

Fujitsu Network Si-R Si-R GX500

コマンドリファレンス-構成定義編-
V1

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。

2017年 8月 初 版
2017年 12月 第2版
2018年 3月 第3版
2018年 6月 第4版
2018年 11月 第5版
2021年 12月 第6版
2023年 6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。
Copyright Fujitsu Limited 2017-2023

目次

はじめに	2
本書の構成と使いかた	28
第 1 章 CLI の操作	30
1.1 コマンド操作について	31
1.2 使用可能文字	32
1.3 コマンドプロンプト	35
1.3.1 hostname	35
1.4 コマンドレベル	36
1.4.1 privilege	36
1.4.2 show privilege	37
1.5 コマンドモード	39
1.5.1 configure terminal	44
1.5.2 disable	45
1.5.3 enable	45
1.5.4 exit	46
1.5.5 end	46
1.6 コマンドヘルプ	48
1.6.1 help	48
1.7 コマンドヒストリ	49
1.7.1 show history	49
1.8 コマンドログ	50
1.8.1 show command-log	50
1.9 コマンドエイリアス	51
1.9.1 alias	51
1.9.2 show alias	51
第 2 章 装置の設定	53
2.1 時刻に関する設定	54
2.1.1 clock summer-time	54
2.1.2 clock timezone	55
2.1.3 ntp authenticate	56
2.1.4 ntp authentication-key	56
2.1.5 ntp server	57
2.1.6 ntp source	58
2.1.7 ntp trusted-key	59
2.1.8 sntp poll-interval	59
2.1.9 sntp retry	60
2.1.10 sntp server	61
2.2 パスワードの設定	63
2.2.1 password enable	63
2.2.2 password login	64
2.3 端末の設定	65
2.3.1 line	65
2.3.2 exec-timeout	65
2.3.3 login authentication	66
2.3.4 password	67
2.3.5 prompt timestamp	67

2.4	TELNET サーバの設定	69
2.4.1	telnet-server access-class	69
2.4.2	telnet-server shutdown	69
2.5	SSH サーバの設定	71
2.5.1	ip ssh authentication-retries	71
2.5.2	ip ssh port	71
2.5.3	ip ssh time-out	72
2.5.4	ip scp server enable	73
2.5.5	ip sftp server enable	73
2.5.6	ssh-server access-class	74
2.5.7	ssh-server version	74
2.6	FTP サーバの設定	76
2.6.1	ftp-server access-class	76
2.6.2	ftp-server exec-timeout	76
2.6.3	ftp-server shutdown	77
2.7	NTP サーバの設定	78
2.7.1	ntp-server enable	78
2.8	DNS サーバの設定	79
2.8.1	ip name-server	79
2.8.2	ip name-server source-interface	80
2.8.3	dns-server enable	80
2.8.4	dns-server access-class	81
2.8.5	proxymdns domain	82
2.8.6	proxymdns address	83
2.9	認証／許可の設定	86
2.9.1	aaa authentication enable	86
2.9.2	aaa authentication login	87
2.9.3	aaa authentication login-prompt	88
2.9.4	aaa authentication password-prompt	88
2.9.5	aaa authentication server-fail-message	89
2.9.6	aaa authentication suppress-log	90
2.9.7	aaa authorization commands	91
2.9.8	no aaa authorization config-commands	92
2.9.9	aaa authorization exec	92
2.9.10	user session-limit	93
2.9.11	username	94
2.9.12	authorization	95
2.10	ユーザ認証用 RADIUS サーバの設定	97
2.10.1	radius-server host	97
2.10.2	radius-server retransmit-count	98
2.10.3	radius-server source-interface	98
2.10.4	radius-server timeout	99
2.11	ユーザ認証用 TACACS+ サーバの設定	100
2.11.1	tacacs-server host	100
2.11.2	tacacs-server key	101
2.11.3	tacacs-server source-interface	101
2.11.4	tacacs-server timeout	102
2.12	TACACS+ アカウンティングの設定	104
2.12.1	aaa accounting commands	104
2.12.2	aaa accounting connection	105
2.12.3	aaa accounting exec	105
2.12.4	aaa accounting send stop-record authentication failure	107
2.12.5	aaa accounting suppress null-username	107

2.12.6	aaa accounting system default	108
2.12.7	ip finger	109
2.12.8	accounting	109
2.13	バナー表示の設定	111
2.13.1	banner motd enable	111
2.13.2	banner motd text	111
2.14	設定情報の設定	113
2.14.1	auto config save enable	113
2.14.2	config comment	113
2.15	ファームウェアの設定	115
2.15.1	update firmware	115
2.15.2	updateinfo	115
2.16	装置情報の設定	117
2.16.1	notify-nhid-usage	117
2.16.2	periodic-log	118

第3章 インタフェースの設定..... 119

3.1	802.1Q TPID 設定	120
3.1.1	dot1q tunnel tpid	120
3.2	インタフェースの省電力設定	121
3.2.1	eee	121
3.3	インタフェース設定モード	122
3.3.1	interface gigabitEthernet	122
3.3.2	interface management	123
3.3.3	interface loopback	123
3.3.4	interface port-channel	124
3.3.5	interface tunnel	124
3.3.6	interface trunk-channel	125
3.3.7	interface usb-ethernet	126
3.4	MAC アドレス学習設定	127
3.4.1	mac-address-table aging-time	127
3.4.2	mac-address-table total-max-entry	128
3.4.3	mac-address-table static	129
3.5	bridge 設定	130
3.5.1	bridge-group	130
3.6	インタフェース関連設定	132
3.6.1	channel-group	132
3.7	インタフェース description 設定	134
3.7.1	description	134
3.8	fragment パケット中継設定	135
3.8.1	ip fragment-cache disable	135
3.9	フロー制御機能設定	136
3.9.1	flowcontrol	136
3.10	インタフェース統計情報設定	137
3.10.1	load-interval	137
3.11	MAC アドレス設定	138
3.11.1	mac-address	138
3.12	インタフェースメディア設定	139
3.12.1	media	139
3.13	MTU 設定	140
3.13.1	mtu	140

3.14	MSS 設定 (port-channel インタフェース)	141
3.14.1	mss	141
3.15	QoS インタフェース設定	142
3.15.1	service-policy	142
3.16	MSS 設定 (トンネルインタフェース)	143
3.16.1	set mss	143
3.17	インタフェースリンク状態設定	145
3.17.1	link-state always-up	145
3.17.2	shutdown	145
3.18	インタフェースリンク状態変化の設定	147
3.18.1	ethernet linkdown-delay-time	147
3.18.2	ethernet linkup-delay-time	147
3.19	インタフェーススピード/デュプレックス設定	149
3.19.1	speed-duplex	149
3.20	トンネルインタフェース動作モード設定	150
3.20.1	tunnel mode	150
3.21	VLAN ID 設定	152
3.21.1	vlan-id	152
3.21.2	vlan-id	153
3.21.3	ip redirect dp-forward	154

第 4 章 PPPoE の設定 155

4.1	PPPoE の設定	156
4.1.1	account	156
4.1.2	authentication accept	157
4.1.3	ncp	157
4.1.4	pppoe enable	158
4.1.5	pppoe interface	159
4.1.6	pppoe profile	159
4.1.7	server-name	160
4.1.8	service-name	161
4.1.9	set mtu	161

第 5 章 リンクアグリゲーションの設定 163

5.1	リンクアグリゲーション設定	164
5.1.1	bridge-group	164
5.1.2	switchport mode dot1q tunnel	165
5.1.3	switchport passthrough	166
5.1.4	switchport transparent	167
5.1.5	trunk-group	167
5.1.6	trunk-member port-priority	168
5.1.7	trunk-group mode	169
5.1.8	trunk-group lacpdu-timeout	170
5.1.9	trunk-group lacpdu-dst-mac	171
5.1.10	trunk-group max-active-port	171
5.1.11	trunk-group min-active-port	172
5.1.12	trunk-group standby-no-receive	173
5.1.13	trunk-group system-priority	173
5.1.14	trunk-group transmit-pause-time	174
5.1.15	trunk-group collector-max-delay	175
5.1.16	trunk-group load-balance	176

第 6 章	RIP の設定	177
6.1	IPv4 経路交換の設定	178
6.1.1	router rip	178
6.1.2	default-information originate	178
6.1.3	default-metric	179
6.1.4	distance	180
6.1.5	distribute-list	181
6.1.6	ip rip authentication mode	182
6.1.7	ip rip authentication string	182
6.1.8	no ip rip receive-packet	183
6.1.9	no ip rip send-packet	184
6.1.10	ip rip split-horizon	184
6.1.11	maximum-prefix	185
6.1.12	neighbor	186
6.1.13	network	186
6.1.14	offset-list	187
6.1.15	passive-interface	188
6.1.16	recv-buffer-size	189
6.1.17	redistribute	190
6.1.18	timers basic	190
第 7 章	OSPF の設定	192
7.1	IPv4 経路交換の設定	193
7.1.1	router ospf	193
7.1.2	area authentication	193
7.1.3	area default-cost	194
7.1.4	area export-list	195
7.1.5	area import-list	196
7.1.6	area nssa	196
7.1.7	area range	198
7.1.8	area shortcut	199
7.1.9	area stub	199
7.1.10	auto-cost reference-bandwidth	200
7.1.11	capability restart graceful	201
7.1.12	compatible rfc1583	201
7.1.13	default-information originate	202
7.1.14	default-metric	203
7.1.15	distance	204
7.1.16	distance ospf	205
7.1.17	distribute-list	205
7.1.18	instance-metric	206
7.1.19	ip ospf authentication	207
7.1.20	ip ospf authentication-key	208
7.1.21	ip ospf cost	208
7.1.22	ip ospf database-filter all out	209
7.1.23	ip ospf dead-interval	210
7.1.24	ip ospf disable all	210
7.1.25	ip ospf hello-interval	211
7.1.26	ip ospf message-digest-key	212
7.1.27	ip ospf mtu	212
7.1.28	ip ospf network	213
7.1.29	ip ospf priority	214

7.1.30	ip ospf retransmit-interval	215
7.1.31	ip ospf transmit-delay	215
7.1.32	log-adjacency-changes	216
7.1.33	maximum-paths	217
7.1.34	max-metric router-lsa	218
7.1.35	neighbor	218
7.1.36	network	219
7.1.37	opaque-lsa-capable	220
7.1.38	ospf abr-type	220
7.1.39	ospf restart helper max-grace-period	222
7.1.40	ospf restart helper policy	222
7.1.41	overflow database external	223
7.1.42	passive-interface	224
7.1.43	queue-length update	225
7.1.44	redistribute	226
7.1.45	refresh timer	227
7.1.46	router-id	228
7.1.47	summary-address	228
7.1.48	timers lsa arrival	229
7.1.49	timers throttle lsa	230
7.1.50	timers throttle spf	231
7.1.51	trap lsa maxage	232
7.1.52	trap lsa originate	232
7.1.53	trap tx-retransmit	233
7.1.54	trap vlink-tx-retransmit	234
7.2	Virtual Link の設定	235
7.2.1	area virtual-link	235
7.2.2	area virtual-link authentication	235
7.2.3	area virtual-link authentication-key	236
7.2.4	area virtual-link dead-interval	237
7.2.5	area virtual-link hello-interval	238
7.2.6	area virtual-link message-digest-key	239
7.2.7	area virtual-link retransmit-interval	239
7.2.8	area virtual-link transmit-delay	240
7.3	IPv6 経路交換の設定	242
7.3.1	router ipv6 ospf	242
7.3.2	area default-cost	242
7.3.3	area range	243
7.3.4	area stub	244
7.3.5	default-metric	245
7.3.6	distance	245
7.3.7	ipv6 ospf cost	246
7.3.8	ipv6 ospf dead-interval	247
7.3.9	ipv6 ospf display route single-line	248
7.3.10	ipv6 ospf hello-interval	248
7.3.11	ipv6 ospf priority	249
7.3.12	ipv6 ospf retransmit-interval	250
7.3.13	ipv6 ospf transmit-delay	250
7.3.14	ipv6 router ospf area	251
7.3.15	log-adjacency-changes	252
7.3.16	overflow database external	253
7.3.17	passive-interface	253
7.3.18	redistribute	254
7.3.19	router-id	256

7.3.20	summary-prefix	256
7.3.21	timers spf	257
7.4	Virtual Link の設定	259
7.4.1	area virtual-link	259
7.4.2	area virtual-link dead-interval	259
7.4.3	area virtual-link hello-interval	260
7.4.4	area virtual-link retransmit-interval	261
7.4.5	area virtual-link transmit-delay	262
7.5	VRF 経路交換の設定	263
7.5.1	router ospf-vrf	263

第 8 章 BGP の設定 264

8.1	BGP の設定	265
8.1.1	router bgp	265
8.1.2	bgp aggregate-nexthop-check	265
8.1.3	bgp anvl-dampening-config	266
8.1.4	no bgp extended-asn-cap	266
8.1.5	bgp rfc1771-path-select	267
8.1.6	bgp rfc1771-strict	267
8.1.7	ip as-path access-list	268
8.1.8	ip community-list	269
8.1.9	ip extcommunity-list	270
8.1.10	bgp always-compare-med	272
8.1.11	bgp bestpath as-path ignore	272
8.1.12	bgp bestpath compare-routerid	273
8.1.13	bgp bestpath igp-metric ignore	273
8.1.14	bgp bestpath med	274
8.1.15	bgp bundle-time	276
8.1.16	no bgp client-to-client reflection	276
8.1.17	bgp cluster-id	277
8.1.18	bgp dampening	278
8.1.19	no bgp default ipv4-unicast	278
8.1.20	bgp default local-preference	279
8.1.21	bgp deterministic-med	280
8.1.22	bgp enforce-first-as	280
8.1.23	no bgp fast-external-failover	281
8.1.24	bgp listen range	281
8.1.25	bgp log-neighbor-changes	282
8.1.26	bgp log-update-error	283
8.1.27	bgp multi-path	283
8.1.28	bgp network import-check	284
8.1.29	bgp nexthop-validation-timer	285
8.1.30	bgp router-id	286
8.1.31	distance	286
8.1.32	distance bgp	287
8.1.33	neighbor advertisement-interval	288
8.1.34	neighbor advertisement-limit	289
8.1.35	neighbor capability route-refresh	290
8.1.36	neighbor description	291
8.1.37	neighbor dont-capability-negotiate	292
8.1.38	neighbor ebgp-multihop	293
8.1.39	neighbor enforce-multihop	293
8.1.40	neighbor interface	294

8.1.41	neighbor override-capability	295
8.1.42	neighbor passive	296
8.1.43	neighbor password	296
8.1.44	neighbor peer-group	297
8.1.45	neighbor peer-group	298
8.1.46	neighbor port	299
8.1.47	neighbor remote-as	299
8.1.48	neighbor retain-stale time	300
8.1.49	neighbor shutdown	301
8.1.50	neighbor start-interval	302
8.1.51	neighbor strict-capability-match	303
8.1.52	neighbor timers	303
8.1.53	neighbor update-source	304
8.1.54	neighbor version	305
8.1.55	neighbor weight	306
8.1.56	timers bgp	307
8.2	IPv4 経路交換の設定	309
8.2.1	address-family ipv4 unicast	309
8.2.2	aggregate-address	309
8.2.3	default-information originate	310
8.2.4	neighbor activate	311
8.2.5	neighbor allowas-in	312
8.2.6	neighbor attribute-unchanged	312
8.2.7	neighbor capability graceful-restart	313
8.2.8	neighbor default-originate	314
8.2.9	neighbor disable-nexthop-validation	315
8.2.10	neighbor distribute-list	316
8.2.11	neighbor filter-list	317
8.2.12	neighbor maximum-prefix	318
8.2.13	neighbor next-hop-self	319
8.2.14	neighbor prefix-list	319
8.2.15	neighbor remove-private-as	320
8.2.16	neighbor route-map	321
8.2.17	neighbor route-server-client	322
8.2.18	neighbor send-community	323
8.2.19	neighbor soft-reconfiguration inbound	324
8.2.20	neighbor soo	324
8.2.21	network	325
8.2.22	no bgp lookup default-information	326
8.2.23	redistribute	327
8.2.24	table-map	328
8.3	IPv6 経路交換の設定	330
8.3.1	address-family ipv6 unicast	330
8.3.2	aggregate-address	330
8.3.3	default-information originate	331
8.3.4	neighbor activate	332
8.3.5	neighbor allowas-in	333
8.3.6	neighbor attribute-unchanged	333
8.3.7	neighbor capability graceful-restart	334
8.3.8	neighbor default-originate	335
8.3.9	neighbor disable-nexthop-validation	336
8.3.10	neighbor distribute-list	337
8.3.11	neighbor filter-list	338
8.3.12	neighbor maximum-prefix	339

8.3.13	neighbor next-hop-self	340
8.3.14	neighbor prefix-list	340
8.3.15	neighbor remove-private-as	341
8.3.16	neighbor route-map	342
8.3.17	neighbor route-reflector-client	343
8.3.18	neighbor route-server-client	344
8.3.19	neighbor send-community	344
8.3.20	neighbor soft-reconfiguration inbound	345
8.3.21	neighbor soo	346
8.3.22	network	347
8.3.23	no bgp lookup default-information	348
8.3.24	redistribute	348
8.3.25	table-map	349
8.4	IPv4VRF 経路交換の設定	351
8.4.1	address-family ipv4 vrf	351
8.5	IPv6VRF 経路交換の設定	352
8.5.1	address-family ipv6 vrf	352

第 9 章 route-map の設定..... 353

9.1	route-map の設定	354
9.1.1	route-map	354
9.1.2	continue	354
9.1.3	match as-path	355
9.1.4	match community	356
9.1.5	match interface	357
9.1.6	match ip address	357
9.1.7	match ip next-hop	358
9.1.8	match ipv6 address	359
9.1.9	match ipv6 next-hop	360
9.1.10	match metric	360
9.1.11	match origin	361
9.1.12	match route-type external	362
9.1.13	match tag	362
9.1.14	set aggregator	363
9.1.15	set as-path prepend	364
9.1.16	set atomic-aggregate	364
9.1.17	set community	365
9.1.18	set extcommunity	366
9.1.19	set ip next-hop	367
9.1.20	set ipv6 next-hop	367
9.1.21	set local-preference	368
9.1.22	set metric	369
9.1.23	set metric-type	370
9.1.24	set next-hop	370
9.1.25	set origin	371
9.1.26	set originator-id	372
9.1.27	set tag	372
9.1.28	set weight	373

第 10 章 アクセスリストの設定..... 375

10.1	アクセスリスト／アクセスグループの設定	376
10.1.1	access-list	376

10.1.2	access-list (IPv4 標準設定)	376
10.1.3	access-list (IPv4 拡張設定)	377
10.1.4	access-list (IPv6 標準設定)	379
10.1.5	access-list (IPv6 拡張設定)	380
10.1.6	access-list (MAC アドレス設定)	381
10.1.7	access-list description	383
10.1.8	ip access-group	383
10.1.9	ipv6 access-group	384
10.1.10	ip access-group default spi	386
10.1.11	ipv6 access-group default spi	386
10.1.12	ip access-group spi ftp-data enable	387
10.1.13	ipv6 access-group spi ftp-data enable	388
10.1.14	ip access-group spi timeout	388
10.1.15	ipv6 access-group spi timeout	389
10.1.16	ip spi entry tcp-syn-timeout	391
10.1.17	ipv6 spi entry tcp-syn-timeout	391
10.1.18	ip spi entry tcp-fin-timeout	392
10.1.19	ipv6 spi entry tcp-fin-timeout	393
10.1.20	ip spi entry tcp-idle-timeout	394
10.1.21	ipv6 spi entry tcp-idle-timeout	394
10.1.22	ip spi entry udp-idle-timeout	395
10.1.23	ipv6 spi entry udp-idle-timeout	396
10.1.24	ip spi entry icmp-timeout	397
10.1.25	ipv6 spi entry icmp-timeout	397
10.1.26	ip spi entry others-timeout	398
10.1.27	ipv6 spi entry others-timeout	399
10.1.28	mac access-group	399

第 11 章 IPv4 の設定..... 401

11.1	ARP キャッシュの設定	402
11.1.1	arp	402
11.1.2	ip arp packet-hold	402
11.1.3	ip arp polling disable	403
11.1.4	ip arp pre-solution disable	404
11.1.5	ip arp max-request	404
11.2	DNS の設定	406
11.2.1	ip domain-name	406
11.2.2	ip host	406
11.3	ICMP の設定	408
11.3.1	ip icmp disable-sending-errors	408
11.3.2	ip icmp source	409
11.4	アドレスプールの設定 (IPv4)	410
11.4.1	ip local pool	410
11.5	IPv4 プレフィックスリストの設定	411
11.5.1	ip prefix-list	411
11.5.2	ip prefix-list description	412
11.6	IPv4 スタティックルートの設定	414
11.6.1	ip route	414
11.7	IPv4 インタフェースアドレスの設定	416
11.7.1	ip address	416
11.8	Proxy-ARP の設定	417
11.8.1	ip proxy-arp	417

11.9 送信元 IPv4 アドレスの設定	418
11.9.1 ip unnumbered	418
11.10 DHCPv4 クライアント／サーバ／リレーエージェント機能設定	419
11.10.1 ip dhcp service	419
11.10.2 ip dhcp client-profile	420
11.10.3 ip dhcp server-profile	420
11.10.4 ip dhcp host-database	421
11.10.5 ip dhcp client-profile	421
11.10.6 client-id	422
11.10.7 retries infinity	423
11.10.8 ip dhcp server-profile	423
11.10.9 address	424
11.10.10 dns	425
11.10.11 domain	426
11.10.12 gateway	426
11.10.13 lease-time	427
11.10.14 ntp-server	428
11.10.15 option	428
11.10.16 sip-server	429
11.10.17 time-server	430
11.10.18 wins-server	431
11.10.19 host	431

第 12 章 IPv6 の設定..... 433

12.1 DNS の設定	434
12.1.1 ipv6 host	434
12.2 ICMP の設定	435
12.2.1 ipv6 icmp disable-sending-errors	435
12.2.2 ipv6 icmp source	436
12.3 アドレスプールの設定 (IPv6)	437
12.3.1 ipv6 local pool	437
12.4 IPv6 プレフィックスリストの設定	438
12.4.1 ipv6 prefix-list	438
12.4.2 ipv6 prefix-list description	439
12.5 IPv6 スタティックルートの設定	441
12.5.1 ipv6 route	441
12.6 IPv6 インタフェースアドレスの設定	443
12.6.1 ipv6 address	443
12.6.2 ipv6 address dhcp	444
12.7 DHCPv6 クライアント／サーバ／リレーエージェント機能設定	446
12.7.1 ipv6 dhcp service	446
12.7.2 ipv6 dhcp client-profile	447
12.7.3 ipv6 dhcp server-profile	447
12.7.4 ipv6 dhcp host-database	448
12.7.5 ipv6 dhcp client-profile	449
12.7.6 laid	449
12.7.7 option-request	450
12.7.8 retries infinity	451
12.7.9 ipv6 dhcp server-profile	451
12.7.10 address	452
12.7.11 dns	453
12.7.12 domain	454

12.7.13	duid	455
12.7.14	option	456
12.7.15	preference	457
12.7.16	prefix	457
12.7.17	sip-server address	459
12.7.18	sip-server domain	460
12.7.19	sntp-server	461
12.7.20	host	462
12.8	IPv6 アドレス有効設定	463
12.8.1	ipv6 enable	463
12.9	IPv6 Neighbor Discovery Protocol 設定	464
12.9.1	ipv6 hop-limit	464
12.9.2	ipv6 nd max-solicit	464
12.9.3	ipv6 nd packet-hold	465
12.9.4	ipv6 neighbor	466
12.9.5	ipv6 hoplimit-receive-enable	467
12.9.6	ipv6 mtu-receive-enable	467
12.9.7	ipv6 nd managed-config-flag	468
12.9.8	ipv6 nd ns-interval	468
12.9.9	ipv6 nd other-config-flag	469
12.9.10	ipv6 nd prefix-advertisement	470
12.9.11	ipv6 nd pre-solution disable	471
12.9.12	ipv6 nd ra-delay	471
12.9.13	ipv6 nd ra-interval	472
12.9.14	ipv6 nd ra-lifetime	473
12.9.15	ipv6 nd reachable-time	473
12.9.16	ipv6 reachable-time-receive-enable	474
12.9.17	ipv6 nd receive-ra	475
12.9.18	ipv6 nd rs-delay	476
12.9.19	ipv6 nd rs-times	476
12.9.20	ipv6 nd send-ra	477
12.9.21	ipv6 nd curhoplimit	478
12.9.22	ipv6 nd mtu	479
12.9.23	ipv6 ns-interval-receive-enable	479
12.9.24	ipv6 router-lifetime-receive-enable	480
12.10	送信元 IPv6 アドレスの設定	481
12.10.1	ipv6 unnumbered	481

第 13 章 NAT の設定..... 482

13.1	NAT の設定	483
13.1.1	ip nat pool	483
13.1.2	ip nat list	483
13.1.3	ip nat inside source list pool	484
13.1.4	ip nat inside source list interface	486
13.1.5	ip nat inside source static	487
13.1.6	ip nat inside source static-subnet	488
13.1.7	ip nat inside destination static	489
13.1.8	ip nat inside destination static-subnet	490
13.1.9	ip nat outside source static	491
13.1.10	ip nat outside source static-subnet	492
13.1.11	ip nat outside destination static	493
13.1.12	ip nat outside destination static-subnet	494
13.1.13	ip nat acl	495

13.1.14	ip nat acl permit	496
13.1.15	ip nat translation finrst-timeout	497
13.1.16	ip nat translation icmp-timeout	497
13.1.17	ip nat translation tcp-timeout	498
13.1.18	ip nat translation udp-timeout	499
13.1.19	ip nat translation timeout	499
13.1.20	ip nat wellknown	500
13.1.21	ip nat default action	501
第 14 章	EtherIP の設定.....	502
14.1	EtherIP の設定	503
14.1.1	ether-ip tunnel-profile	503
14.1.2	I2-encapsulation map cos-dscp	503
14.1.3	set mtu	504
14.1.4	tunnel destination	505
14.1.5	tunnel protection	506
14.1.6	tunnel source	506
第 15 章	IPinIP の設定.....	508
15.1	IPinIP の設定	509
15.1.1	ipinip tunnel-profile	509
15.1.2	source address	509
15.1.3	destination address	510
15.1.4	ipinip fragment	511
15.1.5	profile-mode	511
15.1.6	set mtu	512
15.1.7	set ip df-bit	513
15.1.8	ipinip propagate-ttl	514
15.1.9	ipinip propagate-tos	514
第 16 章	BFD の設定.....	516
16.1	BFD の設定	517
16.1.1	bfd-map	517
16.1.2	ip route bfd-map	517
16.1.3	ipv6 route bfd-map	518
16.1.4	ip route vrf bfd-map	519
16.1.5	ipv6 route vrf bfd-map	520
16.1.6	designated-source	521
16.1.7	interval	522
16.1.8	min_rx	523
16.1.9	multi-hop ttl-drop-threshold	523
16.1.10	multiplier	524
16.1.11	neighbor	525
16.1.12	session-mode	525
16.1.13	ip ospf bfd	526
16.1.14	ipv6 ospf bfd	527
16.1.15	bfd all-interface	528
16.1.16	trunk-group fall-over bfd-map	528

第 17 章	IPsec の設定	530
17.1	ISAKMP-SA/IKE SA の設定	531
17.1.1	crypto isakmp policy	531
17.1.2	crypto isakmp keepalive-params no-reconnect	531
17.1.3	crypto isakmp rekey continuous-channel	532
17.1.4	crypto isakmp security-association softlimit	533
17.1.5	crypto isakmp tos	533
17.1.6	crypto ipsec udp-encapsulation-force	534
17.1.7	authentication	535
17.1.8	dont-route	536
17.1.9	encryption	536
17.1.10	encryption-keysize	537
17.1.11	group	538
17.1.12	hash	539
17.1.13	lifetime	540
17.1.14	crypto keyring	540
17.1.15	pre-shared-key	541
17.1.16	initiate-mode	543
17.1.17	set negotiation expire-time	543
17.1.18	set negotiation retry	544
17.1.19	set rekey continuous-channel	545
17.1.20	set security-association softlimit	546
17.1.21	set udp-encapsulation-force	547
17.2	IPSEC-SA/CHILD SA の設定	548
17.2.1	crypto ipsec policy	548
17.2.2	set pfs	548
17.2.3	set security-association always-up	549
17.2.4	crypto ipsec security-association lifetime seconds	550
17.2.5	set security-association lifetime seconds	551
17.2.6	crypto ipsec security-association softlimit	551
17.2.7	set security-association softlimit	553
17.2.8	set security-association transform-keysize aes	554
17.2.9	set security-association transform	555
17.2.10	set esn	556
17.2.11	set udp-encapsulation	556
17.3	IPSEC セレクタの設定	558
17.3.1	crypto ipsec selector	558
17.3.2	src	558
17.3.3	dst	559
17.4	ISAKMP プロファイルの設定	561
17.4.1	crypto isakmp profile	561
17.4.2	accounting	561
17.4.3	fvr	562
17.4.4	ike-version	563
17.4.5	isakmp authorization list	563
17.4.6	keyring	564
17.4.7	local-address	565
17.4.8	local-key	566
17.4.9	match identity	567
17.4.10	self-identity	568
17.4.11	set ipsec-policy	569
17.4.12	set isakmp-policy	570
17.4.13	set peer	570

17.5	VPN セレクタの設定	572
17.5.1	crypto map	572
17.5.2	link-state	572
17.5.3	match address	573
17.5.4	set isakmp-profile	574
17.5.5	tunnel mode	575
17.5.6	vrf	576
17.6	データベースの設定	577
17.6.1	aaa local group	577
17.6.2	username	577
17.6.3	username interface tunnel	578
17.6.4	username isakmp keepalive	579
17.6.5	username isakmp negotiation retry	580
17.6.6	username isakmp negotiation expire-time	581
17.7	拡張認証の各種設定	583
17.7.1	aaa authentication ike-client	583
17.7.2	client authentication list	584
17.7.3	client authentication my-name	584
17.7.4	client authentication type	585
17.7.5	client authentication eap-identity request	586
17.8	Mode-config/Config Payload の設定	588
17.8.1	crypto isakmp client configuration group	588
17.8.2	dns	588
17.8.3	pool	589
17.8.4	aaa authorization network	590
17.8.5	client configuration address	591
17.9	電子証明書の設定	593
17.9.1	ca trustpoint	593
17.9.2	pki revocation-check	593
17.9.3	pki validity-check	594
17.9.4	crypto pki startup-import store file	595
17.9.5	crypto pki startup-import pkcs12	596
17.9.6	crypto pki startup-import delete other-certificate	597
17.10	DPD の設定	598
17.10.1	crypto isakmp keepalive	598
17.10.2	crypto isakmp keepalive-icmp	599
17.10.3	keepalive	600
17.10.4	keepalive-icmp	601
17.10.5	local-address-icmp	601
17.10.6	remote-address-icmp	602
17.10.7	vrf-icmp	603
17.11	ESP の設定	604
17.11.1	crypto ipsec selector-check	604
17.11.2	set selector-check	604
17.11.3	crypto ipsec replay-check disable	605
17.11.4	set replay-check	606
17.11.5	crypto ipsec sequence-overflow disable	607
17.11.6	set sequence-overflow	607
17.11.7	set mtu	608
17.11.8	set ip tos	609
17.11.9	set ip df-bit	610
17.11.10	set ip fragment	611
17.11.11	crypto ipsec esn	612

17.11.12	crypto ipsec udp-encapsulation	612
17.11.13	crypto ipsec responder udp-encapsulation spoofed	613
17.12	SA アップルートの設定	615
17.12.1	sa-up route	615
17.12.2	sa-up route-dvpn	616
17.12.3	sa-up route-radius	617
17.12.4	sa-up route-sip-radius	618
17.13	SA 数制限、および IPsec MIB の設定	619
17.13.1	crypto ipsec-tunnel ike limit	619
17.13.2	crypto ipsec-tunnel ike threshold	619
17.13.3	crypto ipsec-tunnel ipsec-in limit	620
17.13.4	crypto ipsec-tunnel ipsec-in threshold	621
17.13.5	crypto ipsec-tunnel session limit	622
17.13.6	crypto ipsec-tunnel session threshold	622
17.13.7	description	623
17.13.8	set ipsec-tunnel ike limit	624
17.13.9	set ipsec-tunnel ike threshold	625
17.13.10	set ipsec-tunnel ipsec-in limit	625
17.13.11	set ipsec-tunnel ipsec-in threshold	626
17.13.12	set ipsec-tunnel index	627
17.13.13	set ipsec-tunnel name	628
17.13.14	set ipsec-tunnel session limit	628
17.13.15	set ipsec-tunnel session threshold	629
17.13.16	crypto isakmp negotiation limit	630
17.13.17	crypto isakmp negotiation cookie-req	631
17.14	IPsec の各種設定	632
17.14.1	crypto ip dns-params	632
17.14.2	crypto ip dns-query auto-refresh	633
17.14.3	crypto ip dns-query negotiation	633
17.14.4	crypto ip dns-query timeout	634
17.14.5	crypto ip domain-name	635
17.14.6	crypto ip name-server	636
17.14.7	crypto ipsec ikev2 delay old-sa-delete	636
17.14.8	crypto ipsec ikev2 delay old-sa-delete-ack	637
17.14.9	crypto isakmp negotiation always-up-params	638
17.14.10	crypto isakmp negotiation expire-time	639
17.14.11	crypto isakmp negotiation protected-rekey-interval	640
17.14.12	crypto isakmp negotiation retry	641
17.14.13	crypto ipsec qm-addr-zero-any	642
17.14.14	crypto session identification address	642
17.14.15	crypto session reject-duplicated-request	643
17.14.16	crypto session release idle-time	644
17.14.17	crypto session release ipsec-lost-time	645
17.14.18	crypto session release isakmp-lost-time	646
17.14.19	crypto session release reset acct-stop-send	647
17.14.20	crypto session release reset delete-send	647
17.14.21	crypto session release reset delay	648
17.14.22	crypto session release session-time	648
17.14.23	link-state	649
17.14.24	set rekey dont-initiate	650
17.14.25	negotiation protected-rekey-interval	651
17.14.26	set session identification address	651
17.14.27	set session reject-duplicated-request	652
17.14.28	set session release ipsec-lost-time	653

17.14.29	set session release idle-time	654
17.14.30	set session release isakmp-lost-time	654
17.14.31	set ikev2 delay old-sa-delete-ack	655
17.14.32	set security-association rekey	656
17.15	ログの設定	658
17.15.1	crypto isakmp log	658

第 18 章 動的 VPN の設定 659

18.1	INVITE の発信契機の設定	660
18.1.1	dvpn autoignore	660
18.1.2	dvpn ip	660
18.2	DVPN プロファイル設定	662
18.2.1	dvpn profile	662
18.2.2	description	662
18.2.3	dvpn-interface	663
18.2.4	keep connect	664
18.2.5	remotenet	665
18.2.6	remoteid	666
18.2.7	set dvpn client	667
18.2.8	watch	668
18.3	DVPN クライアント情報の設定	670
18.3.1	dvpn client	670
18.3.2	client-priority	670
18.3.3	domain	671
18.3.4	dvpn-server address	672
18.3.5	dvpn-server username	673
18.3.6	dvpn sip encode-off	674
18.3.7	localnet	674
18.3.8	localid	675
18.3.9	sip expire-register	677
18.3.10	sip expire-session	677
18.3.11	sip expire-session-disable	678
18.3.12	sip encrypt-enable	678
18.3.13	sip local-address	679
18.4	DVPN サーバの設定	681
18.4.1	dvpn server auth aaa	681
18.4.2	dvpn server auth use	681
18.4.3	dvpn server domain	682
18.4.4	dvpn server sips max-sessions	682
18.4.5	dvpn server use enable	683

第 19 章 データコネクトの設定 685

19.1	SIP の設定	686
19.1.1	incoming-call disable	686
19.1.2	ipsec-timeout	686
19.1.3	ngn enable	687
19.1.4	ngn sip agent bind port-channel	688
19.1.5	ngn sip agent call-timeout	689
19.1.6	ngn sip agent charge-setting	689
19.1.7	ngn sip agent control session	690
19.1.8	ngn sip agent ipsec-timeout	691
19.1.9	ngn sip agent limit	692

19.1.10	ngn sip agent proxy server address	693
19.1.11	ngn sip agent proxy server domain	694
19.1.12	ngn sip agent registrar expire	694
19.1.13	ngn sip agent registrar retry	695
19.1.14	ngn sip agent registrar server address	696
19.1.15	ngn sip agent sessiontimer default	697
19.1.16	ngn sip agent sessiontimer use disable	698
19.1.17	ngn sip agent survey sip-server invite	698
19.1.18	ngn sip agent user	699
19.1.19	ngn sip profile	700
19.1.20	ngn sip use enable	700
19.1.21	outgoing-call disable	701
19.1.22	remote dial number	702
19.1.23	remote dial speed	702
19.1.24	sip limit	703

第 20 章 データコネクトおよび IPsec で用いる RADIUS サーバの設定..... 705

20.1	IPsec で用いる RADIUS サーバの設定	706
20.1.1	aaa accounting network	706
20.1.2	ip vrf forwarding	707
20.1.3	attribute ignore	708
20.1.4	attribute 31 include-in-access-req	708
20.1.5	attribute 31 include-in-acct-req	709
20.1.6	attribute 31 extend-with-prefixlen	710
20.1.7	attribute 81 include-in-access-req	710
20.1.8	attribute 81 include-in-acct-req	711
20.1.9	nas-port-type	712
20.1.10	service-type	712
20.1.11	user-password	713
20.2	データコネクトで用いる RADIUS サーバの設定	715
20.2.1	aaa accounting ngn-sip start-stop group	715
20.2.2	aaa authentication ngn-sip group	715
20.2.3	accounting	716
20.2.4	client authentication type	717
20.2.5	password	717
20.2.6	ngn sip profile-radius	718
20.2.7	ngn sip radius acct	719
20.2.8	ngn sip radius auth	719
20.3	共通で用いる RADIUS サーバの設定	721
20.3.1	aaa group server radius	721
20.3.2	changeback-time	721
20.3.3	nas-ip-address	722
20.3.4	retransmit	723
20.3.5	server-private	723
20.3.6	source-address	724
20.3.7	timeout	725

第 21 章 モデム通信機能の設定..... 726

21.1	モデム通信機能の設定	727
21.1.1	modem profile	727
21.1.2	tunnel mode modem profile	727
21.1.3	remote dial number	728

21.1.4	account	729
21.1.5	auto connect	730
21.1.6	authentication accept	731
21.1.7	max-call	731
21.1.8	modem out-strings init	732
21.1.9	set mtu	733
21.1.10	set mss	734
21.1.11	set session release idle-time	735
21.1.12	monitor signal-quality enable level	735
21.1.13	monitor signal-quality interval	736

第 22 章 VRF の設定 738

22.1	VRF の設定	739
22.1.1	ip vrf	739
22.1.2	arp vrf	739
22.1.3	ip route vrf	741
22.1.4	ipv6 neighbor vrf	742
22.1.5	ipv6 route vrf	743
22.1.6	ip vrf forwarding	744
22.1.7	bgp local-as	744
22.1.8	description	745
22.1.9	rd	746

第 23 章 L2TPv3 の設定 747

23.1	L2TPv3 の設定	748
23.1.1	l2-encapsulation map cos-dscp	748
23.1.2	l2tpv3 tunnel-profile	748
23.1.3	l2tpv3 pseudowire	749
23.1.4	l2tpv3 always-up	750
23.1.5	l2tpv3 always-up-params	750
23.1.6	l2tpv3 hello interval	751
23.1.7	l2tpv3 log	752
23.1.8	l2tpv3 retransmit retries	752
23.1.9	l2tpv3 retransmit timer	753
23.1.10	digest type	754
23.1.11	hello interval	755
23.1.12	hidden	756
23.1.13	hostname local	756
23.1.14	hostname remote	757
23.1.15	mode	758
23.1.16	retransmit retries	758
23.1.17	retransmit timer	759
23.1.18	router-id local	760
23.1.19	router-id remote	761
23.1.20	tunnel destination	761
23.1.21	tunnel protection	762
23.1.22	tunnel source	763
23.1.23	always-up	764
23.1.24	cookie size	764
23.1.25	pw-type	765
23.1.26	remote-end-id ascii	766
23.1.27	sequencing both	766

