <count> <qtype> <qname> <address>/<mask> to <remote_number>
(相手ネットワークの DNS サーバ指定)
proxydns domain <count> <qtype> <qname> <address>/<mask> on <remote_number> [<route>]
(相手ネットワーク指定)
proxydns domain <count> <qtype> <qname> <address>/<mask> dhcp <interface>
(DHCP 指定)

[オプション]

<count>

・ 転送先定義番号
転送先定義番号として、0～31 の 10 進数を指定します。
指定した値は、設定完了時に順方向にソートされてリナンバリングされます。
また、指定した定義番号と同じ値を持つ転送先定義番号が存在する場合は、既存定義の前に挿入されます。

<qtype>

・ 問い合わせタイプ番号
1～11、または 13～65535 の 10 進数を指定します。
以下に、問い合わせタイプの一部分を示します。

名称	番号	説明
A	1	ホスト・アドレス
NS	2	ドメインに対して認証されたネーム・サーバ
CNAME	5	別名(Alias 名、ドメイン名)
SOA	6	ゾーン管理開始
PTR	12	ドメイン名空間のほかの部分へのポインタ
HINFO	13	ホストが使用する CPU と OS
MX	15	ドメインに対するメール交換
SRV	33	サービス

・ any
PTR(12)を除くすべてのタイプを対象にする場合に指定します。

<qname>

・ ホスト名
条件となるホスト名を、80 文字以内で指定します。
ホスト名には、以下のワイルドカードを使用できます。
- *(アスタリスク)
  0 文字以上の任意の文字列とみなされます。
- ?(クェスチョンマーク)

任意の一文字とみなされます。

以下に、ワイルドカードを使用したホスト名の記述例および一致例を示します。

www.*.com

以下のどの文字列とも一致するとみなされます。

・www.testa.com
・www.test1.test.com

test

以下のどの文字列とも一致するとみなされます。

・www.test.com
・test.com
・test.co.jp

www.test?.com

以下のどの文字列とも一致するとみなされます。

・www.test1.com
・www.test2.com
・www.testA.com

なお、ホスト名をチェックするときに、大文字と小文字の区別はされません。

<address>/<mask>

対象となる送信元 IPv4 アドレス/マスクビット数または送信元 IPv6 アドレス/プレフィックス長を指定します。

・ 送信元 IPv4 アドレス/マスクビット数(またはマスク値)
  対象となる送信元 IPv4 アドレスとマスクビット数の組み合わせを指定します。
  マスク値は、最上位ビットから 1 で連続した値にしてください。
・ 送信元 IPv6 アドレス/プレフィックス長
  対象となる送信元 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
・ any
  すべてのアドレスを対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0)または 0:0:0:0:0:0:0:0/0 を指定するのと同じ意味になります。

<ipaddress>

・ DNS サーバ IP アドレス
  要求を転送する DNS サーバの IPv4 アドレスまたは IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  IPv4:

  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  IPv6:

  ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<remote_number>

・ 転送先相手定義番号
  相手ネットワークの通し番号を、10 進数で指定します。

範囲	機種
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～49	Si-R180B

<route>

DNS 問い合わせにより経路を設定するかどうかを設定します。

・ on
経路を設定します。
・ off
経路を設定しません。
省略時は、off を指定したものとみなされます。

<interface>

DHCP クライアントが動作しているインタフェースを以下の範囲で指定します。

範囲	機種
lan0～lan19 rmt0～rmt999	Si-R570 Si-R570B
lan0～lan19 rmt0～rmt499	Si-R370 Si-R370B
lan0～lan19 rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
lan0～lan9 rmt0～rmt49	Si-R180B

[動作モード]

構成定義モード(管理者クラス)

[説明]

プロキシ DNS の順引き動作条件を設定します。
各コマンドについて説明します。

転送要求の破棄

proxydns domain <count> <qtype> <qname> <address>/<mask> reject
指定した DNS 要求の転送を無効にするフィルタを設定します。
<qname>で指定するホスト名は、DNS データベースに登録されていても、そのホスト(群)へのアクセスを制限する場合に使用します。条件と一致した場合は破棄されます。

固定 DNS サーバの指定

proxydns domain <count> <qtype> <qname> <address>/<mask> static <ipaddress>
指定した DNS 要求の転送先 IP アドレスを指定します。
以下の場合に有効です。
・ 専用線に接続する場合
・ LAN 側に DNS サーバが存在する場合
・ リモート側の DNS サーバを固定にする場合

相手ネットワークの DNS サーバ指定

proxydns domain <count> <qtype> <qname> <address>/<mask> to <remote_number>
回線から通知された DNS サーバを使用します。
相手情報でマルチルーティングを定義している場合は、その設定に従います。回線切断中は、接続先情報の接続優先順位に従います。

相手ネットワークの指定

proxydns domain <count> <qtype> <qname> <address>/<mask> on <remote_number> [<route>]
回線から通知された DNS サーバへ指定のネットワークを使用して DNS 要求を転送します。
回線切断中は、接続先情報の接続優先順位に従います。
<route>に on を指定すると DNS 要求を転送した相手ネットワークへの経路を動的に設定します。

DHCP 指定

proxydns domain <count> <qtype> <qname> <address>/<mask> dhcp <interface>指定のインタフェースで動作している DHCP クライアントが取得した DNS サーバへ DNS 要求を転送します。

[未設定時]

プロキシ DNS の順引き動作条件を設定しないものとみなされます。

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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

proxydns address <count> <address>/<mask> reject
(転送要求の破棄)
proxydns address <count> <address>/<mask> static <ipaddress>
(固定 DNS サーバ指定)
proxydns address <count> <address>/<mask> to <remote_number>
(相手ネットワークの DNS サーバ指定)
proxydns address <count> <address>/<mask> on <remote_number> [<route>]
(相手ネットワーク指定)
proxydns address <count> <address>/<mask> dhcp <interface>
(DHCP 指定)

[オプション]

<count>

・転送先定義番号
転送先定義番号として、0～31 の 10 進数を指定します。
指定した値は、設定完了時に順方向にソートされてリナンバリングされます。
また、指定した定義番号と同じ値を持つ転送先定義番号が存在する場合は、既存定義の前に挿入されます。

<address>/<mask>

逆引き対象 IPv4 アドレス/マスクビット数または IPv6 アドレス/プレフィックス長を指定します。

・逆引き対象 IPv4 アドレス/マスクビット数(またはマスク値)
逆引き対象 IPv4 アドレスとマスクビット数の組み合わせを指定します。
マスク値は、最上位ビットから 1 で連続した値にしてください。

・逆引き対象 IPv6 アドレス/プレフィックス長
逆引き対象 IPv6 アドレスとプレフィックス長の組み合わせを指定します。

・any4
IPv4 アドレスの逆引きのすべてを対象とする場合に指定します。

・any6
IPv6 アドレスの逆引きのすべてを対象とする場合に指定します。

・any
すべてのアドレスの逆引きを対象とする場合に指定します。

<ipaddress>

・DNS サーバ IP アドレス
要求を転送する DNS サーバの IPv4 アドレスまたは IPv6 アドレスを指定します。
指定可能な範囲は以下のとおりです。

IPv4:

1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

IPv6:

::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<remote_number>

・ 転送先相手定義番号
相手ネットワークの通し番号を、10 進数で指定します。

範囲	機種
0～999	Si-R570 Si-R570B
0～499	Si-R370 Si-R370B
0～99	Si-R260B Si-R240B Si-R220C Si-R220D
0～49	Si-R180B

<route>

DNS 問い合わせにより経路を設定するかどうかを設定します。

・ on
経路を設定します。

・ off
経路を設定しません。

省略時は、off を指定したものとみなされます。

<interface>

DHCP クライアントが動作しているインタフェースを以下の範囲で指定します。

範囲	機種
lan0～lan19 rmt0～rmt999	Si-R570 Si-R570B
lan0～lan19 rmt0～rmt499	Si-R370 Si-R370B
lan0～lan19 rmt0～rmt99	Si-R260B Si-R240B Si-R220C Si-R220D
lan0～lan9 rmt0～rmt49	Si-R180B

[動作モード]

構成定義モード(管理者クラス)

[説明]

プロキシ DNS の逆引き動作条件を設定します。
各コマンドについて説明します。

転送要求の破棄

proxydns address <count> <address>/<mask> reject
指定した DNS 要求の転送を無効にするフィルタを設定します。
<qname>で指定するホスト名は、DNS データベースに登録されていても、そのホスト(群)へのアクセスを制限する場合に使用します。条件と一致した場合は破棄されます。

固定 DNS サーバの指定

proxydns address <count> <address>/<mask> static <ipaddress>
指定した DNS 要求の転送先 IP アドレスを指定します。
転送先への経路は、IP ルーティングに従って決められます。
以下の場合に有効です。

・ 専用線に接続する場合
・ LAN 側に DNS サーバが存在する場合
・ リモート側の DNS サーバを固定にする場合

相手ネットワークの DNS サーバ指定

proxydns address <count> <address>/<mask> to <remote_number>

回線から通知された DNS サーバを使用します。

相手情報でマルチルーティングを定義している場合は、その設定に従います。回線切断中は、接続先情報の接続優先順位に従います。

相手ネットワークの指定

proxydns address <count> <address>/<mask> on <remote_number> [<route>]