23.1.28	set mtu	767
23.1.29	set profile	768

第 24 章 bridge の設定 769

24.1	bridge の設定	770
24.1.1	bridge-group	770
24.1.2	bridge loop-detect-disable	770
24.1.3	bridge loop-detect-time	771
24.1.4	bridge transparent eap	772
24.1.5	bridge transparent bpdu	772
24.1.6	bridge transparent lacp	773
24.1.7	bridge transparent other	774
24.1.8	mac-address-table max-entry	774
24.1.9	mac-address-table cvid-enable	775

第 25 章 QoS/CoS の設定 777

25.1	classifier の登録	779
25.1.1	class-map	779
25.1.2	match-all	779
25.1.3	match-any	780
25.1.4	match 802.1p priority	780
25.1.5	match any	781
25.1.6	match ip access-group	782
25.1.7	match ip dscp	782
25.1.8	match ip precedence	783
25.1.9	match ip tos	784
25.1.10	match local-source	785
25.1.11	match ipv6 access-group	785
25.1.12	match mac access-group	786
25.1.13	match mac unknown-unicast	787
25.1.14	match mac stag-priority	787
25.1.15	match mac ctag-priority	788
25.2	service-policy の登録	789
25.2.1	policy-map	789
25.2.2	class	789
25.2.3	bandwidth	790
25.2.4	count	791
25.2.5	drop	791
25.2.6	extended-queue	792
25.2.7	police	793
25.2.8	policing-header	794
25.2.9	queue	794
25.2.10	search-sequence	795
25.2.11	service-policy	796
25.2.12	set 802.1p priority	797
25.2.13	set ip dscp	797
25.2.14	set ip prec	798
25.2.15	set ip tos	799
25.2.16	set ipv6 dscp	799
25.2.17	set ipv6 traffic-class	800
25.2.18	set mac stag-priority	801
25.2.19	transmit	801

25.3	Traffic Manager の設定	803
25.3.1	traffic-manager network	803
25.3.2	traffic-manager extended	803
25.3.3	bandwidth profile	804
25.3.4	port profile	804
25.3.5	port scheduler	805
25.3.6	port scheduler	806
25.3.7	to-host protocol	807
25.3.8	to-host police	809
25.3.9	to-host reason	810
25.3.10	frame-overhead	812
25.3.11	shape	813
25.3.12	shape	814
25.3.13	shape	814
25.3.14	bandwidth scale	815
25.3.15	queue normal rate	816
25.3.16	queue limit	817
25.3.17	port profile	817
25.3.18	frame-overhead	818
25.3.19	queue limit	819
25.3.20	queue shape	820
25.4	データコネク트의 QoS/CoS の設定	821
25.4.1	set service-policy	821
25.4.2	ngn sip agent service-policy	822
25.4.3	dataconnect-policy-map	823
25.4.4	burst	823
25.4.5	queue limit	824
25.4.6	queue normal rate	825
25.4.7	match-list	826
25.4.8	set dscp	827
第 26 章	ポリシールーティングの設定	828
26.1	classifier の登録	829
26.1.1	policy-route input	829
26.1.2	local policy-route	830
26.2	ポリシーマップの定義	831
26.2.1	policy-route-map	831
26.2.2	class	831
26.2.3	search-sequence	832
26.2.4	count	833
26.2.5	action	833
26.2.6	watch	834
第 27 章	IDS の設定	836
27.1	IDS の設定	837
27.1.1	ids profile	837
27.1.2	ip ids	837
27.1.3	ipv6 ids	838
27.1.4	type	839

第 28 章	VRRP の設定	841
28.1	VRRP の設定	842
28.1.1	ip vrrp enable	842
28.1.2	track down-action	842
28.1.3	track management	843
28.1.4	track port-channel	844
28.1.5	track survey	845
28.1.6	track vhost	846
28.1.7	vrrp version	847
28.2	IPv4 VRRP の設定	849
28.2.1	ip vrrp advertise_delay_timer	849
28.2.2	ip vrrp initialize_delay_time	850
28.2.3	ip vrrp np_delay_timer	850
28.2.4	ip vrrp mode interface-delegation	851
28.2.5	ip vrrp mode trap-enable-all	852
28.2.6	track ip	852
28.2.7	vrrp address	853
28.2.8	vrrp adver-interval	854
28.2.9	vrrp delegated-interface	855
28.2.10	vrrp preempt	855
28.2.11	vrrp priority	856
28.2.12	vrrp track	857
28.3	IPv6 VRRP の設定	859
28.3.1	ipv6 vrrp advertise_delay_timer	859
28.3.2	ipv6 vrrp initialize_delay_time	860
28.3.3	ipv6 vrrp np_delay_timer	860
28.3.4	ipv6 vrrp address	861
28.3.5	ipv6 vrrp adver-interval	862
28.3.6	ipv6 vrrp delegated-interface	863
28.3.7	ipv6 vrrp mode interface-delegation	863
28.3.8	ipv6 vrrp mode trap-enable-all	864
28.3.9	ipv6 vrrp preempt	864
28.3.10	ipv6 vrrp priority	865
28.3.11	ipv6 vrrp track	866
28.3.12	track ipv6	867
第 29 章	survey の設定	869
29.1	survey の設定	870
29.1.1	survey-map	870
29.1.2	ip route survey	871
29.1.3	ip route vrf survey	872
29.1.4	ipv6 route survey	873
29.1.5	ipv6 route vrf survey	875
29.1.6	survey	876
29.1.7	neighbor surveillance nexthop-validation-check	878
29.1.8	neighbor surveillance peer-address	879
29.1.9	neighbor surveillance down-action	880
29.1.10	dont-route	881
29.1.11	dscp	881
29.1.12	frequency	882
29.1.13	hop-limit	883
29.1.14	retry	883

29.1.15	size	884
29.1.16	stability	885
29.1.17	timeout	886
29.1.18	traffic-class	886
29.1.19	ttl	887
29.1.20	tunnel-unused	888

第 30 章 SNMP の設定 889

30.1	SNMPv1、v2 の設定	890
30.1.1	snmp-server community	890
30.1.2	snmp-server contact	890
30.1.3	snmp-server enable traps	891
30.1.4	snmp-server host	892
30.1.5	snmp-server host-queue timeout	893
30.1.6	snmp-server location	894
30.1.7	snmp-server name	895
30.1.8	snmp-server queue-length	895
30.1.9	snmp-server source-interface	896
30.1.10	snmp-server trap-timeout	897
30.1.11	no snmp trap link-status	898
30.1.12	no snmp trap link-status	898
30.2	SNMPv3 の設定	900
30.2.1	snmp-server engine-id	900
30.2.2	snmp-server group	900
30.2.3	snmp-server host	901
30.2.4	snmp-server user	903
30.2.5	snmp-server view	904

第 31 章 SYSLOG の設定 905

31.1	SYSLOG の設定	906
31.1.1	syslog filter	906
31.1.2	no logging buffer	907
31.1.3	logging buffer facility	907
31.1.4	logging buffer level	908
31.1.5	logging buffer timestamps msec	909
31.1.6	no logging console	910
31.1.7	logging console facility	910
31.1.8	logging console level	911
31.1.9	logging console timestamps msec	912
31.1.10	logging facility	913
31.1.11	logging filter	914
31.1.12	logging fixed-facility	916
31.1.13	logging host	917
31.1.14	logging host-queue length	918
31.1.15	logging host-queue level	918
31.1.16	logging host-queue timeout	919
31.1.17	logging host-queue retry-interval	920
31.1.18	logging host facility	921
31.1.19	logging host level	922
31.1.20	logging level	923
31.1.21	logging source-interface	924
31.1.22	logging suppress-repeated	925

31.1.23	logging telnet	925
31.1.24	logging telnet facility	926
31.1.25	logging telnet level	927
31.1.26	logging telnet timestamps msec	928
31.1.27	facility	928
31.1.28	level	929
31.1.29	message	930
31.1.30	dvpn client-log	931
31.1.31	dvpn server-log	931
31.1.32	ip acl logging enable	932
31.1.33	ip nat table logging enable	933
31.1.34	ip nat table logging enable	933
31.1.35	ip vrrp mode logging-enable-all	934
31.1.36	ipv6 vrrp mode logging-enable-all	934
31.1.37	monitor signal-quality logging usb-ethernet	935
31.1.38	ngn sip log	936
31.1.39	process	936

第 32 章 アラームの設定 938

32.1	アラームの設定	939
32.1.1	environment profile	939
32.1.2	cpu utilization	939
32.1.3	temp-sensor expected temperature	940
32.1.4	physical memory	941
32.1.5	psu-output-error timer	942
32.1.6	psu-temp-sensor safety control power-down	942
32.1.7	temp-sensor safety control	943

第 33 章 ハードウェア故障検出の設定 945

33.1	ハードウェア故障検出の設定	946
33.1.1	hardware-fault-detection action	946
33.1.2	hardware-fault-detection level-up	947

第 34 章 イベントアクション機能の設定 948

34.1	イベントアクション機能の設定	949
34.1.1	event-action	949
34.1.2	description	949
34.1.3	event-condition	950
34.1.4	replay-action	951
34.1.5	retry	952
34.1.6	event interface	953
34.1.7	event interface counter	954
34.1.8	event manual	956
34.1.9	event ping	957
34.1.10	event syslog filter	958
34.1.11	event timer countdown	959
34.1.12	event timer uptime	960
34.1.13	event timer schedule	960
34.1.14	action cli exec command	962
34.1.15	action snmp-trap message	963
34.1.16	action syslog	964

34.1.17	action interface	965
34.1.18	action wait time	965

第 35 章 付録..... 967

35.1	正規表現について	968
35.1.1	使用例	969
35.2	VRF 設定の関連付け動作について	970
35.2.1	vrf 設定モード追加時の関連付け動作	970
35.2.2	vrf 設定モード削除時の関連付け動作	970
35.2.3	router bgp 設定追加時の関連付け動作	971
35.2.4	ip vrf forwarding 設定追加時の関連付け動作	972
35.2.5	ip vrf forwarding 設定削除時の関連付け動作	973
35.2.6	ip vrf 設定の確認	973

索引..... 974

本書の構成と使いかた

本書では、本装置のコンソールから入力するコマンドについて説明します。

構成定義編では、装置の機能の動作を設定するためのコマンドについて記載しています。

本書の読者と前提知識

本書は、ネットワーク管理を行っている方を対象に記述しています。



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

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

本書の構成

本書では、装置の機能の動作を設定するためのコマンドについて説明しています。

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。
【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。 <code>< ></code> : パラメタ名称を示しています。 <code>[]</code> : 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。 <code>{ }</code> : 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。
【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。
【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。
 補足	操作手順で説明しているもののほかに、補足情報を説明しています。
 参照	操作方法など関連事項を説明している箇所を示します。

使用上の注意事項

コマンドを使用する場合は、以下の点にご注意ください。

- コマンドの設定および変更が終了したら、save コマンドを実行してから commit コマンドまたは reset コマンドを実行し、設定を有効にしてください。save コマンドを実行せず reset コマンドまたは電源再投入を行った場合は、コマンドの設定が元の状態に戻ります。
また、save コマンドを実行しないで commit コマンドを実行した場合、一時的に設定は有効になりますが、reset コマンドまたは電源再投入を行った場合にコマンドの設定が元の状態に戻ります。
- 設定を削除する場合には、各設定コマンドに応じた削除コマンドを実行してください。
削除した設定情報は、show working.cfg(show candidate-config)に表示されなくなります。

本書における商標の表記について

本書に記載されている会社名および製品名は、各社の商標または登録商標です。

本装置のマニュアルの構成

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

マニュアル名称	内容
Si-R GX500 ご利用にあたって	本装置の設置方法やソフトウェアのインストール方法を説明しています。
コマンドリファレンス - 構成定義編 - (本書)	装置の機能の動作を設定するためのコマンドについて、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 -	装置の再起動など運用に関わるコマンド、およびプロトコルセッションのクリアや統計情報のクリアなど装置を制御するためのコマンドについて、パラメタの詳細な情報を説明しています。
機能説明書	本装置の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。

第1章 CLI の操作



この章では、CLIの操作に関するコマンドについて説明します。

1.1	コマンド操作について.....	31
1.2	使用可能文字.....	32
1.3	コマンドプロンプト.....	35
1.4	コマンドレベル.....	36
1.5	コマンドモード.....	39
1.6	コマンドヘルプ.....	48
1.7	コマンドヒストリ.....	49
1.8	コマンドログ.....	50
1.9	コマンドエイリアス.....	51

1.1 コマンド操作について

本装置では、コンソールやTELNETからのコマンド操作時に、以下に示す便利な機能（キー操作）をサポートしています。

キー操作	機能	キー操作	機能
Ctrl+a	行の先頭にカーソルを移動する。	Ctrl+k	カーソルから後の文字列を消去する。
Ctrl+b	カーソルを1文字戻す。	Ctrl+l	画面をクリアする。
Ctrl+c	コマンドを無視してプロンプトに戻る。	Ctrl+n	以降に入力したコマンドを1つずつ表示する。
Ctrl+d	コマンドの最後にカーソルがある場合は、補完できるコマンドの一覧を表示する。 コマンドの途中でカーソルがある場合は、カーソル上の文字を1文字消去する。	Ctrl+p	以前に入力したコマンドを1つずつ表示する。
Ctrl+e	カーソルを行の最後に進める。	Ctrl+t	カーソル位置とその前1文字を入れ替える。
Ctrl+f	カーソルを1文字進める。	Ctrl+u、 Ctrl+w	カーソルまでの文字列を消去する。
Ctrl+h	カーソルの左の文字を削除する。	Ctrl+y	Ctrl+kで消去された文字列を貼り付ける。
Ctrl+i	コマンドを補完する。 <TAB> キーと同じ。	Ctrl+z	特権ユーザモードに移行する（ユーザモード時以外）。
Ctrl+j、 Ctrl+m	<Enter> と同じ。	<TAB> キー	コマンドを補完する。Ctrl+iと同じ。

【コマンド補完について】

入力した文字列に対して、コマンドやオプションが一意に決まる場合に有効です。

例) hostname コマンド（基本設定モード）を補完する。

h<TAB>	補完されない。hだけでは、hostname コマンドのほかには help コマンドなども存在するため。
ho<TAB>	補完される。ho で始まるコマンドは、hostname コマンドのほかにはないため。

何も入力しなくてもコマンドやオプションが一意に決まる場合にも使用できます。

例) configure terminal コマンド（特権ユーザモード）を補完する。

configure <TAB>	configure コマンドのオプションは "terminal" のみなので、何も入力しなくても <TAB> 入力で補完される。
-----------------	--

こんな事に気をつけて

- <TAB> キーによる補完は、カーソルがコマンド行の最後にある場合に有効です。
 - <SPACE> はコマンドやオプションの区切りとして使用します。
- 入力した文字列でコマンドが一意に決まる場合は、後ろの文字列を入力しなくてもコマンドは認識されます。
- 例) "hostname GX500" を設定する場合、"ho GX500<Enter>" でも設定可能です。

1.2 使用可能文字

コマンドに使用する文字列の型により、使用不可な文字が異なります。

【CDATA型】

エスケープシーケンス、コントロールキャラクタ、および、日本語文字は使用できません。また、ASCIIコードで指定されている文字の中でも、以下の文字は使用できません。

ASCIIコード	文字
0x20	SP
0x21	!
0x22	"
0x26	&
0x27	'
0x3c	<
0x3e	>
0x3f	?
0x5c	¥
0x60	`
0x7c	

【CDATA-X型】

エスケープシーケンス、コントロールキャラクタ、および、日本語文字は使用できません。また、ASCIIコードで指定されている文字の中でも、以下の文字は使用できません。

ASCIIコード	文字
0x20	SP
0x21	!
0x22	"
0x26	&
0x27	'
0x2c	,
0x2f	/
0x3c	<
0x3e	>
0x3f	?
0x5c	¥
0x60	`
0x7c	

【WORD 型】

エスケープシーケンス、コントロールキャラクタ、および、日本語文字は使用できません。また、ASCII コードで指定されている文字の中でも、以下の文字は使用できません。

ASCII コード	文字
0x20	SP
0x21	!
0x22	"
0x27	'
0x3c	<
0x3e	>
0x3f	?
0x5c	¥
0x60	`
0x7c	

【TMNAME 型】

エスケープシーケンス、コントロールキャラクタ、および、日本語文字は使用できません。また、ASCII コードで指定されている文字の中でも、以下の文字は使用できません。文字列の先頭に "\$" は使えません。文字列中に開き括弧 "(" と閉じ括弧 ")" は使えません。

ASCII コード	文字
0x20	SP
0x21	!
0x22	"
0x27	'
0x3c	<
0x3e	>
0x3f	?
0x5c	¥
0x60	`
0x7c	

【STRING 型】

エスケープシーケンス、コントロールキャラクタ、および、日本語文字を使用することはできません。また、ASCII コードで指定されている文字の中でも、以下の文字は使用できません。

ASCII コード	文字
0x20	SP
0x3f	?

【FILENAME 型】

エスケープシーケンス、コントロールキャラクタ、および、日本語文字は使用できません。また、ASCII コードで指定されている文字の中でも、以下の文字は使用できません。

ASCII コード	文字
0x20	SP
0x22	"
0x2a	*
0x2c	,
0x3a	:
0x3b	;
0x3c	<
0x3e	>
0x3f	?
0x5c	¥
0x7c	

【DOMAINWORD 型】

大文字 (A～Z)、小文字 (a～z)、数字 (0～9)、ハイフン (-)、ドット (.) のみが使用可能です。大文字、小文字は区別して扱われます。

文字列をドットで区切る形式であり、その各文字列の先頭は必ずアルファベットでなければなりません。また、文字列の最後にハイフンは使えません。

ドット間の文字列の長さは63文字以内であり、それを超えて使用することはできません。

1.3 コマンドプロンプト

1.3.1 hostname

【機能】

ホスト名の設定

【入力形式】

hostname <ホスト名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ホスト名	ホスト名を指定します。	254 文字以内の WORD 型	省略不可

【動作モード】

基本設定モード

【説明】

ホスト名を設定します。プロンプトのほかにも、ログのホスト名や TELNET でログインする場合のホスト名として使用します。

【実行例】

ホスト名を設定します（ホスト名：GX500）。

```
#configure terminal
(config)#hostname GX500
(config)#
```

【未設定時】

モードを示す文字列のみがプロンプトとなります。ログや TELNET のホスト名は空白となります。

1.4 コマンドレベル

各コマンドには 0～15 のレベル（コマンドレベル）があり、ユーザレベル (privilege-level) に従って実行できるコマンドが規定されています。ユーザレベル以上のレベルを持つコマンドは実行できません。

各コマンドのコマンドレベルは、privilege コマンドで指定できます。

ユーザレベルを指定するには、以下の 2 つの方法があります。

- ログイン後の enable コマンドのオプションで指定

例) ユーザレベル 14 に移行する場合

```
>enable 14
password:
#
```

- ユーザごとにログイン後のユーザレベルを指定

例) ユーザ名：user-A（パスワード：admin123）にレベル 14 を割り当てる場合

```
username user-A privilege 14 password admin123
aaa authorization exec user-A local
```

1.4.1 privilege

【機能】

コマンドレベルの設定

【入力形式】

privilege {exec | configure | <コマンドモード移行コマンド名>} [all] {level <コマンドレベル> <コマンド名> | reset}

no privilege {exec | configure | <コマンドモード移行コマンド名>} [all] level <コマンドレベル> <コマンド名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
exec configure <コマンドモード移行コマンド名>	コマンドモード移行コマンド名を指定します。	exec: 実行コマンド configure: 設定コマンド コマンドモード移行コマンド名	省略不可
all	指定したコマンドのすべてのオプションに適用する場合に指定します。	-	指定したコマンドのみ適用
コマンドレベル	コマンドレベルを指定します。	0～15	省略不可
コマンド名	コマンド名を指定します。	64 文字以内の STRING 型	
reset	コマンドレベルを一時的にデフォルトに戻す場合に指定します。	-	本設定が有効

【動作モード】

基本設定モード

【説明】

コマンドごとにコマンドレベルを設定します。ユーザモードで実行できるコマンドのコマンドレベルを指定する場合は "exec"、基本設定モードで設定できるコマンドのコマンドレベルを指定する場合は "configure"、各種コマンドモードに移行したあとに設定できるコマンドのコマンドレベルを指定する場合は、"コマンドモード移行コマンド名" を指定します。

【実行例】

コマンドレベルを設定します (exec、コマンドレベル：1、コマンド名：show version)。

```
#configure terminal
(config)#privilege exec level 1 show version
```

コマンドレベルを設定します (configure、コマンドレベル：10、コマンド名：telnet-server shutdown)。

```
#configure terminal
(config)#privilege configure level 10 telnet-server shutdown
```

コマンドレベルを設定します (configure、all、コマンドレベル：11、コマンド名：telnet-server)。

```
#configure terminal
(config)#privilege configure all level 11 telnet-server
```

コマンドレベルを設定します (コマンドモード移行コマンド名：interface port-channel、コマンドレベル：13、コマンド名：ip address)。

```
#configure terminal
(config)#privilege interface port-channel level 13 ip address
```

コマンドレベルをデフォルトに戻します (コマンドモード移行コマンド名：interface port-channel、コマンドレベル：13、コマンド名：ip address)。

```
#configure terminal
(config)#no privilege interface port-channel level 13 ip address
```

【未設定時】

コマンドレベルはデフォルトで動作します。

1.4.2 show privilege

【機能】

コマンドレベルの表示

【入力形式】

show privilege

【動作モード】

ユーザモード

【説明】

現在のコマンドレベルを表示します。

【実行例】

コマンドレベルを設定します。

```
#show privilege  
  
Current privilege level is 15  
  
#
```

【各フィールドの意味】

Current privilege level is

.....現在のコマンドレベルを表示します。

1.5 コマンドモード

コマンドラインインタフェースは、さまざまなコマンドモードに分かれます。コマンドモードごとに入力可能なコマンドが定義され、コマンドモードに移行することでコマンドの入力が可能となります。ヘルプ機能で表示されるコマンドは、そのコマンドモードにおいて利用可能なもののみであり、他のコマンドモードのコマンドが表示されることはありません。

以下に、コマンドモード一覧を示します。

コマンドモード	モードへ入る方法	プロンプト文字列	モードから抜ける方法
ユーザモード	ログインまたは特権ユーザモードで disable コマンド入力	>	exit コマンドでログアウト
特権ユーザモード	ユーザモードで enable コマンド入力	#	disable コマンドでユーザモードへ移行
基本設定モード	特権ユーザモードで configure terminal コマンド入力	(config)#	end コマンドで特権ユーザモードへ移行
CLIENT-データベース設定モード	基本設定モードで aaa local group コマンド入力	(config-lg-user)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
CLIENT-RADIUS サーバ設定モード	基本設定モードで aaa group server radius コマンド入力	(config-sg-radius)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
Pre-shared Key リング設定モード	基本設定モードで crypto keyring コマンド入力	(config-keyring)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
ISAKMP グループポリシー設定モード	基本設定モードで crypto isakmp client configuration group コマンド入力	(config-isakmp-group)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
ISAKMP ポリシー設定モード	基本設定モードで crypto isakmp policy コマンド入力	(config-isakmp)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
ISAKMP プロファイル設定モード	基本設定モードで crypto isakmp profile コマンド入力	(conf-isa-prof)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
IPSEC ポリシー設定モード	基本設定モードで crypto ipsec policy コマンド入力	(conf-ipsec)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
IPSEC セレクタ設定モード	基本設定モードで crypto ipsec selector コマンド入力	(config-ip-selector)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行

コマンドモード	モードへ入る方法	プロンプト文字列	モードから抜ける方法
VPN セレクタ設定モード	基本設定モードで crypto map コマンド入力	(config-crypto-map)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
動的 VPN プロファイル設定モード	基本設定モードで dvpn profile コマンド入力	(dvpn-prof)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
動的 VPN クライアント設定モード	基本設定モードで dvpn client コマンド入力	(conf-dvpn-client)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
gigaethernet インタフェース設定モード	基本設定モードで interface gigaethernet コマンド入力	(config-if-ge 1/1)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
gigaethernet サブインタフェース設定モード	基本設定モードで interface gigaethernet コマンド入力	(config-if-ge 1/1.1)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
management インタフェース設定モード	基本設定モードで interface management コマンド入力	(config-if-manage 1)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
loopback インタフェース設定モード	基本設定モードで interface loopback コマンド入力	(config-if-lo 1)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
port-channel インタフェース設定モード	基本設定モードで interface port-channel コマンド入力	(config-if-ch 1)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
tunnel インタフェース設定モード	基本設定モードで interface tunnel コマンド入力	(config-if-tun 1)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
trunk-channel インタフェース設定モード	基本設定モードで interface trunk-channel コマンド入力	(config-if-tr 1)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
trunk-channel サブインタフェース設定モード	基本設定モードで interface trunk-channel コマンド入力	(config-if-tr 1.1)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
USB Ethernet インタフェース設定モード	基本設定モードで interface usb-ethernet コマンド入力	(config-if-usb 1)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行

コマンドモード	モードへ入る方法	プロンプト文字列	モードから抜ける方法
RIP サービス設定モード	基本設定モードで router rip コマンド入力	(config-rip)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
OSPF サービス設定モード	基本設定モードで router ospf コマンド入力	(config-ospf)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
OSPF-VRF サービス設定モード	基本設定モードで router ospf-vrf コマンド入力	(config-ospf-vrf vrf-A 1 daemon-id 1)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
BGP サービス設定モード	基本設定モードで router bgp コマンド入力	(config-bgp)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
address-family ipv4 設定モード	BGP サービス設定モードで address-family ipv4 unicast コマンド入力	(config-af ipv4 unicast)#	exit コマンドで BGP サービス設定モードへ移行 end コマンドで特権ユーザモードへ移行
address-family ipv6 設定モード	BGP サービス設定モードで address-family ipv6 unicast コマンド入力	(config-af ipv6 unicast)#	exit コマンドで BGP サービス設定モードへ移行 end コマンドで特権ユーザモードへ移行
address-family ipv4 VRF 設定モード	BGP サービス設定モードで address-family ipv4 vrf コマンド入力	(config-af ipv4 vrf vrf-A)#	exit コマンドで BGP サービス設定モードへ移行 end コマンドで特権ユーザモードへ移行
address-family ipv6 VRF 設定モード	BGP サービス設定モードで address-family ipv6 vrf コマンド入力	(config-af ipv6 vrf vrf-A)#	exit コマンドで BGP サービス設定モードへ移行 end コマンドで特権ユーザモードへ移行
OSPF6 サービス設定モード	基本設定モードで router ipv6 ospf コマンド入力	(config-ospf6)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
route-map 設定モード	基本設定モードで route-map コマンド入力	(config-rmap route-map-A permit 1)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
survey-map 設定モード	基本設定モードで survey-map コマンド入力	(config-svmap survey-map-A)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
ライン設定モード (コンソール/ TELNET ポートの 設定)	基本設定モードで line コマンド入力	(config-line)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行

コマンドモード	モードへ入る方法	プロンプト文字列	モードから抜ける方法
policy-map 設定モード	基本設定モードで policy-map コマンド入力	(config-pmap)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
policy-map-class 設定モード	policy-map 設定モードで class コマンド入力	(config-pmap-c)#	exit コマンドで policy-map 設定モードへ移行 end コマンドで特権ユーザモードへ移行
policy-route-map 設定モード	基本設定モードで policy-route-map コマンド入力	(config-prmap-c)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
policy-route-map-class 設定モード	policy-route-map 設定モードで class コマンド入力	(config-pmap-c)#	exit コマンドで policy-route-map 設定モードへ移行 end コマンドで特権ユーザモードへ移行
class-map 設定モード	基本設定モードで class-map コマンド入力	(config-cmap)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
environment プロファイル設定モード	基本設定モードで environment profile コマンド入力	(config-env-profile)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
syslog filter 設定モード	基本設定モードで syslog filter コマンド入力	(config-syslog-filter)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
traffic-manager network 設定モード	基本設定モードで traffic-manager network コマンド入力	(config-tm-n)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
traffic-manager-network-bandwidth プロファイル設定モード	traffic-manager network 設定モードで bandwidth profile コマンド入力	(config-tm-n-bw-t bw-A)#	exit コマンドで traffic-manager network 設定モードへ移行 end コマンドで特権ユーザモードへ移行
traffic-manager-network-port プロファイル設定モード	traffic-manager network 設定モードで port profile コマンド入力	(config-tm-n-port port-A)#	exit コマンドで traffic-manager network 設定モードへ移行 end コマンドで特権ユーザモードへ移行
traffic-manager-network-ids プロファイル設定モード	traffic-manager network 設定モードで ids profile コマンド入力	(config-tm-n-ids sample)#	exit コマンドで traffic-manager network 設定モードへ移行 end コマンドで特権ユーザモードへ移行

コマンドモード	モードへ入る方法	プロンプト文字列	モードから抜ける方法
traffic-manager extended 設定モード	基本設定モードで traffic-manager extended コマンド入力	(config-tm-n)#	exit コマンドで基本設定 モードへ移行 end コマンドで特権ユーザ モードへ移行
traffic-manager- extended-port プ ロファイル設定 モード	traffic-manager extended 設定 モードで port profile コマンド入力	(config-tm-e-port port-A)#	exit コマンドで traffic- manager extended 設定 モードへ移行 end コマンドで特権ユーザ モードへ移行
bfd-map 設定モード	基本設定モードで bfd-map コマン ド入力	(config-bfdmap bfd-map-A)#	exit コマンドで基本設定 モードへ移行 end コマンドで特権ユーザ モードへ移行
bridge 設定モード	基本設定モードで bridge-group コ マンド入力	(config-bridge 1)#	exit コマンドで基本設定 モードへ移行 end コマンドで特権ユーザ モードへ移行
イベントアクショ ン設定モード	基本設定モードで event-action コ マンド入力	(config-event-action)#	exit コマンドで基本設定 モードへ移行 end コマンドで特権ユーザ モードへ移行
PPPoE プロファ イル設定モード	基本設定モードで pppoe profile コ マンド入力	(config-pppoe-profile)#	exit コマンドで基本設定 モードへ移行 end コマンドで特権ユーザ モードへ移行
EtherIP プロファ イル設定モード	基本設定モードで ether-ip tunnel- profile コマンド入力	(config-ether-ip)#	exit コマンドで基本設定 モードへ移行 end コマンドで特権ユーザ モードへ移行
L2TPv3 プロファ イル設定モード	基本設定モードで l2tpv3 tunnel- profile コマンド入力	(config-l2tpv3)#	exit コマンドで基本設定 モードへ移行 end コマンドで特権ユーザ モードへ移行
L2TPv3 Pseudowire 設定 モード	基本設定モードで l2tpv3 pseudowire コマンド入力	(config-l2tpv3-pseudowire)#	exit コマンドで基本設定 モードへ移行 end コマンドで特権ユーザ モードへ移行
ipinip tunnel プ ロファイル設定モード	基本設定モードで ipinip tunnel- profile コマンド入力	(config-ipinip-profile)#	exit コマンドで基本設定 モードへ移行 end コマンドで特権ユーザ モードへ移行
ip dhcp client プ ロファイル設定モード	基本設定モードで ip dhcp client- profile コマンド入力	(config-dhcp PROF1)#	exit コマンドで基本設定 モードへ移行 end コマンドで特権ユーザ モードへ移行
ip dhcp server プ ロファイル設定 モード	基本設定モードで ip dhcp server- profile コマンド入力	(config-dhcps prof1)#	exit コマンドで基本設定 モードへ移行 end コマンドで特権ユーザ モードへ移行

コマンドモード	モードへ入る方法	プロンプト文字列	モードから抜ける方法
ip dhcp host-database 設定モード	基本設定モードで ip dhcp host-database コマンド入力	(config-dhcp-host)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
ipv6 dhcp client プロファイル設定モード	基本設定モードで ipv6 dhcp client-profile コマンド入力	(config-dhcp6 PROF1)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
ipv6 dhcp server プロファイル設定モード	基本設定モードで ipv6 dhcp server-profile コマンド入力	(config-dhcps6 prof1)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
ipv6 dhcp host-database 設定モード	基本設定モードで ipv6 dhcp host-database コマンド入力	(config-dhcp6-host)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
SIP RADIUS 認証プロファイル設定モード	基本設定モードで ngn sip profile-radius コマンド入力	(sip-prof-radius)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
SIP プロファイル設定モード	基本設定モードで ngn sip profile コマンド入力	(sip-prof)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
データコネク用 policy-map 設定モード	基本設定モードで dataconnect-policy-map コマンド入力	(config-dcpmap 100)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
モデムプロファイル設定モード	基本設定モードで modem profile コマンド入力	(config-modem-profile)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
VRF 設定モード	ip vrf コマンド	(config-vrf vrf-A)#	exit コマンドで基本設定モードへ移行 end コマンドで特権ユーザモードへ移行
メンテナンスモード	ターミナルソフトウェアでコンソールに接続し、本装置の起動開始時に約 10 秒間 Ctrl+x キーを押し続ける	MAINT>	quit コマンドまたは exit コマンドで起動シーケンスを再開

1.5.1 configure terminal

【機能】

基本設定モードへの移行

【入力形式】

configure terminal

【動作モード】

特権ユーザモード（コマンドレベル 14）

【説明】

基本設定モードに移行します。

【実行例】

基本設定モードに移行します。

```
#configure terminal
(config)#
```

1.5.2 disable

【機能】

ユーザレベルへの移行

【入力形式】

disable [<ユーザレベル>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ユーザレベル	移行するユーザレベルを指定します。	0 ～ 15	1

【動作モード】

ユーザモード、特権ユーザモード（コマンドレベル 14）

【説明】

ユーザレベルを移行します。高いユーザレベルから低いユーザレベルへの移行ができます。

【実行例】

ユーザレベルを移行します（ユーザレベル：1）。

```
#disable
>
```

1.5.3 enable

【機能】

ユーザレベルへの移行

【入力形式】

enable [<ユーザレベル>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ユーザレベル	移行するユーザレベルを指定します。	0 ～ 15	15

【動作モード】

ユーザモード

【説明】

ユーザレベルを移行します。上位のユーザレベルに移行する際は、パスワードの入力が必要となります。特権ユーザモードのユーザレベルにより、使用できるコマンドが異なります。

【実行例】

ユーザレベルを移行します（ユーザレベル：7）。

```
>enable 7
password:admin123
#
```

1.5.4 exit

【機能】

元のモードへの復帰

【入力形式】

exit

【動作モード】

基本設定モード以外のすべてのモード

【説明】

現在のモードを終了し、元のモードに復帰します。ユーザモードと特権ユーザモードの場合はログアウトします。基本設定モードはendコマンドで終了してください。

【実行例】

基本設定モードに移行します。

```
#configure terminal
(config)#interface management 1
(config-if-manage 1)#exit
(config)#
```

1.5.5 end

【機能】

特権ユーザモードへの移行

【入力形式】

end

【動作モード】

ユーザモード、特権ユーザモード以外のすべてのモード

【説明】

モードを終了し、特権ユーザモードに移行します。

【実行例】

特権ユーザモードに移行します。

```
#configure terminal
(config)#end
#
```

1.6 コマンドヘルプ

1.6.1 help

【機能】

ヘルプの表示

【入力形式】

help

【動作モード】

すべてのモード

【説明】

"?" によるヘルプシステムの簡易解説が表示されます。

【実行例】

簡易解説を表示します。

```
>help
```

1.7 コマンドヒストリ

1.7.1 show history

【機能】

過去に実行したコマンド履歴の表示

【入力形式】

show history

【動作モード】

すべてのモード

【説明】

過去に実行したコマンドの履歴を表示します。

ユーザモードと設定モードのコマンド履歴を合わせて 100 件分まで表示できます。

【実行例】

過去に実行したコマンドの履歴を表示します。

```
#show history
enable
show calendar
show uptime
show history
#
```

1.8 コマンドログ

1.8.1 show command-log

【機能】

コマンド履歴（実行時刻・端末名・実行ユーザ名）の表示

【入力形式】

show command-log [last-messages] [reverse]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
last-messages	装置再起動前のコマンド履歴のみを表示する場合に指定します。	-	装置再起動後のコマンド履歴も表示
reverse	時系列を逆に表示する場合に指定します。	-	古い順
なし	装置再起動後のコマンド履歴を古い順に表示する場合に指定します。	-	-

【動作モード】

特権ユーザモード（コマンドレベル 15）

【説明】

全ユーザの発行したコマンド履歴（実行時刻・端末名・実行ユーザ名）を表示します。

【実行例】

コマンド履歴を表示します。

```
#show command-log

2013/01/01 00:00:00 ttyS0 operator >enable
2013/01/01 00:00:00 ttyS0 operator #show running.cfg
2013/01/01 00:00:00 pts/0 operator >enable
2013/01/01 00:00:00 pts/0 operator >enable
2013/01/01 00:00:00 pts/0 operator #exit
2013/01/01 00:00:00 pts/0 operator >enable
2013/01/01 00:00:00 pts/0 operator #show calendar
2013/01/01 00:00:00 pts/0 operator #show uptime
2013/01/01 00:00:00 pts/0 operator #show history
2013/01/01 00:00:00 pts/0 operator #show command-log
#
```

1.9 コマンドエイリアス

1.9.1 alias

【機能】

エイリアス（省略コマンド登録）の設定

【入力形式】

alias <エイリアス名> <コマンド>

no alias <エイリアス名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エイリアス名	登録する省略形コマンド名を指定します。	254 文字以内の WORD 型	省略不可
コマンド	省略するコマンドを指定します。	254 文字以内の WORD 型 (*1)	

*1) 1 文字の空白（スペース）は使用可能です。複数の空白（スペース）は 1 文字にまとめられます。

【動作モード】

基本設定モード

【説明】

エイリアス（省略コマンド登録）を設定します。

【注意】

エイリアス名に既存のコマンドを設定しないでください。

【設定してはいけない例】

```
alias save save /drive/boot.cfg
```

save コマンドがすでに存在するため、このような設定はできません。

【実行例】

エイリアスを設定します（エイリアス名：sv、コマンド：show version）。

```
#configure terminal
(config)#alias sv show version
```

1.9.2 show alias

【機能】

設定したコマンドエイリアス情報の表示

【入力形式】

show alias

【動作モード】

ユーザモード

【説明】

設定したコマンドエイリアス情報を表示します。

【実行例】

設定したコマンドエイリアス情報を表示します。

```
#show alias  
  
a alias  
c configure terminal  
e exit  
r refresh  
  
#
```


第2章 装置の設定



この章では、本装置の設定に関するコマンドについて説明します。

2.1	時刻に関する設定	54
2.2	パスワードの設定	63
2.3	端末の設定	65
2.4	TELNET サーバの設定	69
2.5	SSH サーバの設定	71
2.6	FTP サーバの設定	76
2.7	NTP サーバの設定	78
2.8	DNS サーバの設定	79
2.9	認証／許可の設定	86
2.10	ユーザ認証用 RADIUS サーバの設定	97
2.11	ユーザ認証用 TACACS+ サーバの設定	100
2.12	TACACS+ アカウンティングの設定	104
2.13	バナー表示の設定	111
2.14	設定情報の設定	113
2.15	ファームウェアの設定	115
2.16	装置情報の設定	117