回線から通知された DNS サーバへ指定のネットワークを使用して DNS 要求を転送します。

回線切断中は、接続先情報の接続優先順位に従います。

<route>に on を指定すると DNS 要求を転送した相手ネットワークへの経路を動的に設定します。

DHCP 指定

proxydns address <count> <address>/<mask> dhcp <interface>指定のインタフェースで動作している DHCP クライアントが取得した DNS サーバへ DNS 要求を転送します。

[未設定時]

プロキシ DNS の逆引き動作条件を設定しないものとみなされます。

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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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 multi-server

[機能]

プロキシ DNS の複数サーバ問い合わせの可否の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

proxydns multi-server <mode>

[オプション]

<mode>

複数サーバに問い合わせを転送するかどうかを指定します。

- enable
  複数サーバが利用できる場合は、そのすべてに問い合わせを転送します。
- disable
  複数サーバが利用できる場合でも、プライマリ DNS サーバのみに問い合わせを転送します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

プロキシ DNS による DNS 問い合わせ転送時に、複数 DNS サーバに対し問い合わせを転送するかどうかを設定します。

[注意]

複数サーバ問い合わせを行うことができるのは、以下の条件を満たす場合です。

1) proxydns domain 定義、proxydns address 定義で、「相手ネットワークの DNS サーバ指定」または「相手ネットワーク指定」を行う。かつ、
   2-1) remote ap ip dns 定義で、複数の DNS サーバを定義する。または
   2-2) IPCP によりプライマリ DNS サーバアドレスおよびセカンダリ DNS サーバアドレスの通知を受ける。

[未設定時]

プライマリ DNS サーバのみに問い合わせを転送します。

```
proxydns multi-server disable
```

25.5 ホストデータベース情報

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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。
以下に、各機能とパラメタの関係を示します。

パラメタ 機能	name	ip_address	ip6_address	mac_address	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

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。
以下に、各機能とパラメタの関係を示します。

パラメタ 機能	name	ip_address	ip6_address	mac_address	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

[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 ip6 address

[機能]

ホストデータベース情報の IPv6 アドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

host <number> ip6 address <ip6_address>

[オプション]

<number>

・ 定義番号
ホストデータベース情報の定義番号を、0～63 の 10 進数で指定します。

<ip6_address>

・ IPv6 アドレス
ホストの IPv6 アドレスを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

本装置配下に接続されたホストの IPv6 アドレスをホストデータベースに設定します。
本コマンドは、簡易 DNS サーバ機能、IPv6 DHCP スタティック機能から利用されます。
以下に、各機能とパラメタの関係を示します。

パラメタ 機能	name	ip_address	ip6_address	mac_address	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

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。
以下に、各機能とパラメタの関係を示します。

パラメタ 機能	name	ip_address	ip6_address	mac_address	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

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。
以下に、各機能とパラメタの関係を示します。

パラメタ 機能	name	ip_address	ip6_address	mac_address	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

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。
以下に、各機能とパラメタの関係を示します。

パラメタ 機能	name	ip_address	ip6_address	mac_address	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

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

schedule <number> at <day> <time> <command>

[オプション]

<number>

スケジュール定義を指定します。

・スケジュール定義番号
スケジュール定義番号を、0〜15 の 10 進数で指定します。

・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 isdn account
ISDN 課金情報をクリアする場合に指定します(※Si-R260B Si-R240B Si-R180B では無効です)。

・clear modem account
モデム課金情報をクリアする場合に指定します(※Si-R220C Si-R220D だけ有効です)。

・clear cardmodem account
データ通信カード課金情報をクリアする場合に指定します(※Si-R240B だけ有効です)。

・offline remote
強制切断する場合に指定します(※Si-R260B Si-R180B では無効です)。

・rpon all
リモートパワーオンを実行する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

システムスケジュールを設定します。
このスケジュールに従って、指定した時刻にコマンドを実行します。

[未設定時]

スケジュール情報を設定しないものとみなされます。

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-R570 | Si-R570B | Si-R370 | Si-R370B | | Si-R240B | Si-R220C | Si-R220D |

[入力形式]

schedule <number> in <day> <time> <action>

[オプション]

<number>

スケジュール定義を指定します。

- スケジュール定義番号
  スケジュール定義番号を、0～15 の 10 進数で指定します。
- 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

schedule <number> syslog <syslog>

[オプション]

<number>

スケジュール定義を指定します。

- スケジュール定義番号
  スケジュール定義番号を、0～15 の 10 進数で指定します。
- 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-R240B Si-R220C Si-R220D Si-R180B

[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-R240B Si-R220C Si-R220D Si-R180B

[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、ファーム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-R570 Si-R570B Si-R370 Si-R370B Si-R240B Si-R220C Si-R220D

[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。

[実行例]

以下に、構成定義情報に定義されている電話番号 123456789 を、1999 年 1 月 1 日午前 2 時にすべて 999999999 へ変更する場合の設定例を示します。

```
# dnconvinfo 0 date 9901010200
# dnconvinfo 0 dial 0 123456789 99999999
# show dnconvinfo
0 date 9901010200
0 dial 0 123456789 99999999
#
```

[未設定時]

電話番号変更予約情報を設定しないものとみなされます。

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-R570 | Si-R570B | Si-R370 | Si-R370B | | Si-R240B | Si-R220C | Si-R220D |

[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。

[実行例]

以下に、構成定義情報に定義されている電話番号 123456789 を、1999 年 1 月 1 日午前 2 時にすべて 999999999 へ変更する場合の設定例を示します。

```
# dnconvinfo 0 date 9901010200
# dnconvinfo 0 dial 0 123456789 to 99999999
# show dnconvinfo
0 date 9901010200
0 dial 0 123456789 to 99999999
#
```

[未設定時]

電話番号変更予約情報を設定しないものとみなされます。

25.9 ファームウェア更新情報

25.9.1 updateinfo

[機能]

ファームウェア更新情報の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

updateinfo <host> <user> <password> <pathname>

[オプション]

<host>

更新するファームウェアの転送元ホスト(ftp サーバ)を、以下の形式で指定します。

ホスト名を指定する場合は、ホストデータベース情報に該当するホスト名が登録されているか、または本装置が DNS サーバを使用できる状態でなければなりません。

・ ホスト名

ホスト名を、0x21,0x23～0x7e の 128 文字以内の ASCII 文字列で指定します。

・ IPv4 アドレス

指定可能な範囲は以下のとおりです。

1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

・ IPv6 アドレス

指定可能な範囲は以下のとおりです。

::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

リンクローカルアドレスを指定する場合、アドレスに続けて"%<interface>"を指定して、どのインタフェースを使用するのか指定してください。たとえば、"fe80::1%lan0"のように指定します。

<user>

・ ユーザ名

ftp ユーザ名を、0x21,0x23～0x7e の 16 文字以内の ASCII 文字列で指定します。

<password>

・ パスワード

ftp パスワードを、0x21,0x23～0x7e の 32 文字以内の ASCII 文字列で指定します。

anonymous FTP サーバの場合は、管理者のメールアドレスを指定します。

<pathname>

・ パス名

更新するファームウェアの ftp サーバ上のパス名を、0x21,0x23～0x7e の 80 文字以内の ASCII 文字列で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ファームウェアを更新するための情報を設定します。

update コマンドで ftp サーバ上のファームウェアを取得する場合は、必ず本コマンドを実行してください。

[未設定時]

ファームウェア更新情報を設定しないものとみなされます。

25.10 MAC アドレス認証情報

25.10.1 macauth password

[機能]

MAC アドレス認証情報(パスワード)の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

[未設定時]

MAC アドレス認証情報を認証端末の MAC アドレスを使用するものとみなされます。

25.10.2 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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 PAP が指定されたものとみなされます。

```
macauth type pap
```

25.11 その他

25.11.1 addact

[機能]

コマンド実行予約の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

[実行例]

以下に、1999 年 1 月 1 日 午前 2 時 に構成定義 2 に切り替えて再起動する場合の設定例を示します。

```
# addact 0 9901010200 reset config2
# show addact
0 9901010200 reset config2
#
```

[未設定時]

コマンドの実行予約を行わないものとみなされます。

25.11.2 watchdog service

[機能]

ウォッチドッグリセットの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.11.3 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

consoleinfo autologout <time>

[オプション]

<time>

・強制ログアウト時間

シリアルコンソールでログインしたままコマンド実行が行われない状態が続いたときに強制ログアウトさせる時間を、0秒～86400秒(1日)の範囲で指定します。

単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。

0秒を指定した場合は、強制ログアウトしません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

シリアルコンソールでログインしたまま<time>で指定した時間内にコマンド実行されなかった場合、強制的にログアウトさせるように設定します。

[未設定時]

強制ログアウトさせないものとみなされます。

```
consoleinfo autologout 0s
```

25.11.4 telnetinfo

[機能]

TELNET 接続サービスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

telnetinfo autologout <time>

[オプション]

<time>

・自動切断時間

telnet 接続したクライアントからコマンド入出力が行われない状態で自動切断するまでの時間を、0 秒～86400 秒(1 日)の範囲で指定します。

単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

TELNET コネクションの入出力がない場合にコネクションを切断するまでの時間を設定します。

[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
```

25.11.5 sysdown harderr fan

[機能]

冷却ファン異常時の動作の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R240B

[入力形式]

sysdown harderr fan <mode>

[オプション]

<mode>

- yes
  システムダウンさせる場合に指定します。(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]

冷却ファン異常(複数ある場合はすべての冷却ファン異常)発生時の動作を設定します。

また、Si-R570 Si-R570B では以下のコマンドを使用して、システムダウン時に本装置の電源を切断するかどうかを設定することができます。

- sysdown power <mode>

[未設定時]

冷却ファン異常時に運用を継続するものとみなされます。