2.1 時刻に関する設定

本装置では、Network Time Protocol(NTP)による時刻同期を推奨します。

NTPによる時刻同期を使用しない場合には、装置電源投入時に時刻を確認し、calendar set コマンドで現在時刻を設定してください。

2.1.1 clock summer-time

【機能】

サマータイムの設定

【入力形式】

clock summer-time <ゾーン名> recurring [<開始週> <開始曜日> <開始月 1> <開始時刻 1> <終了週> <終了曜日> <終了月 1> <終了時刻 1> [<オフセット時間 1>]]

clock summer-time <ゾーン名> date <開始月 2> <開始日> <開始年> <開始時刻 2> <終了月 2> <終了日> <終了年> <終了時刻 2> [<オフセット時間 2>]

no clock summer-time

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ゾーン名	ゾーン名を指定します。	254 文字以内の WORD 型	省略不可
recurring date	日時の設定方法を指定します。	-	
開始週	開始週を指定します。	1～6	常時
開始曜日	開始曜日を指定します。	254 文字以内の WORD 型	
開始月 1	開始月を指定します。	254 文字以内の WORD 型	
開始時刻 1	開始時刻を指定します。	時：分	
終了週	終了週を指定します。	1～6	
終了曜日	終了曜日を指定します。	254 文字以内の WORD 型	
終了月 1	終了月を指定します。	254 文字以内の WORD 型	
終了時刻 1	終了時刻を指定します。	時：分	
オフセット時間 1	オフセット時刻を指定します。	254 文字以内の WORD 型	1
開始月 2	開始月を指定します。	254 文字以内の WORD 型	省略不可
開始日	開始日を指定します。	254 文字以内の WORD 型	
開始年	開始年を指定します。	4 桁の西暦	
開始時刻 2	開始時刻を指定します。	時：分	
終了月 2	終了月を指定します。	254 文字以内の WORD 型	
終了日	終了日を指定します。	254 文字以内の WORD 型	
終了年	終了年を指定します。	4 桁の西暦	
終了時刻 2	終了時刻を指定します。	時：分	
オフセット時間 2	オフセット時間を指定します。	254 文字以内の WORD 型	1

【動作モード】

基本設定モード

【説明】

サマータイムの開始時期と終了時期、およびサマータイム適用時のオフセット時間を設定します。設定の方法として第何週の何曜日の何時という指定と、カレンダー上の日付の何時という指定ができます。
recurringのあとをすべて省略した場合は、常にサマータイムが適用されます。

オフセット時間を省略した場合は1時間として扱われます。日付指定の場合、終了日時については、標準表記ではなくサマータイム表記とします。

【実行例】

サマータイムの開始時期と終了時期、およびサマータイム適用時のオフセット時刻を設定します（ゾーン名：JST、recurring、開始週：第4週、開始曜日：月曜日、開始月：6月、開始時刻：02:00、終了週：第1週、終了曜日：月曜日、終了月：10月、終了時刻：02:00、オフセット時間：+4時間）。

```
#configure terminal
(config)#clock summer-time JST recurring 4 mon jun 02:00 1 mon oct 02:00 +4
```

【未設定時】

サマータイム考慮なしで動作します。

2.1.2 clock timezone

【機能】

タイムゾーンの設定

【入力形式】

clock timezone <タイムゾーン名> <hours-offset>:<minutes-offset>

no clock timezone

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
タイムゾーン名	タイムゾーン名を指定します。	254文字以内のWORD型	省略不可
hours-offset	オフセット（単位：時）を指定します。	-	
minutes-offset	オフセット（単位：分）を指定します。	-	

【動作モード】

基本設定モード

【説明】

タイムゾーンを設定します。

【実行例】

タイムゾーンを設定します（タイムゾーン名：JST、hours-offset：09、minutes-offset：00）。

```
#configure terminal
(config)#clock timezone JST 09:00
```

【未設定時】

タイムゾーンは JST(UTC+09:00) で動作します。

2.1.3 ntp authenticate

【機能】

NTP 認証機能の設定

【入力形式】

ntp authenticate

no ntp authenticate

【動作モード】

基本設定モード

【説明】

NTP の認証機能を有効にする場合に設定します。

【実行例】

NTP の認証機能を有効にします。

```
#configure terminal
(config)#ntp authenticate
```

【未設定時】

NTP の認証機能は無効で動作します。

2.1.4 ntp authentication-key

【機能】

NTP 認証キーの設定

【入力形式】

ntp authentication-key <キー番号> md5 <認証キー>

no ntp authentication-key <キー番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
キー番号	キー番号を指定します。	1 ～ 4294967295	省略不可
認証キー	認証キーを指定します。	8文字以内の WORD 型	

【動作モード】

基本設定モード

【説明】

NTP の認証キーを設定します。

【実行例】

NTP の認証キーを設定します（キー番号：7、認証キー：authkey）。

```
#configure terminal
(config)#ntp authentication-key 7 md5 authkey
```

【未設定時】

NTP の認証機能は無効で動作します。

2.1.5 ntp server

【機能】

NTP サーバの登録

【入力形式】

```
ntp server <NTP サーバ> [linklocal-interface <インタフェース名 1> <インタフェース番号 1>] [version
<NTP バージョン>] [key <認証キー>] [source <インタフェース名 2> <インタフェース番号 2>] [prefer]
```

```
no ntp server <NTP サーバ> [linklocal-interface <インタフェース名 1> <インタフェース番号 1>]
[version <NTP バージョン>] [key <認証キー>] [source <インタフェース名 2> <インタフェース番号 2>]
[prefer]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
NTP サーバ	NTP サーバを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 ホスト名： 254 文字以内の WORD 型	省略不可
インタフェース名 1	NTP サーバに IPv6 リンクローカルアドレスを指定した場合のインタフェース名を指定します。	-	
インタフェース番号 1	NTP サーバに IPv6 リンクローカルアドレスを指定した場合のインタフェース番号を指定します。	-	
NTP バージョン	NTP バージョンを指定します。	1 ～ 4	3
認証キー	認証キーを指定します。	1 ～ 4294967295	サーバとの通信を暗号化しない
インタフェース名 2	送信元アドレスとして使用するインタフェース名を指定します。	-	送信インタフェース名
インタフェース番号 2	送信元アドレスとして使用するインタフェース番号を指定します。	-	送信インタフェース番号
prefer	優先的に問い合わせるサーバの場合に指定します。	-	非優先

【動作モード】

基本設定モード

【説明】

NTP サーバを登録します。複数登録した場合には、show current.cfg(show running.cfg) コマンドで表示される上位 20 個までが有効となります。21 個以上は設定上、無効となります。本設定は、設定順にソートされます。

なお、登録した複数の NTP サーバ間で時刻差が生じている場合は、すべてを信頼性が低いサーバと見なし、時刻同期しない場合がありますので注意してください。

【実行例】

NTP サーバを登録します (NTP サーバ：192.0.2.1)。

```
#configure terminal
(config)#ntp server 192.0.2.1
```

【未設定時】

NTP による現在時刻の問い合わせを行いません。

2.1.6 ntp source

【機能】

NTP パケットの送信元アドレスとして使用するインタフェースの設定

【入力形式】

ntp source <インタフェース名> <インタフェース番号>

no ntp source

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース名	送信元アドレスとして使用するインタフェース名を指定します。	-	省略不可
インタフェース番号	送信元アドレスとして使用するインタフェース番号を指定します。	-	

【動作モード】

基本設定モード

【説明】

NTP パケットを送信する際の送信元アドレスとして使用するインタフェースを設定します。

【実行例】

NTP パケットを送信する際の送信元アドレスとして使用するインタフェースを設定します (インタフェース名：loopback、インタフェース番号：1)。

```
#configure terminal
(config)#ntp source loopback 1
```

【未設定時】

送信元アドレスは送信インタフェースのアドレスとなります。

2.1.7 ntp trusted-key

【機能】

信用できる認証キーのキー番号の設定

【入力形式】

ntp trusted-key <キー番号>

no ntp trusted-key <キー番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
キー番号	キー番号を指定します。	1～4294967295	省略不可

【動作モード】

基本設定モード

【説明】

NTPの信用できる認証キーのキー番号を設定します。

【実行例】

信用できる認証キーのキー番号を設定します（キー番号：100）。

```
#configure terminal
(config)#ntp trusted-key 100
```

【未設定時】

NTP 認証キーなしで動作します。

2.1.8 sntp poll-interval

【機能】

時刻同期する間隔の設定

【入力形式】

sntp poll-interval <Polling 間隔>

no sntp poll-interval [<Polling 間隔>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
Polling 間隔	SNTP サーバへリクエストを送信して時刻同期する間隔（単位：秒）を指定します。"off"を指定すると、装置起動時に一度だけリクエストを送信して時刻同期します。	60～86400 off	省略不可

【動作モード】

基本設定モード

【説明】

SNTP サーバへリクエストを送信して時刻同期を行う間隔を設定します。

【実行例】

時刻同期を行う間隔を設定します（Polling 間隔：10 分（600 秒））。

```
#configure terminal
(config)#sntp poll-interval 600
```

【未設定時】

1 時間（3600 秒）間隔で時刻同期を行います。

2.1.9 sntp retry

【機能】

再送回数、再送間隔の設定

【入力形式】

sntp retry limit <再送回数> interval <再送間隔>

no sntp retry [limit <再送回数> interval <再送間隔>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
再送回数	SNTP サーバから応答がなかった場合の再送回数を指定します。 "0"を指定した場合は再送は行いません。	0～10	省略不可
再送間隔	SNTP サーバから応答がなかった場合の再送間隔（単位：秒）を指定します。	5～1024	省略不可

【動作モード】

基本設定モード

【説明】

SNTP サーバからの応答がなかった場合の再送回数、再送間隔を設定します。

【実行例】

再送回数、再送間隔を設定します（再送回数：4、再送間隔：30 秒）。

```
#configure terminal
(config)#sntp retry limit 4 interval 30
```

【未設定時】

回数 5 回、再送間隔 64 秒で動作します。

2.1.10 sntp server

【機能】

SNTP サーバの設定

【入力形式】

sntp server dhcp <DHCP クライアントインタフェース> [version <NTP バージョン>] [source <送信元インタフェース>]

sntp server <SNTP サーバ> [linklocal-interface <IPv6 インタフェース>] [version <NTP バージョン>]
[source <送信元インタフェース>]

no sntp server [dhcp <DHCP クライアントインタフェース> [version <NTP バージョン>] [source <送信元インタフェース>]]

no sntp server [<SNTP サーバ> [linklocal-interface <IPv6 インタフェース>] [version <NTP バージョン>]
[source <送信元インタフェース>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
dhcp	DHCP クライアントとして動作時に DHCP サーバから取得した SNTP サーバを指定します。	-	DHCP サーバから取得した SNTP サーバを使用しない
DHCP クライアントインタフェース	DHCP クライアントが動作しているインタフェースを指定します。	-	省略不可
送信元インタフェース	SNTP パケットの送信元アドレスとして使用するインタフェースを指定します。	-	省略不可
SNTP サーバ	SNTP サーバを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 ホスト名：254 文字以内の WORD 型	省略不可
IPv6 インタフェース	SNTP サーバに IPv6 リンクローカルアドレスを指定した場合のインタフェースを指定します。	-	省略不可
NTP バージョン	NTP バージョンを指定します。	1～4	4

【動作モード】

基本設定モード

【説明】

接続する SNTP サーバおよび、NTP バージョンを設定します。

サーバはスタティックに IPv4 アドレス、IPv6 アドレス、ホスト名のどちらかを指定して設定できます。
設定できるサーバの数は1つとなります。

また、DHCP クライアントが動作している場合、DHCP サーバから取得したサーバを使用することもできます。以下のオプションに含まれているサーバを使用します。

DHCPv4 NTP servers option(42)

DHCPv6 option-code:OPTION_Sntp_SERVERS(31)

【実行例】

SNTP サーバを設定します (SNTP サーバ：100.0.0.10)。

```
#configure terminal
(config)#sntp server 100.0.0.10
```

【未設定時】

SNTP クライアントとして動作しません。

2.2 パスワードの設定

2.2.1 password enable

【機能】

特権ユーザパスワードの設定

【入力形式】

password enable [level <ユーザレベル>] <パスワード>

no password enable level <ユーザレベル>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ユーザレベル	ユーザレベルを指定します。	1 ～ 15	15
パスワード	特権ユーザパスワードを指定します。	30 文字以内の STRING 型	省略不可

【動作モード】

特権ユーザモード（コマンドレベル 15）

【説明】

特権ユーザパスワードを設定します。レベルごとにパスワードを指定できます。

なお、本パスワードは設定情報には保存されません（装置の内部領域に保存されます）。

8 文字未満、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、以下のようなメッセージが表示されます。

入力したパスワード長が 0、またはパスワードを削除した場合：

"<WARNING> weak enable password: set the password"

入力したパスワード長が 8 文字未満：

"<WARNING> weak enable password: contain at least 8 characters"

入力したパスワードが英字または数字のみ：

"<WARNING> weak enable password: contain a different kind of character"

【実行例】

特権ユーザパスワードを設定します（ユーザレベル：15、パスワード：admin123）。

```
#password enable level 15 admin123
```

【未設定時】

enable パスワードは NULL（Enter のみを入力）で動作します。

2.2.2 password login

【機能】

ログインパスワードの設定

【入力形式】

password login <パスワード>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
パスワード	ログインパスワードを指定します。	30文字以内のSTRING型	省略不可

【動作モード】

特権ユーザモード（コマンドレベル 15）

【説明】

ログインパスワードを設定します。ログインパスワードは、aaa authentication login コマンドで "login" を指定した場合、または aaa authentication login コマンド設定がない場合のパスワード（ログインIDは operator）となります。

なお、本パスワードは設定情報には保存されません（装置の内部領域に保存されます）。

8文字未満、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、以下のようなメッセージが表示されます。

入力したパスワード長が0、またはパスワードを削除した場合：

"<WARNING> weak login password: set the password"

入力したパスワード長が8文字未満：

"<WARNING> weak login password: contain at least 8 characters"

入力したパスワードが英字または数字のみ：

"<WARNING> weak login password: contain a different kind of character"

【実行例】

ログインパスワードを設定します（パスワード：admin123）。

```
#password login admin123
```

2.3 端末の設定

2.3.1 line

【機能】

ライン設定モードへの移行

【入力形式】

line {console | telnet}

no line {console | telnet}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
console telnet	設定するログイン媒体を指定します。	console : コンソール telnet : TELNET	省略不可

【動作モード】

基本設定モード

【説明】

ライン設定モードに移行します。コマンドの先頭に "no" を指定することで、該当ライン設定モードの内容がすべて消去されます。

【実行例】

ライン設定モードに移行します（ログイン媒体：コンソール）。

```
#configure terminal
(config)#line console
(config-line)#
```

2.3.2 exec-timeout

【機能】

自動ログアウト時間の設定

【入力形式】

exec-timeout <自動ログアウト時間>

no exec-timeout

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
自動ログアウト時間	自動ログアウト時間（単位：分）を指定します。ここで設定した時間、入力がない場合は、自動的にログアウトします。	0～60	省略不可

【動作モード】

ライン設定モード

【説明】

自動ログアウト時間（単位：分）を設定します。自動ログアウトしない場合は"0"を指定します。

【実行例】

自動ログアウト時間を設定します（自動ログアウト時間：5分）。

```
#configure terminal
(config)#line console
(config-line)#exec-timeout 5
```

【未設定時】

自動ログアウト時間は30分で動作します。

2.3.3 login authentication

【機能】

ライン設定モードに対する認証方式の設定

【入力形式】

login authentication {enable | oldstyle}

no login authentication

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
enable oldstyle	認証方式を指定します。	enable:enable パスワード oldstyle: ライン設定モードのパスワード	省略不可

【動作モード】

ライン設定モード（コンソールのみ）

【説明】

ライン設定モードに対する認証方式を設定します。

このコマンドを設定した場合は、ログイン時にパスワードの問い合わせのみが行われます。

【実行例】

ライン設定モードに対する認証方式を設定します (enable)。

```
#configure terminal
(config)#line console
(config-line)#login authentication enable
```

【未設定時】

基本設定モードの aaa authentication コマンド設定に従います。

2.3.4 password

【機能】

パスワードの設定

【入力形式】

password {<パスワード> | <暗号化キー> <暗号化されたパスワード>}

no password

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
パスワード	パスワード文字列を指定します。	72文字以内のSTRING型	省略不可
暗号化キー (*1)	暗号化に使用するキーを指定します。	0～7	
暗号化されたパスワード	暗号化されたパスワード文字列を指定します。	13文字または34文字のSTRING型	

*1) すでに設定された username 情報を他の装置にコピーする場合に使用します。設定した username のパスワード情報は、暗号化されて装置内に格納されます。show current.cfg(show running.cfg) コマンドなどで内容を確認すると、<暗号化キー>と<暗号化されたパスワード>の形式で表示されます。表示された内容をそのまま他の装置に入力することで、パスワードをオープンにすることなく他の装置へコピーできます。

【動作モード】

ライン設定モード（コンソールのみ）

【説明】

login authentication oldstyle コマンドを設定した場合のパスワードを設定します。

【実行例】

login authentication oldstyle コマンドを設定した場合のパスワードを設定します（パスワード：admin123）。

```
#configure terminal
(config)#line console
(config-line)#password admin123
```

【未設定時】

パスワードなしで動作します。

2.3.5 prompt timestamp

【機能】

タイムスタンプ、CPU使用率、メモリ使用率の表示

【入力形式】

prompt timestamp {msec | sec}

no prompt timestamp [msec | sec]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
msec sec	タイムスタンプを秒単位で表示するか、ミリ秒単位で表示するかを指定します。	msec：ミリ秒単位 sec：秒単位	省略不可

【動作モード】

ライン設定モード

【説明】

各端末のコマンド実行結果に、タイムスタンプ、CPU使用率、メモリ使用率を表示する場合に設定します。

【実行例】

タイムスタンプ、CPU使用率、メモリ使用率を表示します（秒単位）。

```
#configure terminal
(config)#line console
(config-line)#prompt timestamp sec
```

【prompt timestamp secを設定後のコマンド実行結果】

```
#show calendar

CP utilization for five seconds: 3%/0%; one minute: 3%; five minutes: 2%
NP utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
SP utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
Total: 2822418432 Byte, Used: 716587008 Byte, Free: 2105831424 Byte
Tue Dec 26 17:40:23 JST 2017

Tue Dec 26 17:40:23 JST 2017
#
```

【未設定時】

タイムスタンプ、CPU使用率、メモリ使用率を表示しません。

2.4 TELNET サーバの設定

2.4.1 telnet-server access-class

【機能】

Telnet クライアントのフィルタリング

【入力形式】

telnet-server access-class <アクセスリスト番号>

no telnet-server access-class <アクセスリスト番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アクセスリスト番号	アクセスリスト番号を指定します。	-	省略不可

【動作モード】

基本設定モード

【説明】

指定したアクセスリストに従い、Telnet クライアントをフィルタリングします。許可と判断された時のみ、アクセスは許可されます。設定がない場合、および該当アクセスリストがない場合には、フィルタリング機能自体が動作せず、すべてのアクセスが許可されます。本設定は、設定順にソートされます。

【実行例】

Telnet クライアントをフィルタリングします（アクセスリスト番号：10）。

```
#configure terminal
(config)#telnet-server access-class 10
```

【未設定時】

すべての TELNET アクセスが許可されます。

2.4.2 telnet-server shutdown

【機能】

TELNET サーバ機能の停止

【入力形式】

telnet-server shutdown

no telnet-server shutdown

【動作モード】

基本設定モード

【説明】

TELNET サーバ機能を停止します。再度 TELNET サーバ機能を動作させる場合には、no telnet-server shutdown コマンドを設定します。

【実行例】

TELNET サーバ機能を停止します。

```
#configure terminal
(config)#telnet-server shutdown
```

【未設定時】

TELNET サーバ機能は動作します。

2.5 SSH サーバの設定

2.5.1 ip ssh authentication-retries

【機能】

SSH 認証失敗時のリトライ回数の設定

【入力形式】

ip ssh authentication-retries <リトライ回数>

no ip ssh authentication-retries

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
リトライ回数	認証失敗時のリトライ回数を指定します。	1～5	省略不可

【動作モード】

基本設定モード

【説明】

SSH の認証失敗時のリトライ回数を設定します。

【実行例】

SSH の認証失敗時のリトライ回数を設定します（リトライ回数：5 回）。

```
#configure terminal
(config)#ip ssh authentication-retries 5
```

【未設定時】

リトライ回数は 3 回で動作します。

2.5.2 ip ssh port

【機能】

SSH サーバが使用するポート番号の設定

【入力形式】

ip ssh port <ポート番号>

no ip ssh port [<ポート番号>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ポート番号	SSHサーバが使用するポート番号を指定します。	1025 ～ 65535	省略不可

【動作モード】

基本設定モード

【説明】

SSHサーバが使用するポート番号を設定します。

【実行例】

SSHサーバが使用するポート番号を設定します（ポート番号：2020）。

```
#configure terminal
(config)#ip ssh port 2020
```

【未設定時】

ポート番号は22で動作します。

2.5.3 ip ssh time-out

【機能】

SSHの認証可能時間を設定

【入力形式】

ip ssh time-out < 認証可能時間 >

no ip ssh time-out

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
認証可能時間	認証可能時間（単位：秒）を指定します。	1 ～ 120	省略不可

【動作モード】

基本設定モード

【説明】

SSHでユーザが認証を完了させるまでの認証可能時間（単位：秒）を設定します。

【実行例】

SSHの認証可能時間を設定します（認証可能時間：60 秒）。

```
#configure terminal
(config)#ip ssh time-out 60
```

【未設定時】

SSH の認証可能時間は 120 秒で動作します。

2.5.4 ip scp server enable

【機能】

Secure Copy の機能を有効にする設定

【入力形式】

ip scp server enable

no ip scp server enable

【動作モード】

基本設定モード

【説明】

Secure Copy の機能を有効にします。

【実行例】

Secure Copy の機能を有効にします。

```
#configure terminal
(config)#ip scp server enable
```

【未設定時】

Secure Copy は動作しません。

2.5.5 ip sftp server enable

【機能】

SFTP の機能を有効にする設定

【入力形式】

ip sftp server enable

no ip sftp server enable

【動作モード】

基本設定モード

【説明】

SFTP の機能を有効にします。

【実行例】

SFTPの機能を有効にします。

```
#configure terminal
(config)#ip sftp server enable
```

【未設定時】

SFTPは動作しません。

2.5.6 ssh-server access-class

【機能】

SSHクライアントのフィルタリング

【入力形式】

ssh-server access-class <アクセスリスト番号>

no ssh-server access-class <アクセスリスト番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アクセスリスト番号	アクセスリスト番号を指定します。	-	省略不可

【動作モード】

基本設定モード

【説明】

指定したアクセスリストに従い、SSHクライアントをフィルタリングします。許可と判断された場合のみ、アクセスは許可されます。設定がない場合、および該当アクセスリストがない場合には、フィルタリング機能自体が動作せず、すべてのアクセスが許可されます。該当するSSH認証用の鍵が生成されていない場合は、本設定は無効となります。本設定は、設定順にソートされます。

【実行例】

SSHクライアントをフィルタリングします（アクセスリスト番号：10）。

```
#configure terminal
(config)#ssh-server access-class 10
```

【未設定時】

すべてのSSHアクセスが許可されます。

2.5.7 ssh-server version

【機能】

SSHバージョンの設定

【入力形式】

ssh-server version {1 | 2}

no ssh-server version {1 | 2}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
1 2	SSHバージョンを指定します。	1:SSHバージョン1 2:SSHバージョン2	省略不可

【動作モード】

基本設定モード

【説明】

SSHバージョンを設定します。該当するSSH認証用の鍵が生成されていない場合、本設定は無効となります。

【実行例】

SSHバージョンを設定します (2)。

```
#configure terminal
(config)#ssh-server version 2
```

【未設定時】

SSH1 RSA 鍵はバージョン1、SSH2 RSA、およびSSH2 DSA 鍵はバージョン2で動作します。

2.6 FTP サーバの設定

2.6.1 ftp-server access-class

【機能】

FTP クライアントのフィルタリング

【入力形式】

ftp-server access-class <アクセスリスト番号>

no ftp-server access-class <アクセスリスト番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アクセスリスト番号	アクセスリスト番号を指定します。	-	省略不可

【動作モード】

基本設定モード

【説明】

指定したアクセスリストに従い、FTP クライアントをフィルタリングします。許可と判断された場合のみ、アクセスは許可されます。設定がない場合、および該当アクセスリストがない場合には、フィルタリング機能自体が動作せず、すべてのアクセスが許可されます。本設定は、設定順にソートされます。

【実行例】

FTP クライアントをフィルタリングします（アクセスリスト番号：10）。

```
#configure terminal
(config)#ftp-server access-class 10
```

【未設定時】

すべてのFTP アクセスが許可されます。

2.6.2 ftp-server exec-timeout

【機能】

無通信による自動切断時間の設定

【入力形式】

ftp-server exec-timeout <タイムアウト時間>

no ftp-server exec-timeout

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
タイムアウト時間	無通信による自動切断を行うまでの時間（単位：分）を指定します。	0～60	省略不可

【動作モード】

基本設定モード

【説明】

FTPクライアントとの接続中に、無通信による自動切断を行うまでの時間（単位：分）を設定します。
"0"を指定した場合は、120分で切断します。

【実行例】

無通信による自動切断を行うまでの時間（単位：分）を設定します（タイムアウト時間：10分）。

```
#configure terminal
(config)#ftp-server exec-timeout 10
```

【未設定時】

タイムアウト時間は30分で動作します。

2.6.3 ftp-server shutdown

【機能】

FTPサーバ機能の停止

【入力形式】

ftp-server shutdown

no ftp-server shutdown

【動作モード】

基本設定モード

【説明】

FTPサーバ機能を停止します。再度FTPサーバ機能を動作させる場合には、no ftp-server shutdown コマンドを設定します。

【実行例】

FTPサーバ機能を停止します。

```
#configure terminal
(config)#ftp-server shutdown
```

【未設定時】

FTPサーバ機能は動作します。

2.7 NTP サーバの設定

2.7.1 ntp-server enable

【機能】

NTP サーバの設定

【入力形式】

ntp-server enable [<stratum>]

no ntp-server enable [<stratum>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
stratum	NTP サーバ機能を使用する際の stratum 値を指定します。	1 ～ 15	8

【動作モード】

基本設定モード

【説明】

NTP サーバとして動作させる場合に設定します。

NTP サーバを enable にすると、すべての時刻問い合わせに関するパケットを受け付けるようになります。

stratum は、外部の NTP サーバとの通信が途絶えた場合に、自装置の時刻を設定した stratum 値としてクライアントに提供する設定です。外部サーバと通信している場合は、外部サーバの stratum+1 の値が自装置の stratum となります。

NTP サーバ機能は、外部の NTP サーバから時刻情報を受信していなくても利用可能ですが、時刻の精度が本装置の内蔵時計の精度となるため、NTP クライアント機能の設定を行い、外部の NTP サーバから時刻情報を受信するようにしてください。

【実行例】

NTP サーバとして動作させます (stratum : 5)。

```
#configure terminal
(config)#ntp-server enable stratum 5
```

【未設定時】

NTP サーバとして動作しません。

2.8 DNS サーバの設定

2.8.1 ip name-server

【機能】

DNS サーバアドレスの設定

【入力形式】

ip name-server <DNS サーバ> [source-interface <インタフェース名> <インタフェース番号>]

no ip name-server <DNS サーバ> [source-interface <インタフェース名> <インタフェース番号>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
DNS サーバ	DNS サーバを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
インタフェース名	送信元アドレスとして使用するインタフェース名を指定します。	-	ip name-server source-interface コマンド設定、または送信インタフェースのアドレス
インタフェース番号	送信元アドレスとして使用するインタフェース番号を指定します。	-	ip name-server source-interface コマンド設定、または送信インタフェースのアドレス

【動作モード】

基本設定モード

【説明】

DNS サーバのアドレスを設定します。IPv4、IPv6 含めて複数登録した場合には、show current.cfg(show running.cfg) コマンドで表示される上位 3 個までが有効となります。4 個以上は設定上、無効となります。本設定は、設定順に有効となります。

ip name-server source-interface コマンドより、本コマンドの "source-interface" 設定が優先されます。ip name-server source-interface コマンドもコマンドの "source-interface" 設定もない場合は、送信インタフェースのアドレスで動作します。

【実行例】

DNS サーバのアドレスを設定します (DNS サーバ : 192.0.2.1)。

```
#configure terminal
(config)#ip name-server 192.0.2.1 source-interface port-channel 1
```

【未設定時】

DNS サーバを登録しません。

2.8.2 ip name-server source-interface

【機能】

DNS サーバへのリクエストパケットの送信元アドレスとして使用するインタフェースの設定

【入力形式】

ip name-server source-interface <インタフェース名> <インタフェース番号>

no ip name-server source-interface

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース名	送信元アドレスとして使用するインタフェース名を指定します。	-	省略不可
インタフェース番号	送信元アドレスとして使用するインタフェース番号を指定します。	-	

【動作モード】

基本設定モード

【説明】

DNS サーバへのリクエストパケットを送信する際に、送信元アドレスとして使用するインタフェースを設定します。

【実行例】

送信元アドレスとして使用するインタフェースを設定します（インタフェース名：loopback、インタフェース番号：1）。

```
#configure terminal
(config)#ip name-server source-interface loopback 1
```

【未設定時】

ソースアドレスは送信インタフェースのアドレスで動作します。

2.8.3 dns-server enable

【機能】

DNS サーバ機能および ProxyDNS 機能の有効化

【入力形式】

dns-server {ip | ipv6} enable

no dns-server {ip | ipv6} enable

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ip ipv6	IPv4 か IPv6 かを指定します。	-	省略不可

【動作モード】

基本設定モード

【説明】

スタティック DNS サーバ機能および ProxyDNS 機能を有効にします。

自装置からの問い合わせに関しては、ip name-server に 127.0.0.1 を設定した場合に、ProxyDNS 対象になり proxydns 設定に従います。

【実行例】

スタティック DNS サーバ機能および ProxyDNS 機能を有効にします (IPv4、IPv6 両方)。

```
#configure terminal
(config)#dns-server ip enable
(config)#dns-server ipv6 enable
```

【未設定時】

DNS サーバ機能は動作しません。

2.8.4 dns-server access-class

【機能】

DNS クライアントのフィルタリングの設定

【入力形式】

dns-server access-class <アクセスリスト番号>

no dns-server access-class <アクセスリスト番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アクセスリスト番号	アクセスリスト番号を指定します。	-	省略不可

【動作モード】

基本設定モード

【説明】

指定したアクセスリストに従い、DNS クライアントをフィルタリングします。

許可と判断された場合のみ、アクセスは許可されます。設定がない場合、および該当アクセスリストがない場合には、フィルタリング機能自体が動作せず、すべてのアクセスが許可されます。

本設定は、設定順にソートされます。

【実行例】

DNS クライアントをフィルタリングします (アクセスリスト番号: 1)。

```
#configure terminal
(config)#dns-server access-class 1
```

【未設定時】

フィルタリング機能が動作しません。

2.8.5 proxydns domain

【機能】

ProxyDNS の正引き動作条件の設定

【入力形式】

proxydns domain <エントリ番号> <QTYPE 値> <ドメイン名> <送信元ネットワーク/プレフィックス長> {reject | static <プライマリ DNS サーバ IP アドレス> [<セカンダリ DNS サーバ IP アドレス>] | ipcp tunnel <tunnel インタフェース番号> | dhcp <DHCP クライアントインタフェース名> <DHCP クライアントインタフェース番号>} [source-interface <送信元インタフェース名> <送信元インタフェース番号>]

no proxydns domain <エントリ番号> [<QTYPE 値> <ドメイン名> <送信元ネットワーク> / <プレフィックス長> {reject | static <プライマリ DNS サーバ IP アドレス> [<セカンダリ DNS サーバ IP アドレス>] | ipcp tunnel <tunnel インタフェース番号> | dhcp <DHCP クライアントインタフェース名> <DHCP クライアントインタフェース番号>} [source-interface <送信元インタフェース名> <送信元インタフェース番号>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エントリ番号	エントリ番号を指定します。エントリ番号の小さい方が高優先となります。	1～32	省略不可
QTYPE 値	QTYPE 値を指定します。	1～11 13～65535 any：PTR(12)を除くすべてのタイプ	省略不可
ドメイン名	ドメイン名を指定します。	80文字以内のWORD型 *：0文字以上の任意の文字列	省略不可
送信元ネットワーク/ プレフィックス長	対象となる送信元ネットワーク/プレフィックス長を指定します。	IPv4 アドレス形式 IPv6 アドレス形式 any：すべてのネットワーク	省略不可
reject	リレー処理は行わず DNS クエリメッセージの破棄を指定します。	-	省略不可
static	リレー先 DNS サーバをアドレスで指定する場合に指定します。2つ指定した場合、両方にリレーし、先に受信した応答を返します。	-	省略不可
プライマリ DNS サーバ IP アドレス	プライマリ DNS サーバ IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
セカンダリ DNS サーバ IP アドレス	セカンダリ DNS サーバ IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	セカンダリ DNS サーバの指定なし
ipcp	tunnel インタフェースに IPCP で通知された DNS サーバ IP アドレスをリレー先に使用する場合に指定します。	-	省略不可

パラメタ	設定内容	設定範囲	省略時
tunnel インタフェース番号	tunnel インタフェース番号を指定します。	1～16777215	省略不可
dhcp	DHCP クライアントが取得した DNS サーバ IP アドレスをリレー先に使用する場合に指定します。	-	省略不可
DHCP クライアントインタフェース名	DHCP クライアントが動作しているインタフェース名を指定します。	-	省略不可
DHCP クライアントインタフェース番号	DHCP クライアントが動作しているインタフェース番号を指定します。	-	省略不可
送信元インタフェース名	DNS サーバへリレーする際の送信元アドレスとして使用するインタフェース名を指定します。	-	省略不可
送信元インタフェース番号	DNS サーバへリレーする際の送信元アドレスとして使用するインタフェース番号を指定します。	-	省略不可

【動作モード】

基本設定モード

【説明】

ProxyDNS の正引き動作条件を設定します。

ipcp、dhcp 指定をしており有効な DNS サーバ情報を取得できていない場合は、エントリ無効となります。

【実行例】

ProxyDNS の正引き動作条件の設定をします（エントリ番号：1、QTYPE 値：any、ドメイン名：*.example.co.jp、送信元ネットワーク/プレフィックス長：any、プライマリ DNS サーバ IP アドレス：172.16.100.5）。

```
#configure terminal
(config)#proxydns domain 1 any *.example.co.jp any static 172.16.100.5
```

【未設定時】

ProxyDNS 機能の正引きは動作しません。

2.8.6 proxydns address

【機能】

ProxyDNS の逆引き動作条件の設定

【入力形式】

proxydns address <エントリ番号> <逆引き対象アドレス/プレフィックス長> {reject | static <プライマリ DNS サーバ IP アドレス> [<セカンダリ DNS サーバ IP アドレス>]} | ipcp tunnel <tunnel インタフェース番号> | dhcp <DHCP クライアントインタフェース番号> [source-interface <送信元インタフェース名> <送信元インタフェース番号>]

no proxydns address <エントリ番号> [<逆引き対象アドレス/プレフィックス長> [reject | static <プライマリ DNS サーバ IP アドレス> [<セカンダリ DNS サーバ IP アドレス>] | ipcp tunnel <tunnel インタフェース番号>] | dhcp <DHCP クライアントインタフェース番号> [source-interface <送信元インタフェース名> <送信元インタフェース番号>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エントリ番号	エントリ番号を指定します。エントリ番号の小さい方が高優先となります。	1～32	省略不可
逆引き対象アドレス/プレフィックス長	逆引き対象アドレスの範囲を指定します。	IPv4 アドレス形式 IPv6 アドレス形式 any：すべてのネットワーク	省略不可
reject	リレー処理は行わず DNS クエリメッセージの破棄を指定します。	-	省略不可
static	リレー先 DNS サーバをアドレスで指定する場合に指定します。2つ指定した場合、両方にリレーし、先に受信した応答を返します。	-	省略不可
プライマリ DNS サーバ IP アドレス	プライマリ DNS サーバ IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
セカンダリ DNS サーバ IP アドレス	セカンダリ DNS サーバ IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	セカンダリ DNS サーバの指定なし
ipcp	tunnel インタフェースに IPCP で通知された DNS サーバ IP アドレスをリレー先に使用する場合に指定します。	-	省略不可
tunnel インタフェース番号	tunnel インタフェース番号を指定します。	1～16777215	省略不可
dhcp	DHCP クライアントが取得した DNS サーバ IP アドレスをリレー先に使用する場合に指定します。	-	省略不可
DHCP クライアントインタフェース名	DHCP クライアントが動作しているインタフェース名を指定します。	-	省略不可
DHCP クライアントインタフェース番号	DHCP クライアントが動作しているインタフェース番号を指定します。	-	省略不可
送信元インタフェース名	DNS サーバへリレーする際の送信元アドレスとして使用するインタフェース名を指定します。	-	省略不可
送信元インタフェース番号	DNS サーバへリレーする際の送信元アドレスとして使用するインタフェース番号を指定します。	-	省略不可

【動作モード】

基本設定モード

【説明】

ProxyDNS の逆引き動作条件を設定します。

ipcp、dhcp 指定をしており有効な DNS サーバ情報を取得できていない場合はエントリ無効となります。

【実行例】

ProxyDNS の逆引き動作条件の設定をします（エントリ番号：1、逆引き対象アドレス／プレフィックス長：10.0.0.0/24、プライマリ DNS サーバ IP アドレス：172.16.100.5）。

```
#configure terminal
(config)#proxydns address 1 10.0.0.0/24 static 172.16.100.5
```

【未設定時】

ProxyDNS 機能の逆引きは動作しません。

2.9 認証／許可の設定

本装置ではログインする際の認証方法として、装置に設定するパスワード情報に加えて、RADIUS サーバや TACACS+ サーバを利用できます。

また、装置にログインしたユーザ、および装置上で実行可能なコマンドに対して、16 段階のレベル (0～15) が割り当てられます。

ユーザに割り当てられたレベル (privilege-level) に応じて、使用可能なコマンドが制限されます。ユーザが実行できるコマンドは、そのユーザが持つユーザレベル以下のレベルに割り当てられたコマンドのみとなります。

認証 (authentication) とともに許可 (authorization) の設定を行うことによって、ログイン直後のユーザレベルを設定できます。許可の設定がない場合は、ユーザレベル 1 が割り当てられます。上位のレベルへアクセスするためには、enable コマンドを実行します。

2.9.1 aaa authentication enable

【機能】

enable コマンド実行時の認証方法の設定

【入力形式】

aaa authentication enable default < 認証方式 >

no aaa authentication enable default

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
認証方式 (*1)	認証方式を指定します。	tacacs+ : TACACS+ による認証 enable : enable パスワードによる認証 none : 認証しない	省略不可

*1) 認証方式を複数登録した場合は、登録順に認証されます。ただし、none 以降の設定については機能しません。

【動作モード】

基本設定モード

【説明】

enable コマンド実行時の認証方法を設定します。このコマンドは、TELNET でログインする場合にのみ適用されます。

【実行例】

enable コマンド実行時の認証方式を設定します (認証方式: TACACS+)。

```
#configure terminal
(config)#aaa authentication enable default tacacs+
```

【未設定時】

認証方式は enable で動作します。

2.9.2 aaa authentication login

【機能】

ログイン認証方式の設定

【入力形式】

aaa authentication login {<ユーザ名> | default} <認証方式>

no aaa authentication login {<ユーザ名> | default}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ユーザ名 default	認証方式を適用するユーザ名を指定します。	ユーザ名：16文字以内のWORD型 default：全ユーザ	省略不可
認証方式(*1)	認証方式を指定します。	radius:RADIUSによる認証 tacacs+:TACACS+による認証 local:usernameで登録した内容で認証 login:loginパスワードによる認証(ユーザ名は"operator") enable:enableパスワードによる認証 none:認証しない	

*1) 認証方式を複数登録した場合は、登録順に認証されます。ただし、none以降の設定については機能しません。

【動作モード】

基本設定モード

【説明】

本装置にログインする場合の認証方式を設定します。ユーザ名に対して認証方式を割り付けます。

【実行例】

本装置にログインする場合の認証方式を設定します (ユーザ名：全ユーザ、認証方式：local)。