```
sysdown harderr fan no
```

25.11.6 sysdown harderr thermal

[機能]

温度異常時の動作の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D

[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。

また、Si-R570 Si-R570B では以下のコマンドを使用して、システムダウン時に本装置の電源を切断するかどうかを設定することができます。

- sysdown power <mode>

[未設定時]

温度異常時に運用を継続するものとみなされます。

```
sysdown harderr thermal no
```

25.11.7 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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、温度異常および電源異常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
```

25.11.8 sysdown power

[機能]

ハードエラー発生によるシステムダウン時の電源制御の設定

[適用機種]

Si-R570 Si-R570B

[入力形式]

sysdown power <mode>

[オプション]

<mode>

ハードエラー発生によりシステムダウンした場合に、本装置の電源を切断するかどうかを指定します。

- off
  本装置の電源を切断します。
- on
  本装置の電源を切断しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

以下のコマンドによりシステムダウンさせる設定にしたハードエラーが発生した場合に、本装置の電源を切断するかどうかを設定します。

- sysdown harderr fan yes
- sysdown harderr thermal yes
- sysdown harderr other yes

電源を切断しない設定の場合、システムダウンさせる設定にしたハードエラーが発生すると、本装置はコンソールポートだけ使用可、その他の通信はすべて不可となります。

[未設定時]

ハードエラー発生によりシステムダウンした場合に、本装置の電源を切断するものとみなされます。

```
sysdown power off
```

25.11.9 mflag

[機能]

CE 保守ログインの可否の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.11.10 sysname

[機能]

本装置の名称の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

sysname <name>

[オプション]

<name>

・名称
本装置の名称を、0x21,0x23～0x7e の 32 文字以内の ASCII 文字列で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

本装置の名称を設定します。

ここで設定した名称は、DHCP クライアント機能で DHCP サーバに対して広報されます。

本コマンドで設定する名称は、SNMP で使用する MIB 変数 sysName としても使用することができます。その場合、snmp agent sysname コマンドで設定している sysName を削除しておくことで本コマンドで設定したホスト名が sysName として使用されます。

本コマンドと snmp agent sysname コマンドとはネットワーク動作として直接の関連性はありませんが、ネットワークの管理上、同じ名称に統一するべきです。

[未設定時]

本装置の名称を設定しないものとみなされます。

25.11.11 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.11.12 loopback ip ospf use

[機能]

OSPF 利用可否の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

loopback ip ospf use <mode> [<area_number>]

[オプション]

<mode>

・ off
OSPF を利用しません。

・ on
OSPF を利用します。

<area_number>

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

範囲	機種
0～9	Si-R570 Si-R570B
0～3	Si-R370 Si-R370B
0～2	Si-R260B Si-R240B Si-R220C Si-R220D
0～1	Si-R180B

[動作モード]

構成定義モード(管理者クラス)

[説明]

loopback インタフェースで OSPF を利用するかどうかと、属するエリアの定義番号を設定します。
<mode>で on を設定した場合でも、127.0.0.1 の IP アドレスは OSPF の対象外となります。
OSPF は、本装置全体で以下の数まで定義できます。

最大定義数	機種
100	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D
50	Si-R180B

[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
```

25.11.13 loopback mpls ldp interface-label

[機能]

PHP の無効化

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

loopback mpls ldp interface-label <mode>

[オプション]

<mode>

- off
  インタフェースの IP アドレスにラベルを割り当てません。
- on
  インタフェースの IP アドレスにラベルを割り当てます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

インタフェースの IP アドレスに対してラベルを割り当てるかどうかを指定します。
割り当てた場合は、インタフェースあての LSP の PHP を無効にすることができます。

[注意]

MPLS トンネル接続機能を使用する場合、自側エンドポイントと IP アドレスが同一のとき、本設定によらず、PHP 機能は無効となります。

[未設定時]

off が選択されたものとして動作します。

```
loopback mpls ldp interface-label off
```

25.11.14 loopback ip6 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

loopback ip6 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。

25.11.15 serverinfo ftp

[機能]

FTP サーバ機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.11.16 serverinfo ftp ip6

[機能]

FTP サーバ機能の IPv6 の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

serverinfo ftp ip6 <mode>

[オプション]

<mode>

- on
  FTP サーバ機能の IPv6 を有効にします。
- off
  FTP サーバ機能の IPv6 を停止します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

FTP サーバ機能の IPv6 を有効にするかどうかを設定します。

[未設定時]

FTP サーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo ftp ip6 on
```

25.11.17 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

<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。

- ip6

送信元 IPv6 アドレスとプレフィックス長のみを使用します。

ip6 値が設定されていない場合、IPv6 に対するフィルタ定義は無効となり、無視されます。

範囲	機種
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

[動作モード]

構成定義モード(管理者クラス)

[説明]

FTP サーバ機能に対するアプリケーションフィルタを設定します。

[未設定時]

FTP サーバ機能に対するアプリケーションフィルタを設定しないものとみなされます。

25.11.18 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

25.11.19 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.11.20 serverinfo sftp

[機能]

SSH FTP サーバ機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.11.21 serverinfo sftp ip6

[機能]

SSH FTP サーバ機能の IPv6 の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

serverinfo sftp ip6 <mode>

[オプション]

<mode>

- on
  SSH FTP サーバ機能の IPv6 を有効にします。
- off
  SSH FTP サーバ機能の IPv6 を停止します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SSH FTP サーバ機能の IPv6 を有効にするかどうかを設定します。

本設定が off、かつ、serverinfo ssh ip6 コマンドの設定が off の場合、sftp クライアントからの IPv6 アドレスでの接続要求は拒否されます。

本設定が off、かつ、serverinfo ssh ip6 コマンドの設定が on の場合、sftp クライアントからの IPv6 アドレスでの接続要求はパスワード入力したあとに拒否されます。

[注意]

本設定を有効にすると、本装置電源投入時および reset コマンド実行時に SSH ホスト認証鍵を生成するようになり、数十秒～数分の処理時間を要します。

SSH ホスト認証鍵の生成が完了したあとに sftp 接続できるようになります。

ssh および sftp 機能をすべて off の状態で本装置を起動して本機能を有効にした場合にも SSH ホスト認証鍵を生成し、数十秒から数分の処理時間を要します。その場合、セッション監視タイムアウトが発生するなど、ほかの処理に影響することが考えられますので、ご注意ください。

[未設定時]

SSH FTP サーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo sftp ip6 on
```

25.11.22 serverinfo telnet

[機能]

TELNET サーバ機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.11.23 serverinfo telnet ip6

[機能]

TELNET サーバ機能の IPv6 の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

serverinfo telnet ip6 <mode>

[オプション]

<mode>

- on
  TELNET サーバ機能を有効にします。
- off
  TELNET サーバ機能を停止します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

TELNET サーバ機能の IPv6 を有効にするかどうかを設定します。

[未設定時]

TELNET サーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo telnet ip6 on
```

25.11.24 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

<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。

- ip6

送信元 IPv6 アドレスとプレフィックス長のみを使用します。

ip6 値が設定されていない場合、IPv6 に対するフィルタ定義は無効となり、無視されます。

範囲	機種
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

[動作モード]

構成定義モード(管理者クラス)

[説明]

TELNET サーバ機能に対するアプリケーションフィルタを設定します。

[未設定時]

TELNET サーバ機能に対するアプリケーションフィルタを設定しないものとみなされます。

25.11.25 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

25.11.26 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.11.27 serverinfo ssh

[機能]

SSH ログインサーバ機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.11.28 serverinfo ssh ip6

[機能]

SSH ログインサーバ機能の IPv6 の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

serverinfo ssh ip6 <mode>

[オプション]

<mode>

- on
  SSH ログインサーバ機能の IPv6 を有効にします。
- off
  SSH ログインサーバ機能の IPv6 を停止します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SSH ログインサーバ機能の IPv6 を有効にするかどうかを設定します。

本設定が off、かつ、serverinfo sftp ip6 コマンドの設定が off の場合、ssh クライアントからの IPv6 アドレスでの接続要求は拒否されます。

本設定が off、かつ、serverinfo sftp ip6 コマンドの設定が on の場合、ssh クライアントからの IPv6 アドレスでの接続要求はパスワード入力したあとに拒否されます。

[注意]

本設定を有効にすると、本装置電源投入時および reset コマンド実行時に SSH ホスト認証鍵を生成するようになり、数十秒～数分の処理時間を要します。

SSH ホスト認証鍵の生成が完了したあとに ssh 接続できるようになります。

ssh および sftp 機能をすべて off の状態で本装置を起動して本機能を有効にした場合にも SSH ホスト認証鍵を生成し、数十秒から数分の処理時間を要します。その場合、セッション監視タイムアウトが発生するなど、ほかの処理に影響することが考えられますので、ご注意ください。

[未設定時]

SSH ログインサーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo ssh ip6 on
```

25.11.29 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

<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。

- ip6

送信元 IPv6 アドレスとプレフィックス長のみを使用します。

ip6 値が設定されていない場合、IPv6 に対するフィルタ定義は無効となり、無視されます。

範囲	機種
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

[動作モード]

構成定義モード(管理者クラス)

[説明]

SSH サーバ機能に対するアプリケーションフィルタを設定します。
本定義は、SSH ログインサーバ機能および SSH FTP サーバ機能の両方に対して有効となります。
SSH ログインサーバ機能、SSH FTP サーバ機能にそれぞれ異なるフィルタ設定をすることはできません。

[未設定時]

SSH サーバ機能に対するアプリケーションフィルタを設定しないものとみなされます。

25.11.30 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

25.11.31 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.11.32 serverinfo http

[機能]

HTTP サーバ機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.11.33 serverinfo http ip6

[機能]

HTTP サーバ機能の IPv6 の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

serverinfo http ip6 <mode>

[オプション]

<mode>

- on
  HTTP サーバ機能を有効にします。
- off
  HTTP サーバ機能を停止します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

HTTP サーバ機能の IPv6 を有効にするかどうかを設定します。

[未設定時]

HTTP サーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo http ip6 on
```

25.11.34 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

<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。

- ip6

送信元 IPv6 アドレスとプレフィックス長のみを使用します。

ip6 値が設定されていない場合、IPv6 に対するフィルタ定義は無効となり、無視されます。

範囲	機種
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

[動作モード]

構成定義モード(管理者クラス)

[説明]

HTTP サーバ機能に対するアプリケーションフィルタを設定します。

[未設定時]

HTTP サーバ機能に対するアプリケーションフィルタを設定しないものとみなされます。

25.11.35 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

25.11.36 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.11.37 serverinfo dns

[機能]

DNS サーバ機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.11.38 serverinfo dns ip6

[機能]

DNS サーバ機能の IPv6 の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

serverinfo dns ip6 <mode>

[オプション]

<mode>

- on
  DNS サーバ機能を有効にします。
- off
  DNS サーバ機能を停止します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

DNS サーバ(スタティック)機能および ProxyDNS 機能の IPv6 を有効にするかどうかを設定します。

[未設定時]

DNS サーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo dns ip6 on
```

25.11.39 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

<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。

- ip6

送信元 IPv6 アドレスとプレフィックス長のみを使用します。

ip6 値が設定されていない場合、IPv6 に対するフィルタ定義は無効となり、無視されます。

範囲	機種
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

[動作モード]

構成定義モード(管理者クラス)

[説明]

DNS サーバ機能に対するアプリケーションフィルタを設定します。

[未設定時]

DNS サーバ機能に対するアプリケーションフィルタを設定しないものとみなされます。

25.11.40 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

25.11.41 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.11.42 serverinfo sntp

[機能]

SNTP サーバ機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.11.43 serverinfo sntp ip6

[機能]

SNTP サーバ機能の IPv6 の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

serverinfo sntp ip6 <mode>

[オプション]

<mode>

- on
  SNTP サーバ機能を有効にします。
- off
  SNTP サーバ機能を停止します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNTP サーバ機能の IPv6 を有効にするかどうかを設定します。

[未設定時]

SNTP サーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo sntp ip6 on
```

25.11.44 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

<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。

- ip6

送信元 IPv6 アドレスとプレフィックス長のみを使用します。

ip6 値が設定されていない場合、IPv6 に対するフィルタ定義は無効となり、無視されます。

範囲	機種
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNTP サーバ機能に対するアプリケーションフィルタを設定します。

[未設定時]

SNTP サーバ機能に対するアプリケーションフィルタを設定しないものとみなされます。

25.11.45 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

25.11.46 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.11.47 serverinfo time ip tcp

[機能]

TCP による TIME サーバ機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.11.48 serverinfo time ip6 tcp

[機能]

TCP による TIME サーバ機能の IPv6 の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

serverinfo time ip6 tcp <mode>

[オプション]

<mode>

- on
  TCP による TIME サーバ機能を有効にします。
- off
  TCP による TIME サーバ機能を停止します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

TCP による TIME サーバ機能の IPv6 を有効にするかどうかを設定します。

[未設定時]

TCP による TIME サーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo time ip6 tcp on
```

25.11.49 serverinfo time ip udp

[機能]

UDP による TIME サーバ機能の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.11.50 serverinfo time ip6 udp

[機能]

UDP による TIME サーバ機能の IPv6 の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

serverinfo time ip6 udp <mode>

[オプション]

<mode>

- on
  UDP による TIME サーバ機能を有効にします。
- off
  UDP による TIME サーバ機能を停止します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

UDP による TIME サーバ機能の IPv6 を有効にするかどうかを設定します。

[未設定時]

UDP による TIME サーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo time ip6 udp on
```

25.11.51 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

<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。

- ip6

送信元 IPv6 アドレスとプレフィックス長のみを使用します。

ip6 値が設定されていない場合、IPv6 に対するフィルタ定義は無効となり、無視されます。

範囲	機種
0～2999	Si-R570 Si-R570B
0～1499	Si-R370 Si-R370B
0～299	Si-R260B Si-R240B Si-R220C Si-R220D
0～149	Si-R180B

[動作モード]

構成定義モード(管理者クラス)

[説明]

TIME サーバ機能に対するアプリケーションフィルタを設定します。

[未設定時]

TIME サーバ機能に対するアプリケーションフィルタを設定しないものとみなされます。

25.11.52 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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。

25.11.53 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-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
```

25.12 シェーピング情報

25.12.1 shaping timer

[機能]

シェーピング機能の定期送出タイマ利用可否の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

shaping timer <mode>

[オプション]

<mode>

- disable
  定期送出タイマを利用しません。
- enable
  定期送出タイマを利用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

シェーピング機能の定期送出タイマ利用可否を設定します。
定期送出タイマを利用すると、パケット受信をトリガにする送出の判断に加えて、定期送信タイマによりパケットを送出しますので、シェーピングの精度を向上させることができます。

[注意]

定期送出タイマを利用するとシェーピングの精度は向上しますが、装置の負荷が高まります。

[未設定時]

定期送出タイマを利用しないものとみなされます。

```
shaping timer disable
```

第 26 章 SIP-SIP ゲートウェイ情報

26.1 SIP-SIP ゲートウェイ情報

26.1.1 sipgw use

[機能]

SIP-SIP ゲートウェイ機能利用可否の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

sipgw 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]

SIP-SIP ゲートウェイ機能を利用するかどうかを設定します。

[未設定時]

SIP-SIP ゲートウェイ機能を利用しないものとみなされます。

```
sipgw use off
```

26.2 サービス関連情報

26.2.1 sipgw service type

[機能]

サービス種別の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

sipgw <number> service type <type>

[オプション]

<number>

- 0
  内線側サービスに対する設定を行います。
- 1
  外線側サービスに対する設定を行います。

<type>

- off
  使用しません
- fj (内線側のみ)
  IP Pathfinder および CL シリーズ
- ntt-b (外線側のみ)
  ひかり電話ビジネスタイプ

[動作モード]

構成定義モード(管理者クラス)

[説明]

SIP-SIP ゲートウェイ機能でのサービス種別を設定します。
SIP-SIP ゲートウェイ機能を使用する場合は、本コマンドを必ず実行してください。

[未設定時]

SIP-SIP ゲートウェイ機能でのサービス種別を設定しないものとみなされます。

```
sipgw 0 service type off
sipgw 1 service type off
```

26.2.2 sipgw service user name

[機能]

ユーザ名の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

sipgw <number> service user <count> name <username>

[オプション]

<number>

・0
内線側サービスに対する設定を行います。

・1
外線側サービスに対する設定を行います。

<count>

・ユーザ定義番号
ユーザの定義番号を、10 進数で指定します。

範囲	機種
0	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

<username>

・ユーザ名
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。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ゲートウェイのユーザ名を設定します。
ひかり電話ビジネスタイプの場合、IP 電話番号(0AJ 番号)が相当します。
SIP-SIP ゲートウェイ機能を使用する場合は、本コマンドを必ず実行してください。

[未設定時]

ユーザ名を設定しないものとみなされます。

26.2.3 sipgw service user auth id

[機能]

認証ユーザ名の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

sipgw <number> service user <count> auth id <id>

[オプション]

<number>

・ 0
内線側サービスに対する設定を行います。

・ 1
外線側サービスに対する設定を行います。

<count>

・ ユーザ定義番号
ユーザの定義番号を、10 進数で指定します。

範囲	機種
0	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

<id>

・ 認証ユーザ名
認証ユーザ名を、0x21,0x23～0x7e の 32 文字以内の ASCII 文字列で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ユーザの認証ユーザ名を設定します。

[未設定時]

ユーザの認証ユーザ名を設定しないものとみなされます。

26.2.4 sipgw service user auth password

[機能]

認証パスワードの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

sipgw <number> service user <count> auth password <password> [encrypted]

[オプション]

<number>

・0
内線側サービスに対する設定を行います。

・1
外線側サービスに対する設定を行います。

<count>

・ユーザ定義番号
ユーザの定義番号を、10 進数で指定します。

範囲	機種
0	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

<password>

・認証パスワード
認証パスワードを、0x21,0x23～0x7e の 32 文字以内の ASCII 文字列で指定します。

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]

ユーザの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]

ユーザの認証パスワードを設定しないものとみなされます。

26.2.5 sipgw service callin username

[機能]

着信転送先ユーザ名の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

sipgw <number> service callin username <username>

[オプション]

<number>

- 0
  内線側サービスに対する設定を行います。
- 1
  外線側サービスに対する設定を行います。

<username>

- 転送先ユーザ名
  転送先のユーザ名を、0x21,0x23～0x7e の 32 文字以内の ASCII 文字列で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

外線からの着信を内線側サービスに転送する際、あて先ユーザ名を書き換えて転送します。
外線側サービスに対する設定は無視されます。

[未設定時]

外線からの着信を内線側サービスに転送する際、あて先ユーザ名の書き換えを行いません。

26.3 Registrar 連携関連情報

26.3.1 sipgw registrar server address

[機能]

Registrar サーバアドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

sipgw <number> registrar server <count> address <address>

[オプション]

<number>

・0
内線側サービスに対する設定を行います。

・1
外線側サービスに対する設定を行います。

<count>

・定義番号
Registrar サーバ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	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

<address>

・Registrar サーバアドレス
Registrar サーバの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]

SIP-SIP ゲートウェイ機能での Registrar サーバを設定します。

[未設定時]

SIP-SIP ゲートウェイ機能での Registrar サーバを設定しないものとみなされます。Registrar サーバへの登録は行われません。

26.3.2 sipgw registrar server port

[機能]

Registrar サーバポート番号の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

sipgw <number> registrar server <count> port <port>

[オプション]

<number>

- 0
  内線側サービスに対する設定を行います。
- 1
  外線側サービスに対する設定を行います。

<count>

- 定義番号
  Registrar サーバ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	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

<port>

- Registrar サーバポート番号
  Registrar サーバのポート番号を、1～65535 の 10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

Registrar サーバのポート番号を設定します。

[未設定時]

Registrar サーバのポート番号に標準ポート番号である 5060 を指定したものとみなされます。