```
#configure terminal
(config)#aaa authentication login default local
```

【未設定時】

以下の値で動作します。

ユーザ名： operator

認証方式： login

2.9.3 aaa authentication login-prompt

【機能】

ログインプロンプトの文字列の設定

【入力形式】

aaa authentication login-prompt <プロンプト文字列>

no aaa authentication login-prompt

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プロンプト文字列	プロンプト文字列を指定します。	72文字以内のSTRING型	省略不可

【動作モード】

基本設定モード

【説明】

ログイン認証時に表示されるログインプロンプトの文字列を設定します。

【実行例】

ログイン認証時に表示されるログインプロンプトの文字列を設定します（プロンプト文字列：Enter your name here:）。

```
#configure terminal
(config)#aaa authentication login-prompt Enter your name here:
```

【未設定時】

プロンプト文字列は「login:」で動作します。

2.9.4 aaa authentication password-prompt

【機能】

パスワードプロンプトの文字列の設定

【入力形式】

aaa authentication password-prompt <プロンプト文字列>

no aaa authentication password-prompt

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プロンプト文字列	プロンプト文字列を指定します。	72文字以内のSTRING型	省略不可

【動作モード】

基本設定モード

【説明】

ログイン認証時に表示されるパスワードプロンプトの文字列を設定します。

【実行例】

ログイン認証時に表示されるパスワードプロンプトの文字列を設定します（プロンプト文字列：Enter your password now:）。

```
#configure terminal
(config)#aaa authentication password-prompt Enter your password now:
```

【未設定時】

プロンプト文字列は「password:」で動作します。

2.9.5 aaa authentication server-fail-message

【機能】

RADIUS サーバ、TACACS+ サーバ未応答による認証失敗時の出力メッセージの設定

【入力形式】

aaa authentication server-fail-message <メッセージ文字列>

no aaa authentication server-fail-message

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
メッセージ文字列	メッセージ文字列を指定します。	72 文字以内の STRING 型	省略不可

【動作モード】

基本設定モード

【説明】

RADIUS サーバ、および TACACS+ サーバ未応答による認証失敗時の出力メッセージを設定します。サーバが複数登録されている場合は、すべて未応答のあとに出力されます。

【実行例】

RADIUS サーバ、および TACACS+ サーバ未応答による認証失敗時の出力メッセージを設定します（メッセージ文字列：*** Authentication server down）。

```
#configure terminal
(config)#aaa authentication server-fail-message *** Authentication server down
```

【未設定時】

認証失敗時にメッセージを出力しません。

2.9.6 aaa authentication suppress-log

【機能】

ログメッセージの抑制

【入力形式】

```
aaa authentication suppress-log {type <認証ログ> | auth-method <認証方式> | username <ユーザ名> | line console}
```

```
no aaa authentication suppress-log {type | auth-method <認証方式> | username <ユーザ名> | line console}
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
type [<認証ログ>]	認証ログごとに指定します。	login-success：ログイン成功 login-failure：ログイン失敗 logout：ログアウト	ログ出力を抑制しない
auth-method <認証方式>	認証方式ごとに指定します。	login local tacacs+ radius enable none	省略不可
username <ユーザ名>	ユーザ名ごとに指定します。	16文字以内のWORD型	
line console	コンソールを指定します。	-	

【動作モード】

基本設定モード

【説明】

以下のログメッセージを抑制します。

接続方法	ログ出力タイミング	ログメッセージ
コンソール経由	ログイン成功時	LOGIN (%1(*1)) ON %2(*2)
	ログイン失敗時	LOGIN FAILURE ON %2, %1
	ログアウト時	LOGOUT (%1) ON %2
telnet 経由	ログイン成功時	LOGIN (%1) ON %2 FROM %3(*3)
	ログイン失敗時	LOGIN FAILURE FROM %3, %1
	ログアウト時	LOGOUT (%1) ON %2
ftp 経由	ログイン成功時	FTP LOGIN FROM %3 as %1
	ログイン失敗時	FTP LOGIN FAILURE FROM %3, %1
	ログアウト時	FTP LOGOUT FROM %3 as %1
ssh 経由	ログイン成功時	Accepted password for %1 from %3 port %4(*4)
	ログイン失敗時	Failed password for %1 from %3 port %4
	ログアウト時	LOGOUT (%1) ON %2

- *1) ユーザ名
- *2) tty ライン名
- *3) IP アドレス
- *4) ポート番号

【実行例】

ログメッセージを抑制します（ログイン失敗、ログアウト）。

```
#configure terminal
(config)#aaa authentication suppress-log type login-success logout
```

【未設定時】

ログメッセージを抑制しません。

2.9.7 aaa authorization commands

【機能】

許可方式の設定

【入力形式】

aaa authorization commands <コマンドレベル> {<ユーザ名> | default} <許可方式>

no aaa authorization commands <コマンドレベル> {<ユーザ名> | default}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
コマンドレベル	コマンドレベルを指定します。	0 ～ 15	省略不可
ユーザ名 default	許可方式を適用するユーザ名を指定します。	ユーザ名：16文字以内のWORD型 default：全ユーザ	
許可方式(*1)	許可方式を指定します。	tacacs+:TACACS+による許可 local：usernameで登録した内容で許可 if-authenticated: ログイン完了すれば許可 none: 許可しない	

*1) 許可方式を複数登録した場合は、登録順に許可を行います。ただし、none以降の設定については機能しません。

【動作モード】

基本設定モード

【説明】

指定した特権レベルのコマンドに対して、実行を許可するかどうかの許可方式を設定します。本コマンドは、TELNETでログインしている場合にのみ適用されます。

【実行例】

実行を許可するかどうかの許可方式を設定します（コマンドレベル：7、ユーザ名：全ユーザ、許可方式：localとTACACS+）。

```
#configure terminal
(config)#aaa authorization commands 7 default local tacacs+
```

【未設定時】

デフォルトのコマンドレベルで動作します。

2.9.8 no aaa authorization config-commands

【機能】

許可無効の設定

【入力形式】

```
no aaa authorization config-commands
```

```
aaa authorization config-commands
```

【動作モード】

基本設定モード

【説明】

すべての設定コマンドに対する許可判断を無効にする場合に設定します。

【実行例】

すべての設定コマンドに対する許可判断を無効にします。

```
#configure terminal
(config)#no aaa authorization config-commands
```

【未設定時】

すべての設定コマンドに対する許可判断は有効で動作します。

2.9.9 aaa authorization exec

【機能】

許可方式の設定

【入力形式】

```
aaa authorization exec {<ユーザ名> | default} <許可方式>
```

```
no aaa authorization exec {<ユーザ名> | default}
```


【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ユーザ名 default	許可方式を適用するユーザ名を指定します。	ユーザ名：16文字以内のWORD型 default：全ユーザ	省略不可
許可方式(*1)	許可方式を指定します。	tacacs+:TACACS+による許可 local:usernameで登録した内容で許可 if-authenticated：ログイン完了すれば許可 none:許可しない	

*1) 許可方式を複数登録した場合は、登録順に許可を行います。ただし、none以降の設定については機能しません。

【動作モード】

基本設定モード

【説明】

指定したユーザに対して、実行を許可するかどうかの許可方式を設定します。本コマンドは、TELNETログインしている場合にのみ適用されます。

【実行例】

実行を許可するかどうかの許可方式を設定します（ユーザ名：すべてのユーザ、許可方式：tacacs+）。

```
#configure terminal
(config)#aaa authorization exec default tacacs+
```

【未設定時】

許可方式はlocalで動作します。

2.9.10 user session-limit

【機能】

1 ユーザあたりの最大セッション数の設定

【入力形式】

user session-limit <最大セッション数>

no user session-limit

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
最大セッション数	最大セッション数を指定します。	1～15	省略不可

【動作モード】

基本設定モード

【説明】

1 ユーザあたりの最大セッション数を設定します。

【実行例】

1 ユーザあたりの最大セッション数を設定します（最大セッション数：3）。

```
#configure terminal
(config)#user session-limit 3
```

【未設定時】

セッション数は最大17セッション（コンソール：1、TELNET（SSH含む）：16）で動作します。

2.9.11 username

【機能】

ログインユーザ名とパスワードの登録

【入力形式】

username <ユーザ名> [privilege <ユーザレベル>] password {<パスワード> | <暗号化キー> <暗号化されたパスワード>}

no username <ユーザ名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ユーザ名	ユーザ名を指定します。	16文字以内のWORD型	省略不可
ユーザレベル	ログイン直後のユーザレベルを指定します。	0～15	0
パスワード	パスワード文字列を指定します。	72文字以内のSTRING型	省略不可
暗号化キー (*1)	暗号化に使用するキーを指定します。	0～7	
暗号化されたパスワード	暗号化に使用するパスワード文字列を指定します。	13文字または34文字のSTRING型	

*1) すでに設定した username 情報を、他の装置にコピーする場合に使用します。設定した username のパスワード情報は、暗号化されて装置内に格納されます。show current.cfg(show running.cfg) コマンドなどで内容を確認すると、<暗号化キー>と<暗号化されたパスワード>の形式で表示されます。表示された内容をそのまま他の装置に入力することで、パスワードをオープンにすることなく他の装置へコピーできます。

【動作モード】

基本設定モード

【説明】

ログインを許可するユーザ名とパスワードを登録します。

8文字未満、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、以下のようなメッセージが表示されます。

入力したパスワード長が0、またはパスワードを削除した場合：

"<WARNING> weak username password: set the password"

入力したパスワード長が 8 文字未満：

"<WARNING> weak username password: contain at least 8 characters"

入力したパスワードが英字または数字のみ：

"<WARNING> weak username password: contain a different kind of character"

【実行例】

ログインを許可するユーザ名とパスワードを登録します（ユーザ名：user-A、ユーザレベル：15、パスワード：admin123）。

```
#configure terminal
(config)#username user-A privilege 15 password admin123
```

【未設定時】

ログインできません。

2.9.12 authorization

【機能】

ローカルアクセスの許可方式の設定

【入力形式】

authorization {exec | commands <コマンドレベル>} {<ユーザ名> | default} <許可方式>

no authorization {exec | commands <コマンドレベル>} {<ユーザ名> | default}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
exec commands	許可種別を指定します。 commands の場合には、コマンドレベルも指定します。	exec: ユーザに対する許可 commands: 実行コマンドに対する許可	省略不可
コマンドレベル	コマンドレベルを指定します。	0 ～ 15	
ユーザ名 default	許可方式を適用するユーザ名を指定します。	ユーザ名：16 文字以内の WORD 型 default: 全ユーザ	
許可方式(*1)	許可方式を指定します。	tacacs+: TACACS+ による許可 local: username で登録した内容で許可 if-authenticated: ログイン完了すれば許可 none: 許可しない	

*1) 許可方式を複数登録した場合は、登録順に許可を行います。ただし、none 以降の設定については機能しません。

【動作モード】

ライン設定モード（コンソールのみ）

【説明】

ローカルアクセス（コンソールのみ）に対する許可方式を設定します。

この設定を誤った場合、コンソールポートが使用できなくなることがありますので、注意してください。

【実行例】

ローカルアクセス（コンソールのみ）に対する許可方式を設定します（実行コマンドに対する許可、コマンドレベル：7、ユーザ名：全ユーザ、許可方式：tacacs++ と if-authenticated）。

```
#configure terminal
(config)#line console
(config-line)#authorization commands 7 default tacacs+ if-authenticated
```

【未設定時】

ローカルアクセスを許可しません。

2.10 ユーザ認証用 RADIUS サーバの設定

2.10.1 radius-server host

【機能】

RADIUS サーバの登録

【入力形式】

radius-server host <RADIUS サーバ> [auth-port <UDP ポート番号>] key <共有暗号キー>

no radius-server host <RADIUS サーバ>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
RADIUS サーバ	RADIUS サーバを指定します。	IPv4 アドレス形式 ホスト名：254 文字以内の WORD 型	省略不可
UDP ポート番号	UDP ポート番号を指定します。	1025 ～ 65535	1812
共有暗号キー	共有暗号キーを指定します。	64 文字以内の WORD 型	省略不可

【動作モード】

基本設定モード

【説明】

ログイン認証時の RADIUS サーバを登録します。複数登録した場合には、show current.cfg(show running.cfg) コマンドで表示される上位 20 個までが有効となります。21 個以上は設定上、無効となります。上位にエントリされたサーバからの応答がなければ、その次にエントリされたサーバで認証されます（登録順に最後まで認証されます）。指定したサーバから認証成功、あるいは、失敗の応答があれば、その時点で認証を終了します。本設定は、設定順にソートされます。

【実行例】

ログイン認証時の RADIUS サーバを登録します（RADIUS サーバ：192.0.2.1、共有暗号キー：secret）。

```
#configure terminal
(config)#radius-server host 192.0.2.1 key secret
```

【未設定時】

RADIUS サーバによる認証を行いません。

2.10.2 radius-server retransmit-count

【機能】

リクエストパケットの再送回数の設定

【入力形式】

radius-server retransmit-count <リクエスト再送回数>

no radius-server retransmit-count

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
リクエスト再送回数	リクエスト再送回数を指定します。	1～255	省略不可

【動作モード】

基本設定モード

【説明】

ログイン認証でRADIUSサーバを使用する場合に、リクエストパケットの再送回数を設定します。

【実行例】

リクエストパケットの再送回数を設定します（リクエスト再送回数：16回）。

```
#configure terminal
(config)#radius-server retransmit-count 16
```

【未設定時】

リクエスト再送回数は3回で動作します。

2.10.3 radius-server source-interface

【機能】

RADIUSサーバへのリクエストパケットの送信元アドレスとして使用するインタフェースの設定

【入力形式】

radius-server source-interface <インタフェース名> <インタフェース番号>

no radius-server source-interface

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース名	送信元アドレスとして使用するインタフェース名を指定します。	-	省略不可
インタフェース番号	送信元アドレスとして使用するインタフェース番号を指定します。	-	

【動作モード】

基本設定モード

【説明】

ログイン認証でRADIUSサーバを使用する場合に、リクエストパケットの送信元アドレスとして使用するインタフェースを設定します。

【実行例】

送信元アドレスとして使用するインタフェースを設定します（インタフェース名：loopback、インタフェース番号：1）。

```
#configure terminal
(config)#radius-server source-interface loopback 1
```

【未設定時】

送信元アドレスは送信インタフェースのアドレスで動作します。

2.10.4 radius-server timeout

【機能】

RADIUSサーバからの応答タイムアウト時間の設定

【入力形式】

radius-server timeout <タイムアウト時間>

no radius-server timeout

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
タイムアウト時間	RADIUSサーバからの応答タイムアウト時間（単位：秒）を指定します。	1～60	省略不可

【動作モード】

基本設定モード

【説明】

ログイン認証でRADIUSサーバを使用する場合に、RADIUSサーバからの応答タイムアウト時間（単位：秒）を設定します。

【実行例】

RADIUSサーバからの応答タイムアウト時間を設定します（タイムアウト時間：30秒）。

```
#configure terminal
(config)#radius-server timeout 30
```

【未設定時】

タイムアウト時間は5秒で動作します。

2.11 ユーザ認証用 TACACS+ サーバの設定

2.11.1 tacacs-server host

【機能】

ログイン認証時の TACACS+ サーバの登録

【入力形式】

tacacs-server host <TACACS+ サーバ> [port <TCP ポート番号>] [timeout <タイムアウト時間>] [key <共有暗号キー>]

no tacacs-server host <TACACS+ サーバ> [port <TCP ポート番号>] [timeout <タイムアウト時間>] [key <共有暗号キー>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
TACACS+ サーバ	TACACS+ サーバを指定します。	IPv4 アドレス形式 ホスト名：254 文字以内の WORD 型	省略不可
TCP ポート番号	TCP ポート番号を指定します。	1025～65535	49
タイムアウト時間	応答タイムアウト時間（単位：秒）を指定します。本設定は tacacs-server timeout コマンドより優先されます。	1～60	3
共有暗号キー	共有暗号キーを指定します。	254 文字以内の WORD 型(*1)	サーバとの通信を暗号化しない

*1) 1 文字の空白（スペース）は使用可能です。複数の空白（スペース）は 1 文字にまとめられます。

【動作モード】

基本設定モード

【説明】

ログイン認証時の TACACS+ サーバを登録します。複数登録した場合には、show current.cfg(show running.cfg) コマンドで表示される上位 20 個までが有効となります。21 個以上は設定上、無効となります。上位にエントリされたサーバからの応答がなければ、その次にエントリされたサーバで認証されます（登録順に最後まで認証されます）。指定したサーバから認証成功、あるいは、失敗の応答があれば、その時点で認証を終了します。

認証成功時には装置はコマンド実行結果を出力し、認証失敗時にはエラーを表示します。タイムアウトによる TACACS サーバの切り替え時も上記の動作となります。本設定は、設定順にソートされます。

【実行例】

ログイン認証時の TACACS+ サーバを登録します（TACACS+ サーバ：192.0.2.1、共有暗号キー：secret）。

```
#configure terminal
(config)#tacacs-server host 192.0.2.1 key secret
```


【未設定時】

TACACS+ サーバによる認証を行いません。

2.11.2 tacacs-server key

【機能】

TACACS+ サーバとの共有暗号キーの設定

【入力形式】

tacacs-server key <共有暗号キー>

no tacacs-server key

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
共有暗号キー	共有暗号キーを指定します。	254文字以内のWORD型(*1)	省略不可

*1) 文字の空白（スペース）は使用可能です。複数の空白（スペース）は1文字にまとめられます。

【動作モード】

基本設定モード

【説明】

TACACS+ サーバとの共有暗号キーを設定します。tacacs-server host コマンドが設定されている場合は、その共有暗号キーが優先されます。

【実行例】

TACACS+ サーバとの共有暗号キーを設定します（共有暗号キー：secret）。

```
#configure terminal
(config)#tacacs-server key secret
```

【未設定時】

共有暗号キーなしで動作します。

2.11.3 tacacs-server source-interface

【機能】

TACACS+ サーバへのリクエストパケットの送信元アドレスとして使用するインタフェースの設定

【入力形式】

tacacs-server source-interface <インタフェース名> <インタフェース番号>

no tacacs-server source-interface

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース名	送信元アドレスとして使用するインタフェース名を指定します。	-	省略不可
インタフェース番号	送信元アドレスとして使用するインタフェース番号を指定します。	-	

【動作モード】

基本設定モード

【説明】

ログイン認証で TACACS+ サーバを使用する場合に、リクエストパケットの送信元アドレスとして使用するインタフェースを設定します。

【実行例】

リクエストパケットの送信元アドレスとして使用するインタフェースを設定します（インタフェース名：loopback、インタフェース番号：1）。

```
#configure terminal
(config)#tacacs-server source-interface loopback 1
```

【未設定時】

送信元アドレスは送信インタフェースのアドレスで動作します。

2.11.4 tacacs-server timeout

【機能】

応答タイムアウト時間の設定

【入力形式】

tacacs-server timeout <タイムアウト時間>

no tacacs-server timeout

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
タイムアウト時間	TACACS+ サーバからの応答タイムアウト時間（単位：秒）を指定します。	1～60	省略不可

【動作モード】

基本設定モード

【説明】

ログイン認証で TACACS+ サーバを使用する場合に、応答タイムアウト時間（単位：秒）を設定します。tacacs-server host コマンドが設定されている場合は、その値が優先されます。

【実行例】

応答タイムアウト時間を設定します（タイムアウト時間：30 秒）。

```
#configure terminal
(config)#tacacs-server timeout 30
```

【未設定時】

タイムアウト時間は3秒で動作します。

2.12 TACACS+ アカウンティングの設定

2.12.1 aaa accounting commands

【機能】

コマンドアカウンティングの設定

【入力形式】

aaa accounting commands <コマンドレベル> {<ユーザ名> | default} <アカウンティング方式>

no aaa accounting commands <コマンドレベル> {<ユーザ名> | default}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
コマンドレベル	コマンドレベルを指定します。	0 ～ 15	省略不可
ユーザ名 default	アカウンティング方式を適用するユーザ名を指定します。	ユーザ名：254文字以内のWORD型 default：全ユーザ	
アカウンティング方式	アカウンティング方式を指定します。	start-stop tacacs+ stop-only tacacs+ wait-start tacacs+ none	

【動作モード】

基本設定モード

【説明】

コマンドアカウンティングを有効にします。コマンドアカウンティングとは、指定したコマンドレベルのコマンドが実行される場合に、TACACS+ サーバへ通知を行う機能です。なお、このコマンドは TELNET ログインしたユーザが対象になります。コンソールでログインしたユーザで、コマンドアカウンティング機能を動作させる場合は、accounting コマンドを実行します。

【実行例】

コマンドアカウンティングを有効にします（コマンドレベル：1、ユーザ名：全ユーザ、アカウンティング方式：start-stop）。

```
#configure terminal
(config)#aaa accounting commands 1 default start-stop tacacs+
```

【未設定時】

コマンドアカウンティングを行いません。

2.12.2 aaa accounting connection

【機能】

接続アカウントिंगの設定

【入力形式】

aaa accounting connection {<ユーザ名> | default} <アカウントING方式>

no aaa accounting connection {<ユーザ名> | default}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ユーザ名 default	アカウントING方式を適用するユーザ名を指定します。	ユーザ名：254文字以内のWORD型 default：全ユーザ	省略不可
アカウントING方式	アカウントING方式を指定します。	start-stop tacacs+ stop-only tacacs+ wait-start tacacs+ none	

【動作モード】

基本設定モード

【説明】

接続アカウントINGを有効にします。接続アカウントINGとは、指定したユーザが本装置からTELNET/SSH/FTPを利用して他の装置にログイン／ログアウトする事象が発生した場合に、TACACS+サーバへ通知を行う機能です。なお、このコマンドはTELNETログインしたユーザが対象になります。コンソールでログインしたユーザで接続アカウントING機能を動作させる場合は、accounting コマンドを実行します。

【実行例】

接続アカウントINGを有効にします（ユーザ名：全ユーザ、アカウントING方式：start-stop 方式）。

```
#configure terminal
(config)#aaa accounting connection default start-stop tacacs+
```

【未設定時】

接続アカウントINGを行いません。

2.12.3 aaa accounting exec

【機能】

EXEC アカウントINGの設定

【入力形式】

aaa accounting exec {<ユーザ名> | default} <アカウントING方式>

no aaa accounting exec {<ユーザ名> | default}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ユーザ名 default	アカウントティング方式を適用するユーザ名を指定します。	ユーザ名：254 文字以内の WORD 型 default：全ユーザ	省略不可
アカウントティング方式	アカウントティング方式を指定します。	start-stop tacacs+ stop-only tacacs+ wait-start tacacs+ none	

【動作モード】

基本設定モード

【説明】

EXEC アカウントティングを有効にします。EXEC アカウントティングとは、指定したユーザ名で本装置へのログイン／ログアウト（通常ログアウト、または強制ログアウト）／認証失敗など、装置へのアクセスに関する事象が発生した場合に、TACACS+ サーバへ通知を行う機能です。なお、このコマンドは、TELNET ログインしたユーザが対象になります。コンソールでログインしたユーザで EXEC アカウントティング機能を動作させる場合は、accounting コマンドを実行します。

【アカウントティング方式】

本装置では TACACS+ による start-stop、stop-only、wait-start、none の各アカウントティング方式の設定が可能です。

start-stop 方式	アカウントティング開始時に START レコードを、終了時に STOP レコードを送信します。TACACS+ サーバから START レコードに対する REPLY がない場合でも、プロセス自体（ログイン処理など）は動作します。
stop-only 方式	アカウントティング開始時には START レコードを送信せず、終了時にのみ STOP レコードを送信します。
wait-start 方式	アカウントティング開始時に START レコードを、終了時に STOP レコードを送信します。TACACS+ サーバから START レコードに対する REPLY がない場合、プロセス自体（ログイン処理など）は動作しません。
none 方式	アカウントティング動作を行いません。

設定する文字列は、以下のようになります。

start-stop 方式	start-stop tacacs+
stop-only 方式	stop-only tacacs+
wait-start 方式	wait-start tacacs+
none 方式	none

TACACS+ サーバで "MAXESS" を使用する場合は、EXEC アカウントティングを動作させておく必要があります。

【実行例】

EXEC アカウンティングを有効にします（ユーザ名：全ユーザ、アカウンティング方式：start-stop 方式）。

```
#configure terminal
(config)#aaa accounting exec default start-stop tacacs+
```

【未設定時】

EXEC アカウンティングを行いません。

2.12.4 aaa accounting send stop-record authentication failure

【機能】

ユーザ認証失敗に対する "stop" レコードを TACACS+ サーバに送信する設定

【入力形式】

aaa accounting send stop-record authentication failure

no aaa accounting send stop-record authentication failure

【動作モード】

基本設定モード

【説明】

ログイン失敗時などのユーザ認証失敗に対する "stop" レコードを、TACACS+ サーバに送信する場合に設定します。この設定がない場合、aaa accounting exec コマンドで EXEC アカウンティング機能の動作を指定しても、認証失敗時のアカウンティング機能は動作しません。

【実行例】

認証失敗時に対する "stop" レコードを、TACACS+ サーバに送信します。

```
#configure terminal
(config)#aaa accounting send stop-record authentication failure
```

【未設定時】

認証失敗のアカウンティングを行いません。

2.12.5 aaa accounting suppress null-username

【機能】

ユーザ名が NULL のアカウンティングレコードを送信しない設定

【入力形式】

aaa accounting suppress null-username

no aaa accounting suppress null-username

【動作モード】

基本設定モード

【説明】

ユーザ名が NULL のアカウントングレコードの送信を行わない場合に設定します。

【実行例】

ユーザ名が NULL のアカウントングレコードの送信を行いません。

```
#configure terminal
(config)#aaa accounting suppress null-username
```

【未設定時】

ユーザ名が NULL でもアカウントングレコードの送信を行います。

2.12.6 aaa accounting system default

【機能】

システムアカウントングの設定

【入力形式】

aaa accounting system default <アカウントング方式>

no aaa accounting system default

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アカウントング方式	アカウントング方式を指定します。	start-stop tacacs+ stop-only tacacs+ wait-start tacacs+ none	省略不可

【動作モード】

基本設定モード

【説明】

システムアカウントングを有効にします。システムアカウントングとは、各種アカウントング（EXEC/接続/コマンド）自体の動作に変更があった場合に、TACACS+ サーバへ通知を行う機能です。

なお、システムアカウントングの場合、送信する TACACS パケットの username フィールドは NULL となります。

【実行例】

システムアカウントングを有効にします（アカウントング方式：start-stop）。

```
#configure terminal
(config)#aaa accounting system default start-stop tacacs+
```

【未設定時】

システムアカウントングを行いません。

2.12.7 ip finger

【機能】

finger プロトコルの設定

【入力形式】

ip finger

no ip finger

【動作モード】

基本設定モード

【説明】

finger プロトコルを有効にする場合に設定します。TACACS+ サーバで "MAXESS" を使用する場合、TACACS+ サーバは finger プロトコルを利用してユーザの確認を行いますので、その場合には finger プロトコルを有効にしておく必要があります。本装置はデフォルトで finger プロトコルが無効になっていますので、finger プロトコルを有効にしたい場合に設定します。

"MAXESS" を使用する場合は、finger プロトコルだけでなく EXEC アカウンティング機能も動作させておく必要があります。

【実行例】

finger プロトコルを有効にします。

```
#configure terminal
(config)#ip finger
```

【未設定時】

finger プロトコルは無効で動作します。

2.12.8 accounting

【機能】

ローカルアクセスに対するアカウンティング機能の設定

【入力形式】

accounting {exec | connection | commands <コマンドレベル>} {<ユーザ名> | default} <アカウンティング方式>

no accounting <アカウンティング種別> {<ユーザ名> | default}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
exec connection commands	アカウント種別を指定します。commandsの場合には、コマンドレベルも指定します。	exec:EXEC アカウンティング connection: 接続アカウント commands: コマンドアカウント	省略不可
コマンドレベル	コマンドレベルを指定します。	0 ～ 15	
ユーザ名 default	アカウント方式を適用するユーザ名を指定します。	ユーザ名: 254文字以内のWORD型 default: 全ユーザ	
アカウント方式	アカウント方式を指定します。	start-stop tacacs+ stop-only tacacs+ wait-start tacacs+ none	

【動作モード】

ライン設定モード（コンソールのみ）

【説明】

ローカルアクセス（コンソール）に対するアカウント機能を有効にします。設定方法は、基本設定モードのaaa accounting コマンドと同様です。

リモートアクセス (TELNET/FTP/SSH) に対するアカウント機能については、基本設定モードのaaa accounting コマンドで設定します。

【実行例】

ローカルアクセス（コンソール）に対するアカウント機能を有効にします（commands、コマンドレベル：15、ユーザ名：全ユーザ、アカウント方式：start-stop）。

```
#configure terminal
(config)#line console
(config-line)#accounting commands 15 default start-stop tacacs+
```

【未設定時】

コンソールに対するアカウントを行いません。

2.13 バナー表示の設定

本装置ではコンソール、TELNET、FTP、SSHからログインした場合に、メッセージを表示できます（バナー表示機能）。バナー表示機能を使用する場合は、以下のコマンドを実行します。

2.13.1 banner motd enable

【機能】

バナーを表示する端末の設定

【入力形式】

banner motd enable <ログイン端末>

no banner motd enable [<ログイン端末>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ログイン端末	バナーを表示するログイン端末を指定します。	console: コンソール telnet: TELNET ftp: FTP ssh: SSH	省略不可

【動作モード】

基本設定モード

【説明】

バナーを表示する端末を設定します。

【実行例】

バナーを表示する端末を設定します（ログイン端末：コンソール）。

```
#configure terminal
(config)#banner motd enable console
```

【未設定時】

すべての端末にバナーを表示しません。

2.13.2 banner motd text

【機能】

バナーで表示する文字列の設定

【入力形式】

banner motd text <表示する順番> [<文字列>]

no banner motd text [<表示する順番>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
表示する順番	バナーで表示する順番を指定します。	1～24	省略不可
文字列	バナーで表示するテキスト文字列を指定します。	79文字以内のWORD型(*1)	改行

*1) 1文字の空白（スペース）は使用可能です。複数の空白（スペース）は1文字にまとめられます。

【動作モード】

基本設定モード

【説明】

バナーで表示する文字列を設定します。バナーは番号の小さい順に表示を行い、設定されていない番号は無視します。バナーは1行あたり79文字まで、最大24行までの表示が可能です。

【実行例】

バナーで表示する文字列を設定します。

```
#configure terminal
(config)#banner motd text 1 *****
(config)#banner motd text 2 Please ignore this message.
(config)#banner motd text 3 since this message is just a test.
(config)#banner motd text 4 If you want to know about this machine
(config)#banner motd text 5 please consult with administrators.
(config)#banner motd text 6 *****
```

【未設定時】

バナーを表示しません。

2.14 設定情報の設定

2.14.1 auto config save enable

【機能】

refresh または commit コマンド実行時に current.cfg を保存する設定

【入力形式】

auto config save enable

no auto config save enable

【動作モード】

基本設定モード

【説明】

refresh または commit コマンド実行時に current.cfg を保存します。/drive/config/ ディレクトリの下に、"config.XX.gz" (XX は世代番号) のファイル名で保存されます。保存可能な世代数は 20 までとなります。rollback コマンドにより、working.cfg をその世代の設定情報に戻すことができます。

【実行例】

refresh または commit コマンド実行時に current.cfg を保存します。

```
#configure terminal
(config)#auto config save enable
```

【未設定時】

refresh または commit コマンド実行時に current.cfg を保存しません。

2.14.2 config comment

【機能】

設定情報にコメントを付与する設定

【入力形式】

config comment <行番号> [<コメント>]

no config comment [<行番号>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
行番号	コメントの行番号を指定します。	1～24	省略不可
コメント	設定情報のコメントを指定します。	254文字以内のWORD型(*1)	空行

*1) 1文字の空白（スペース）は使用可能です。複数の空白（スペース）は1文字にまとめられます。

【動作モード】

基本設定モード

【説明】

設定情報にコメントを付与します。

【実行例】

設定情報にコメントを付与します。

```
#configure terminal
(config)#config comment 1 *****
(config)#config comment 2 Use this configuration by version XX.XX or more.
(config)#config comment 3
(config)#config comment 4 *****
```

【未設定時】

設定情報にコメントを付与しません。

2.15 ファームウェアの設定

2.15.1 update firmware

【機能】

未使用面のファームウェアで起動する設定

【入力形式】

update firmware other-side

no update firmware [other-side]

【動作モード】

基本設定モード

【説明】

リセットボタン、POWER OFF/ON、ソフトウェアエラーによる自動再起動時に、未使用面のファームウェアで起動します。ファームウェアファイルの展開は完了しているが、即時に再起動ができない場合に有効なコマンドです。ファームウェアの起動面を切り替える場合には、あらかじめ未使用の起動面にファームウェアを展開（extract-firmware コマンド）しておいてください。

【注意】

装置の再起動によりファームウェアの起動面が切り替わったことを確認したら、速やかに本設定を削除してください。削除していない状態で再起動が発生すると、再度起動面の切り替えが発生し、意図しない版数のファームウェアで起動することになります。

【実行例】

次回再起動時に、未使用面で起動します。

```
#configure terminal
(config)#update firmware other-side
```

【未設定時】

次回再起動時、現用面で起動します。

2.15.2 updateinfo

【機能】

リモート FTP サーバに接続するためのユーザ情報と転送するファームウェアファイルのパスの設定

【入力形式】

updateinfo {<FTP サーバ名> | <FTP サーバアドレス>} <ユーザ ID> <パスワード> [encrypted] <パス>

no updateinfo [{<FTP サーバ名> | <FTP サーバアドレス>} <ユーザ ID> <パスワード> [encrypted] <パス>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
FTPサーバ名	FTPサーバ名を指定します。	128文字以内のWORD型	省略不可
FTPサーバアドレス	FTPサーバIPアドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
ユーザID	FTPサーバにログインするためのユーザIDを指定します。	32文字以内のWORD型	省略不可
パスワード	FTPサーバにログインするためのパスワードを指定します。	32文字以内のSTRING型	省略不可
encrypted	暗号化したパスワードを入力する場合は"encrypted"を指定します	-	省略不可
パス	FTPサーバにあるファームウェアファイルのパスを指定します。	32文字以内のSTRING型	省略不可

【動作モード】

基本設定モード

【説明】

update コマンドで必要な情報をセットします。

リモートFTPサーバに接続するためのユーザ情報と転送するファームウェアファイルのパスを指定します。

【実行例】

update コマンドで必要な情報を設定します (ftpサーバ：192.168.1.1、ユーザID：user、パスワード：pass、パス：firmware/GX500.FRM)。

```
(config)#updateinfo 192.168.1.1 user pass firmware/GX500.FRM
```

パスワードは、暗号化されて保存されるため、上記の設定をしたworking.cfgでは以下のように表示されます。

```
updateinfo 192.168.1.1 user mvQhZeS2V9MSiDrnUuRCm4nd0Mz1EZtC encrypted firmware/GX500.FRM
```

【未設定時】

update コマンドが使用できません。

2.16 装置情報の設定

2.16.1 notify-nhid-usage

【機能】

設定された割合に達した際にログを出力する設定

【入力形式】

notify-nhid-usage <WARNING しきい値> <ALERT しきい値>

no notify-nhid-usage [<WARNING しきい値> <ALERT しきい値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
WARNING しきい値	WARNING ログを出力するしきい値（単位：%）を指定します。	1～100	省略不可
ALERT しきい値	ALERT ログを出力するしきい値（単位：%）を指定します。	1～100	空行

【動作モード】

基本設定モード

【説明】

割り当て可能な最大数に対する NextHopID(NHID) 使用数が、設定された割合 (%) に達した際に以下のログを出力します。

- <%1> exceeded warning threshold. (%2 used)
 - <%1> exceeded alert threshold. (<%2 used)
- %1="NHDN NHID", "LINK NHID", "LSP NHID", "RT-EXP-ID", "ILM Counter ID",
"IPv6 Encap Counter ID"
- %2= 割合

<WARNING しきい値> が <ALERT しきい値> より大きな数値でない場合、有効となりません。

設定投入時に、すでに設定された割合 (%) に達していた場合には、その時点でログを出力します。

【実行例】

割合 (%) に達した際にログを出力します（WARNING しきい値：80%、ALERT しきい値：90%）。

```
#configure terminal
(config)#notify-nhid-usage 80 90
```

【未設定時】

以下の値で動作します。

WARNING しきい値： 90%

ALERT しきい値： 99%

2.16.2 periodic-log

【機能】

定期ログ取得の無効化と定期ログ取得間隔の指定

【入力形式】

periodic-log {disable | enable interval <取得間隔>}

no periodic-log [{disable | enable interval <取得間隔> }]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
disable	定期ログ取得を無効化します。	-	省略不可
enable	定期ログ取得を有効化します。	-	省略不可
interval	定期ログ取得間隔を指定します。	-	省略不可
取得間隔	定期ログ取得間隔（単位：分）を指定します。	10～1440	省略不可

【動作モード】

基本設定モード

【説明】

定期ログ取得の無効化と定期ログ取得間隔を指定します。

【実行例】

定期ログ取得を行いません。

```
#configure terminal
(config)#periodic-log disable
```

【未設定時】

定期的ログ取得は有効。取得間隔は60分。

第3章 インタフェースの設定



この章では、インタフェースの設定に関するコマンドについて説明します。

3.1	802.1Q TPID 設定	120
3.2	インタフェースの省電力設定	121
3.3	インタフェース設定モード	122
3.4	MAC アドレス学習設定	127
3.5	bridge 設定	130
3.6	インタフェース関連設定	132
3.7	インタフェース description 設定	134
3.8	fragment パケット中継設定	135
3.9	フロー制御機能設定	136
3.10	インタフェース統計情報設定	137
3.11	MAC アドレス設定	138
3.12	インタフェースメディア設定	139
3.13	MTU 設定	140
3.14	MSS 設定 (port-channel インタフェース)	141
3.15	QoS インタフェース設定	142
3.16	MSS 設定 (トンネルインタフェース)	143
3.17	インタフェースリンク状態設定	145
3.18	インタフェースリンク状態変化の設定	147
3.19	インタフェーススピード／デュプレックス設定	149
3.20	トンネルインタフェース動作モード設定	150
3.21	VLAN ID 設定	152

3.1 802.1Q TPID 設定

3.1.1 dot1q tunnel tpid

【機能】

IEEE801.1Q tunnel の VLAN TAG の TPID の設定

【入力形式】

dot1q tunnel tpid <TPID>

no dot1q tunnel tpid [<TPID>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
TPID	IEEE801.1Q tunnel の VLAN TAG の TPID を指定します。	8000～ffff (16進数)	省略不可

【動作モード】

基本設定モード

【説明】

IEEE801.1Q tunnel の VLAN TAG の TPID を設定します。VLAN TAG の TPID である 8100 (16進数) の他に本コマンドで指定されている TPID 値を STAG の TPID として認識します。受信パケットの認識に使用します。

なお、TPID として 86dd(IPv6)、8847(MPLS)、8848(MPLS) の値 (16進数) を設定した場合、正しくパケットを処理できない可能性がありますので注意してください。

本コマンドで追加できる TPID は 1 エントリです。

【実行例】

IEEE801.1Q tunnel の VLAN TAG の TPID を設定します (TPID : 9100 (16進数))。

```
#configure terminal
(config)#dot1q tunnel tpid 9100
```

【未設定時】

TPID が 8100 (16進数) のみを受信フレームの STAG の TPID として認識します。

3.2 インタフェースの省電力設定

3.2.1 eee

【機能】

インタフェースの省電力モードの設定

【入力形式】

eee {enable | disable}

no eee [{enable | disable}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
enable disable	省電力モードの有効・無効を指定します。	enable: 有効 disable: 無効	省略不可