```
sipgw <number> registrar server <count> port 5060
```

26.4 Proxy 連携関連情報

26.4.1 sipgw proxy server address

[機能]

Proxy サーバアドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

sipgw <number> proxy server <count> address <address>

[オプション]

<number>

・ 0
内線側サービスに対する設定を行います。

・ 1
外線側サービスに対する設定を行います。

<count>

・ 定義番号
Proxy サーバ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
0～2	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

<address>

・ Proxy サーバアドレス
Proxy サーバの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]

Proxy サーバを設定します。
SIP-SIP ゲートウェイ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]

Proxy サーバを設定しないものとみなされます。

26.4.2 sipgw proxy server port

[機能]

Proxy サーバポート番号の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

sipgw <number> proxy server <count> port <port>

[オプション]

<number>

- 0
  内線側サービスに対する設定を行います。
- 1
  外線側サービスに対する設定を行います。

<count>

- 定義番号
  Proxy サーバ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
0～2	Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

<port>

- Proxy サーバポート番号
  Proxy サーバのポート番号を、1～65535 の 10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

Proxy サーバのポート番号を設定します。

[未設定時]

Proxy サーバのポート番号に標準ポート番号である 5060 を指定したものとみなされます。

```
sipgw <number> proxy server <count> port 5060
```

26.5 ユーザエージェント関連情報

26.5.1 sipgw agent address

[機能]

自 IP アドレスの設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

sipgw <number> agent address <address>

[オプション]

<number>

・ 0
内線側サービスに対する設定を行います。

・ 1
外線側サービスに対する設定を行います。

<address>

・ 自 IP アドレス
自 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]

ユーザエージェントの IP アドレスを設定します。
SIP-SIP ゲートウェイ機能を使用する場合は、本コマンドを必ず実行してください。

[未設定時]

ユーザエージェントの IP アドレスを設定しないものとみなされます。

26.5.2 sipgw agent domain name

[機能]

サービスドメイン名の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[入力形式]

sipgw <number> agent domain name <domain>

[オプション]

<number>

・0
内線側サービスに対する設定を行います。

・1
外線側サービスに対する設定を行います。

<domain>

・サービスドメイン名
サービスドメイン名を、0x21,0x23～0x7e の 90 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]

サービスドメイン名を設定します。
SIP-SIP ゲートウェイ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]

サービスドメイン名を設定しないものとみなされます。

第 27 章 証明書関連情報の設定

27.1 証明書関連情報

27.1.1 certificate local name

[機能]

自装置証明書識別名の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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 までの 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。

27.1.2 certificate local line

[機能]

自装置証明書の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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 までの 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。

27.1.3 certificate remote name

[機能]

相手装置証明書識別名の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～499	Si-R570 Si-R570B
0～249	Si-R370 Si-R370B
0～49	Si-R260B Si-R240B Si-R220C Si-R220D
0～24	Si-R180B

<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。

27.1.4 certificate remote line

[機能]

相手装置証明書の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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
0～499	Si-R570 Si-R570B
0～249	Si-R370 Si-R370B
0～49	Si-R260B Si-R240B Si-R220C Si-R220D
0～24	Si-R180B

<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。

27.1.5 certificate ca name

[機能]

認証局証明書識別名の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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 までの 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。

27.1.6 certificate ca line

[機能]

認証局証明書の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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 までの 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。

27.1.7 certificate request line

[機能]

証明書要求の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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 までの 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。

27.1.8 certificate private line

[機能]

秘密鍵の設定

[適用機種]

Si-R570 Si-R570B Si-R370 Si-R370B Si-R260B Si-R240B Si-R220C Si-R220D Si-R180B

[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 までの 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。

索引

A

aaa name.....1049
aaa radius accounting source.....1075
aaa radius auth message-authenticator.....1074
aaa radius auth source.....1073
aaa radius client nas-identifier.....1091
aaa radius client retry.....1090
aaa radius client server-info accounting address.....1085
aaa radius client server-info accounting deadtime.....1087
aaa radius client server-info accounting port.....1086
aaa radius client server-info accounting priority.....1088
aaa radius client server-info accounting secret 1084
aaa radius client server-info accounting source 1089
aaa radius client server-info auth address.....1079
aaa radius client server-info auth deadtime....1081
aaa radius client server-info auth port.....1080
aaa radius client server-info auth priority....1082
aaa radius client server-info auth secret.....1078
aaa radius client server-info auth source.....1083
aaa radius server client-info address.....1077
aaa radius server client-info secret.....1076
aaa radius service.....1071
aaa user called number.....1053
aaa user id.....1050
aaa user ike shared key.....1066
aaa user ip address local.....1054
aaa user ip address remote.....1055
aaa user ip route.....1056
aaa user ip6 ifid.....1058
aaa user ip6 route.....1059
aaa user ipsec extension-range.....1064
aaa user ipsec ike range.....1062
aaa user password.....1051
aaa user sessionwatch.....1061
aaa user supplicant mac.....1069
aaa user supplicant vid.....1068
aaa user user-role.....1070
acl description.....1033
acl icmp.....1031
acl ip.....1024
acl ip6.....1026
acl mac.....1022
acl tcp.....1028
acl udp.....1030
addact.....1198
answer accept.....686
answer ppp auth receive add.....688
answer ppp auth type.....687
answer ppp mp bap use.....690
answer ppp mp use.....689
atm send clock.....63

B

bgp as.....875
bgp id.....876
bgp ip aggregate.....882
bgp ip full-route.....879
bgp ip mpls-resolution.....878
bgp ip network igp.....881
bgp ip network route.....880
bgp ip redist.....883
bgp ip redist move.....885
bgp ip vrf rd.....877
bgp ip6 aggregate.....888
bgp ip6 network igp.....887
bgp ip6 network route.....886
bgp ip6 redist.....889
bgp ip6 redist move.....891
bgp neighbor address.....892
bgp neighbor as.....894
bgp neighbor authentication.....900
bgp neighbor ebgp-multihop.....896
bgp neighbor enforce-multihop.....897
bgp neighbor family.....898
bgp neighbor graceful-restart family.....901
bgp neighbor graceful-restart stale-timer.....902
bgp neighbor ip asprepend.....904
bgp neighbor ip default-originate.....907
bgp neighbor ip filter act.....908
bgp neighbor ip filter as.....911
bgp neighbor ip filter move.....910
bgp neighbor ip filter route.....913
bgp neighbor ip filter set asprepend.....917
bgp neighbor ip filter set localpref.....919
bgp neighbor ip filter set medmetric.....915
bgp neighbor ip localpref.....905
bgp neighbor ip medmetric.....903
bgp neighbor ip nexthopself.....906
bgp neighbor ip6 asprepend.....922
bgp neighbor ip6 default-originate.....925
bgp neighbor ip6 filter act.....926
bgp neighbor ip6 filter as.....929
bgp neighbor ip6 filter move.....928
bgp neighbor ip6 filter route.....930
bgp neighbor ip6 filter set asprepend.....934
bgp neighbor ip6 filter set localpref.....936
bgp neighbor ip6 filter set medmetric.....932
bgp neighbor ip6 localpref.....923
bgp neighbor ip6 medmetric.....921
bgp neighbor ip6 nexthopself.....924
bgp neighbor source.....899
bgp neighbor timers.....895
bridge age.....978
bridge control.....989
bridge inter-remote.....988
bridge ip policy.....984
bridge ip routing.....983
bridge ip6 policy.....986
bridge ip6 routing.....985
bridge stp age.....980
bridge stp delay.....982
bridge stp hello.....981
bridge stp priority.....979
bridge vlan tag transmit.....987

C

certificate ca line.....1279

certificate ca name.....1278
certificate local line.....1275
certificate local name.....1274
certificate private line.....1281
certificate remote line.....1277
certificate remote name.....1276
certificate request line.....1280
consoleinfo.....1201

D

dnconvinfo date.....1190
dnconvinfo dial.....1192
dot1x mode.....997
dot1x use.....996
dvpn client domain.....831
dvpn client encode.....823
dvpn client expire register.....827
dvpn client expire session.....828
dvpn client global.....836
dvpn client interface.....835
dvpn client ip route distance.....838
dvpn client ip6 route distance.....839
dvpn client localid.....834
dvpn client localnet.....832
dvpn client priority.....837
dvpn client server address.....824
dvpn client server auth.....826
dvpn client ua.....829
dvpn server auth aaa.....822
dvpn server auth use.....821
dvpn server domain.....820
dvpn server use.....819

H

host duid.....1181
host ip address.....1178
host ip6 address.....1179
host mac.....1180
host name.....1177
host rpon.....1182

I

ip nat table.....817

L

lan arpauth aaa.....331
lan arpauth authenticated-ip.....337
lan arpauth dummymac.....333
lan arpauth expire.....334
lan arpauth obstruction.....332
lan arpauth overflow.....335
lan arpauth type.....336
lan arpauth use.....330
lan backup bind.....112
lan backup mode.....113
lan bind.....101
lan bridge filter.....275
lan bridge filter move.....278
lan bridge group.....269
lan bridge priority.....279
lan bridge static.....270
lan bridge stp cost.....272
lan bridge stp priority.....274
lan bridge stp use.....271
lan bridge use.....268
lan dot1x aaa.....345
lan dot1x maxreq.....343
lan dot1x mode.....346
lan dot1x portcontrol.....339
lan dot1x quietperiod.....340
lan dot1x reauthperiod.....344
lan dot1x supptimeout.....342
lan dot1x txperiod.....341
lan dot1x use.....338
lan dot1x wol.....347
lan flowctl.....106
lan ip address.....116
lan ip alias.....118
lan ip arp cycle.....192
lan ip arp static.....193
lan ip dhcp info.....121
lan ip dhcp macauth aaa.....126
lan ip dhcp macauth db.....125
lan ip dhcp macauth type.....127
lan ip dhcp macauth use.....124
lan ip dhcp service.....120
lan ip filter.....169
lan ip filter default.....175
lan ip filter move.....174
lan ip icmp redirect.....187
lan ip ids use.....194
lan ip in-policy.....184
lan ip in-policy move.....186
lan ip localproxyarp.....129
lan ip multicast mode.....188
lan ip multicast pim preference.....190
lan ip multicast pim upstream type.....191
lan ip multicast ttl threshold.....189
lan ip nat appli.....167
lan ip nat destination.....165
lan ip nat mode.....156
lan ip nat rule.....161
lan ip nat static.....158
lan ip nat static default.....160
lan ip nat wellknown.....163
lan ip ospf auth md5key.....151
lan ip ospf auth textkey.....150
lan ip ospf auth type.....149
lan ip ospf cost.....143
lan ip ospf dead.....145
lan ip ospf delay.....147
lan ip ospf hello.....144
lan ip ospf passive.....152
lan ip ospf priority.....148
lan ip ospf retrans.....146
lan ip ospf use.....141
lan ip priority.....180
lan ip proxyarp.....128
lan ip rip filter act.....135
lan ip rip filter move.....137
lan ip rip filter route.....138
lan ip rip filter set metric.....140
lan ip rip use.....133
lan ip route.....130
lan ip tos.....176

lan ip tos move.....179
lan ip vrf route.....154
lan ip vrf use.....153
lan ip6 address.....197
lan ip6 dhcp client iaid.....253
lan ip6 dhcp client option dns.....248
lan ip6 dhcp client option domain.....249
lan ip6 dhcp client option pd.....247
lan ip6 dhcp client option sipserver address....250
lan ip6 dhcp client option sipserver domain.....251
lan ip6 dhcp client option sntpserver.....252
lan ip6 dhcp client route.....254
lan ip6 dhcp duid.....246
lan ip6 dhcp relay interface.....255
lan ip6 dhcp relay server.....256
lan ip6 dhcp relay source.....257
lan ip6 dhcp server info address.....259
lan ip6 dhcp server info dns.....261
lan ip6 dhcp server info domain.....262
lan ip6 dhcp server info prefix.....263
lan ip6 dhcp server info sipserver address.....265
lan ip6 dhcp server info sipserver domain.....266
lan ip6 dhcp server info sntpserver.....267
lan ip6 dhcp server preference.....258
lan ip6 dhcp service.....245
lan ip6 filter.....227
lan ip6 filter default.....233
lan ip6 filter move.....232
lan ip6 ifid.....196
lan ip6 in-policy.....242
lan ip6 in-policy move.....244
lan ip6 ospf cost.....220
lan ip6 ospf dead.....222
lan ip6 ospf delay.....224
lan ip6 ospf hello.....221
lan ip6 ospf passive.....226
lan ip6 ospf priority.....225
lan ip6 ospf retrans.....223
lan ip6 ospf use.....218
lan ip6 priority.....238
lan ip6 ra curhoplimit.....204
lan ip6 ra flags.....205
lan ip6 ra interval.....200
lan ip6 ra mode.....199
lan ip6 ra mtu.....201
lan ip6 ra reachabletime.....202
lan ip6 ra retranstimer.....203
lan ip6 rip aggregate.....211
lan ip6 rip filter act.....212
lan ip6 rip filter move.....214
lan ip6 rip filter route.....215
lan ip6 rip filter set metric.....217
lan ip6 rip site-local.....210
lan ip6 rip use.....208
lan ip6 route.....206
lan ip6 trafficclass.....234
lan ip6 trafficclass move.....237
lan ip6 use.....195
lan lldp info.....325
lan lldp mode.....324
lan lldp notification.....329
lan lldp vlan.....328
lan macauth aaa.....320
lan macauth expire.....319
lan macauth security.....321
lan macauth use.....318
lan mdi.....105
lan mode.....103
lan mpls distribution.....302
lan mpls l2-circuit exp.....311
lan mpls l2-circuit vc.....309
lan mpls ldp advertisement.....305
lan mpls ldp hello-timers.....303
lan mpls ldp interface-label.....307
lan mpls ldp ip transport.....308
lan mpls ldp keepalive-timers.....304
lan mpls ldp retention.....306
lan mpls use.....301
lan mtu.....108
lan recovery.....114
lan shaping.....109
lan shaping-opt tc.....111
lan snmp trap linkdown.....322
lan snmp trap linkup.....323
lan type.....107
lan vlan bind.....312
lan vlan tag pri.....315
lan vlan tag primap.....316
lan vlan tag vid.....314
lan vrrp auth.....282
lan vrrp group action.....294
lan vrrp group ad.....285
lan vrrp group id.....283
lan vrrp group preempt.....286
lan vrrp group trigger ifdown.....287
lan vrrp group trigger node.....291
lan vrrp group trigger route.....289
lan vrrp group vaddr etherip.....299
lan vrrp group vaddr icmp.....298
lan vrrp trap.....300
lan vrrp use.....281
lldp notification interval.....994
lldp reinit delay.....993
lldp send hold.....992
lldp send interval.....991
loopback ip address.....1209
loopback ip ospf use.....1210
loopback ip6 address.....1212
loopback mpls ldp interface-label.....1211

M

macauth password.....1196
macauth type.....1197
mflag.....1207
mpls ip propagate-ttl.....1002
mpls ldp control.....1000
mpls ldp ip transport.....1001
mpls ldp router-id.....999
multicast ip igmp report.....1004
multicast ip pimsm candbsr address.....1009
multicast ip pimsm candbsr mode.....1008
multicast ip pimsm candbsr priority.....1010
multicast ip pimsm candrp address.....1006
multicast ip pimsm candrp mode.....1005
multicast ip pimsm candrp priority.....1007
multicast ip pimsm register checksum.....1014
multicast ip pimsm spt mode.....1012

multicast ip pimsm spt rate.....1013
multicast ip pimsm staticrp address.....1011
multicast ip route static.....1015

N

nodemanager collect interval.....1109
nodemanager group name.....1093
nodemanager icmpwatch interval.....1111
nodemanager icmpwatch threshold.....1112
nodemanager log.....1116
nodemanager node address.....1096
nodemanager node group.....1095
nodemanager node name.....1094
nodemanager node user.....1097
nodemanager node wlan neighbor.....1100
nodemanager node wlan scan.....1098
nodemanager node wlan sta.....1099
nodemanager wlan autochannel bandwidth.....1108
nodemanager wlan autochannel channel.....1105
nodemanager wlan autochannel layout.....1106
nodemanager wlan autochannel rssi.....1107
nodemanager wlan autotxpower rssi.....1104
nodemanager wlan filterset description.....1101
nodemanager wlan filterset filter description. .1103
nodemanager wlan filterset filter mac.....1102
nodemanager wlan scan error threshold.....1115
nodemanager wlan scan interval.....1113
nodemanager wlan scan unmanaged.....1110
nodemanager wlan sta rssi.....1117

O

ospf ip area defcost.....942
ospf ip area id.....940
ospf ip area range.....943
ospf ip area type.....941
ospf ip area type3-lsa.....945
ospf ip area type3-lsa move.....947
ospf ip area vlink auth md5key.....964
ospf ip area vlink auth textkey.....962
ospf ip area vlink auth type.....961
ospf ip area vlink dead.....958
ospf ip area vlink delay.....960
ospf ip area vlink hello.....957
ospf ip area vlink id.....956
ospf ip area vlink retrans.....959
ospf ip definfo.....966
ospf ip id.....938
ospf ip redist.....969
ospf ip redist move.....971
ospf ip summary.....968
ospf ip6 area defcost.....950
ospf ip6 area id.....948
ospf ip6 area inter-area-prefix.....953
ospf ip6 area inter-area-prefix move.....955
ospf ip6 area range.....951
ospf ip6 area type.....949
ospf ip6 definfo.....972
ospf ip6 id.....939
ospf ip6 redist.....974
ospf ip6 redist move.....976

P

password aaa.....36
password admin aaa.....32
password admin set.....30
password authtype.....37
password format.....28
password user aaa.....35
password user set.....33
policy-group interface.....1038