【動作モード】

gigaetherenet インタフェース設定モード、management インタフェース設定モード

【説明】

インタフェースの省電力モードの有効・無効を設定します。省電力モードはメディア種別が metal のポートのみ動作します。

【実行例】

省電力モードを有効にします（インタフェース名：gigaetherenet、インタフェース番号：1/1）。

```
#configure terminal(config)#interface gigaetherenet 1/1
(config-if-ge 1/1)#eee enable
```

【未設定時】

インタフェースの省電力モードは無効となります。

3.3 インタフェース設定モード

3.3.1 interface gigabitEthernet

【機能】

gigabitEthernet インタフェース設定モードへの移行

【入力形式】

interface gigabitEthernet <インタフェース番号>[.<サブインタフェースインデックス番号>]

no interface gigabitEthernet <インタフェース番号>[.<サブインタフェースインデックス番号>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース番号	gigabitEthernet インタフェースの番号を、1/ポート番号の順に指定します。	ポート番号：1～10	省略不可
サブインタフェースインデックス番号	サブインタフェースインデックス番号を指定します。	1～9999	サブインタフェースを使用しない

【動作モード】

基本設定モード

【説明】

GbE ポートの設定を行うために、gigabitEthernet インタフェース設定モード（gigabitEthernet サブインタフェース設定モード）に移行します。ポート番号は1～10、サブインタフェースインデックス番号は1～9999を指定します。コマンドの先頭に"no"を指定することで、該当gigabitEthernet インタフェース設定モード（gigabitEthernet サブインタフェース設定モード）の内容がすべて消去されます。

【実行例】

gigabitEthernet インタフェース設定モードに移行します（インタフェース番号：1/1）。

```
#configure terminal
(config)#interface gigabitEthernet 1/1
(config-if-ge 1/1)#
```

gigabitEthernet サブインタフェース設定モードに移行します（インタフェース番号：1/1、サブインタフェースインデックス番号：100）。

```
#configure terminal
(config)#interface gigabitEthernet 1/1.100
(config-if-ge 1/1.100)#
```

3.3.2 interface management

【機能】

management インタフェース設定モードへの移行

【入力形式】

interface management 1

no interface management 1

【動作モード】

基本設定モード

【説明】

管理用 10/100/1000BASE-T ポートの設定を行うために、management インタフェース設定モードに移行します。コマンドの先頭に "no" を指定することで、management インタフェース設定モードの内容がすべて消去されます。

【実行例】

management インタフェース設定モードに移行します。

```
#configure terminal
(config)#interface management 1
(config-if-manage 1)#
```

3.3.3 interface loopback

【機能】

loopback インタフェース設定モードへの移行

【入力形式】

interface loopback <インタフェース番号>

no interface loopback <インタフェース番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース番号	loopback インタフェースの番号を指定します。	1 ~ 16777215	省略不可

【動作モード】

基本設定モード

【説明】

loopback インタフェースの設定を行うために、loopback インタフェース設定モードに移行します。コマンドの先頭に "no" を指定することで、該当 loopback インタフェース設定モードの内容がすべて消去されます。

【実行例】

loopback インタフェース設定モードに移行します（インタフェース番号：1）。

```
#configure terminal
(config)#interface loopback 1
(config-if-lo 1)#
```

3.3.4 interface port-channel

【機能】

port-channel インタフェース設定モードへの移行

【入力形式】

interface port-channel <インタフェース番号>

no interface port-channel <インタフェース番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース番号	port-channel インタフェースの番号を指定します。	0～16777215	省略不可

【動作モード】

基本設定モード

【説明】

port-channel インタフェースの設定を行うために、port-channel インタフェース設定モードに移行します。コマンドの先頭に "no" を指定することで、該当 port-channel インタフェース設定モードの内容がすべて消去されます。

【実行例】

port-channel インタフェース設定モードに移行します（インタフェース番号：1）。

```
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#
```

3.3.5 interface tunnel

【機能】

tunnel インタフェース設定モードへの移行

【入力形式】

interface tunnel <インタフェース番号>

no interface tunnel <インタフェース番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース番号	tunnel インタフェースの番号を指定します。	1～16777215	省略不可

【動作モード】

基本設定モード

【説明】

tunnel インタフェースの設定を行うために、tunnel インタフェース設定モードに移行します。コマンドの先頭に "no" を指定することで、該当 tunnel インタフェース設定モードの内容がすべて消去されます。

【実行例】

tunnel インタフェース設定モードに移行します（インタフェース番号：1）。

```
#configure terminal
(config)#interface tunnel 1
(config-if-tun 1)#
```

3.3.6 interface trunk-channel

【機能】

trunk-channel インタフェース設定モードへの移行

【入力形式】

interface trunk-channel <インタフェース番号>[<サブインタフェースインデックス番号>]

no interface trunk-channel <インタフェース番号>[<サブインタフェースインデックス番号>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース番号	リンクアグリケーションインタフェースの番号を指定します。	1～5	省略不可
サブインタフェースインデックス番号	サブインタフェースインデックス番号を指定します。	1～9999	サブインタフェースを使用しない

【動作モード】

基本設定モード

【説明】

リンクアグリケーションインタフェースの設定を行うために、trunk-channel インタフェース設定モード（trunk-channel サブインタフェース設定モード）に移行します。コマンドの先頭に "no" を指定することで、該当 trunk-channel インタフェース設定モード（trunk-channel サブインタフェース設定モード）の内容がすべて消去されます。

【実行例】

trunk-channel インタフェース設定モードに移行します（インタフェース番号：1）。

```
#configure terminal
(config)#interface trunk-channel 1
(config-if-tr 1)#
```

trunk-channel サブインタフェース設定モードに移行します（インタフェース番号：1、サブインタフェースインデックス番号：100）。

```
#configure terminal
(config)#interface trunk-channel 1.100
(config-if-tr 1.100)#
```

3.3.7 interface usb-ethernet

【機能】

USB Ethernet インタフェースの設定

【入力形式】

interface usb-ethernet <インタフェース番号>

no interface usb-ethernet <インタフェース番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース番号	USB Ethernet インタフェースの番号を指定します。	1	省略不可

【動作モード】

基本設定モード

【説明】

USB Ethernet インタフェース設定モードに移行します。

設定できるインタフェース数は1つとし、物理ポートはUSB ポート2を使用します。

【実行例】

USB Ethernet 1 インタフェースに移行します。

```
#configure terminal
(config)#interface usb-ethernet 1
(config-if-usb 1)#
```

3.4 MAC アドレス学習設定

3.4.1 mac-address-table aging-time

【機能】

MAC アドレスの学習におけるエージアウト時間の設定

【入力形式】

mac-address-table aging-time <エージアウト時間>

no mac-address-table aging-time [<エージアウト時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エージアウト時間	MAC アドレスの学習におけるエージアウト時間（単位：秒）を指定します。	10～100000	省略不可

【動作モード】

基本設定モード

【説明】

MAC アドレスの学習におけるエージアウト時間（単位：秒）を設定します。ただし、設定した時間は最小のエージアウト時間であり、エージアウトする時間は最長で設定した時間の2倍になります。

なお、60秒を超えるエージアウト時間を設定した場合、60秒単位でエージアウト時間が設定されます。60秒で割り切れない余りの時間は切り捨てて設定されます（例：設定時間：299秒→実際の設定：240秒）。

【実行例】

MAC アドレスの学習におけるエージアウト時間（単位：秒）を設定します（エージアウト時間：600秒）。

```
#configure terminal
(config)#mac-address-table aging-time 600
```

【未設定時】

エージアウト時間は300秒で動作します。

3.4.2 mac-address-table total-max-entry

【機能】

装置の最大学習エン트리数の制限

【入力形式】

mac-address-table total-max-entry <最大学習エン트리数> [threshold <警告エン트리数>]

no mac-address-table total-max-entry [<最大学習エン트리数> [threshold [<警告エン트리数>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
最大学習エン트리数	最大学習エン트리数を指定します。	1～64535	省略不可
警告エン트리数	ログを出力する警告エン트리数を指定します。	1～64535	

【動作モード】

基本設定モード

【説明】

装置の最大学習エン트리数を制限する場合に設定します。最大学習エン 트리数に到達した場合、学習できないことを通知するログを出力します。また、警告エン 트리数を指定することで最大学習エン 트리数に到達する前にログを出力できます。警告ログは警告エン 트리数に到達したときに出力されます。なお、いったん警告ログを出力すると、clear mac-address-table total-max-entry warning コマンドを実行されるまでの間、学習数の変化によらず警告ログは出力されなくなります。



- 最大学習エン 트리数 ≤ 警告学習エン 트리数となるように設定を行った場合、警告学習エン 트리数の設定は無視されます。
- 本コマンドを使用して最大学習エン 트리数、警告エン 트리数を変更した場合、現在のエン 트리数の状態に応じて以下の処理が行われます。
 最大学習エン 트리数 > 現在の学習エン 트리数：変化なし
 最大学習エン 트리数 = 現在の学習エン 트리数：最大学習エン 트리数到達ログ出力
 最大学習エン 트리数 < 現在の学習エン 트리数：エラーログを出力
 警告学習エン 트리数 > 現在の学習エン 트리数：変化なし
 警告学習エン 트리数 ≤ 現在の学習エン 트리数：警告ログ出力
- 最大学習エン 트리数は、静的 MAC テーブル数を含みません。

【実行例】

装置の最大学習エン 트리数を制限します（最大学習エン 트리数：10000、警告エン 트리数：9995）。

```
#configure terminal
(config)#mac-address-table total-max-entry 10000 threshold 9995
```

【未設定時】

以下の値で動作します。

最大学習エン 트리数：64535

警告エン 트리数：なし

3.4.3 mac-address-table static

【機能】

MACアドレスを学習テーブルにスタティック登録

【入力形式】

```
mac-address-table static <MAC アドレス> [c-vlan <カスタム VLAN-ID>] bridge-group <ブリッジグループ番号> <インタフェース名> <インタフェース番号> [auto-learn]
```

```
no mac-address-table static <MAC アドレス> [c-vlan <カスタム VLAN-ID>] bridge-group <ブリッジグループ番号> [<インタフェース名> [auto-learn]]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
MACアドレス	MACアドレスを指定します。	HHHH.HHHH.HHHH 型式	省略不可
カスタム VLAN-ID	カスタム VLAN-ID を指定します。	1 ～ 4094	省略不可
ブリッジグループ番号	MACアドレスを指定します。	1 ～ 16777215	省略不可
インタフェース名	宛先インタフェースを指定します。	—	省略不可
インタフェース番号	インタフェース番号を指定します。	—	省略不可
auto-learn	異なる I/F 上で同一 MAC アドレスが検出されたとき宛先インタフェースの書き換えを行います。	—	異なる I/F 上で同一 MAC アドレスが検出されたとき宛先インタフェースの書き換えを行いません。

【動作モード】

基本設定モード

【説明】

MACアドレスを学習テーブルにスタティック登録します。

1つの bridge に対して cvid、mac-address が一致するエントリは複数個登録できません。最後に記述したエントリが有効となります (cvid、mac-address が一致していても bridge が異なる場合は、登録可能)。

スタティック登録する MAC アドレスは最大学習数に含まれないため、最大学習数を超えている場合でもスタティック登録数の上限を超えない範囲で登録が可能です。スタティック登録する MAC アドレスがすでに学習済みエントリが存在する場合、スタティック登録により学習済みエントリが上書きされ、消去されます。また、登録上限を超えて登録に失敗した mac-address は登録数が登録上限を下回った場合でも自動的に登録は行われません。いったんコンフィグから削除してリフレッシュしたあとに、再登録する必要があります。

【実行例】

mac address 0001.0002.0003 を GigaEthernet 1/1 を宛先として登録します。

```
#configure terminal
(config)#mac-address-table static 1.2.3 GigaEthernet 1/1
```

【未設定時】

スタティック MAC アドレスが登録されません。

3.5 bridge 設定

3.5.1 bridge-group

【機能】

インタフェースが属するブリッジグループ番号の設定

【入力形式】

bridge-group <ブリッジグループ番号> [client | server]

no bridge-group [<ブリッジグループ番号> [client | server]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ブリッジグループ番号	ブリッジグループ番号を指定します。	1 ~ 16777215	省略不可
client server	接続する端末の属性を指定します。	—	server

【動作モード】

gigaethernet インタフェース設定モード、gigaethernet サブインタフェース設定モード、tunnel インタフェース設定モード

【説明】

インタフェースが属するブリッジグループ番号を設定します。本設定により、同一ブリッジグループ番号が設定されているインタフェース間でブリッジ中継を行うことが可能になります。また、サーバークライアントモデル（PPPoE 中継など）で使用する場合、サーバが接続されているインタフェースには "server" を、クライアントが接続されているインタフェースには "client" を指定します。この場合、"client" と指定したインタフェースから、別の "client" と指定したインタフェースへの中継は行えなくなります。

bridge-group が設定されているインタフェースに対して port-channel インタフェースを設定する場合は、同一の bridge-group に所属するすべてのインタフェースに対して同一の port-channel インタフェースを設定する必要があります。

【実行例】

インタフェースが属するブリッジグループ番号を設定します（ブリッジグループ番号：4）。

【gigaethernet インタフェース設定モードの場合】

```
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#bridge-group 4
```

【未設定時】

ブリッジ中継を行いません。

【注意】

以下の設定は未サポートであり、動作保証できないため使用しないでください。

- port-channel インタフェースをブリッジグループなしで、複数の gigabitEthernet インタフェース / trunk-channel インタフェースに設定する
(設定した gigabitEthernet インタフェース / trunk-channel インタフェースの通信動作に不備が発生します)。

```
interface gigabitEthernet 1/1
  channel-group 1
exit
!
interface gigabitEthernet 1/2
  channel-group 1
exit
```

- port-channel インタフェースが設定されている gigabitEthernet インタフェース / trunk-channel インタフェースと、port-channel インタフェースが設定されていない gigabitEthernet インタフェース / trunk-channel インタフェースに、同一ブリッジグループ番号を設定する
(設定した gigabitEthernet インタフェース / trunk-channel インタフェースの通信動作に不備が発生します)。

```
interface gigabitEthernet 1/1
  bridge-group 1
  channel-group 1
exit
!
interface gigabitEthernet 1/2
  bridge-group 1
exit
```

ただし、例外として port-channel インタフェースが設定された gigabitEthernet インタフェースと tunnel インタフェースが同一ブリッジグループ番号を設定する場合のみ使用できます。

```
interface gigabitEthernet 1/1
  bridge-group 1
  channel-group 1
exit
!
interface tunnel 1
  bridge-group 1
exit
```

3.6 インタフェース関連設定

3.6.1 channel-group

【機能】

port-channel インタフェースとのリンク付けの設定

【入力形式】

channel-group <port-channel インタフェース番号>

no channel-group [<port-channel インタフェース番号>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
port-channel インタフェース番号	port-channel インタフェース番号を指定します。	0～16777215	省略不可

【動作モード】

各インタフェース設定モード

【説明】

port-channel インタフェースとのリンク付けを行います。port-channel インタフェース設定モードで各種の設定を行い、このコマンドでport-channel インタフェースとの関連付けを行います。

本設定を行った USB Ethernet インタフェースを、ルーティングや VRRP、BFD のインタフェースとして設定することはサポートしていません。

【実行例】

port-channel インタフェースとのリンク付けを行います（port-channel インタフェース番号：2）。

【gigaethernet インタフェース設定モードの場合】

```
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#channel-group 2
```

【未設定時】

IPv4 または IPv6 通信を行うことができません。

【注意】

以下の設定は未サポートであり、動作保証できないため使用しないでください。

- port-channel インタフェースをブリッジグループなしで、複数の gigaethernet インタフェース／trunk-channel インタフェースに設定する

(設定した gigabitEthernet インタフェース / trunk-channel インタフェースの通信動作に不備が発生します)。

```
interface gigabitEthernet 1/1
  channel-group 1
exit
!
interface gigabitEthernet 1/2
  channel-group 1
exit
```

- port-channel インタフェースが設定されている gigabitEthernet インタフェース / trunk-channel インタフェースと、port-channel インタフェースが設定されていない gigabitEthernet インタフェース / trunk-channel インタフェースに、同一ブリッジグループ番号を設定する

(設定した gigabitEthernet インタフェース / trunk-channel インタフェースの通信動作に不備が発生します)。

```
interface gigabitEthernet 1/1
  bridge-group 1
  channel-group 1
exit
!
interface gigabitEthernet 1/2
  bridge-group 1
exit
```

ただし、例外として port-channel インタフェースが設定された gigabitEthernet インタフェースと tunnel インタフェースが同一ブリッジグループ番号を設定する場合のみ使用できます。

```
interface gigabitEthernet 1/1
  bridge-group 1
  channel-group 1
exit
!
interface tunnel 1
  bridge-group 1
exit
```

3.7 インタフェース description 設定

3.7.1 description

【機能】

説明書きの設定

【入力形式】

description <説明>

no description

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
説明	説明を指定します。	254文字以内のWORD型(*1)	省略不可

*1) 1文字の空白（スペース）は使用可能です。複数の空白（スペース）は1文字にまとめられます。

【動作モード】

各インタフェース設定モード

【説明】

説明書きを設定します。わかりやすい名称を割り当ててください。この名称は、データの中継には影響しません。

【実行例】

説明書きを設定します（説明：GigaEther-A）。

```
【gigaethernet インタフェース設定モードの場合】
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#description GigaEther-A
```

【未設定時】

説明書きは設定されません。

3.8 fragement パケット中継設定

3.8.1 ip fragment-cache disable

【機能】

フラグメントキャッシュ機能を無効にする設定

【入力形式】

ip fragment-cache disable

no ip fragment-cache disable

【動作モード】

port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

インタフェースでのフラグメントキャッシュ機能を無効にする場合に設定します。

設定した場合、フラグメントキャッシュを作成しないため、各機能でのクラシフィケーションで、フラグメントされた二番目以降のパケットの評価ができません。

【実行例】

tunnel インタフェースでフラグメントキャッシュ機能を無効にします。

```
#configure terminal
(config)#interface tunnel 1
(config-if-tun 1)#ip fragment-cache disable
```

【未設定時】

フラグメントキャッシュ機能は有効です。

3.9 フロー制御機能設定

3.9.1 flowcontrol

【機能】

フロー制御機能の設定

【入力形式】

flowcontrol <送信設定> <受信設定>

no flowcontrol

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
送信設定	フロー制御パケット (pause frame) の送信を行うかどうかを指定します。	off on	省略不可
受信設定	フロー制御パケット (pause frame) の受信時にフロー制御を行うかどうかを指定します。	off on	

【動作モード】

gigaethernet インタフェース設定モード

【説明】

gigaethernet ポートのフロー制御機能の送信と受信の動作を設定します。

【実行例】

gigaethernet ポートのフロー制御機能の送信と受信の動作を設定する (送信設定 : on、受信設定 : on)。

```
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#flowcontrol on on
```

【未設定時】

以下のとおり動作します。

送信設定 : off

受信設定 : on

3.10 インタフェース統計情報設定

3.10.1 load-interval

【機能】

パケット送受信レートの測定間隔の設定

【入力形式】

load-interval <測定間隔>

no load-interval

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
測定間隔	show interface コマンドで表示するパケット送受信レートの測定間隔（単位：秒）を指定します。	30 ～ 300	省略不可

【動作モード】

gigaethernet インタフェース設定モード、trunk-channel インタフェース設定モード、USB Ethernet インタフェース設定モード

【説明】

show interface コマンドで表示されるパケット送受信レートの測定間隔（単位：秒）を設定します。

【実行例】

パケット送受信レートの測定間隔（単位：秒）を設定します（測定間隔：60 秒）。

```
【gigaethernet インタフェース設定モードの場合】
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#load-interval 60
```

【未設定時】

測定間隔は 300 秒で動作します。

3.11 MACアドレス設定

3.11.1 mac-address

【機能】

インタフェースのMACアドレスの設定

【入力形式】

mac-address <MACアドレス>

no mac-address [<MACアドレス>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
MACアドレス	MACアドレスを指定します。	HHHH.HHHH.HHHH形式	省略不可

【動作モード】

gigaethernet インタフェース設定モード、management インタフェース設定モード

【説明】

インタフェースのMACアドレスを設定します。

MACアドレスの変更は装置起動時のみ行います。装置起動後はcurrent.cfg(running.cfg)への登録は行いますが、MACアドレスの変更は行いません。

management インタフェースのMACアドレスを変更した場合、自動生成されるIPv6 リンクローカルアドレスや、"eui-64"を指定したipv6 address コマンドで自動生成されるIPv6アドレスが変わります。

【実行例】

インタフェースのMACアドレスを設定します (MACアドレス: 2ed4:4401:2345)。

```
【gigaethernet インタフェース設定モードの場合】
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#mac-address 2ed4.4401.2345
```

【未設定時】

装置固有のMACアドレスで動作します。

3.12 インタフェースメディア設定

3.12.1 media

【機能】

インタフェースで使用可能なケーブルの種類の設定

【入力形式】

media <auto | fiber | metal>

no media [<auto | fiber | metal>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
auto fiber metal	インタフェースで使用可能なケーブルの種類を指定します。	auto: 自動判定します。 fiber: ファイバー（光）portに固定します。 metal: metal(copper)portに固定します。	省略不可

【動作モード】

gigaethernet インタフェース設定モード

【説明】

インタフェースで使用可能なケーブルの種類を設定します。

【注意】

- auto 指定の場合に、10/100/1000BASE-T ポートと SFP ポートがともにケーブル接続した場合、SFP ポートが選択されます。
- auto 指定の場合に、10/100/1000BASE-T ポートがリンクアップしている状態で、SFP ポートにケーブルを接続して SFP ポートをリンクアップさせると、SFP ポートの動作となり、10/100/1000BASE-T ポートはリンクダウン状態となります。
- SFP ポートが選択されている場合は、speed-duplex 設定は無視されます。
- media 設定は、gigaethernet 1/1、1/2 のみ有効です。

【実行例】

インタフェースで使用可能なケーブルの種類を設定します（fiber：ファイバー（光））。

```
【gigaethernet インタフェース設定モードの場合】
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#media fiber
```

【未設定時】

auto（自動判定）で動作します。

3.13 MTU 設定

3.13.1 mtu

【機能】

インタフェースのMTU長の設定

【入力形式】

mtu <MTU長>

no mtu

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
MTU長	MTU長（単位：bytes）を指定します。	1280～9100	省略不可

【動作モード】

port-channel インタフェース設定モード

【説明】

インタフェースのMTU長（単位：bytes）を設定します。また、IPv6でRAを送信する場合、MTUオプションとしてこの値を通知します。

MTUに従いパケットを分割する場合、基本的に均等な長さにパケットを分割します。しかし、コントロールプレーンから送信する、またはコントロールプレーンを経由して中継する際に分割するケースでは、MTU長に合わせたパケットの分割を実施します。

【実行例】

MTU長を設定します（MTU長：1280）。

```
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#mtu 1280
```

【未設定時】

インタフェースごとのMTU長を使用します。RAのMTUオプションはなしで送信します。

3.14 MSS 設定 (port-channel インタフェース)

3.14.1 mss

【機能】

MSS 値の設定

【入力形式】

mss <MSS 値>

no mss [<MSS 値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
MSS 値	MSS 値 (単位: bytes) を指定します。 "off" を指定した場合は、MSS 値を変更しません。 "auto" を指定した場合は、自動で MSS 値を決定します。(*1)	1220 ~ 9060 off auto	省略不可

*1) auto 設定時の MSS 値は以下の値となります。

パケットが IPv4 パケットの場合:

port-channel インタフェースの MTU 長 - 40

パケットが IPv6 パケットの場合:

port-channel インタフェースの MTU 長 - 60

【動作モード】

port-channel インタフェース設定モード

【説明】

インタフェースで MSS 書き換えを行う場合に、その書き換え値 (単位: bytes) を設定します。

MSS 書き換えはパケットの送信、受信時に行います。

パケットの MSS オプションが設定値より大きい場合に書き換えを行います。

【実行例】

MSS 値を設定します (MSS 値: 1220)。

```
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#mss 1220
```

【未設定時】

auto で動作します。

3.15 QoS インタフェース設定

3.15.1 service-policy

【機能】

サービスポリシーの設定

【入力形式】

service-policy {input | output} <policy-map 名> [<シーケンス番号>]

no service-policy {input | output} [<policy-map 名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
input output	受信時／送信時、どちらに policy-map を適用するかを指定します。	input: 受信時 output: 送信時	省略不可
policy-map 名	policy-map 名を指定します。	63 文字以内の TMNAME 型	
シーケンス番号	この設定は無効です。	1 ～ 1000000	

【動作モード】

gigetherneut インタフェース設定モード、gigetherneut サブインタフェース設定モード、tunnel インタフェース設定モード（IPsec、PPPoE、EtherIP、L2TPv3、modem、IPinIP(profile-mode ipip)のみ）、trunk-channel インタフェース設定モード、trunk-channel サブインタフェース設定モード

【説明】

当該インタフェースに対して指定した policy-map を適用します。

1つのインタフェースに適用できる policy-map は input と output に対して、それぞれ1つだけです。

本コマンドは、ip access-group コマンド／ipv6 access-group コマンドで deny されたパケットは対象外になります。

フィルタ／QoS／データコネク ト QoS／DVPN ACL／ポリシールーティングのクラシファイエントリはすべて共用です。各機能でエントリを使用していると、データコネク ト QoS のエントリが入らないことがあります。

【実行例】

サービスポリシーを適用します（output、policy-map 名：policy-map-A）。

```
【gigetherneut インタフェース設定モードの場合】
#configure terminal
(config)#interface gigetherneut 1/1
(config-if-ge 1/1)#service-policy output policy-map-A
```

【未設定時】

サービスポリシーは適用されません。

3.16 MSS 設定（トンネルインタフェース）

3.16.1 set mss

【機能】

tunnel インタフェースで MSS 値を書き換える設定

【入力形式】

set mss <MSS 値>

no set mss [<MSS 値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
MSS 値	MSS 値（単位：bytes）を指定します。 "off" を指定した場合は、MSS 値を変更しません。 "auto" を指定した場合は、自動で MSS 値を決定します。（*1）	1220～9060(*2) off auto	省略不可

*1) auto 設定時の MSS 値は以下の値となります。

パケットが IPv4 パケットの場合：

各 tunnel インタフェースの Inner MTU 長 - 40

パケットが IPv6 パケットの場合：

各 tunnel インタフェースの Inner MTU 長 - 60

*2) PPPoE tunnel インタフェースの場合は、設定範囲は 1220～1452 となります。

【動作モード】

IPSEC ポリシー設定モード（IKEv1/IKEv2 で有効）、ipinip tunnel プロファイル設定モード、PPPoE プロファイル設定モード

【説明】

各 tunnel インタフェースで MSS 書き換えを行う場合に、その書き換え値（単位：bytes）を設定します。

MSS 書き換えはパケットの送信、受信時に行います。

パケットの MSS オプションが設定値より大きい場合に書き換えを行います。

IPsec tunnel インタフェースでは、暗号化前・復号化後のパケットの MSS 値を書き換えます。

IPinIP tunnel インタフェースでは、カプセル化前・デカプセル化後のパケットの MSS 値を書き換えます。

post フラグメントの設定の場合、auto の機能は無効となり off の動作となります。

【実行例】

IPsec tunnel インタフェースの MSS 値（単位：bytes）を設定します（MSS 値：1220）。

```
#configure terminal
(config)#crypto ipsec policy policy-A
(config-ipsec)#set mss 1220
```

【未設定時】

auto で動作します。

3.17 インタフェースリンク状態設定

3.17.1 link-state always-up

【機能】

インタフェースのリンク状態を常に up とする設定

【入力形式】

link-state always-up

no link-state always-up

【動作モード】

port-channel インタフェース設定モード

【説明】

インタフェースのリンク状態を常に up とする場合に設定します。

【実行例】

port-channel インタフェースのリンク状態を常に up とします。

```
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#link-state always-up
```

【未設定時】

インタフェースは実際のリンク状態に従い、up/down します。

3.17.2 shutdown

【機能】

インタフェースのみ DOWN させる設定

【入力形式】

shutdown

no shutdown

【動作モード】

各インタフェース設定モード

【説明】

設定内容はそのままインタフェースのみ DOWN させる場合に設定します。インタフェース DOWN を解除する場合は、no shutdown コマンドを設定します。

【実行例】

インタフェースのみ DOWN させます。

```
【gigaethernet インタフェース設定モードの場合】
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#shutdown
```

【未設定時】

インタフェースは DOWN しません (no shutdown)。

3.18 インタフェースリンク状態変化の設定

3.18.1 ethernet linkdown-delay-time

【機能】

リンクダウンと判定する時間の設定

【入力形式】

ethernet linkdown-delay-time <ガードタイム>

no ethernet linkdown-delay-time [<ガードタイム>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ガードタイム	リンクダウンと判定するまでのリンクダウン状態の継続時間（単位：秒）を指定します。	1～60	省略不可

【動作モード】

gigaethernet インタフェース設定モード、USB Ethernet インタフェース設定モード

【説明】

リンクダウンと判定するまでのリンクダウン状態の継続時間（単位：秒）を指定します。

リンクダウン状態の継続時間が指定した時間に満たない場合は、リンクダウンしていないものとして扱います。

【実行例】

リンクダウンと判定するまでの時間（単位：秒）を設定します（ガードタイム：10 秒）。

```
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#ethernet linkdown-delay-time 10
```

【未設定時】

即時にリンクダウンと判定します。

3.18.2 ethernet linkup-delay-time

【機能】

リンクアップと判定する時間の設定

【入力形式】

ethernet linkup-delay-time <ガードタイム>

no ethernet linkup-delay-time [<ガードタイム>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ガードタイム	リンクアップと判定するまでのリンクアップ状態の継続時間（単位：秒）を指定します。	1～60	省略不可

【動作モード】

gigaethernet インタフェース設定モード、USB Ethernet インタフェース設定モード

【説明】

リンクアップと判定するまでのリンクアップ状態の継続時間（単位：秒）を指定します。

リンクアップ状態の継続時間が指定した時間に満たない場合は、リンクアップしていないものとして扱います。

【実行例】

リンクアップと判定するまでの時間（単位：秒）を設定します（ガードタイム：10 秒）。

```
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#ethernet linkup-delay-time 10
```

【未設定時】

即時にリンクアップと判定します。

3.19 インタフェーススピード／デュプレックス設定

3.19.1 speed-duplex

【機能】

インタフェースの speed/duplex の設定

【入力形式】

speed-duplex <インタフェース速度> <duplex>

no speed-duplex [<インタフェース速度> <duplex>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース速度	インタフェースの speed を指定します。 "auto" を指定した場合は、speed/duplex とともに、Auto ネゴシエーションを利用します。	10:10Mbps 100:100Mbps 1000:1000Mbps auto:Auto ネゴシエーション	省略不可
duplex	インタフェースの duplex を指定します。	full:Full デュプレックス half:Half デュプレックス	省略不可

【動作モード】

gigaethernet インタフェース設定モード、management インタフェース設定モード

【説明】

インタフェースの speed/duplex を設定します。

【注意】

gigaethernet 1/1,1/2 の speed-duplex 設定は、10/100/1000BASE-T ポートを選択している場合に有効になります（SFP ポートを選択している場合は無視されます）。

【実行例】

speed/duplex 設定を行います（インタフェース速度：1000Mbps、duplex:full）。

```
#configure terminal
(config)#interface management 1
(config-if-manage 1)#speed-duplex 1000 full
```

【未設定時】

Auto ネゴシエーションで動作します。

3.20 トンネルインタフェース動作モード設定

3.20.1 tunnel mode

【機能】

tunnel インタフェースで有効にする VPN セレクタ、IPinIP トンネルプロファイル、PPPoE プロファイルの設定

【入力形式】

```
tunnel mode {ipsec [map <VPN セレクタ名>] [match address <IPSEC セレクタ名>] | ipinip tunnel-profile
<IPinIP プロファイル名> | pppoe profile <PPPoE プロファイル名>} | l2tpv3 pseudowire
<PSEUDOWIRE 名> | ether-ip tunnel-profile <EtherIP プロファイル名>
```

```
no tunnel mode [ipsec [map <VPN セレクタ名>] [match address <IPSEC セレクタ名>]] | ipinip tunnel-
profile <IPinIP プロファイル名> | pppoe profile <PPPoE プロファイル名> | l2tpv3 pseudowire
<PSEUDOWIRE 名> | ether-ip tunnel-profile <EtherIP プロファイル名>
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VPN セレクタ名	VPN セレクタ名を指定します。	63 文字以内の CDATA 型	ユーザに固定のインタフェースを使用する
IPSEC セレクタ名	暗号化するパケットとしてセレクタ名を指定します。	63 文字以内の CDATA 型	省略不可
IPinIP プロファイル名	IPinIP トンネルプロファイル名を指定します。	63 文字以内の WORD 型	
PPPoE プロファイル名	PPPoE プロファイル名を指定します。	63 文字以内の CDATA 型	
PSEUDOWIRE 名	L2TPv3 PSEUDOWIRE を指定します。	63 文字以内の CDATA 型	省略不可
EtherIP プロファイル名	EtherIP プロファイル名を指定します。	63 文字以内の CDATA 型	省略不可

【動作モード】

tunnel インタフェース設定モード

【説明】

tunnel インタフェースで有効にする VPN セレクタ、IPinIP トンネルプロファイル、PPPoE プロファイル、L2TPv3 PSEUDOWIRE、EtherIP プロファイルを設定します。

VPN セレクタ名は、crypto map コマンドで設定した名称を指定します。

ダイナミックセレクタでユーザに固定のインタフェースを使用したい場合は、VPN セレクタ名を省略します。

また、IKEv1 を使用する際に 1 つの VPN ピアに対して複数の IPsec SA を確立したい場合は、tunnel インタフェースで有効にする VPN セレクタを設定し、それぞれ異なる IPSEC セレクタを設定します。

IPinIP プロファイル名は、ipinip tunnel-profile コマンドで設定した名称を指定します。

PPPoE プロファイル名は、pppoe profile コマンドで設定した名称を指定します。

PSEUDOWIRE 名は、l2tpv3 pseudowire コマンドで設定した名称を指定します。

EtherIP プロファイル名は、ether-ip tunnel-profile コマンドで設定した名称を指定します。

【実行例】

tunnel インタフェースで有効にする VPN セレクタを設定します (VPN セレクタ名: selector-A)。

```
#configure terminal
(config)#interface tunnel 1
(config-if-tun 1)#tunnel mode ipsec map selector-A
```

【未設定時】

tunnel インタフェースで IPsec、IPinIP 通信、PPPoE 通信、L2TPv3、EtherIP 通信の機能が動作しません。

3.21 VLAN ID 設定

3.21.1 vlan-id

【機能】

VLAN-ID 値の設定

【入力形式】

vlan-id <VLAN-ID 値>

no vlan-id

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VLAN-ID 値	VLAN-ID 値を指定します。	1 ～ 4094	省略不可

【動作モード】

gigaethernet インタフェース設定モード、trunk-channel インタフェース設定モード

【説明】

VLAN-ID 値を設定します。この値は 802.1Q フレームの VLAN-ID 値として使用します。

【注意】

本装置では、VLAN-ID 値 "1" が特殊な用途で予約されていますので、802.1Q フレームの VLAN-ID 値に "1" を使用する場合には注意が必要です。サブインタフェースで VLAN-ID 値に "1" を使用する場合は、そのサブインタフェースが属するインタフェースの設定モードで、VLAN-ID 値として "1" 以外を設定しておく必要があります。

【実行例】

VLAN-ID 値を設定します (VLAN-ID 値 : 4)。

```
【gigaethernet インタフェース設定モードの場合】
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#vlan-id 4
```

【未設定時】

VLAN を使用できません。

3.21.2 vlan-id

【機能】

サブインタフェースで受信することができる VLAN タグの VLAN-ID 値の設定

【入力形式】

vlan-id <VLAN-ID 値> [second-vlan-id <2nd VLAN-ID 値>]

no vlan-id

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VLAN-ID 値	802.1Q における VLAN-ID 値、または、Q-in-Q VLAN タグ終端におけるサービスタグ (S-TAG) の VLAN-ID 値を指定します。	1～4094	省略不可
2nd VLAN-ID 値	Q-in-Q VLAN タグ終端におけるカスタムタグ (C-TAG) の VLAN-ID 値を指定します。	1～4094	省略不可

【動作モード】

gigaethernet サブインタフェース設定モード、trunk-channel サブインタフェース設定モード

【説明】

サブインタフェースで受信することができる VLAN タグの VLAN-ID 値を設定します。

VLAN-ID 値に 1 段目の VLAN タグの vlan-id を指定し、Q-in-Q VLAN タグ終端を有効にしたい場合には、2nd VLAN-ID 値に 2 段目のタグの VLAN-ID 値を指定します。

second-vlan-id の指定を省略した場合には、802.1Q の 1 段タグインタフェースとして有効になります。

【注意】

本装置では、VLAN-ID 値 "1" が特殊な用途で予約されていますので、802.1Q フレームの VLAN-ID 値に "1" を使用する場合には注意が必要です。

サブインタフェースで VLAN-ID 値に "1" を使用する場合は、そのサブインタフェースが属するインタフェースの設定モードで、VLAN-ID 値として "1" 以外を設定しておく必要があります。

【実行例】

サブインタフェースで受信することができる VLAN タグの VLAN-ID 値を設定します (VLAN-ID 値 : 100、2nd VLAN-ID 値 : 200)。

```
【gigaethernet サブインタフェース設定モードの場合】
#configure terminal
(config)#interface gigaethernet 1/1.100
(config-if-ge 1/1/100)#vlan-id 100 second-vlan-id 200
```

【未設定時】

VLAN を使用できません。

Q-in-Q VLAN タグ終端機能を使用できません。

3.21.3 ip redirect dp-forward

【機能】

折り返し中継をデータプレーンで行う場合に設定

【入力形式】

ip redirect dp-forward {enable | disable}

no ip redirect dp-forward [enable | disable]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
enable	データプレーンでの折り返し中継を行います。	-	省略不可
disable	データプレーンでの折り返し中継を行いません。	-	省略不可

【動作モード】

port-channel インタフェース設定モード

【説明】

折り返し中継をデータプレーンで行う場合に設定します。

【注意】

設定によりデータプレーンで折り返し中継を行う場合には ICMP リダイレクトメッセージをパケットの送信元には送りません。

なお、本設定を有効(enable)とした場合も IP オプション付きのパケット・ARP 未解決のパケットについてはコントロールプレーンにて折り返し中継を行います。

コントロールプレーンで折り返し中継を行う場合は、設定の有無に限らず ICMP リダイレクトメッセージを送信元に送ります。

【実行例】

```
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ip redirect dp-forward enable
```

【未設定時】

折り返し中継をコントロールプレーンで行います。

折り返し中継時には送信元に ICMP リダイレクトメッセージを送ります。

第4章 PPPoE の設定



この章では、PPPoE の設定に関するコマンドについて説明します。

4.1 PPPoE の設定

4.1.1 account

【機能】

PPPoE サーバからの認証に使用するユーザ ID、パスワードの設定

【入力形式】

account <ユーザ ID> <パスワード> [{secret | private} [encrypted]]

no account [<ユーザ ID> <パスワード> [{secret | private} encrypted]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ユーザ ID	PPPoE サーバに接続する際のユーザ ID を設定します。	127 文字以内の STRING 型	省略不可
パスワード	PPPoE サーバに接続する際のパスワードを設定します。	128 文字以内の STRING 型 (暗号化されていない場合) 254 文字以内の STRING 型 (暗号化されている場合)	省略不可
secret private	パスワードとして使用する文字列の暗号化／復号化に共通の鍵を使用するか、固有の鍵を使用するかを指定します。	secret：共通の鍵を使用する private：固有の鍵を使用する	暗号化せずに保存
encrypted	パスワードとして使用する文字列が暗号化されている場合に指定します。	-	非暗号化文字列

【動作モード】

PPPoE プロファイル設定モード

【説明】

PPPoE サーバからの認証に使用するユーザ ID、パスワードを設定します。

"secret" を指定した場合は、すべての GX500 に共通の鍵を使って暗号化／復号化し、"private" を指定した場合は、装置固有の鍵を使って暗号化／復号化します。"secret" または "private" を指定した場合、show current.cfg(show running.cfg) コマンドなどで内容を確認すると、暗号化されたパスワードの形式で表示されます。

"encrypted" を指定した場合は、パスワードとして使用する文字列を暗号化された文字列と判断します。

【実行例】

PPPoE サーバにユーザ ID：user@xxxx.ne.jp、パスワード：pass で接続します。

```
#configure terminal
(config)# pppoe profile pppoe-profile-A
(config-pppoe-profile)#account user@xxxx.ne.jp pass
```

【未設定時】

相手から認証を求められた場合、PPPoE セッションを確立できません。

4.1.2 authentication accept

【機能】

PPPoE で認証を許可する認証プロトコルの設定

【入力形式】

authentication accept <認証プロトコル>

no authentication accept [<認証プロトコル>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
認証プロトコル	認証を許可する認証プロトコル (CHAP または PAP) を設定します。	any:CHAP、PAP chap:CHAP pap:PAP	省略不可

【動作モード】

PPPoE プロファイル設定モード

【説明】

PPPoE で認証を許可する認証プロトコルを指定します。

【実行例】

CHAP での認証を許可します。

```
#configure terminal
(config)# pppoe profile pppoe-profile-A
(config-pppoe-profile)#authentication accept chap
```

【未設定時】

CHAP、PAP での認証を許可します。

4.1.3 ncp

【機能】

PPP で使用する NCP の設定

【入力形式】

ncp <NCP>

no ncp [<NCP>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
NCP	PPP で使用する NCP を指定します。	ipcp:IPCP ipv6cp:IPv6CP both:IPCP、IPv6CP	省略不可

【動作モード】

PPPoE プロファイル設定モード

【説明】

PPP で使用する NCP を設定します。

【実行例】

PPP で NCP として IPCP を使用します。

```
#configure terminal
(config)# pppoe profile pppoe-profile-A
(config-pppoe-profile)#ncp ipcp
```

【未設定時】

IPCP を使用します。

4.1.4 pppoe enable

【機能】

PPPoE 通信で使用する物理インタフェースの設定

【入力形式】

pppoe enable

no pppoe enable

【動作モード】

gigaethernet インタフェース設定モード

【説明】

PPPoE 通信で使用する物理インタフェースに設定します。

【実行例】

gigaethernet 1/1 で PPPoE を使用します。

```
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#pppoe enable
```

【未設定時】

その物理インタフェースで PPPoE 通信の機能が動作しません。

4.1.5 pppoe interface

【機能】

tunnel インタフェースと関連付ける PPPoE 通信で使用する物理インタフェースの設定

【入力形式】

pppoe interface gigabitEthernet <インタフェース番号>

no pppoe interface gigabitEthernet [<インタフェース番号>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース番号	インタフェース番号を指定します。	-	省略不可

【動作モード】

tunnel インタフェース設定モード

【説明】

tunnel インタフェースと関連付ける PPPoE 通信で使用する物理インタフェースを設定します。

【実行例】

tunnel インタフェースと関連付ける PPPoE 通信で使用する物理インタフェースを設定します（物理インタフェース：gigabitEthernet1/1）。

```
#configure terminal
(config)#interface tunnel 1
(config-if-tun 1)#pppoe interface gigabitEthernet 1/1
```

【未設定時】

tunnel インタフェースで PPPoE 通信の機能が動作しません。

4.1.6 pppoe profile

【機能】

PPPoE 情報を設定する PPPoE プロファイル設定モードへの移行

【入力形式】

pppoe profile <PPPoE プロファイル名>

no pppoe profile <PPPoE プロファイル名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
PPPoE プロファイル名	PPPoE 設定情報を識別する文字列を指定します。	63 文字以内の WORD 型	省略不可

【動作モード】

基本設定モード

【説明】

PPPoE 情報を設定する PPPoE プロファイル設定モードに移行します。

【実行例】

PPPoE プロファイル設定モードに移行します（プロファイル名：pppoe-profile-A）。

```
#configure terminal
(config)#pppoe profile pppoe-profile-A
(config-pppoe-profile)#
```

4.1.7 server-name

【機能】

PPPoE サーバの名称の設定

【入力形式】

server-name <サーバ名>

no server-name [<サーバ名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
サーバ名	PPPoE サーバの名称を設定します。	64 文字以内の STRING 型	省略不可

【動作モード】

PPPoE プロファイル設定モード

【説明】

PPPoE サーバの名称を指定します。本コマンドが設定されている場合には、PADO 内の AC-Name TAG と設定されたサーバ名が一致するサーバにのみ PADR を送信します。サーバ名が一致するサーバが存在しない場合には、PADR を送信しません。

【実行例】

A-Provider と PPPoE セッションを確立します。

```
#configure terminal
(config)# pppoe profile pppoe-profile-A
(config-pppoe-profile)# server-name A-Provider
```

【未設定時】

PADO を受信した際、サーバ名を確認しません。

4.1.8 service-name

【機能】

PPPoE のネゴシエーションで使用するサービス名の設定

【入力形式】

service-name <サービス名>

no service-name [<サービス名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
サービス名	PPPoE のネゴシエーションで使用するサービス名を指定します。	20 文字以内の STRING 型	省略不可

【動作モード】

PPPoE プロファイル設定モード

【説明】

PPPoE のネゴシエーションで使用するサービス名を設定します。

【実行例】

サービス名として xxxx.ne.jp を設定します。

```
#configure terminal
(config)# pppoe profile pppoe-profile-A
(config-pppoe-profile)# service-name xxxx.ne.jp
```

【未設定時】

サービス名なしで PPPoE のネゴシエーションを行います。

4.1.9 set mtu

【機能】

PPPoE で使用する tunnel インタフェースの MTU 長の設定

【入力形式】

set mtu <MTU 長>

no set mtu [<MTU 長>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
MTU 長	MTU 長（単位：bytes）を指定します。	1280～1492	省略不可

【動作モード】

PPPoE プロファイル設定モード

【説明】

PPPoE で使用する tunnel インタフェースの MTU 長を指定します。

MTU に従いパケットを分割する場合、基本的に均等な長さにパケットを分割します。しかし、コントロールプレーンから送信する、またはコントロールプレーンを経由して中継する際に分割するケースでは、MTU 長に合わせたパケットの分割を実施します。

【実行例】

PPPoE で使用する tunnel インタフェースの MTU 長を 1454bytes にします。

```
#configure terminal
(config)# pppoe profile pppoe-profile-A
(config-pppoe-profile)#set mtu 1454
```

【未設定時】

MTU 長 1454bytes として動作します。

第5章 リンクアグリゲー ションの設定



この章では、リンクアグリゲーションの設定に関するコマンドについて説明します。

5.1 リンクアグリゲーション設定

5.1.1 bridge-group

【機能】

インタフェースが属するブリッジグループ番号の設定

【入力形式】

bridge-group <ブリッジグループ番号> [client | server]

no bridge-group [<ブリッジグループ番号> [client | server]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ブリッジグループ番号	ブリッジグループ番号を指定します。	1～16777215	省略不可
client server	接続する端末の属性を指定します。	-	server

【動作モード】

trunk-channel インタフェース設定モード、trunk-channel サブインタフェース設定モード

【説明】

インタフェースが属するブリッジグループ番号を設定します。

bridge-group が設定されているインタフェースに対して port-channel を設定する場合は、同一の bridge-group に所属するすべてのインタフェースに対して同一の port-channel を設定する必要があります。

【実行例】

インタフェースが属するブリッジグループ番号を設定します（ブリッジグループ番号：4）。

```
【trunk-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface trunk-channel 1
(config-if-tr 1)#bridge-group 4
```

【未設定時】

ブリッジ中継を行いません。

【注意】

以下の設定は未サポートであり、動作保証できないため使用しないでください。

- port-channel インタフェースをブリッジグループなしで、複数の gigaethernet インタフェース／trunk-channel インタフェースに設定する

(設定した gigabitEthernet インタフェース / trunk-channel インタフェースの通信動作に不備が発生します)。

```
interface gigabitEthernet 1/1
  channel-group 1
exit
!
interface gigabitEthernet 1/2
  channel-group 1
exit
```

- port-channel インタフェースが設定されている gigabitEthernet インタフェース / trunk-channel インタフェースと、port-channel インタフェースが設定されていない gigabitEthernet インタフェース / trunk-channel インタフェースに、同一ブリッジグループ番号を設定する

(設定した gigabitEthernet インタフェース / trunk-channel インタフェースの通信動作に不備が発生します)。

```
interface gigabitEthernet 1/1
  bridge-group 1
  channel-group 1
exit
!
interface gigabitEthernet 1/2
  bridge-group 1
exit
```

ただし、例外として port-channel インタフェースが設定された gigabitEthernet インタフェースと tunnel インタフェースが同一ブリッジグループ番号を設定する場合のみ使用できます。

```
interface gigabitEthernet 1/1
  bridge-group 1
  channel-group 1
exit
!
interface tunnel 1
  bridge-group 1
exit
```

5.1.2 switchport mode dot1q tunnel

【機能】

サブインタフェースでフレームを送信する際の TPID 値の設定

【入力形式】

switchport mode dot1q tunnel tpid <TPID 値>

no switchport mode dot1q tunnel tpid [<TPID 値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
TPID 値	サブインタフェースでフレームを送信する際の TPID 値で指定します。	8000 ~ ffff (16 進数)	省略不可

【動作モード】

gigabitEthernet インタフェース設定モード、trunk-channel インタフェース設定モード

【説明】

サブインタフェースでフレームを送信する際のTPID値を設定します。

【実行例】

サブインタフェースでフレームを送信する際のTPID値を設定します（TPID値：9100（16進数））。

```
【gigaethernet インタフェース設定モードの場合】
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#switchport mode dot1q tunnel tpid 9100
```

【未設定時】

8100（16進数）をVLAN TAGのTPIDとします。

5.1.3 switchport passthrough

【機能】

特定の2インタフェース間の中継パスの設定

【入力形式】

switchport passthrough <インタフェース名> <インタフェース番号>[.<サブインタフェースインデックス番号>]

no switchport passthrough [<インタフェース名> <インタフェース番号>[.<サブインタフェースインデックス番号>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース名	インタフェース名を指定します。	gigaethernet tunnel trunk-channel	省略不可
インタフェース番号	インタフェース番号を指定します。	-	省略不可
サブインタフェースインデックス番号	サブインタフェースインデックス番号を指定します。	1～9999	サブインタフェースを使用しない

【動作モード】

gigaethernet インタフェース設定モード、gigaethernet サブインタフェース設定モード、trunk-channel インタフェース設定モード、trunk-channel サブインタフェース設定モード、tunnel インタフェース設定モード

【説明】

IEEE802.1Q トンネリングにおいて、特定の2インタフェース間の中継（point-to-point 中継）パスを設定します。

【実行例】

特定の 2 インタフェース間の中継パスを設定します（インタフェース番号：1）。

```
【trunk-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface trunk-channel 1
(config-if-tr 1)#switchport passthrough trunk-channel 1
```

【未設定時】

特定の 2 インタフェース間の中継パスを設定しません。

5.1.4 switchport transparent

【機能】

受信フレームの VLAN TAG を CTAG として扱い、TAG の有無に関わらずインタフェースで受信する設定

【入力形式】

switchport transparent

no switchport transparent

【動作モード】

gigaethernet インタフェース設定モード、trunk-channel インタフェース設定モード

【説明】

受信フレームの VLAN TAG を CTAG として扱い、TAG の有無に関わらずインタフェースで受信する場合に設定します。

本設定を行ったインタフェース上に設定されているサブインタフェースはすべて無効設定扱いとなります。

【実行例】

受信フレームの VLAN TAG を CTAG として扱い、TAG の有無に関わらずインタフェースで受信します。

```
【gigaethernet インタフェース設定モードの場合】
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#switchport transparent
```

【未設定時】

なし。

5.1.5 trunk-group

【機能】

物理インタフェースをリンクアグリケーション機能で使用する設定

【入力形式】

trunk-group <インタフェース番号>

no trunk-group [<インタフェース番号>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース番号	インタフェース番号を指定します。	1～5	省略不可

【動作モード】

gigaethernet インタフェース設定モード

【説明】

物理インタフェースをリンクアグリケーション機能で使用する際に設定します。

本設定を行った場合は、インタフェース設定モードの以下のコマンド以外は無効となります。

- description
- shutdown
- ethernet linkup-delay-time
- ethernet linkdown-delay-time
- snmp trap link-status
- trunk-member port-priority
- speed-duplex
- media

本設定を行った場合は、サブインタフェースの設定も無効となります。

【実行例】

物理インタフェースをリンクアグリケーション機能で使します（インタフェース番号：1）。

```
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#trunk-group 1
```

【未設定時】

リンクアグリゲーション機能を利用できません（通常の物理インタフェースとして動作）。

5.1.6 trunk-member port-priority

【機能】

リンクアグリケーション用ポートの優先度の設定

【入力形式】

trunk-member port-priority <優先度>

no trunk-member port-priority [<優先度>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
優先度	リンクアグリゲーション用ポートの優先度を指定します。	0～65535	省略不可

【動作モード】

gigaethernet インタフェース設定モード

【説明】

リンクアグリケーション用ポートの優先度を設定します。小さい値が優先されます。

同じ優先度の場合は、以下の順番で優先度が決まります。

giga 1/1 > giga 1/2 > . . . > giga 1/10

【実行例】

リンクアグリケーション用ポートの優先度を設定します（優先度：128）。

```
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#trunk-member port-priority 128
```

【未設定時】

優先度は 32768 で動作します。

5.1.7 trunk-group mode

【機能】

リンクアグリケーションの動作モードの設定

【入力形式】

trunk-group mode <動作モード>

no trunk-group mode [<動作モード>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
動作モード	リンクアグリゲーションの動作モードを指定します。	static:static モード active:active モード (lacp) passive:passive モード (lacp)	省略不可

【動作モード】

trunk-channel インタフェース設定モード

【説明】

リンクアグリケーションの動作モードを設定します。

リモート装置とリンクアップできるモードの組み合わせは以下です。

sstatic - static: static モードでtrunk-channelを接続します。

sactive - active: LACP モードでtrunk-channelを接続します。

sactive - passive: LACP モードでtrunk-channelを接続します。

"passive" と指定した側の装置は、LACP を受信するまで LACPDU の送受信を開始しません。

【実行例】

リンクアグリケーションの動作モードを設定します（動作モード：active）。

```
#configure terminal
(config)#interface trunk-channel 1
(config-if-tr 1)#trunk-group mode active
```

【未設定時】

動作モードは static モードで動作します。

5.1.8 trunk-group lacpdu-timeout

【機能】

LACPDU のタイムアウト値の設定

【入力形式】

trunk-group lacpdu-timeout <タイムアウト値>

no trunk-group lacpdu-timeout [<タイムアウト値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
タイムアウト値	LACPDU のタイムアウト値を指定します。	short : 3 秒 long : 90 秒	省略不可

【動作モード】

trunk-channel インタフェース設定モード

【説明】

LACPDU のタイムアウト値を設定します。本コマンドを設定することで、リモート装置の LACPDU 送信周期が変わります。

【実行例】

LACPDU のタイムアウト値を設定します（タイムアウト値：short）。

```
#configure terminal
(config)#interface trunk-channel 1
(config-if-tr 1)#trunk-group lacpdu-timeout short
```

【未設定時】

タイムアウト値は 90 秒(long) で動作します。

5.1.9 trunk-group lacpdu-dst-mac

【機能】

LACPDU の宛先 MAC アドレスの設定

【入力形式】

trunk-group lacpdu-dst-mac <宛先 MAC アドレス>

no trunk-group lacpdu-dst-mac [<宛先 MAC アドレス>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
宛先 MAC アドレス	LACPDU の宛先 MAC アドレスを指定します。	0180.c200.0000 : 01:80:C2:00:00:00 0180.c200.0002 : 01:80:C2:00:00:02 0180.c200.0003 : 01:80:C2:00:00:03	省略不可

【動作モード】

trunk-channel インタフェース設定モード

【説明】

LACPDU の宛先 MAC アドレスを設定します。

【実行例】

LACPDU の宛先 MAC アドレスを設定します（宛先 MAC アドレス：01:80:C2:00:00:03）。

```
#configure terminal
(config)#interface trunk-channel 1
(config-if-tr 1)#trunk-group lacpdu-dst-mac 0180.c200.0003
```

【未設定時】

宛先 MAC アドレスは 01:80:C2:00:00:02 で動作します。

5.1.10 trunk-group max-active-port

【機能】

アクティブポートの最大数の設定

【入力形式】

trunk-group max-active-port <ポート数>

no trunk-group max-active-port [<ポート数>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ポート数	アクティブポートの最大数を指定します。	1～10	省略不可

【動作モード】

trunk-channel インタフェース設定モード

【説明】

アクティブポートの最大数を設定します。指定したポート数以上の物理インタフェースは、スタンバイポートとなります。

【実行例】

アクティブポートの最大数を設定します（ポート数：1）。

```
#configure terminal
(config)#interface trunk-channel 1
(config-if-tr 1)#trunk-group max-active-port 1
```

【未設定時】

スタンバイリンク機能を使用しません。

5.1.11 trunk-group min-active-port

【機能】

アクティブポートの最小数の設定

【入力形式】

trunk-group min-active-port <ポート数>

no trunk-group min-active-port [<ポート数>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ポート数	アクティブポートの最小数を指定します。	1～10	省略不可

【動作モード】

trunk-channel インタフェース設定モード

【説明】

アクティブポートの最小数を設定します。

指定したポート数未満になると、trunk-channel がリンクダウンします。

【実行例】

アクティブポートの最小数を設定します（ポート数：10）。

```
#configure terminal
(config)#interface trunk-channel 1
(config-if-tr 1)#trunk-group min-active-port 10
```

【未設定時】

最小リンク機能を使用しません。

5.1.12 trunk-group standby-no-receive

【機能】

スタンバイポートでパケットを受信しない設定

【入力形式】

trunk-group standby-no-receive

no trunk-group standby-no-receive

【動作モード】

trunk-channel インタフェース設定モード

【説明】

スタンバイポートでパケットを受信ないようにします。

【実行例】

スタンバイポートでパケットを受信しません。

```
#configure terminal
(config)#interface trunk-channel 1
(config-if-tr 1)#trunk-group standby-no-receive
```

【未設定時】

スタンバイポートでパケットを受信します。

5.1.13 trunk-group system-priority

【機能】

リンクアグリケーション用システムの優先度の設定

【入力形式】

trunk-group system-priority <優先度>

no trunk-group system-priority [<優先度>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
優先度	リンクアグリゲーション用システムの優先度を指定します。	0～65535	省略不可

【動作モード】

trunk-channel インタフェース設定モード

【説明】

リンクアグリゲーション用システムの優先度を設定します。小さい値ほど優先度が高くなります。
対向装置と同じ優先度の場合は、trunk-channel の MAC アドレスで優先度が決まります。

【実行例】

リンクアグリゲーション用システムの優先度を設定します（優先度：128）。

```
#configure terminal
(config)#interface trunk-channel 1
(config-if-tr 1)#trunk-group system-priority 128
```

【未設定時】

優先度は 32768 で動作します。

5.1.14 trunk-group transmit-pause-time

【機能】

ポートステータスが変化した際に中継停止する時間の設定

【入力形式】

trunk-group transmit-pause-time <中継停止時間>

no trunk-group transmit-pause-time [<中継停止時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
中継停止時間	ポートステータスが変化した際に、中継停止する時間（単位：10 マイクロ秒）を指定します。	lacp：リモート装置から通知された時間 (collector max delay) 中継停止 0～65535：指定した時間（10 マイクロ秒） 中継停止 off：中継停止しない	省略不可

【動作モード】

trunk-channel インタフェース設定モード

【説明】

ポートステータスが変化した際に、中継停止する時間（単位：10 マイクロ秒）を設定します。
trunk-channelの構成が変化したときにパケット順序が入れ替わる場合に使用します。

【実行例】

ポートステータスが変化した際に、切り替わるフローを中継停止する時間（単位：10 マイクロ秒）を設定します（中継停止時間：0 マイクロ秒）。

```
#configure terminal
(config)#interface trunk-channel 1
(config-if-tr 1)#trunk-group transmit-pause-time 0
```

【未設定時】

中継停止時間は1ミリ秒(100)で動作します。

5.1.15 trunk-group collector-max-delay

【機能】

LACPでリモート装置に通知する collector max delay 値の設定

【入力形式】

trunk-group collector-max-delay <collector max delay 値>

no trunk-group collector-max-delay [<collector max delay 値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
collector max delay 値	LACPでリモート装置に通知する collector max delay 値（単位：10 マイクロ秒）を指定します。	0～65535	省略不可

【動作モード】

trunk-channel インタフェース設定モード

【説明】

LACPでリモート装置に通知する collector max delay 値（単位：10 マイクロ秒）を設定します。

【実行例】

LACPでリモート装置に通知する collector max delay 値（単位：10 マイクロ秒）を設定します（collector max delay 値：2ミリ秒）。

```
#configure terminal
(config)#interface trunk-channel 1
(config-if-tr 1)#trunk-group collector-max-delay 200
```

【未設定時】

collector max delay 値は1ミリ秒(100)で動作します。

5.1.16 trunk-group load-balance

【機能】

負荷分散方式の設定

【入力形式】

trunk-group load-balance <負荷分散方式>

no trunk-group load-balance [<負荷分散方式>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
負荷分散方式	負荷分散方式を指定します。	mac:MAC DA/SA l3: 中継データに応じた バランシング vlan: 送信 SVID(sub- interface vlan-id) q-in-q: 送信 SVID/ CVID	省略不可

【動作モード】

trunk-channel インタフェース設定モード

【説明】

負荷分散方式を設定します。

【実行例】

負荷分散方式を設定します（負荷分散方式：mac）。

```
#configure terminal
(config)#interface trunk-channel 1
(config-if-tr 1)#trunk-group load-balance mac
```

【未設定時】

負荷分散方式は中継データに応じたバランシング (l3) で動作します。

第6章 RIPの設定



この章では、RIPの設定に関するコマンドについて説明します。

6.1	IPv4 経路交換の設定	178
-----	--------------------	-----

6.1 IPv4 経路交換の設定

6.1.1 router rip

【機能】

RIP サービス設定モードへの移行

【入力形式】

router rip

no router rip

【動作モード】

基本設定モード

【説明】

RIP サービス設定モードに移行します。コマンドの先頭に "no" を指定することで、RIP サービス設定モードの内容がすべて消去されます。

【実行例】

RIP サービス設定モードに移行します。

```
#configure terminal
(config)#router rip
(config-rip)#
```

6.1.2 default-information originate

【機能】

デフォルトルートを生成し広告する設定

【入力形式】

default-information originate

no default-information originate

【動作モード】

RIP サービス設定モード

【説明】

自身をデフォルトルートとして、RIP で通知するかどうかを指定します。

スタティック設定でデフォルトルートを設定していたり、ルーティングプロトコルによりデフォルトルートを学習していた場合にも、この設定が優先されます。

【実行例】

デフォルトルートを生成し広告します。

```
#configure terminal
(config)#router rip
(config-rip)#default-information originate
```

【未設定時】

デフォルトルートを生成しません。

6.1.3 default-metric

【機能】

メトリック値の設定

【入力形式】

default-metric <メトリック値>

no default-metric [<メトリック値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
メトリック値	メトリック値を指定します。	1 ～ 16	省略不可

【動作モード】

RIP サービス設定モード

【説明】

再広告した経路情報（connected 経路は除く）のデフォルトのメトリック値を設定します。

connected 経路の場合には、デフォルトのメトリック値は 1 になります。

redistribute コマンドで metric を指定した場合には、そちらの設定が優先されます。

【実行例】

メトリック値を設定します（メトリック値：8）。

```
#configure terminal
(config)#router rip
(config-rip)#default-metric 8
```

【未設定時】

メトリック値は 1 で動作します。

6.1.4 distance

【機能】

ディスタンス値の設定

【入力形式】

distance <ディスタンス値> [<IPv4 アドレス> <ネットマスク> [<アクセスリスト番号>]]

no distance <ディスタンス値> [<IPv4 アドレス> <ネットマスク> [<アクセスリスト番号>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ディスタンス値	ディスタンス値を指定します。	1～255	省略不可
IPv4 アドレス	IPv4 アドレスを指定します。	IPv4 アドレス形式	対象経路を限定しない
ネットマスク	ネットマスクを指定します。	IPv4 アドレス形式	
アクセスリスト番号	アクセスリスト番号を指定します。	-	

【動作モード】

RIP サービス設定モード

【説明】

同じ宛先への経路情報が複数存在した場合、どの情報を有効にするかを決定するために用いるディスタンス値（優先度）を設定します。RIP サービス設定モードでは、送信ルータまたはアクセスリスト番号を用いて対象経路を限定することができます。

【実行例】

ディスタンス値を設定します（ディスタンス値：100）。

```
#configure terminal
(config)#router rip
(config-rip)#distance 100
```

【未設定時】

以下の値で動作します（RIP は 120）。

プロトコル	デフォルト値	備考
スタティック	1	設定変更可能
直接経路	-	設定変更不可
BGP(external)	20	設定変更可能
BGP(internal)	200	
BGP(local)		
RIP	120	設定変更可能
OSPF(external)	110	設定変更可能
OSPF(inter-area)		
OSPF(intra-area)		

6.1.5 distribute-list

【機能】

フィルタリングの設定

【入力形式】

distribute-list {prefix <プレフィックスリスト名> | <アクセスリスト番号>} {in | out} [<インタフェース名> <インタフェース番号>]

no distribute-list {prefix <プレフィックスリスト名> | <アクセスリスト番号>} {in | out} [<インタフェース名> <インタフェース番号>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プレフィックスリスト名	広告するプレフィックスのプレフィックスリスト名を指定します。	254 文字以内の WORD 型	省略不可
アクセスリスト番号	広告するプレフィックスのアクセスリスト番号を指定します。	-	省略不可
in out	受信時に適用するか、送信時に適用するかを指定します。	in: 受信時 out: 送信時	省略不可
インタフェース名	インタフェース名を指定します。	-	全インタフェース
インタフェース番号	インタフェース番号を指定します。	-	全インタフェース

【動作モード】

RIP サービス設定モード

【説明】

プレフィックスリスト名またはアクセスリスト番号で設定したアドレスを用いて、RIP 経路のフィルタリングを行う場合に設定します。フィルタリングを行うインタフェースを指定することもできます。

【実行例】

フィルタリングを行います（プレフィックスリスト名：prefix-list-A、受信時）。

```
#configure terminal
(config)#router rip
(config-rip)#distribute-list prefix prefix-list-A in
```

【未設定時】

フィルタリングを行いません。

6.1.6 ip rip authentication mode

【機能】

パスワードを送る方式の設定

【入力形式】

ip rip authentication mode {md5 | text}

no ip rip authentication mode [md5 | text]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
md5 text	RIP バージョン 2 においてパスワードを送る方式を指定します。	md5:MD5 ハッシュ計算後のデータ text:simpletext	省略不可

【動作モード】

port-channel インタフェース設定モード、tunnel インタフェース設定モード（tunnel mode ipsec のみ）

【説明】

RIP バージョン 2 を送信する場合の、パスワードを送る方式を設定します。key フレーズを Simple Text で送信する場合は "text" を、MD5 ハッシュ計算したあとのデータ（Unrecognized Authentication Type）で送信する場合は "md5" を設定します。ip rip authentication string コマンドで key フレーズを設定します。この設定が異なるルータとは、RIP バージョン 2 の経路交換を行いません。

【実行例】

パスワードを送る方式を設定します（MD5 ハッシュ計算後のデータ）。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ip rip authentication mode md5
```

【未設定時】

パスワードを送る方式は simple-text で動作します。

6.1.7 ip rip authentication string

【機能】

認証キーワードの設定

【入力形式】

ip rip authentication string <認証キーワード>

no ip rip authentication string <認証キーワード>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
認証キーワード	RIP Version2 の認証キーワードを設定します。	16 文字以内の STRING 型	省略不可

【動作モード】

port-channel インタフェース設定モード、tunnel インタフェース設定モード（tunnel mode ipsec のみ）

【説明】

RIP Version2 の認証キーワードを設定します。認証キーワードを送信する場合に必要な設定です。設定が異なるルータとは、RIP Version2 での経路交換を行いません。

【実行例】

RIP Version2 の認証キーワードを設定します（認証キーワード：secret）。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ip rip authentication string secret
```

【未設定時】

認証キーワードなしで動作します。

6.1.8 no ip rip receive-packet

【機能】

RIP パケットを受信しない設定

【入力形式】

no ip rip receive-packet

ip rip receive-packet

【動作モード】

port-channel インタフェース設定モード、tunnel インタフェース設定モード（tunnel mode ipsec のみ）

【説明】

RIP パケットを受信しない場合に設定します。

【実行例】

RIP パケットを受信しません。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#no ip rip receive-packet
```

【未設定時】

RIP パケットを受信します。

6.1.9 no ip rip send-packet

【機能】

RIP パケットを送信しない設定

【入力形式】

no ip rip send-packet

ip rip send-packet

【動作モード】

port-channel インタフェース設定モード、tunnel インタフェース設定モード (tunnel mode ipsec のみ)

【説明】

RIP パケットを送信しない場合に設定します。

【実行例】

RIP パケットを送信しません。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#no ip rip send-packet
```

【未設定時】

RIP パケットを送信します。

6.1.10 ip rip split-horizon

【機能】

Split-Horizon 制御の設定

【入力形式】

ip rip split-horizon {enable | disable | poisoned}

no ip rip split-horizon

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
enable disable poisoned	Split-Horizon 制御を指定します。	enable: 動作 disable: 非動作 poisoned: Split-Horizon with PoisonedReverse 動作	省略不可

【動作モード】

port-channel インタフェース設定モード、tunnel インタフェース設定モード (tunnel mode ipsec のみ)

【説明】

Split-Horizon 制御を行う場合に設定します。"poisoned"を指定した場合は、Split-Horizon with Poisoned Reverse 機能が動作します。



Split-Horizon 制御とは、RIP 送信制御の方法です。

受信した RIP の宛先情報を、RIP を受信したインタフェースに対して送信するかどうかを規定します。Split-Horizon 制御を行う場合は、RIP を受信したインタフェースには送信しません。

Split-Horizon 制御を行っていないルータがネットワーク上に存在する場合、RIP で送信した情報を同じインタフェースから受信するため、そのインタフェース側にも経路が存在すると判断され、実際に送信するインタフェースが使用不可となっても、そちら側のインタフェースに経路が存在すると考えられ、データを送信してしまいます。

この機能がない場合は、経路がなくなった場合の収束が遅くなる原因となります。

Split-Horizon の拡張機能で、Split-Horizon with Poisoned Reverse という機能があります。

この機能は、Split-Horizon のように、RIP を受信したインタフェースに同じ宛先の情報をもつ RIP を送信しないのではなく、その宛先の情報のメトリックを 16 (到達不能) として RIP を送信する機能です。この機能により、さらに誤動作が防止できます。

【実行例】

Split-Horizon 制御を行います。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-manage 1)#ip rip split-horizon enable
```

【未設定時】

Split-Horizon 制御を行います。

6.1.11 maximum-prefix

【機能】

プレフィックス数の最大値の設定

【入力形式】

maximum-prefix <プレフィックス数>

no maximum-prefix <プレフィックス数>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プレフィックス数	プレフィックス数の最大値を指定します。	1～65535	省略不可

【動作モード】

RIP サービス設定モード

【説明】

受け付けるプレフィックス数の最大値を設定します。

【実行例】

受け付けるプレフィックス数の最大値を設定します（プレフィックス数：100）。

```
#configure terminal
(config)#router rip
(config-rip)#maximum-prefix 100
```

【未設定時】

プレフィックス数は制限されません。

6.1.12 neighbor

【機能】

RIP のネイバーアドレスの設定

【入力形式】

neighbor <IPv4 アドレス>

no neighbor <IPv4 アドレス>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
IPv4 アドレス	RIP のネイバーアドレスを指定します。	IPv4 アドレス形式	省略不可

【動作モード】

RIP サービス設定モード

【説明】

RIP のネイバーアドレスを設定します。通常 RIP Version2 ではマルチキャスト宛に送信しますが、RIP を広告する相手を限定したい場合に、ネイバーアドレスを指定します。

【実行例】

ネイバーアドレスを設定します（IPv4 アドレス：192.0.2.1）。

```
#configure terminal
(config)#router rip
(config-rip)#neighbor 192.0.2.1
```

【未設定時】

Version2 ではマルチキャスト宛に送信します。

6.1.13 network

【機能】

RIP を動作させるインタフェースの設定

【入力形式】

network {<ネットワークアドレス> <ネットマスク> | <インタフェース名> <インタフェース番号>}

no network {<ネットワークアドレス> <ネットマスク> | <インタフェース名> <インタフェース番号>}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ネットワークアドレス	RIP を動作させるネットワークアドレスを指定します。	IPv4 アドレス形式	省略不可
ネットマスク	ネットマスクを指定します。	IPv4 アドレス形式	省略不可
インタフェース名	RIP を動作させるインタフェース名を指定します。	-	省略不可
インタフェース番号	RIP を動作させるインタフェース番号を指定します。	-	省略不可

【動作モード】

RIP サービス設定モード

【説明】

RIP を動作させるインタフェースを、ネットワークアドレスまたはインタフェース名で設定します。

【実行例】

RIP を動作させるインタフェースを設定します（ネットワークアドレス：192.0.2.0、ネットマスク：255.255.255.0）。

```
#configure terminal
(config)#router rip
(config-rip)#network 192.0.2.0 255.255.255.0
```

【未設定時】

RIP は動作しません。

6.1.14 offset-list

【機能】

経路の送受信時に加算するメトリックの設定

【入力形式】

offset-list <アクセスリスト番号> {in | out} <メトリック値> {<インタフェース名> <インタフェース番号> | default}

no offset-list <アクセスリスト番号> [{in | out} [<メトリック値> [<インタフェース名> <インタフェース番号> | default]]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アクセスリスト番号	アクセスリスト番号を指定します。	-	省略不可

パラメタ	設定内容	設定範囲	省略時
in out	受信時に加算するか／送信時に加算するかを指定します。	in: 受信時 out: 送信時	省略不可
メトリック値	加算するメトリック値を指定します。	0 ～ 16	省略不可
インタフェース名	インタフェース名を指定します。	-	省略不可
インタフェース番号	インタフェース番号を指定します。	-	省略不可
default	全インタフェースに適用する場合に指定します。	-	省略不可

【動作モード】

RIP サービス設定モード

【説明】

アクセスリストで指定した経路情報に対して、送信時または受信時に任意のメトリック値を加算する場合に設定します。メトリック加算を行うインタフェースを指定することもできます。

【実行例】

経路の送受信時に加算するメトリックを設定します（アクセスリスト番号：10、受信時、メトリック値：3）。

```
#configure terminal
(config)#router rip
(config-rip)#offset-list 10 in 3
```

【未設定時】

受信時にメトリックを1加算します。送信時には加算しません。

6.1.15 passive-interface

【機能】

RIP 受信のみの設定

【入力形式】

passive-interface <インタフェース名> <インタフェース番号>

no passive-interface <インタフェース名> <インタフェース番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース名	RIP の受信のみを行うインタフェース名を指定します。	-	省略不可
インタフェース番号	RIP の受信のみを行うインタフェース番号を指定します。	-	省略不可

【動作モード】

RIP サービス設定モード

【説明】

RIP の送信は行わず、受信のみを行うインタフェースを設定します。

この設定を行っても、neighbor コマンドで指定したネイバーアドレスへの送信は行われます。

【実行例】

受信のみを行うインタフェースを設定します（インタフェース名：port-channel、インタフェース番号：1）。

```
#configure terminal
(config)#router rip
(config-rip)#passive-interface port-channel 1
```

【未設定時】

RIP の送受信を行います。

6.1.16 recv-buffer-size

【機能】

受信バッファサイズの設定

【入力形式】

recv-buffer-size <受信バッファサイズ>

no recv-buffer-size

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
受信バッファサイズ	受信バッファサイズ（単位：bytes）を指定します。	8192 ～ 55000000	省略不可

【動作モード】

RIP サービス設定モード

【説明】

RIP で使用する受信バッファサイズ（単位：bytes）を設定します。

【実行例】

RIP で使用する受信バッファサイズを設定する（受信バッファサイズ：23,456,789byte）。

```
#configure terminal
(config)#router rip
(config-rip)#recv-buffer-size 23456789
```

【未設定時】

1000000byte で動作します。

6.1.17 redistribute

【機能】

経路情報の再広告の設定

【入力形式】

```
redistribute { <再広告する経路情報> | isakmp sa-up { local-prot1 | local-prot2 } } [metric <メトリック値>]
[route-map <route-map 名>]
```

```
no redistribute { <再広告する経路情報> | isakmp sa-up { local-prot1 | local-prot2 } } [metric <メトリック
値>] [route-map <route-map 名>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
再広告する経路情報	RIP以外の手段で取得した経路情報のうち、RIPで広告するものを指定します。	connected:connected 経路 static:スタティック経路 ospf:OSPF で学習した経路 bgp:BGP で学習した経路	省略不可
isakmp sa-up	SA-UPルートをRIPで広告する場合に指定します。	-	
local-prot1 local-prot2	SA-UPルートを管理するプロトコル名を指定します。	-	
メトリック値	RIPで経路を広告する際のメトリック値を指定します。	0～16	0
route-map 名	適用する route-map 名を指定します。	254文字以内のWORD型	route-map を適用しない

【動作モード】

RIP サービス設定モード

【説明】

異なるルートドメインに対して、経路情報の再広告を行う場合に設定します。

【実行例】

経路情報の再広告を行います（再広告する経路情報：static、メトリック値：5）。

```
#configure terminal
(config)#router rip
(config-rip)#redistribute static metric 5
```

【未設定時】

再広告を行いません。

6.1.18 timers basic

【機能】

RIPに関する各種タイマ値の設定

【入力形式】

timers basic <定期送信間隔> <経路情報を一時到達不能にするまでの時間> <経路情報を削除するまでの時間>

no timers basic

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
定期送信間隔	定期送信間隔（単位：秒）を指定します。	5～2147483647	省略不可
経路情報を一時到達不能にするまでの時間	経路情報を一時到達不能にするまでの時間（単位：秒）を指定します。	5～2147483647	省略不可
経路情報を削除するまでの時間	経路情報を削除するまでの時間（単位：秒）を指定します。	5～2147483647	省略不可

【動作モード】

RIP サービス設定モード

【説明】

RIP に関する各種タイマ値を設定します。

RIP の定期送信間隔、経路情報を受信しなくなってからメトリックを 16 に変更するまでのタイムアウト時間、メトリック 16 になってから経路情報を削除するまでの時間を設定します。

【実行例】

RIP に関する各種タイマ値を設定します（定期送信間隔：30 秒、経路情報を一時到達不能にするまでの時間：180 秒、経路情報を削除するまでの時間：120 秒）。

```
#configure terminal
(config)#router rip
(config-rip)#timers basic 30 180 120
```

【未設定時】

以下の値で動作します。

- 定期送信間隔：30 秒
- 経路情報を一時到達不能にするまでの時間：180 秒
- 経路情報を削除するまでの時間：120 秒

第7章 OSPF の設定



この章では、OSPF の設定に関するコマンドについて説明します。

7.1	IPv4 経路交換の設定	193
7.2	Virtual Link の設定	235
7.3	IPv6 経路交換の設定	242
7.4	Virtual Link の設定	259
7.5	VRF 経路交換の設定	263

7.1 IPv4 経路交換の設定

7.1.1 router ospf

【機能】

OSPF サービス設定モードへの移行

【入力形式】

router ospf <インスタンス番号>

no router ospf <インスタンス番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インスタンス番号	インスタンス番号を指定します。	1～65535	省略不可