policy-group nexthop.....1039
policy-group nexthop6.....1040
policy-group pattern.....1035
policy-group pattern move.....1037
policy-group sessionwatch address.....1041
policy-group sessionwatch error-wait.....1047
policy-group sessionwatch interval.....1043
policy-group sessionwatch recovery.....1046
policy-group sessionwatch ttl.....1045
proxydns address.....1171
proxydns address move.....1174
proxydns domain.....1166
proxydns domain move.....1170
proxydns multi-server.....1176
proxydns unicode.....1175

R

remote ap atm ast.....404
remote ap atm oam.....406
remote ap atm rate.....403
remote ap atm vci.....401
remote ap atm vcwatch.....407
remote ap called accept.....390
remote ap called clid.....391
remote ap called number.....392
remote ap connect priority.....393
remote ap datalink bind.....366
remote ap datalink bundle.....368
remote ap datalink type.....364
remote ap dial number.....387
remote ap dial speed.....388
remote ap disconnect packet.....379
remote ap disconnect time.....378
remote ap dvpn client.....474
remote ap dvpn remoteid.....477
remote ap dvpn remotenet.....475
remote ap fr cir.....400
remote ap fr dlci.....399
remote ap idle.....394
remote ap ike bind.....458
remote ap ike certificate expired.....465
remote ap ike certificate key.....464
remote ap ike certificate local.....463
remote ap ike certificate remote.....462
remote ap ike certificate request.....467
remote ap ike certificate send.....466
remote ap ike dpd idle.....472
remote ap ike dpd retry.....473
remote ap ike dpd use.....471
remote ap ike idtype.....449
remote ap ike initial.....453
remote ap ike local-idtype.....468
remote ap ike mode.....456
remote ap ike name local.....450

remote ap ike name remote.....451
remote ap ike nat-traversal use.....460
remote ap ike port.....438
remote ap ike proposal auth-method.....442
remote ap ike proposal encrypt.....443
remote ap ike proposal hash.....444
remote ap ike proposal lifetime.....446
remote ap ike proposal move.....441
remote ap ike proposal pfs.....445
remote ap ike proposal prf.....447
remote ap ike release.....452
remote ap ike remote-id-send.....470
remote ap ike remote-idtype.....469
remote ap ike retry.....448
remote ap ike sessionwatch.....454
remote ap ike shared key.....439
remote ap ip dns.....370
remote ap ipsec extension-range.....436
remote ap ipsec ike auth.....428
remote ap ipsec ike encrypt.....427
remote ap ipsec ike esn.....435
remote ap ipsec ike lifebyte.....431
remote ap ipsec ike lifetime.....430
remote ap ipsec ike newsa initiator.....432
remote ap ipsec ike newsa responder.....433
remote ap ipsec ike pfs.....429
remote ap ipsec ike protocol.....426
remote ap ipsec ike range.....434
remote ap ipsec receive auth.....424
remote ap ipsec receive encrypt.....422
remote ap ipsec receive protocol.....420
remote ap ipsec receive range.....421
remote ap ipsec receive spi.....419
remote ap ipsec send auth.....417
remote ap ipsec send encrypt.....415
remote ap ipsec send protocol.....412
remote ap ipsec send range.....414
remote ap ipsec send spi.....411
remote ap ipsec type.....409
remote ap keep.....398
remote ap limit charge.....376
remote ap limit time.....377
remote ap move.....363
remote ap mpls nexthop.....495
remote ap mpls to.....493
remote ap multiroute pattern.....372
remote ap multiroute pattern move.....375
remote ap name.....362
remote ap overlap nexthop.....483
remote ap overlap nexthop6.....484
remote ap overlap to.....481
remote ap ppp auth receive.....382
remote ap ppp auth send.....381
remote ap ppp auth type.....380
remote ap ppp mp bap use.....384
remote ap ppp mp use.....383
remote ap pppoe acname.....385
remote ap pppoe svname.....386
remote ap recovery.....369
remote ap sessionwatch address.....485
remote ap sessionwatch error-wait.....492
remote ap sessionwatch interval.....487
remote ap sessionwatch mode.....490
remote ap sessionwatch recovery.....491
remote ap sessionwatch ttl.....489
remote ap snmp trap linkdown.....496
remote ap snmp trap linkup.....497
remote ap step.....395
remote ap step2.....396
remote ap step3.....397
remote ap tunnel local.....478
remote ap tunnel remote.....480
remote autodial.....357
remote bridge filter.....668
remote bridge filter move.....671
remote bridge group.....662
remote bridge priority.....672
remote bridge static.....663
remote bridge stp cost.....665
remote bridge stp priority.....667
remote bridge stp use.....664
remote bridge use.....661
remote ip address local.....509
remote ip address remote.....510
remote ip clp.....562
remote ip clp move.....565
remote ip dvpn.....574
remote ip dvpn move.....576
remote ip exp.....577
remote ip exp move.....580
remote ip filter.....547
remote ip filter default.....553
remote ip filter move.....552
remote ip ids use.....581
remote ip in-policy.....566
remote ip in-policy move.....568
remote ip msschange.....569
remote ip multicast mode.....570
remote ip multicast pim preference.....572
remote ip multicast pim upstream type.....573
remote ip multicast ttl threshold.....571
remote ip nat appli.....545
remote ip nat destination.....543
remote ip nat mode.....534
remote ip nat rule.....539
remote ip nat static.....536
remote ip nat static default.....538
remote ip nat wellknown.....541
remote ip ospf auth md5key.....530
remote ip ospf auth textkey.....529
remote ip ospf auth type.....528
remote ip ospf checkmtu.....533
remote ip ospf cost.....523
remote ip ospf dead.....525
remote ip ospf delay.....527
remote ip ospf hello.....524
remote ip ospf multicast.....532
remote ip ospf passive.....531
remote ip ospf retrans.....526
remote ip ospf use.....521
remote ip priority.....558
remote ip rip filter act.....515
remote ip rip filter move.....517
remote ip rip filter route.....518
remote ip rip filter set metric.....520
remote ip rip use.....513
remote ip route.....511
remote ip tos.....554

remote ip tos move.....557
remote ip6 address.....584
remote ip6 clp.....658
remote ip6 clp move.....660
remote ip6 dhcp client iaid.....639
remote ip6 dhcp client option dns.....634
remote ip6 dhcp client option domain.....635
remote ip6 dhcp client option pd.....633
remote ip6 dhcp client option sipserver address. 636
remote ip6 dhcp client option sipserver domain. .637
remote ip6 dhcp client option sntpserver.....638
remote ip6 dhcp client route.....640
remote ip6 dhcp duid.....632
remote ip6 dhcp relay interface.....641
remote ip6 dhcp relay server.....642
remote ip6 dhcp relay source.....643
remote ip6 dhcp server info dns.....645
remote ip6 dhcp server info domain.....646
remote ip6 dhcp server info prefix.....647
remote ip6 dhcp server info sipserver address...649
remote ip6 dhcp server info sipserver domain....650
remote ip6 dhcp server info sntpserver.....651
remote ip6 dhcp server preference.....644
remote ip6 dhcp service.....631
remote ip6 dvpn.....652
remote ip6 dvpn move.....654
remote ip6 exp.....655
remote ip6 exp move.....657
remote ip6 filter.....613
remote ip6 filter default.....619
remote ip6 filter move.....618
remote ip6 ifid.....583
remote ip6 in-policy.....628
remote ip6 in-policy move.....630
remote ip6 ospf checkmtu.....612
remote ip6 ospf cost.....606
remote ip6 ospf dead.....608
remote ip6 ospf delay.....610
remote ip6 ospf hello.....607
remote ip6 ospf passive.....611
remote ip6 ospf retrans.....609
remote ip6 ospf use.....604
remote ip6 priority.....624
remote ip6 ra curhoplimit.....591
remote ip6 ra flags.....592
remote ip6 ra interval.....587
remote ip6 ra mode.....586
remote ip6 ra mtu.....588
remote ip6 ra reachabletime.....589
remote ip6 ra retranstimer.....590
remote ip6 rip aggregate.....598
remote ip6 rip filter act.....599
remote ip6 rip filter move.....601
remote ip6 rip filter route.....602
remote ip6 rip filter set metric.....603
remote ip6 rip site-local.....597
remote ip6 rip use.....595
remote ip6 route.....593
remote ip6 trafficclass.....620
remote ip6 trafficclass move.....623
remote ip6 use.....582
remote mpls distribution.....675
remote mpls ldp advertisement.....678
remote mpls ldp hello-timers.....676
remote mpls ldp interface-label.....680
remote mpls ldp ip transport.....681
remote mpls ldp keepalive-timers.....677
remote mpls ldp multicast-hello.....682
remote mpls ldp retention.....679
remote mpls use.....674
remote mtu.....358
remote name.....356
remote ppp compress.....498
remote ppp ipcp iphc.....507
remote ppp ipcp vjcomp.....506
remote ppp ipv6cp iphc.....508
remote ppp mp divide.....501
remote ppp mp max.....500
remote ppp mp order.....505