【動作モード】

基本設定モード

【説明】

OSPF サービス設定モードに移行します。コマンドの先頭に "no" を指定することで、該当 OSPF サービス設定モードの内容がすべて消去されます。

【実行例】

OSPF サービス設定モードに移行します（インスタンス番号：1）。

```
#configure terminal
(config)#router ospf 1
(config-ospf 1)#
```

7.1.2 area authentication

【機能】

OSPF 認証機能の設定

【入力形式】

area <エリア ID> authentication [message-digest]

no area <エリア ID> authentication [message-digest]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリア ID	対象とするエリア ID を指定します。	0～4294967295 または IPv4 アドレス形式	省略不可

パラメタ	設定内容	設定範囲	省略時
message-digest	認証機構に MD5 を用いる場合に指定します。	-	MD5 を使用しない

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

OSPF 認証機能を有効にします。認証キーは ip ospf authentication-key コマンド、または ip ospf message-digest-key コマンドで設定します。

【実行例】

OSPF 認証機能を有効にします（エリア ID：1、message-digest）。

```

【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#area 1 authentication message-digest

```

【未設定時】

OSPF 認証を行いません。

7.1.3 area default-cost

【機能】

summary-LSA を通知するコスト値の設定

【入力形式】

area <エリア ID> default-cost <コスト値>

no area <エリア ID> default-cost [<コスト値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリア ID	対象とするエリア ID を指定します。	0～4294967295 または IPv4 アドレス形式	省略不可
コスト値	スタブエリアまたは NSSA に対して、summary-LSA を通知する場合のコスト値を指定します。	0～16777215	

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

スタブエリアまたは NSSA に対して、summary-LSA を通知する場合のコスト値を設定します。

【実行例】

summary-LSA を通知する場合のコスト値を設定します（エリア ID：192.0.2.1、コスト値：100）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#area 192.0.2.1 default-cost 100
```

【未設定時】

コスト値は 1 で動作します。

7.1.4 area export-list

【機能】

他エリアに広告する経路をフィルタリングする設定

【入力形式】

area <エリア ID> export-list <アクセスリスト番号>

no area <エリア ID> export-list <アクセスリスト番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリア ID	対象とするエリア ID を指定します	0 ～ 4294967295 または IPv4 アドレス形式	省略不可
アクセスリスト番号	アクセスリスト番号を指定します。	-	

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

他エリアに広告する経路のフィルタリングを行う場合に設定します。アクセスリストに match しない経路は広告しません。

【実行例】

他エリアに広告する経路のフィルタリングを行います（エリア ID：1、アクセスリスト番号：1）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#area 1 export-list 1
```

【未設定時】

フィルタリングを行いません。

7.1.5 area import-list

【機能】

他エリアから広告された経路をフィルタリングする設定

【入力形式】

area <エリア ID> import-list <アクセスリスト番号>

no area <エリア ID> import-list <アクセスリスト番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリア ID	対象とするエリア ID を指定します。	0～4294967295 または IPv4 アドレス形式	省略不可
アクセスリスト番号	アクセスリスト番号を指定します。	-	

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

他エリアから広告された経路のフィルタリングを行う場合に設定します。アクセスリストに match しない経路は受け入れません。

【実行例】

他エリアから広告された経路のフィルタリングを行います（エリア ID：1、アクセスリスト番号：1）。

```

【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#area 1 import-list 1

```

【未設定時】

フィルタリングを行いません。

7.1.6 area nssa

【機能】

NSSA エリアの設定

【入力形式】

area <エリア ID> nssa {translate {never | always | candidate [stability-interval <インターバル>]} | default-information-originate [metric <メトリック値>] [metric-type <メトリックタイプ>] | no-redistribution | no-summary}

no area <エリア ID> nssa [translate {never | always | candidate [stability-interval <インターバル>]} | default-information-originate [metric <メトリック値>] [metric-type <メトリックタイプ>] | no-redistribution | no-summary]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリア ID	対象とするエリア ID を指定します。	0 ～ 4294967295 または IPv4 アドレス形式	省略不可
translate	translator 動作、および translator 選択を指定します。	never : translator 動作を行わない always : translator 動作を行う candidate : translator の候補となる	
インターバル	stability-interval タイマ (単位: 秒) を指定します。	0 ～ 3600	40
default-information-originate	タイプ 7 のデフォルトルートを生成する場合に指定します。	-	省略不可
メトリック値	メトリック値を指定します。	0 ～ 16777214	1
メトリックタイプ	メトリックタイプを指定します。	1 ～ 2	2
no-redistribution	外部経路を NSSA に再配布しない場合に指定します。ASBR が NSSA ABR を兼務している場合のみ	-	省略不可
no-summary	NSSA 完全スタブエリアを設定する場合に指定します。	-	

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

バックボーンでないエリアを、NSSA とする場合に設定します。

エリアボーダルータは、NSSA として定義したエリアへほかのエリアから学習した AS 外経路を広告しません。

NSSA を設定することで、NSSA 内では経路情報を減らし、ルータの情報の交換や経路選択の負荷を減らすことができます。

【実行例】

NSSA エリアを設定します (エリア ID : 192.0.2.1、no-redistribution)。

```

【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#area 192.0.2.1 nssa no-redistribution

```

【未設定時】

NSSA エリアを設定しません。

7.1.7 area range

【機能】

エリアに属するネットワークの範囲の設定

【入力形式】

area <エリア ID> range {<ネットワークアドレス 1> <ネットマスク 1> | <ネットワークアドレス 1> / <プレフィックス長>} [substitute <ネットワークアドレス 2> <ネットマスク 2> | not-advertise]

no area <エリア ID> range {<ネットワークアドレス 1> <ネットマスク 1> | <ネットワークアドレス 1> / <プレフィックス長>} [substitute [<ネットワークアドレス 2> <ネットマスク 2>] | not-advertise]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリア ID	対象とするエリア ID を指定します。	0～4294967295 または IPv4 アドレス形式	省略不可
ネットワークアドレス 1	このエリアに属するネットワークアドレスを指定します。	IPv4 アドレス型式 IPv6 アドレス形式	
ネットマスク 1	ネットマスクを指定します。	IPv4 アドレス形式	
プレフィックス長(*1)	プレフィックス長を指定します。	0～128	
ネットワークアドレス 2(*2)	異なるプレフィックスとして通知する場合に、ネットワークアドレスを指定します	IPv4 アドレス型式	異なるプレフィックスとして通知しない
ネットマスク 2(*2)	異なるプレフィックスとして通知する場合に、そのネットマスクを指定します。	IPv4 アドレス形式	
not-advertise	集約した経路を広告しない場合に指定します。	-	集約経路を広告

*1) OSPF サービス設定モード、OSPF-VRF サービス設定モードでは指定できません。

*2) OSPF6 サービス設定モードでは指定できません。

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

エリアに属するネットワークの範囲を設定します。

【実行例】

ネットワーク範囲を設定します（エリア ID：1、ネットワークアドレス：192.0.2.0、ネットマスク：255.255.255.0）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#area 1 range 192.0.2.0 255.255.255.0
```

【未設定時】

エリアに属するネットワークを設定しません。

7.1.8 area shortcut

【機能】

バックボーンを介さずにエリアをショートカットするかどうかの設定

【入力形式】

area <エリア ID> shortcut {default | disable | enable}

no area <エリア ID> shortcut [default | disable | enable]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリア ID	対象とするエリア ID を指定します。	0～4294967295 または IPv4 アドレス形式	省略不可
default disable enable	ショートカット属性を指定します。	default: ショートカットしない disable: ショートカットしない enable: ショートカットする	

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

メトリックが小さい経路に関して、バックボーンを介さずにエリアをショートカットするかどうかを設定します。ospf abr-type shortcut コマンドと同時に設定して、ABR タイプを shortcut モードにしておく必要があります。

【実行例】

バックボーンを介さずにエリアをショートカットします（エリア ID：1）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#area 1 shortcut enable
```

【未設定時】

default で動作します。

7.1.9 area stub

【機能】

スタブエリアの設定

【入力形式】

area <エリア ID> stub [no-summary]

no area <エリア ID> stub [no-summary]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリア ID	対象とするエリア ID を指定します	0 ～ 429496729 または IPv4 アドレス形式	省略不可
no-summary	スタブエリアに、summary-LSA を広告しない場合に指定します。	-	summary-LSA を広告

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

スタブエリアを設定します。スタブエリアの ABR の場合は、area default-cost コマンドで設定されたコストで、summary-LSA をスタブエリア内に広告します。

【実行例】

スタブエリアを設定します（エリア ID：1、no-summary）。

```

【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#area 1 stub no-summary

```

【未設定時】

スタブエリアを設定しません。

7.1.10 auto-cost reference-bandwidth

【機能】

OSPF コスト値を自動計算する際にベースとなる帯域の設定

【入力形式】

auto-cost reference-bandwidth <帯域>

no auto-cost reference-bandwidth [<帯域>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
帯域	OSPF コスト値計算時のベースとなる帯域値（単位：Mbps）を指定します。	1 ～ 4294967	省略不可

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

インタフェースの OSPF コスト値を自動計算する際に、そのベースとなる帯域（単位：Mbps）を設定します。高速なリンクを使用する場合は、この値を大きくします。

【実行例】

ベースとなる帯域（単位：Mbps）を設定します（帯域：80Mbps）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#auto-cost reference-bandwidth 80
```

【未設定時】

帯域は 100Mbps で動作します。

7.1.11 capability restart graceful

【機能】

Graceful-restart のヘルパールータとして動作する設定

【入力形式】

capability restart graceful

no capability restart graceful

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

Graceful-restart のヘルパールータとして動作する場合に設定します。

【実行例】

OSPF Graceful-restart のヘルパールータとして動作します。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#capability restart graceful
```

【未設定時】

OSPF Graceful-restart 機能は無効となります。

7.1.12 compatible rfc1583

【機能】

RFC1583 互換で動作する設定

【入力形式】

compatible rfc1583

no compatible rfc1583

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

AS 外の経路の計算方法について、RFC1583 互換で動作する場合に設定します。RFC1583 で動作するルータが存在する場合には、このコマンドを指定する必要があります。

【実行例】

RFC1583 互換で動作します。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#compatible rfc1583
```

【未設定時】

RFC1583 互換で動作しません (RFC2328 準拠)。

7.1.13 default-information originate

【機能】

デフォルトルートを広告する設定

【入力形式】

default-information originate [always] [metric <メトリック値>]

[metric-type {type-1 | type-2}] [route-map <route-map 名>]

no default-information originate [always] [metric <メトリック値>]

[metric-type {type-1 | type-2}] [route-map <route-map 名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
always	ルーティングテーブルにデフォルトルートが存在しなくても、自分自身をデフォルトルートとして広告する場合に指定します。	-	デフォルトルートが存在する場合のみ広告
メトリック値	デフォルトルートを広告する際に、そのメトリック値を指定します。	0～16777214	10 (ただし、always オプションがある場合は 1)
type-1 type-2	デフォルトルートを広告する際に、そのメトリックタイプを指定します。	type-1 type-2	type-2
route-map 名	適用する route-map 名を指定します。	254 文字以内の WORD 型	route-map を適用しない

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

ルーティングテーブルにデフォルトルート (0.0.0.0/0) があれば、その情報を AS 外 LSA として広告するように設定します。デフォルトルート広告時のメトリック値と、メトリックタイプを設定します。

【実行例】

デフォルトルートを広告します (メトリック値：10、メトリックタイプ：type-2)。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#default-information originate metric 10 metric-type type-2
```

【未設定時】

デフォルトルートを広告しません。

7.1.14 default-metric

【機能】

AS 外の経路情報を OSPF で広告する際のメトリック値の設定

【入力形式】

default-metric <メトリック値>

no default-metric [<メトリック値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
メトリック値	AS 外の経路情報を OSPF で広告する際に、そのメトリック値を指定します。	0 ～ 16777214	省略不可

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

AS 外の経路情報を OSPF(OSPF6) で広告する際のメトリック値を設定します。

【実行例】

AS 外の経路情報を OSPF で広告する際のメトリック値を設定します (メトリック値：10)。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#default-metric 10
```

【未設定時】

メトリック値は 20 で動作します。

7.1.15 distance

【機能】

OSPF のディスタンス値の設定

【入力形式】

distance <ディスタンス値>

no distance <ディスタンス値>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ディスタンス値	ディスタンス値を指定します。	1～255	省略不可

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

OSPF(OSPF6)のディスタンス値を設定します。同じ宛先への経路を異なる手段で学習した場合に、どの情報を採用するかのパラメタとなります。

【実行例】

OSPF のディスタンス値を設定します (ディスタンス値：120)。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#distance 120
```

【未設定時】

以下の値で動作します (OSPF は 110)。

プロトコル	デフォルト値	備考
スタティック	1	設定変更可能
直接経路	-	設定変更不可
BGP(external)	20	設定変更可能
BGP(internal)	200	
BGP(local)		
RIP	120	設定変更可能
OSPF(external)	110	設定変更可能
OSPF(inter-area)		
OSPF(intra-area)		

7.1.16 distance ospf

【機能】

external ルート、inter-area ルート、intra-area ルートのディスタンス値の設定

【入力形式】

distance ospf {external | inter-area | intra-area} <ディスタンス値>

no distance ospf [{external | inter-area | intra-area} [<ディスタンス値>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
external inter-area intra-area	ルートを指定します。	external: external ルート inter-area: inter-area ルート intra-area: intra-area ルート	省略不可
ディスタンス値	各 LSA のディスタンス値を指定します。	1 ～ 255	

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

external ルート、inter-area ルート、intra-area ルートのディスタンス値を設定します。同じ宛先への経路を異なる手段で学習した場合に、どの情報を採用するかのパラメタとなります。

【実行例】

ディスタンス値を設定します（external ルート、ディスタンス値：150）。

```

【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#distance ospf external 150

```

【未設定時】

distance コマンドの設定に従います。

7.1.17 distribute-list

【機能】

OSPF の LSA 送信をフィルタリングする設定

【入力形式】

distribute-list <アクセスリスト番号> out <広告する経路情報>

no distribute-list <アクセスリスト番号> out <広告する経路情報>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アクセスリスト番号	広告する経路情報の宛先を、アクセスリストで指定します。	-	省略不可
広告する経路情報	OSPF 以外の手段で取得した経路情報のうち、OSPF で広告するものを指定します。	connected:connected 経路 kernel:CP にセットされた経路 static: スタティック経路 bgp:BGP で学習した経路 isakmp:ISAKMP で学習した経路 rip:RIP で学習した経路	

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

アクセスリスト番号と取得したプロトコルを指定して、OSPF のLSA送信をフィルタリングします。

【実行例】

LSA送信をフィルタリングします（アクセスリスト番号：1、広告する経路情報：static）。

```

【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#distribute-list 1 out static

```

【未設定時】

フィルタリングしません。

7.1.18 instance-metric

【機能】

インスタンスの優先度の設定

【入力形式】

instance-metric <インスタンスメトリック値>

no instance-metric [<インスタンスメトリック値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インスタンスメトリック値	インスタンスの優先度を指定します。	1～128	省略不可

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

インスタンスの優先度を設定します。インスタンスメトリック値の小さい方が優先されます。

【実行例】

インスタンスの優先度を設定します（インスタンスメトリック値：3）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#instance-metric 3
```

【未設定時】

インスタンスメトリック値は 64 で動作します。

7.1.19 ip ospf authentication

【機能】

認証方式の設定

【入力形式】

ip ospf authentication [message-digest | null]

no ip ospf authentication [message-digest | null]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
message-digest null	認証方式を指定します。	message-digest: 暗号化したパスワードを使用 null: 認証を行わない	simple-password で認証

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

認証方式を設定します。"message-digest" を指定した場合は ip ospf message-digest-key コマンドで、パラメタ省略 (=simple password) の場合は ip ospf authentication-key コマンドでパスワード文字列を設定してください。

【実行例】

認証方式を設定します (message-digest)。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ip ospf authentication message-digest
```

【未設定時】

area authentication コマンドに従います。

7.1.20 ip ospf authentication-key

【機能】

simple-password で認証する認証キーの設定

【入力形式】

```
ip ospf authentication-key <認証キー>
```

```
no ip ospf authentication-key [<認証キー>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
認証キー	simple-password で認証する場合の認証キーを指定します。	8文字以内のSTRING型	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

simple-password で認証する場合の認証キーを設定します。

【実行例】

simple-password で認証する場合の認証キーを設定します（認証キー：authkey）。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ip ospf authentication-key authkey
```

【未設定時】

simple-password による認証を行いません。

7.1.21 ip ospf cost

【機能】

OSPF を使用する場合のコスト値の設定

【入力形式】

```
ip ospf cost <OSPF コスト値>
```

```
no ip ospf cost [<OSPF コスト値>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
OSPF コスト値	OSPF のコスト値を指定します。	1～65535	省略不可

【動作モード】

management インタフェース設定モード、loopback インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

OSPF を使用する場合のコスト値を設定します。

【実行例】

OSPF を使用する場合のコスト値を設定します（OSPF コスト値：100）。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ip ospf cost 100
```

【未設定時】

OSPF コスト値は回線速度と auto-cost reference-bandwidth コマンドの設定値に基づいて決定します。

7.1.22 ip ospf database-filter all out

【機能】

新しいLSAの情報を受け付けない設定

【入力形式】

ip ospf database-filter all out

no ip ospf database-filter [all out]

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

新しいLSAの情報を受け付けないようにする場合に設定します。

【実行例】

新しいLSAの情報を受け付けないようにします。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ip ospf database-filter all out
```

【未設定時】

新しいLSAの情報を受け付けます。

7.1.23 ip ospf dead-interval

【機能】

OSPF の dead-interval 値の設定

【入力形式】

ip ospf dead-interval <dead-interval 値>

no ip ospf dead-interval [<dead-interval 値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
dead-interval 値	dead-interval 値（単位：秒）を指定します。	1～65535	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

OSPF の dead-interval 値（単位：秒）を設定します。ここで設定した時間、OSPF の Hello を受信しなかった場合は、そのネイバーをテーブルから削除します。

【実行例】

OSPF の dead-interval 値を設定します（dead-interval 値：100 秒）。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ip ospf dead-interval 100
```

【未設定時】

dead-interval 値は40秒で動作します。

7.1.24 ip ospf disable all

【機能】

OSPF を使用しない設定

【入力形式】

ip ospf disable all

no ip ospf disable all

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

OSPF を使用しない場合に設定します。

【実行例】

OSPF を使用しません。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ip ospf disable all
```

【未設定時】

OSPF を使用します。

7.1.25 ip ospf hello-interval

【機能】

OSPF の Hello メッセージの送信間隔の設定

【入力形式】

ip ospf hello-interval <送信間隔>

no ip ospf hello-interval [<送信間隔>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
送信間隔	Hello メッセージの送信間隔（単位：秒）を指定します。	1～65535	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

OSPF の Hello メッセージの送信間隔（単位：秒）を設定します。

【実行例】

OSPF の Hello メッセージの送信間隔を設定します（送信間隔：20 秒）。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ip ospf hello-interval 20
```

【未設定時】

送信間隔は 10 秒で動作します。

7.1.26 ip ospf message-digest-key

【機能】

OSPF で MD5 認証機能を使用する場合の MD5 認証キーの設定

【入力形式】

```
ip ospf message-digest-key <キー ID> md5 <認証キー >
```

```
no ip ospf message-digest-key <キー ID> [md5 <認証キー >]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
キー ID	キー ID を指定します。	1 ～ 255	省略不可
認証キー	MD5 認証する場合の認証キーを指定します。	16 文字以内の STRING 型	

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

OSPF で MD5 認証機能を使用する場合の MD5 認証キーを設定します。

【実行例】

OSPF で MD5 認証キーを設定します（キー ID：1、認証キー：authkey）。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ip ospf message-digest-key 1 md5 authkey
```

【未設定時】

MD5 による認証を行いません。

7.1.27 ip ospf mtu

【機能】

Database Description メッセージで通知する MTU 長の設定

【入力形式】

```
ip ospf mtu <MTU 長>
```

```
no ip ospf mtu [<MTU 長>]
```


【パラメタ】

パラメタ	設定内容	設定範囲	省略時
MTU 長	Database Description で通知する MTU 長（単位：bytes）を指定します。	1280～9100	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

Database Description メッセージで通知する MTU 長（単位：bytes）を設定します。OSPF ルータ間で同一の値にする必要があります。

【実行例】

Database Description メッセージで通知する MTU 長を設定します（MTU 長：1500bytes）。

```

【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ip ospf mtu 1500

```

【未設定時】

インタフェースの MTU 長を通知します。

7.1.28 ip ospf network

【機能】

OSPF インタフェースのネットワーク型の設定

【入力形式】

ip ospf network {broadcast | non-broadcast | point-to-multipoint | point-to-point}

no ip ospf network [broadcast | non-broadcast | point-to-multipoint | point-to-point]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
broadcast non-broadcast point-to-multipoint point-to-point	OSPF インタフェースのネットワーク型を指定します。	broadcast non-broadcast point-to-multipoint point-to-point	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

OSPF インタフェースのネットワーク型を明示的に設定します。

【実行例】

OSPF インタフェースのネットワーク型を明示的に設定します (non-broadcast)。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ip ospf network non-broadcast
```

【未設定時】

ネットワーク型は broadcast で動作します。

7.1.29 ip ospf priority

【機能】

OSPF の優先度の設定

【入力形式】

ip ospf priority <優先度>

no ip ospf priority [<優先度>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
優先度	OSPF の優先度を指定します。	0 ～ 255	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

OSPF の優先度を設定します。同一インタフェース上に複数の OSPF ルータが存在した場合、優先度の大きいルータが Designated Router(DR) となります。各ルータは、Hello メッセージで優先度を広告します。

【実行例】

OSPF の優先度を設定します (優先度：20)。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ip ospf priority 20
```

【未設定時】

優先度は 1 で動作します。

7.1.30 ip ospf retransmit-interval

【機能】

Database Description、Link State Request パケットの再送間隔の設定

【入力形式】

ip ospf retransmit-interval <再送間隔>

no ip ospf retransmit-interval [<再送間隔>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
再送間隔	Database Description、および Link State Request パケットの再送間隔 (単位：秒) を指定します。	3～65535	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

Database Description、および Link State Request パケットの再送間隔（単位：秒）を設定します。

【実行例】

Database Description、および Link State Request パケットの再送間隔を設定します（再送間隔：100 秒）。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ip ospf retransmit-interval 100
```

【未設定時】

再送間隔は 5 秒で動作します。

7.1.31 ip ospf transmit-delay

【機能】

遅延時間の設定

【入力形式】

ip ospf transmit-delay <遅延時間>

no ip ospf transmit-delay [<遅延時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
遅延時間	遅延時間（単位：秒）を指定します。	1～65535	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

遅延時間（単位：秒）を設定します。ここで設定した値がLSAのAgeに加算されます。

【実行例】

遅延時間を設定します（遅延時間：10 秒）。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ip ospf transmit-delay 10
```

【未設定時】

遅延時間は 1 秒で動作します。

7.1.32 log-adjacency-changes

【機能】

OSPF ネイバースタートマシンの状態遷移をログ情報に出力する設定

【入力形式】

log-adjacency-changes [detail]

no log-adjacency-changes [detail]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
detail	すべての状態遷移でログ情報を出力します。	-	FULL ステートからの状態遷移、または FULL ステートへの状態遷移のみログ情報を出力

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

OSPF(OSPF6) ネイバースタートマシンの状態遷移をログ情報に出力します。出力内容は状態遷移前後のステート、および状態遷移を引き起こしたイベントの種類です。"detail" を指定した場合は、すべての状態

遷移時にログ情報を出力します。"detail" を指定しない場合は、FULL ステートと FULL ステート以外のステート間で状態遷移が発生した場合のみ、ログ情報を出力します。

【実行例】

OSPF ネイバーステートマシンの状態遷移をログ情報に出力します。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#log-adjacency-changes
```

【未設定時】

OSPF(OSPF6) ネイバーステートマシンの状態遷移をログ情報に出力しません。

7.1.33 maximum-paths

【機能】

ECMP として登録できる経路数の設定

【入力形式】

maximum-paths <経路数>

no maximum-paths

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
経路数	ECMP として登録できる経路数を指定します。	1～8	省略不可

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

ECMP として登録できる経路数を設定します。

【実行例】

ECMP として登録できる経路数を設定します（経路数：8）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#maximum-paths 8
```

【未設定時】

経路数は 8 で動作します。

7.1.34 max-metric router-lsa

【機能】

Router LSA の link のコストを RFC3137 に準拠した値で広告する設定

【入力形式】

max-metric router-lsa [on-startup < 広告時間 >]

no max-metric router-lsa [on-startup < 広告時間 >]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
広告時間	on-startup を指定した場合には、OSPF インスタンス起動後、コストを 65535 で広告し続ける時間（単位：秒）を指定します。	5 ～ 86400	省略不可

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

Router LSA の link（type 3 以外）のコストを RFC3137 に準拠した値 (65535) で広告する場合に設定します。

【実行例】

Router LSA の link（type 3 以外）のコストを RFC3137 に準拠した値 (65535) で広告します。

```

【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#max-metric router-lsa

```

【未設定時】

設定されたコスト値、または自動計算されたコスト値で動作します。

7.1.35 neighbor

【機能】

Non-Broadcast MultiAccess(NBMA) ネットワーク上の OSPF ルータの登録

【入力形式】

neighbor <OSPF ネイバー> [priority < 優先度 >] [poll-interval < 送信間隔 >]

no neighbor <OSPF ネイバー> [priority [< 優先度 >]] [poll-interval [< 送信間隔 >]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
OSPF ネイバー	OSPF ネイバーの IPv4 アドレスを指定します。	IPv4 アドレス形式	省略不可
優先度	指定したネイバーの優先度を指定します。	0～255	0
送信間隔	ポーリング間隔（単位：秒）を指定します。	1～65535	60

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

Non-Broadcast MultiAccess(NBMA) ネットワーク上の OSPF ルータを登録します。ブロードキャストネットワークでは、OSPF Hello によりダイナミックにネイバーを学習します。

【実行例】

NBMA ネットワーク上の OSPF ルータを登録します（OSPF ネイバー：192.0.2.1、優先度：16）。

```

【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#neighbor 192.0.2.1 priority 16

```

【未設定時】

ダイナミックに学習します。

7.1.36 network

【機能】

OSPF エリアに含まれるネットワーク範囲の設定

【入力形式】

network <ネットワークアドレス> <Wildcard マスク> area <エリア ID>

no network <ネットワークアドレス> <Wildcard マスク> area <エリア ID>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ネットワークアドレス	Router-LSA に含めるネットワークアドレスを指定します。OSPF で広告するネットワークです。	IPv4 アドレス形式	省略不可
Wildcard マスク	Wildcard マスクを指定します。	IPv4 アドレス形式	
エリア ID	対象とするエリア ID を指定します	0～4294967295 または IPv4 アドレス形式	

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

OSPF エリアに含まれるネットワーク範囲を設定します。

【実行例】

OSPF エリアに含まれるネットワーク範囲を設定します（ネットワークアドレス：192.0.2.0、Wildcard マスク 0.0.0.255、エリア ID：192.0.2.1）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#network 192.0.2.0 0.0.0.255 area 192.0.2.1
```

【未設定時】

OSPF で経路情報を広告しません。

7.1.37 opaque-lsa-capable

【機能】

LSA state-type 9,10,11 を有効にする設定

【入力形式】

opaque-lsa-capable

no opaque-lsa-capable

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

LSA state-type 9,10,11(opaque-LSA) を有効にする場合に設定します。

【実行例】

opaque-LSA を有効にします。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#opaque-lsa-capable
```

【未設定時】

opaque-LSA は有効で動作します。

7.1.38 ospf abr-type

【機能】

ABR タイプの設定

【入力形式】

```
ospf abr-type <ABR タイプ>
```

```
no ospf abr-type <ABR タイプ>
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ABR タイプ	Area Border Router(ABR) タイプを指定します。タイプにより、エリア間ルートの計算方法が異なります。	standard cisco ibm shortcut	省略不可

【ABR タイプの詳細】

standard	エリア間ルートの計算はバックボーンエリア、およびトランジットエリア (Virtual Link) でのみ summary-LSA を計算。
cisco	バックボーンエリアに隣接していて、かつ、バックボーンエリアの1台以上のルータと FULL ステータスとなっている場合に、バックボーンエリア、およびトランジットエリアの summary-LSA を計算。それ以外は全エリアの summary-LSA を計算。
ibm	バックボーンエリアに隣接していて、かつ、バックボーンエリアの1台以上のルータと FULL ステータスとなっている場合に、バックボーンエリア、およびトランジットエリアの summary-LSA を計算。それ以外は全エリアの summary-LSA を計算。
shortcut	バックボーンエリアに関しては、バックボーンエリアの1台以上のルータと FULL ステータスとなっている場合に、summary-LSA を計算。バックボーンエリア以外のエリアに関しては、以下のエリアに関して summary-LSA を計算。 <ul style="list-style-type: none"> トランジットエリア ルータがバックボーンに隣接していなく、shortcut モードが disable 以外 (default or enable) のエリア shortcut モードが enable のエリア

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

ABR タイプを設定します。オプションにより、エリア間ルートの計算方法が変わります。

【実行例】

ABR タイプを設定します (ABR タイプ: shortcut)。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#ospf abr-type shortcut
```

【未設定時】

ABR タイプは standard で動作します。

7.1.39 ospf restart helper max-grace-period

【機能】

リスタートイングルータのグレースピリオドの許容値の設定

【入力形式】

ospf restart helper max-grace-period <許容値>

no ospf restart helper max-grace-period [<許容値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
許容値	リスタートイングルータのグレースピリオドの許容値（単位：秒）を指定します。	1～1800	省略不可

【動作モード】

基本設定モード

【説明】

リスタートイングルータのグレースピリオドの許容値（単位：秒）を設定します。許容値以内の場合しかヘルパールータとして機能しないようにできます。

【実行例】

リスタートイングルータのグレースピリオドの許容値（単位：秒）を設定します（許容値：1000 秒）。

```
#configure terminal
(config)#ospf restart helper max-grace-period 1000
```

【未設定時】

グレースピリオドの値に関わらず、OSPF Graceful-restart のヘルパールータとして動作します。

7.1.40 ospf restart helper policy

【機能】

OSPF Graceful-restart のヘルパールータとして機能する場合のポリシーの設定

【入力形式】

ospf restart helper policy {never | only-reload | only-upgrade}

no ospf restart helper policy [{never | only-reload | only-upgrade}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
never only-reload only-upgrade	OSPF Graceful-restart のヘルパー ルータとして機能する場合のポリ シーを指定します。	never: ヘルパールータ として動作しない only-reload: リス タートリズンがソフ トウェアリロードの場 合のみヘルパールータ として機能 only-upgrade: リス タートリズンがソフ トウェアアップグレー ドの場合のみヘルパー ルータとして機能	省略不可

【動作モード】

基本設定モード

【説明】

OSPF Graceful-restart のヘルパールータとして機能する場合のポリシーを設定します。特定のリスタート
リズンの場合しかヘルパールータとして機能しないようにできます。

【実行例】

リスタートリズンがソフトウェアリロードの場合のみヘルパールータとして機能します (only-reload)。

```
#configure terminal
(config)#ospf restart helper policy only-reload
```

【未設定時】

リスタートリズンに関わらず OSPF Graceful-restart のヘルパールータとして動作します。

7.1.41 overflow database external

【機能】

External データベースのサイズ、overflow 状態から回復するのを待つための時間の設定

【入力形式】

overflow database external <MAXDBSIZE> <WAITTIME>

no overflow database external [<MAXDBSIZE> <WAITTIME>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
MAXDBSIZE	AS-EXTERNAL-LSA の上限値を指 定します。同じ AS 内のルータで は、同じ値としてください。	0 ～ 4294967294	省略不可
WAITTIME	overflow 状態から回復するための待 ち時間（単位：秒）を指定します。 "0" を指定した場合は、overflow 状 態から戻ることできません。	0 ～ 65535	

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

External データベースのサイズ、および overflow 状態から回復するのを待つための時間（単位：秒）を設定します。

【実行例】

External データベースのサイズ、および overflow 状態から回復するのを待つための時間（単位：秒）を設定します（MAXDBSIZE:1000000 LSA、WAITTIME:30 秒）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#overflow database external 1000000 30
```

【未設定時】

External データベースのサイズ、および overflow 状態から回復するのを待つための時間を規定しません。

7.1.42 passive-interface

【機能】

Hello パケットを送信しないインタフェースの設定

【入力形式】

passive-interface <インタフェース名> <インタフェース番号> [<IPv4 アドレス>]

no passive-interface <インタフェース名> <インタフェース番号> [<IPv4 アドレス>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース名	OSPF(OSPF6)のHelloパケットの送信は行わず、受信のみ行うインタフェース名を指定します。	-	省略不可
インタフェース番号	OSPF(OSPF6)のHelloパケットの送信は行わず、受信のみ行うインタフェース番号を指定します。	-	
IPv4 アドレス(*1)	OSPFのHelloパケットの送信は行わず、受信のみ行うインタフェースアドレスを指定します。	IPv4 アドレス形式	設定したインタフェースのすべてのアドレスでHelloの送信は行いません。

*1) OSPF6 サービス設定モードでは指定できません。インタフェース名に port-channel を指定した場合のみ指定できます。

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

Hello パケットの送信を行わないインタフェースを設定します。ルータ ID 決定時の計算対象からも除外されます。

【実行例】

Hello パケットの送信を行わないインタフェースを設定します（インタフェース名：port-channel、インタフェース番号：1）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#passive-interface port-channel 1
```

【未設定時】

Hello パケットの送信を行います。

7.1.43 queue-length update

【機能】

Link State Update パケットの送信処理で一度に処理する最大メッセージ数の設定

【入力形式】

queue-length update <最大メッセージ(LSA)数>

no queue-length update [<最大メッセージ(LSA)数>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
最大メッセージ(LSA)数	最大メッセージ(LSA)数を指定します。	0～2147483647	省略不可

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

Link State Update パケットの送信処理で一度に処理する最大メッセージ(LSA)数を設定します。処理するメッセージ(LSA)数を制限しない場合には"0"を指定します。

【実行例】

Link State Update パケットの送信処理で一度に処理する最大メッセージ(LSA)数を設定します（最大メッセージ(LSA)数：20000）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#queue-length update 20000
```

【未設定時】

最大メッセージ(LSA)数は10000で動作します。

7.1.44 redistribute

【機能】

異なるルートドメインに対して経路情報を再広告する設定

【入力形式】

```
redistribute { <再広告する経路情報> | isakmp sa-up { local-prot1 | local-prot2 } | ospf <インスタンス番号> }
[metric <メトリック値>] [metric-type { type-1 | type-2 } ] [route-map <route-map 名>]
```

```
no redistribute { <再広告する経路情報> | isakmp sa-up { local-prot1 | local-prot2 } | ospf <インスタンス番号> }
[metric <メトリック値>] [metric-type { type-1 | type-2 } ] [route-map <route-map 名>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
再広告する経路情報	OSPF 以外の手段で取得した経路情報のうち、OSPF で広告するものを指定します。	connected:connected 経路 kernel(*1):kernel にセットされた経路 static: スタティック経路 rip:RIP で学習した経路 bgp:BGP で学習した経路	省略不可
isakmp sa-up	SA-UP ルートを OSPF で広告する場合に指定します。	-	
local-prot1 local-prot2	SA-UP ルートを管理するプロトコル名を指定します。	-	
ospf (*1)	他の OSPF インスタンスで取得した経路情報を OSPF で広告する場合に指定します。	-	
インスタンス番号 (*1)	他の OSPF インスタンス番号を指定します。	1 ～ 65535	
メトリック値	OSPF で経路を広告する際のメトリック値を指定します。	0 ～ 16777214	default-metric コマンドの設定値に従う
type-1 type-2	メトリックタイプを指定します。	type-1 type-2	type-2
route-map 名	適用する route-map 名を指定します。	254 文字以内の WORD 型	route-map を適用しない

*1) OSPF6 サービス設定モードでは設定できません。

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

異なるルートドメインに対して、経路情報の再広告を行う場合に設定します。

【実行例】

経路情報の再広告を行います（再広告する経路情報：static、メトリック値：3、type-1）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#redistribute static metric 3 metric-type type-1
```

【未設定時】

再広告を行いません。

7.1.45 refresh timer

【機能】

LSA リフレッシュ間隔の設定

【入力形式】

refresh timer <リフレッシュ間隔>

no refresh timer [<リフレッシュ間隔>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
リフレッシュ間隔	LSA リフレッシュ間隔（単位：秒）を指定します。	10～1800	省略不可

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

LSA リフレッシュ間隔（単位：秒）を設定します。対象は summary-LSA（タイプ 3、4）と AS 外 LSA になります。

【実行例】

リフレッシュ間隔を設定します（リフレッシュ間隔：30 秒）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#refresh timer 30
```

【未設定時】

リフレッシュ間隔は 10 秒で動作します。

7.1.46 router-id

【機能】

OSPF のルータ ID の設定

【入力形式】

router-id <ルータ ID>

no router-id <ルータ ID>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ルータ ID	ルータ ID を指定します。	IPv4 アドレス形式	省略不可

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

OSPF(OSPF6)のルータ ID を設定します。

【実行例】

OSPF のルータ ID を設定します (ルータ ID : 192.0.2.1)。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#router-id 192.0.2.1
```

【未設定時】

全インタフェースの IPv4 アドレスのうち、最大のものをルータ ID とします。

7.1.47 summary-address

【機能】

経路情報の集約

【入力形式】

summary-address <ネットワークアドレス> <ネットマスク> [not-advertise] [tag <tag 値>]

no summary-address <ネットワークアドレス> <ネットマスク> [not-advertise] [tag [<tag 値>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ネットワークアドレス	集約後の経路情報を指定します	IPv4 アドレス形式	省略不可
ネットマスク	ネットマスクを指定します。	IPv4 アドレス形式	
not-advertise	この経路自体を OSPF で広告しない場合に指定します。	-	この経路を OSPF で広告
tag 値	tag 値を指定します。この値は route-map の match tag コマンドで指定する場合の tag 値になります。	0 ～ 4294967295	tag 値を利用しない

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

経路情報を集約します。この経路を OSPF で広告しない場合は、"not-advertise" を指定します。また、tag 値を設定することもできます。tag 値は、route-map の match tag コマンドで指定する場合に使用します。ここで指定した集約後の経路情報は、宛先のない経路（Null インタフェース）として登録されます。この機能により、集約後のアドレス宛のデータを受信しても、実在する経路には中継し、実在しない経路宛は廃棄できます。

【実行例】

経路情報を集約します（ネットワークアドレス：192.0.2.0、ネットマスク：255.255.255.0、tag 値：0）。

```

【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#summary-address 192.0.2.0 255.255.255.0 tag 0

```

【未設定時】

経路を集約しません。

7.1.48 timers lsa arrival

【機能】

LSA を受信する最小時間間隔の設定

【入力形式】

timers lsa arrival <lsa-hold>

no timers lsa arrival [<lsa-hold>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
lsa-hold	同じ LSA を受信する最小待機時間（単位：ミリ秒）を指定します。	1 ～ 600000	省略不可

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

同じ LSA ID 番号、LSA タイプ、およびアドバタイズルータ ID を含む LSA（同じ LSA）を受信する最小時間間隔（単位：ミリ秒）を設定します。

LSA を受信する最小時間間隔は、timers throttle lsa コマンドの hold-interval 時間以内にすることを推奨します。

【実行例】

同じ LSA ID 番号、LSA タイプ、およびアドバタイズルータ ID を含む LSA（同じ LSA）を受信する最小時間間隔（単位：ミリ秒）を設定します（lsa-hold：500 ミリ秒）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#timers lsa arrival 500
```