remote ppp mp start.....499
remote ppp mp traffic decrease.....504
remote ppp mp traffic increase.....503
remote ppp mp traffic use.....502
remote shaping.....359
remote shaping-opt tc.....361
remote snmp trap linkdown.....683
remote snmp trap linkup.....684
rip ip gwfilter.....868
rip ip gwfilter move.....869
rip ip multipath.....863
rip ip neighbor.....867
rip ip redist.....864
rip ip redist move.....866
rip ip timers basic.....861
rip ip timers jitter.....862
rip ip6 multipath.....871
rip ip6 redist.....872
rip ip6 redist move.....874
rip ip6 timers basic.....870
routemanage interface floating.....852
routemanage ip distance.....841
routemanage ip ecmp mode.....849
routemanage ip ecmp ospf.....850
routemanage ip redist bgp.....845
routemanage ip redist ldp.....851
routemanage ip redist ospf.....847
routemanage ip redist rip.....843
routemanage ip6 distance.....854
routemanage ip6 redist bgp.....858
routemanage ip6 redist ospf.....859
routemanage ip6 redist rip.....856

S

schedule at.....1183
schedule in.....1185
schedule syslog.....1187
serial modem dial.....351
serial modem speaker mode.....353
serial modem speaker volume.....354
serial modem tonedetect.....352
serial speed.....350
serial use.....349
serverinfo dns.....1239
serverinfo dns filter.....1241
serverinfo dns filter default.....1244
serverinfo dns filter move.....1243
serverinfo dns ip6.....1240

serverinfo ftp.....1213
serverinfo ftp filter.....1215
serverinfo ftp filter default.....1218
serverinfo ftp filter move.....1217
serverinfo ftp ip6.....1214
serverinfo http.....1233
serverinfo http filter.....1235
serverinfo http filter default.....1238
serverinfo http filter move.....1237
serverinfo http ip6.....1234
serverinfo sftp.....1219
serverinfo sftp ip6.....1220
serverinfo sntp.....1245
serverinfo sntp filter.....1247
serverinfo sntp filter default.....1250
serverinfo sntp filter move.....1249
serverinfo sntp ip6.....1246
serverinfo ssh.....1227
serverinfo ssh filter.....1229
serverinfo ssh filter default.....1232
serverinfo ssh filter move.....1231
serverinfo ssh ip6.....1228
serverinfo telnet.....1221
serverinfo telnet filter.....1223
serverinfo telnet filter default.....1226
serverinfo telnet filter move.....1225
serverinfo telnet ip6.....1222
serverinfo time filter.....1255
serverinfo time filter default.....1258
serverinfo time filter move.....1257
serverinfo time ip tcp.....1251
serverinfo time ip udp.....1253
serverinfo time ip6 tcp.....1252
serverinfo time ip6 udp.....1254
shaping timer.....1259
sipgw agent address.....1271
sipgw agent domain name.....1272
sipgw proxy server address.....1269
sipgw proxy server port.....1270
sipgw registrar server address.....1267
sipgw registrar server port.....1268
sipgw service callin username.....1266
sipgw service type.....1262
sipgw service user auth id.....1264
sipgw service user auth password.....1265
sipgw service user name.....1263
sipgw use.....1261
snmp agent address.....1127
snmp agent contact.....1124
snmp agent engineid.....1128
snmp agent location.....1126
snmp agent sysname.....1125
snmp manager.....1129
snmp service.....1123
snmp trap authfail.....1134
snmp trap coldstart.....1131
snmp trap linkdown.....1132
snmp trap linkup.....1133
snmp trap lldpremtableschange.....1141
snmp trap newroot.....1135
snmp trap noserror.....1140
snmp trap topologychange.....1136
snmp trap vrrpauthfail.....1138
snmp trap vrrpnewmaster.....1137
snmp trap vrrpprotoerror.....1139
snmp user address.....1143
snmp user auth.....1145
snmp user name.....1142
snmp user notification.....1144
snmp user notify.....1149
snmp user priv.....1146
snmp user read.....1148
snmp user write.....1147
snmp view subtree.....1150
storage setup machine.....1189
storage setup mode.....1188
switch age.....67
switch port duplex.....70
switch port flowctl.....72
switch port mdi.....71
switch port mode.....69
switch port use.....68
switch port vlan tag.....73
switch port vlan untag.....74
switch tag transparent.....66
switch use.....65
sysdown harderr fan.....1203
sysdown harderr other.....1205
sysdown harderr thermal.....1204
sysdown power.....1206
syslog command-logging.....1158
syslog dupcut.....1157
syslog event arpauth.....1160
syslog event dot1x.....1159
syslog facility.....1155
syslog header.....1161
syslog pri.....1154
syslog security.....1156
syslog server address.....1152
syslog server pri.....1153
syslog source address.....1162
sysmemwatch interval.....1121
sysmemwatch mode.....1119
sysmemwatch threshold.....1120
sysname.....1208

T

telnetinfo.....1202
template aaa.....697
template combine use.....700
template datalink bind.....699
template datalink type.....698
template dvpn client.....768
template dvpn domain.....776
template dvpn expire register.....772
template dvpn expire session.....773
template dvpn global.....782
template dvpn interface.....780
template dvpn localid.....779
template dvpn localnet.....777
template dvpn server address.....769
template dvpn server auth.....771
template dvpn ua.....774
template idle.....694
template ike certificate expired.....808
template ike certificate key.....807
template ike certificate local.....806

template ike certificate request.....810
template ike certificate send.....809
template ike dpd idle.....812
template ike dpd retry.....813
template ike dpd use.....811
template ike idtype.....800
template ike mode.....803
template ike name local.....801
template ike nat-traversal use.....804
template ike proposal auth-method.....794
template ike proposal encrypt.....795
template ike proposal hash.....796
template ike proposal lifetime.....798
template ike proposal move.....793
template ike proposal pfs.....797
template ike release.....802
template ike retry.....799
template ike shared key.....791
template interface pool.....695
template ip address remote-pool.....714
template ip dns.....712
template ip filter.....728
template ip filter default.....734
template ip filter move.....733
template ip ids use.....744
template ip in-policy.....745
template ip in-policy move.....747
template ip msschange.....743
template ip nat appli.....726
template ip nat destination.....724
template ip nat mode.....715
template ip nat rule.....720
template ip nat static.....717
template ip nat static default.....719
template ip nat wellknown.....722
template ip priority.....739
template ip tos.....735
template ip tos move.....738
template ip6 filter.....750
template ip6 filter default.....756
template ip6 filter move.....755
template ip6 ifid.....749
template ip6 in-policy.....765
template ip6 in-policy move.....767
template ip6 priority.....761
template ip6 trafficclass.....757
template ip6 trafficclass move.....760
template ip6 use.....748
template ipsec ike auth.....785
template ipsec ike encrypt.....784
template ipsec ike lifebyte.....788
template ipsec ike lifetime.....787
template ipsec ike newsa initiator.....789
template ipsec ike newsa responder.....790
template ipsec ike pfs.....786
template ipsec ike protocol.....783
template mtu.....693
template name.....692
template ppp auth type.....707
template ppp compress.....708
template ppp ipcp iphc.....710
template ppp ipcp vjcomp.....709
template ppp ipv6cp iphc.....711
template sessionwatch address.....703
template sessionwatch interval.....705
template snmp trap linkdown.....814
template snmp trap linkup.....815
template tunnel local.....701
time auto interval.....1164
time auto server.....1163
time zone.....1165

U

updateinfo.....1194
upnp portmapping lease.....1020
upnp use.....1018

W

wan atm oam.....60
wan atm rate.....59
wan atm vpi.....58
wan bind.....39
wan cardmodem pin.....61
wan fr becn.....56
wan fr cllm.....57
wan fr fecn.....55
wan fr lmi.....54
wan hsd flagdetect.....53
wan isdn accept.....50
wan isdn activation.....52
wan isdn autodial.....51
wan isdn global.....43
wan isdn limit charge.....48
wan isdn limit time.....49
wan isdn number.....44
wan isdn numbersend.....46
wan line.....41
watchdog service.....1200
wlan auth.....88
wlan beacon interval.....87
wlan bind.....76
wlan channel.....78
wlan dtim period.....86
wlan filter.....97
wlan filter move.....99
wlan hide.....80
wlan mode.....77
wlan protection mode.....84
wlan rts threshold.....85
wlan ssid.....79
wlan sta limit.....81
wlan txpower.....82
wlan wep key.....90
wlan wep mode.....89
wlan wep send.....92
wlan wpa cipher.....93
wlan wpa countermeasures.....96
wlan wpa psk.....94
wlan wpa rekey.....95

Si-R シリーズ　コマンドリファレンス -構成定義編 -

P3NK-3992-07Z0

発行日　　2019 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。