【未設定時】

lsa-hold は 1000 ミリ秒で動作します。

7.1.49 timers throttle lsa

【機能】

LSA の生成を開始するまでの待機時間、連続した LSA 生成の最小待機時間、連続した LSA 生成の最大待機時間の設定

【入力形式】

timers throttle lsa <start-interval> <hold-interval> <max-interval>

no timers throttle lsa [<start-interval> <hold-interval> <max-interval>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
start-interval	LSA 生成待機時間の初期値（単位：ミリ秒）を指定します。	0～600000	省略不可
hold-interval	連続した同じ LSA 生成の最小待機時間（単位：ミリ秒）を指定します。	1～600000	
max-interval	連続した同じ LSA 生成の最大待機時間（単位：ミリ秒）を指定します。	1～600000	

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

同じ LSA ID 番号、LSA タイプ、およびアドバタイズ ルータ ID を含む LSA（同じ LSA）の生成を開始するまでの待機時間（単位：ミリ秒）、連続した LSA 生成の最小待機時間（単位：ミリ秒）、および連続した LSA 生成の最大待機時間（単位：ミリ秒）を設定します。

【実行例】

同じLSA ID 番号、LSA タイプ、およびアドバタイズルータ ID を含むLSA (同じLSA) の生成を開始するまでの待機時間 (単位: ミリ秒)、連続したLSA 生成の最小待機時間 (単位: ミリ秒)、および連続したLSA 生成の最大待機時間 (単位: ミリ秒) を設定します (start-interval: 50 ミリ秒、hold-interval: 1000 ミリ秒、max-interval: 10000 ミリ秒)。

```

【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#timers throttle lsa 50 1000 10000

```

【未設定時】

以下の値で動作します。

start-interval: 500 ミリ秒

hold-interval: 5000 ミリ秒

max-interval: 5000 ミリ秒

7.1.50 timers throttle spf

【機能】

LSA の更新を受信してから Shortest Path First(SPF) 計算を開始するまでの待機時間、連続した SPF 計算の最小待機時間、連続した SPF 計算の最大待機時間の設定

【入力形式】

timers throttle spf <spf-start> <spf-hold> <spf-max-wait>

no timers throttle spf [<spf-start> <spf-hold> <spf-max-wait>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
spf-start	LSA の更新を受信してから、実際に SPF 計算を開始するまでの遅延時間 (単位: ミリ秒) の初期値を指定します。	1 ~ 600000	省略不可
spf-hold	連続した SPF 計算の最小待機時間 (単位: ミリ秒) を指定します。	1 ~ 600000	
spf-max-wait	連続した SPF 計算の最大待機時間 (単位: ミリ秒) を指定します。	1 ~ 600000	

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

LSA の更新を受信してから、実際に Shortest Path First(SPF) 計算を開始するまでの待機時間 (単位: ミリ秒)、連続した SPF 計算の最小待機時間 (単位: ミリ秒)、および連続した SPF 計算の最大待機時間 (単位: ミリ秒) を設定します。

【実行例】

LSAの更新を受信してから、実際に Shortest Path First(SPF) 計算を開始するまでの待機時間 (単位: ミリ秒)、連続した SPF 計算の最小待機時間 (単位: ミリ秒)、および連続した SPF 計算の最大待機時間 (単位: ミリ秒) を設定します (spf-start: 50 ミリ秒、spf-hold: 1000 ミリ秒、spf-max-wait: 10000 ミリ秒)。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#timers throttle spf 50 1000 10000
```

【未設定時】

以下の値で動作します。

```
spf-start:      5000 ミリ秒
spf-hold:       10000 ミリ秒
spf-max-wait:   10000 ミリ秒
```

7.1.51 trap lsa maxage

【機能】

ospfMaxAgeTrap の設定

【入力形式】

```
trap lsa maxage

no trap lsa [maxage]
```

【動作モード】

OSPF サービス設定モード

【説明】

ospfMaxAgeTrap を有効にします。

【実行例】

ospfMaxAgeTrap を有効にします。

```
#configure terminal
(config)#router ospf 1
(config-ospf 1)#trap lsa maxage
```

【未設定時】

ospfMaxAgeTrap は無効となります。

7.1.52 trap lsa originate

【機能】

ospfOriginateLsaTrap の設定

【入力形式】

trap lsa originate

no trap lsa [originate]

【動作モード】

OSPF サービス設定モード

【説明】

ospfOriginateLsaTrap を有効にします。

【実行例】

ospfOriginateLsaTrap を有効にします。

```
#configure terminal
(config)#router ospf 1
(config-ospf 1)#trap lsa originate
```

【未設定時】

ospfOriginateLsaTrap は無効となります。

7.1.53 trap tx-retransmit

【機能】

ospfTxRetransmitTrap の設定

【入力形式】

trap tx-retransmit

no trap tx-retransmit

【動作モード】

OSPF サービス設定モード

【説明】

ospfTxRetransmitTrap を有効にします。

【実行例】

ospfTxRetransmitTrap を有効にします。

```
#configure terminal
(config)#router ospf 1
(config-ospf 1)#trap tx-retransmit
```

【未設定時】

ospfTxRetransmitTrap は無効となります。

7.1.54 trap vlink-tx-retransmit

【機能】

ospfVirtIfTxRetransmitTrap の設定

【入力形式】

trap vlink-tx-retransmit

no trap vlink-tx-retransmit

【動作モード】

OSPF サービス設定モード

【説明】

ospfVirtIfTxRetransmitTrap を有効にします。

【実行例】

ospfVirtIfTxRetransmitTrap を有効にします。

```
#configure terminal
(config)#router ospf 1
(config-ospf 1)#trap vlink-tx-retransmit
```

【未設定時】

ospfVirtIfTxRetransmitTrap は無効となります。

7.2 Virtual Link の設定

7.2.1 area virtual-link

【機能】

Virtual-link を確立する OSPF ネイバーのルータ ID の設定

【入力形式】

area <エリア ID> virtual-link <ルータ ID>

no area <エリア ID> virtual-link <ルータ ID>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリア ID	対象とするエリア ID を指定します	0 ～ 4294967295 または IPv4 アドレス形式	省略不可
ルータ ID	Virtual-Link を確立する OSPF ネイバーのルータ ID を指定します。	IPv4 アドレス形式	

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

Virtual-link を確立する OSPF ネイバーのルータ ID を設定します。

【実行例】

Virtual-link を確立する OSPF ネイバーのルータ ID を設定します（エリア ID：1、ルータ ID：192.0.2.1）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf)#area 1 virtual-link 192.0.2.1
```

【未設定時】

Virtual-link を確立しません。

7.2.2 area virtual-link authentication

【機能】

認証機能を使用するかどうかの設定

【入力形式】

area <エリア ID> virtual-link <ルータ ID> authentication [message-digest | null]

no area <エリア ID> virtual-link <ルータ ID> authentication [message-digest | null]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリア ID	対象とするエリア ID を指定します	0 ～ 4294967295 または IPv4 アドレス形式	省略不可
ルータ ID	Virtual-Link を確立する OSPF ネイバーに、そのルータ ID を指定します。	IPv4 アドレス形式	
message-digest null	MD5 認証を行う場合は message-digest、認証を行わない場合は null を指定します。	message-digest:md5 認証を行う null：認証を行わない	simple-password で認証する

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

認証機能を使用するかどうかを設定します。

【実行例】

認証機能を使用します（エリア ID：1、ルータ ID：192.0.2.1、message-digest）。

```

【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf)#area 1 virtual-link 192.0.2.1 authentication message-digest

```

【未設定時】

指定した Virtual-Link においては、simple-password で認証します。

7.2.3 area virtual-link authentication-key

【機能】

Virtual-Link で認証機能を使用する場合の認証キーの設定

【入力形式】

area <エリア ID> virtual-link <ルータ ID> authentication-key <認証キー>

no area <エリア ID> virtual-link <ルータ ID> authentication-key [<認証キー>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリア ID	対象とするエリア ID を指定します	0 ～ 4294967295 または IPv4 アドレス形式	省略不可
ルータ ID	Virtual-Link を確立する OSPF ネイバーのルータ ID を指定します。	IPv4 アドレス形式	
認証キー	simple-password で認証する場合の認証キーを指定します。	254 文字以内の WORD 型	

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

Virtual-Link で認証機能を使用する場合の認証キーを設定します。認証する場合は、認証キーが同じである必要があります。

【実行例】

Virtual-Link で認証機能を使用する場合の認証キーを設定します（エリア ID：1、ルータ ID：192.0.2.1、認証キー：authkey）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf)#area 1 virtual-link 192.0.2.1 authentication-key authkey
```

【未設定時】

simple-password による認証を行いません。

7.2.4 area virtual-link dead-interval

【機能】

OSPF の dead interval 値の設定

【入力形式】

area <エリア ID> virtual-link <ルータ ID> dead-interval <dead-interval 値>

no area <エリア ID> virtual-link <ルータ ID> dead-interval <dead-interval 値>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリア ID	対象とするエリア ID を指定します	0～4294967295 または IPv4 アドレス形式	省略不可
ルータ ID	Virtual-Link を確立する OSPF ネイバーのルータ ID を指定します。	IPv4 アドレス形式	
dead-interval 値	dead-interval 値（単位：秒）を設定します。	1～65535	

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

OSPF(OSPF6)の dead interval 値（単位：秒）を設定します。ここで設定した時間、OSPF(OSPF6)の Hello を受信しなかった場合、その OSPF ネイバーをテーブルから削除します。

【実行例】

OSPF の dead interval 値を設定します（エリア ID：1、ルータ ID：192.0.2.1、dead-interval 値：100 秒）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf)#area 1 virtual-link 192.0.2.1 dead-interval 100
```

【未設定時】

dead interval 値は 40 秒で動作します。

7.2.5 area virtual-link hello-interval

【機能】

Virtual-Link の Hello メッセージの送信間隔の設定

【入力形式】

area <エリア ID> virtual-link <ルータ ID> hello-interval <送信間隔>

no area <エリア ID> virtual-link <ルータ ID> hello-interval <送信間隔>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリア ID	対象とするエリア ID を指定します。	0 ～ 4294967295 または IPv4 アドレス形式	省略不可
ルータ ID	Virtual-Link を確立する OSPF ネイバーのルータ ID を指定します。	IPv4 アドレス形式	
送信間隔	Hello メッセージの送信間隔（単位：秒）を指定します。	1 ～ 65535	

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

Virtual-Link の Hello メッセージの送信間隔（単位：秒）を設定します。

【実行例】

Virtual-Link の Hello メッセージの送信間隔を設定します（エリア ID：1、ルータ ID：192.0.2.1、送信間隔：20 秒）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf)#area 1 virtual-link 192.0.2.1 hello-interval 20
```

【未設定時】

送信間隔は 10 秒で動作します。

7.2.6 area virtual-link message-digest-key

【機能】

Virtual-Link で MD5 認証機能を使用する場合の認証キーの設定

【入力形式】

area <エリア ID> virtual-link <ルータ ID> message-digest-key <キー ID> md5 <認証キー>

no area <エリア ID> virtual-link <ルータ ID> message-digest-key [<キー ID>] [md5 [<認証キー>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリア ID	対象とするエリア ID を指定します	0 ～ 4294967295 または IPv4 アドレス形式	省略不可
ルータ ID	Virtual-Link を確立する OSPF ネイバーのルータ ID を指定します。	IPv4 アドレス形式	
キー ID	キー ID を指定します。	1 ～ 255	
認証キー	simple-password で認証する場合の認証キーを指定します。	254 文字以内の WORD 型	

【動作モード】

OSPF サービス設定モード、OSPF-VRF サービス設定モード

【説明】

Virtual-Link で MD5 認証機能を使用する場合の認証キーを設定します。認証する場合は、キー ID、および認証キーが同じである必要があります。

【実行例】

Virtual-Link で MD5 認証機能を使用する場合の認証キーを設定します（エリア ID：1、ルータ ID：192.0.2.1、キー ID：1、認証キー：authkey）。

```

【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf)#area 1 virtual-link 192.0.2.1 message-digest-key 1 md5 authkey

```

【未設定時】

MD5 による認証を行いません。

7.2.7 area virtual-link retransmit-interval

【機能】

Virtual-Link の Database Description、Link State Request パケットの送信間隔の設定

【入力形式】

area <エリア ID> virtual-link <ルータ ID> retransmit-interval <送信間隔>

no area <エリア ID> virtual-link <ルータ ID> retransmit-interval <送信間隔>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリア ID	対象とするエリア ID を指定します	0 ～ 4294967295 または IPv4 アドレス形式	省略不可
ルータ ID	Virtual-Link を確立する OSPF ネイバーのルータ ID を指定します。	IPv4 アドレス形式	
送信間隔	Database Description、および Link State Request パケットの送信間隔 (単位: 秒) を指定します。	1 ～ 65535	

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

Virtual-Link の Database Description、および Link State Request パケットの送信間隔 (単位: 秒) を設定します。

【実行例】

Virtual-Link の Database Description、および Link State Request パケットの送信間隔を設定します (エリア ID : 1、ルータ ID : 192.0.2.1、送信間隔 : 100 秒)。

```

【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf)#area 1 virtual-link 192.0.2.1 retransmit-interval 100

```

【未設定時】

送信間隔は 10 秒で動作します。

7.2.8 area virtual-link transmit-delay

【機能】

Virtual-Link の LinkStateUpdate 中継遅延時間の設定

【入力形式】

area <エリア ID> virtual-link <ルータ ID> transmit-delay <中継遅延時間>

no area <エリア ID> virtual-link <ルータ ID> transmit-delay <中継遅延時間>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリア ID	対象とするエリア ID を指定します	0 ～ 4294967295 または IPv4 アドレス形式	省略不可
ルータ ID	Virtual-Link を確立する OSPF ネイバーのルータ ID を指定します。	IPv4 アドレス形式	
中継遅延時間	LinkStateUpdate 中継遅延時間 (単位: 秒) を指定します。	1 ～ 65535	

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

Virtual-Link の LinkStateUpdate 中継遅延時間（単位：秒）を設定します。ここで設定した値が、LSA の Age に加算されます。

【実行例】

Virtual-Link の LinkStateUpdate 中継時間時間を設定します（エリア ID：1、ルータ ID：192.0.2.1、中継遅延時間：10 秒）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf)#area 1 virtual-link 192.0.2.1 transmit-delay 10
```

【未設定時】

中継遅延時間は 1 秒で動作します。

7.3 IPv6 経路交換の設定

7.3.1 router ipv6 ospf

【機能】

OSPF6 サービス設定モードへの移行

【入力形式】

router ipv6 ospf

no router ipv6 ospf

【動作モード】

基本設定モード

【説明】

OSPF6 サービス設定モードへ移行します。コマンドの先頭に "no" を指定することで、OSPF6 サービス設定モードの内容がすべて消去されます。

【実行例】

OSPF6 サービス設定モードに移行します。

```
#configure terminal
(config)#router ipv6 ospf
(config-ospf6)#
```

7.3.2 area default-cost

【機能】

summary-LSA を通知する場合のコスト値の設定

【入力形式】

area <エリア ID> default-cost <コスト値>

no area <エリア ID> default-cost [<コスト値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリア ID	対象とするエリア ID を指定します	0 ～ 4294967295 または IPv4 アドレス形式	省略不可
コスト値	スタブエリアまたは NSSA に対して、summary-LSA を通知する場合のコスト値を指定します。	0 ～ 16777215	

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

スタブエリアまたはNSSAに対して、summary-LSAを通知する場合のコスト値を設定します。

【実行例】

summary-LSAを通知する場合のコスト値を設定します（エリアID：192.0.2.1、コスト値：100）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#area 192.0.2.1 default-cost 100
```

【未設定時】

コスト値は1で動作します。

7.3.3 area range

【機能】

エリアに属するネットワークの範囲の設定

【入力形式】

area <エリアID> range {<ネットワークアドレス1> <ネットマスク1> | <ネットワークアドレス1> /
プレフィックス長>} [substitute <ネットワークアドレス2> <ネットマスク2> | not-advertise]

no area <エリアID> range {<ネットワークアドレス1> <ネットマスク1> | <ネットワークアドレス1> /
<プレフィックス長>} [substitute [<ネットワークアドレス2> <ネットマスク2>] | not-advertise]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリアID	対象とするエリアIDを指定します	0～4294967295またはIPv4アドレス形式	省略不可
ネットワークアドレス1	このエリアに属するネットワークアドレスを指定します。	IPv4アドレス型式 IPv6アドレス形式	
ネットマスク1	ネットマスクを指定します。	IPv4アドレス形式	
プレフィックス長(*1)	プレフィックス長を指定します。	0～128	
ネットワークアドレス2(*2)	異なるプレフィックスとして通知する場合に、そのネットワークアドレスを指定します。	IPv4アドレス型式	異なるプレフィックスとして通知しない
ネットマスク2(*2)	異なるプレフィックスとして通知する場合に、ネットマスクを指定します。	IPv4アドレス形式	
not-advertise	集約した経路を広告しない場合に指定します。	-	集約経路を広告

*1) OSPF サービス設定モード、OSPF-VRF サービス設定モードでは指定できません。

*2) OSPF6 サービス設定モードでは指定できません。

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

エリアに属するネットワークの範囲を設定します。

【実行例】

ネットワーク範囲を設定します（エリア ID：1、ネットワークアドレス：192.0.2.0、ネットマスク：255.255.255.0）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#area 1 range 192.0.2.0 255.255.255.0
```

【未設定時】

エリアに属するネットワークを設定しません。

7.3.4 area stub

【機能】

スタブエリアの設定

【入力形式】

area <エリア ID> stub [no-summary]

no area <エリア ID> stub [no-summary]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリア ID	対象とするエリア ID を指定します。	0～429496729 または IPv4 アドレス形式	省略不可
no-summary	スタブエリアに、summary-LSA を広告しない場合に指定します。	-	summary-LSA を広告

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

スタブエリアを設定します。スタブエリアの ABR の場合は、area default-cost コマンドで設定されたコストで、summary-LSA をスタブエリア内に広告します。

【実行例】

スタブエリアを設定します（エリア ID:1、no-summary）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#area 1 stub no-summary
```

【未設定時】

スタブエリアを設定しません。

7.3.5 default-metric

【機能】

AS 外の経路情報を OSPF で広告する際のメトリック値の設定

【入力形式】

default-metric <メトリック値>

no default-metric [<メトリック値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
メトリック値	AS 外の経路情報を OSPF で広告する際に、そのメトリック値を指定します。	0～16777214	省略不可

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

AS 外の経路情報を OSPF(OSPF6) で広告する際のメトリック値を設定します。

【実行例】

AS 外の経路情報を OSPF で広告する際のメトリック値を設定します（メトリック値：10）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#default-metric 10
```

【未設定時】

メトリック値は 20 で動作します。

7.3.6 distance

【機能】

OSPF のディスタンス値の設定

【入力形式】

distance <ディスタンス値>

no distance <ディスタンス値>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ディスタンス値	ディスタンス値を指定します。	1～255	省略不可

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

OSPF(OSPF6)のディスタンス値を設定します。同じ宛先への経路を異なる手段で学習した場合に、どの情報を採用するかのパラメタとなります。

【実行例】

OSPF のディスタンス値を設定します（ディスタンス値：120）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#distance 120
```

【未設定時】

以下の値で動作します（OSPF は 110）。

プロトコル	デフォルト値	備考
スタティック	1	設定変更可能
直接経路	-	設定変更不可
BGP(external)	20	設定変更可能
BGP(internal)	200	
BGP(local)		
RIP	120	設定変更可能
OSPF(external)	110	設定変更可能
OSPF(inter-area)		
OSPF(intra-area)		

7.3.7 ipv6 ospf cost

【機能】

OSPF6 を使用する場合のコスト値の設定

【入力形式】

ipv6 ospf cost <コスト値>

no ipv6 ospf cost

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
コスト値	OSPF6 のコスト値を指定します。	1～65535	省略不可

【動作モード】

management インタフェース設定モード、loopback インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

OSPF6 を使用する場合のコスト値を設定します。

【実行例】

OSPF6 を使用する場合のコスト値を設定します（コスト値：100）。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 ospf cost 100
```

【未設定時】

コスト値は 10 で動作します。

7.3.8 ipv6 ospf dead-interval

【機能】

OSPF6 の dead-interval 値の設定

【入力形式】

ipv6 ospf dead-interval <dead-interval 値>

no ipv6 ospf dead-interval

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
dead-interval 値	dead-interval 値（単位：秒）を指定します。	1～65535	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

OSPF6 の dead-interval 値（単位：秒）を設定します。ここで設定した時間、OSPF6 の Hello を受信しなかった場合は、そのネイバーをテーブルから削除します。

【実行例】

OSPF6 の dead-interval 値（単位：秒）を設定します（dead-interval 値：100 秒）。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 ospf dead-interval 100
```

【未設定時】

dead-interval 値は 40 秒で動作します。

7.3.9 ipv6 ospf display route single-line

【機能】

show ipv6 ospf route コマンド出力表示の設定

【入力形式】

ipv6 ospf display route single-line

no ipv6 ospf display route single-line

【動作モード】

基本設定モード

【説明】

show ipv6 ospf route コマンドの出力を 1 行ずつ表示する場合に設定します。

【実行例】

show ipv6 ospf route コマンドの出力を 1 行ずつ表示します。

```
#configure terminal
(config)#ipv6 ospf display route single-line
```

【未設定時】

複数ライン出力となります。

7.3.10 ipv6 ospf hello-interval

【機能】

OSPF の Hello メッセージの送信間隔の設定

【入力形式】

ipv6 ospf hello-interval <送信間隔>

no ipv6 ospf hello-interval

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
送信間隔	Hello メッセージの送信間隔（単位：秒）を指定します。	1～65535	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

OSPF の Hello メッセージの送信間隔（単位：秒）を設定します。

【実行例】

OSPF の Hello メッセージの送信間隔を設定します（送信間隔：20 秒）。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 ospf hello-interval 20
```

【未設定時】

送信間隔は 10 秒で動作します。

7.3.11 ipv6 ospf priority

【機能】

OSPF の優先度の設定

【入力形式】

ipv6 ospf priority <優先度>

no ipv6 ospf priority

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
優先度	OSPF の優先度を設定します。	0 ～ 255	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

OSPF の優先度を設定します。同一インタフェース上に複数の OSPF ルータが存在した場合、優先度の大きいルータが Designated Router(DR) となります。各ルータは Hello メッセージで優先度を広告します。

【実行例】

OSPF の優先度を設定します（優先度：20）。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 ospf priority 20
```

【未設定時】

優先度は 1 で動作します。

7.3.12 ipv6 ospf retransmit-interval

【機能】

Database Description、Link State Request パケットの再送間隔の設定

【入力形式】

```
ipv6 ospf retransmit-interval <再送間隔>
```

```
no ipv6 ospf retransmit-interval
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
再送間隔	Database Description、および Link State Request パケットの再送間隔 (単位：秒) を指定します。	1～65535	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

Database Description、および Link State Request パケットの再送間隔（単位：秒）を設定します。

【実行例】

Database Description、および Link State Request パケットの再送間隔を設定します（再送間隔：100 秒）。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 ospf retransmit-interval 100
```

【未設定時】

再送間隔は 5 秒で動作します。

7.3.13 ipv6 ospf transmit-delay

【機能】

遅延時間の設定

【入力形式】

```
ipv6 ospf transmit-delay <遅延時間>
```

```
no ipv6 ospf transmit-delay
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
遅延時間	遅延時間（単位：秒）を指定します。	1～65535	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

遅延時間（単位：秒）を設定します。ここで設定した値が LSA の Age に加算されます。

【実行例】

遅延時間（単位：秒）を設定します（遅延時間：10 秒）。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 ospf transmit-delay 10
```

【未設定時】

遅延時間は 1 秒で動作します。

7.3.14 ipv6 router ospf area

【機能】

エリア ID の設定

【入力形式】

ipv6 router ospf area <エリア ID>

no ipv6 router ospf area <エリア ID>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリア ID	エリア ID を指定します。	0～4294967295、または、IPv4 アドレス形式	省略不可

【動作モード】

management インタフェース設定モード、loopback インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

エリア ID を設定します。

loopback インタフェースに設定する場合、リンクローカルアドレスを設定していないと、有効になりません。

【実行例】

エリア ID を設定します（エリア ID：1）。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 router ospf area 1
```

【未設定時】

OSPF6 は動作しません。

7.3.15 log-adjacency-changes

【機能】

OSPF ネイバーステートマシンの状態遷移ログ情報の出力

【入力形式】

log-adjacency-changes [detail]

no log-adjacency-changes [detail]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
detail	すべての状態遷移でログ情報を出力します。	-	FULL ステートからの状態遷移、または、FULL ステートへの状態遷移のみログ情報を出力

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

OSPF(OSPF6) ネイバーステートマシンの状態遷移をログ情報に出力します。出力内容は状態遷移前後のステート、および状態遷移を引き起こしたイベントの種類です。"detail" を指定した場合は、すべての状態遷移時にログ情報を出力します。"detail" を指定しない場合は、FULL ステートと FULL ステート以外のステート間で状態遷移が発生した場合のみ、ログ情報を出力します。

【実行例】

OSPF ネイバーステートマシンの状態遷移をログ情報に出力します。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#log-adjacency-changes
```

【未設定時】

OSPF(OSPF6) ネイバーステートマシンの状態遷移をログ情報に出力しません。

7.3.16 overflow database external

【機能】

External データベースのサイズ、overflow 状態からの回復を待つための時間の設定

【入力形式】

overflow database external <MAXDBSIZE> <WAITTIME>

no overflow database external [<MAXDBSIZE> <WAITTIME>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
MAXDBSIZE	AS-EXTERNAL-LSA の上限値を指定します。同じ AS 内のルータでは、同じ値としてください。	0 ～ 4294967294	省略不可
WAITTIME	overflow 状態から回復するための待ち時間（単位：秒）を指定します。 "0" を指定した場合は、overflow 状態から戻ることはできません。	0 ～ 65535	

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

External データベースのサイズ、および overflow 状態から回復するのを待つための時間（単位：秒）を設定します。

【実行例】

External データベースのサイズ、および overflow 状態から回復するのを待つための時間（単位：秒）を設定します（MAXDBSIZE：1000000LSA、WAITTIME：30 秒）。

```

【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#overflow database external 1000000 30

```

【未設定時】

External データベースのサイズ、および overflow 状態から回復するのを待つための時間を規定しません。

7.3.17 passive-interface

【機能】

Hello パケットを送信しないインタフェースの設定

【入力形式】

passive-interface <インタフェース名> <インタフェース番号> [<IPv4 アドレス>]

no passive-interface <インタフェース名> <インタフェース番号> [<IPv4 アドレス>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース名	OSPF(OSPF6)のHelloパケットの送信は行わず、受信のみ行うインタフェース名を指定します。	-	省略不可
インタフェース番号	OSPF(OSPF6)のHelloパケットの送信は行わず、受信のみ行うインタフェース番号を指定します。	-	
IPv4 アドレス(*1)	OSPFのHelloパケットの送信は行わず、受信のみ行うインタフェースアドレスを指定します。	IPv4 アドレス形式	設定したインタフェースのすべてのアドレスでHelloの送信は行いません。

*1) OSPF6 サービス設定モードでは指定できません。インタフェース名に port-channel を指定した場合のみ指定できます。

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

Helloパケットの送信を行わないインタフェースを設定します。ルータ ID 決定時の計算対象からも除外されます。

【実行例】

Helloパケットの送信を行わないインタフェースを設定します（インタフェース名：port-channel、インタフェース番号：1）。

```

【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#passive-interface port-channel 1

```

【未設定時】

Helloパケットの送信を行います。

7.3.18 redistribute

【機能】

経路情報を再広告する設定

【入力形式】

```
redistribute { <再広告する経路情報> | isakmp sa-up { local-prot1 | local-prot2 } | ospf <インスタンス番号> } [metric <メトリック値>] [metric-type { type-1 | type-2 }] [route-map <route-map 名>]
```

```
no redistribute { <再広告する経路情報> | isakmp sa-up { local-prot1 | local-prot2 } | ospf <インスタンス番号> } [metric <メトリック値>] [metric-type { type-1 | type-2 }] [route-map <route-map 名>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
再広告する経路情報	OSPF 以外の手段で取得した経路情報のうち、OSPF で広告するものを指定します。	connected:connected 経路 kernel(*1):kernel にセットされた経路 static : スタティック経路 rip:RIP で学習した経路 bgp:BGP で学習した経路	省略不可
isakmp sa-up	SA-UP ルートを OSPF で広告する場合に指定します。	-	
local-prot1 local-prot2	SA-UP ルートを管理するプロトコル名を指定します。	-	
ospf (*1)	他の OSPF インスタンスで取得した経路情報を OSPF で広告する場合に指定します。	-	
インスタンス番号(*1)	他の OSPF インスタンス番号を指定します。	1 ～ 65535	
メトリック値	OSPF で経路を広告する際のメトリック値を指定します。	0 ～ 16777214	default-metric コマンドの設定値に従う
type-1 type-2	メトリックタイプを指定します。	type-1 type-2	type-2
route-map 名	適用する route-map 名を指定します。	254 文字以内の WORD 型	route-map を適用しない

*1) OSPF6 サービス設定モードでは指定できません。

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

異なるルートドメインに対して、経路情報の再広告を行う場合に設定します。

【実行例】

経路情報の再広告を行います（再広告する経路情報：static、メトリック値：3、type-1）。

```

【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#redistribute static metric 3 metric-type type-1

```

【未設定時】

再広告を行いません。

7.3.19 router-id

【機能】

OSPF のルータ ID の設定

【入力形式】

router-id <ルータ ID>

no router-id <ルータ ID>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ルータ ID	ルータ ID を指定します。	IPv4 アドレス形式	省略不可

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

OSPF(OSPF6)のルータ ID を設定します。

【実行例】

OSPF のルータ ID を設定します (ルータ ID : 192.0.2.1)。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#router-id 192.0.2.1
```

【未設定時】

全インタフェースの IPv4 アドレスのうち、最大のものをルータ ID とします。

7.3.20 summary-prefix

【機能】

AS 外の経路情報の集約

【入力形式】

summary-prefix <ネットワークアドレス><プレフィックス長> [not-advertise]

no summary-prefix <ネットワークアドレス><プレフィックス長> [not-advertise]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ネットワークアドレス	集約後の経路情報を指定します。	IPv6 アドレス形式	省略不可
プレフィックス長	プレフィックス長を指定します。	0 ~ 128	
not-advertise	この経路自体を OSPF6 で広告しない場合に指定します。	-	OSPF6 で広告

【動作モード】

OSPF6 サービス設定モード

【説明】

AS 外の経路情報を集約します。

【実行例】

AS 外の経路情報を集約します（ネットワークアドレス：2001:db8::、プレフィックス長：32、OSPF6 で広告しない）。

```
#configure terminal
(config)#router ipv6 ospf
(config-ospf6)#summary-prefix 2001:db8::/32 not-advertise
```

【未設定時】

経路を集約しません。

7.3.21 timers spf

【機能】

LSA の更新を受信してから Shortest Path First(SPF) 計算を開始するまでの遅延時間、SPF 計算を行ってから次の計算に入るまでのホールドタイムの設定

【入力形式】

timers spf <spf-delay> <spf-holdtime>

no timers spf <spf-delay> <spf-holdtime>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
spf-delay	LSA の更新を受信してから、実際に SPF 計算を開始するまでの遅延時間（単位：秒）を指定します。	0 ～ 4294967295	省略不可
spf-holdtime	SPF 計算を行ってから次の計算に入るまでのホールドタイム（単位：秒）を指定します。	0 ～ 4294967295	

【動作モード】

OSPF6 サービス設定モード

【説明】

LSA の更新を受信してから、実際に Shortest Path First(SPF) 計算を開始するまでの遅延時間（単位：秒）、および SPF 計算を行ってから次の計算に入るまでのホールドタイム（単位：秒）を設定します。

【実行例】

実際に Shortest Path First(SPF) 計算を開始するまでの遅延時間 (単位: 秒)、および SPF 計算を行ってから次の計算に入るまでのホールドタイムを設定します (spf-delay: 100 秒、spf-holdtime: 500 秒)。

```
#configure terminal
(config)#router ipv6 ospf
(config-ospf6)#timers spf 100 500
```

【未設定時】

以下の値で動作します。

spf-delay: 5 秒

spf-holdtime: 10 秒

7.4 Virtual Link の設定

7.4.1 area virtual-link

【機能】

Virtual-link を確立する OSPF ネイバーのルータ ID の設定

【入力形式】

area <エリア ID> virtual-link <ルータ ID>

no area <エリア ID> virtual-link <ルータ ID>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリア ID	対象とするエリア ID を指定します	0 ～ 4294967295 または IPv4 アドレス形式	省略不可
ルータ ID	Virtual-Link を確立する OSPF ネイバーのルータ ID を指定します。	IPv4 アドレス形式	

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

Virtual-link を確立する OSPF ネイバーのルータ ID を設定します。

【実行例】

Virtual-link を確立する OSPF ネイバーのルータ ID を設定します（エリア ID：1、ルータ ID：192.0.2.1）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf)#area 1 virtual-link 192.0.2.1
```

【未設定時】

Virtual-link を確立しません。

7.4.2 area virtual-link dead-interval

【機能】

OSPF の dead interval 値の設定

【入力形式】

area <エリア ID> virtual-link <ルータ ID> dead-interval <dead-interval 値>

no area <エリア ID> virtual-link <ルータ ID> dead-interval <dead-interval 値>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリア ID	対象とするエリア ID を指定します	0 ～ 4294967295 または IPv4 アドレス形式	省略不可
ルータ ID	Virtual-Link を確立する OSPF ネイバーのルータ ID を指定します。	IPv4 アドレス形式	
dead-interval 値	dead-interval 値（単位：秒）を設定します。	1 ～ 65535	

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

OSPF(OSPF6)の dead interval 値（単位：秒）を設定します。ここで設定した時間、OSPF(OSPF6)の Hello を受信しなかった場合、その OSPF ネイバーをテーブルから削除します。

【実行例】

OSPF の dead interval 値を設定します（エリア ID：1、ルータ ID：192.0.2.1、dead-interval 値：100 秒）。

```

【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf)#area 1 virtual-link 192.0.2.1 dead-interval 100

```

【未設定時】

dead interval 値は 40 秒で動作します。

7.4.3 area virtual-link hello-interval

【機能】

Virtual-Link の Hello メッセージの送信間隔の設定

【入力形式】

area <エリア ID> virtual-link <ルータ ID> hello-interval <送信間隔>

no area <エリア ID> virtual-link <ルータ ID> hello-interval <送信間隔>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリア ID	対象とするエリア ID を指定します	0 ～ 4294967295 または IPv4 アドレス形式 省略不可	省略不可
ルータ ID	Virtual-Link を確立する OSPF ネイバーのルータ ID を指定します。	IPv4 アドレス形式	
送信間隔	Hello メッセージの送信間隔（単位：秒）を指定します。	1 ～ 65535	

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

Virtual-Link の Hello メッセージの送信間隔（単位：秒）を設定します。

【実行例】

Virtual-Link の Hello メッセージの送信間隔を設定します（エリア ID：1、ルータ ID：192.0.2.1、送信間隔：20 秒）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf)#area 1 virtual-link 192.0.2.1 hello-interval 20
```

【未設定時】

送信間隔は 10 秒で動作します。

7.4.4 area virtual-link retransmit-interval

【機能】

Virtual-Link の Database Description、Link State Request パケットの送信間隔の設定

【入力形式】

area <エリア ID> virtual-link <ルータ ID> retransmit-interval <送信間隔>

no area <エリア ID> virtual-link <ルータ ID> retransmit-interval <送信間隔>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリア ID	対象とするエリア ID を指定します。	0～429496729 または IPv4 アドレス形式	省略不可
ルータ ID	Virtual-Link を確立する OSPF ネイバーのルータ ID を指定します。	IPv4 アドレス形式	
送信間隔	Database Description、および Link State Request パケットの送信間隔（単位：秒）を指定します。	1～65535	

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

Virtual-Link の Database Description、および Link State Request パケットの送信間隔（単位：秒）を設定します。

【実行例】

Virtual-Link の Database Description、および Link State Request パケットの送信間隔を設定します（エリア ID：1、ルータ ID：192.0.2.1、送信間隔：100 秒）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf)#area 1 virtual-link 192.0.2.1 retransmit-interval 100
```

【未設定時】

送信間隔は 10 秒で動作します。

7.4.5 area virtual-link transmit-delay

【機能】

Virtual-Link の LinkStateUpdate 中継遅延時間の設定

【入力形式】

area <エリア ID> virtual-link <ルータ ID> transmit-delay <中継遅延時間>

no area <エリア ID> virtual-link <ルータ ID> transmit-delay <中継遅延時間>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エリア ID	対象とするエリア ID を指定します	0～4294967295 または IPv4 アドレス形式	省略不可
ルータ ID	Virtual-Link を確立する OSPF ネイバーのルータ ID を指定します。	IPv4 アドレス形式	
中継遅延時間	LinkStateUpdate 中継遅延時間（単位：秒）を指定します。	1～65535	

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード、OSPF-VRF サービス設定モード

【説明】

Virtual-Link の LinkStateUpdate 中継遅延時間（単位：秒）を設定します。ここで設定した値が、LSA の Age に加算されます。

【実行例】

Virtual-Link の LinkStateUpdate 中継遅延時間を設定します（エリア ID：1、ルータ ID：192.0.2.1、中継遅延時間：10 秒）。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf)#area 1 virtual-link 192.0.2.1 transmit-delay 10
```

【未設定時】

中継遅延時間は 1 秒で動作します。

7.5 VRF 経路交換の設定

7.5.1 router ospf-vrf

【機能】

OSPF-VRF サービス設定モードへの移行

【入力形式】

router ospf-vrf <VRF 名> <インスタンス番号> daemon-id <プロセス番号>

no router ospf-vrf <VRF 名> <インスタンス番号> daemon-id <プロセス番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VRF 名	OSPF を使用する VRF 名を指定します。	63 文字以内の WORD 型	省略不可
インスタンス番号	インスタンス番号を指定します。	1～65535	
プロセス番号	プロセス番号を指定します。	1～5	

【動作モード】

基本設定モード

【説明】

OSPF-VRF サービス設定モードに移行します。複数の VRF に OSPF を設定する場合は、プロセス番号を均等に指定してください。

ip vrf コマンドで設定がされていない VRF では、OSPF 設定を行うことができません。

ip vrf コマンドを削除した場合は、該当する VRF の OSPF 設定が自動的に削除されます。

INET の OSPF は、router ospf コマンドを使用してください。

コマンドの先頭に "no" を指定することで、該当 OSPF-VRF サービス設定モードの内容がすべて消去されます。

同一 daemon-id で設定可能なインスタンス数の上限は 60 個となります。

【実行例】

OSPF-VRF サービス設定モードに移行します (VRF 名: vrf-A、インスタンス番号: 100、プロセス番号: 1)。

```
#configure terminal
(config)#router ospf-vrf vrf-A 100 daemon-id 1
(config-ospf-vrf vrf-A 100 daemon-id 1)#
```

第8章 BGPの設定



この章では、BGPの設定に関するコマンドについて説明します。

8.1	BGPの設定	265
8.2	IPv4経路交換の設定	309
8.3	IPv6経路交換の設定	330
8.4	IPv4VRF経路交換の設定	351
8.5	IPv6VRF経路交換の設定	352

8.1 BGP の設定

8.1.1 router bgp

【機能】

BGP サービス設定モードへの移行

【入力形式】

router bgp <AS 番号>

no router bgp <AS 番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
AS 番号	本装置が属する AS 番号を指定します。	1 ～ 4294967295	省略不可

【動作モード】

基本設定モード

【説明】

BGP サービス設定モードに移行します。コマンドの先頭に "no" を指定することで、該当 BGP サービス設定モードの内容がすべて消去されます。

【実行例】

BGP サービス設定モードに移行します (AS 番号：64496)。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#
```

8.1.2 bgp aggregate-nextthop-check

【機能】

Next-hop が一致する経路情報に関してのみ集約する設定

【入力形式】

bgp aggregate-nextthop-check

no bgp aggregate-nextthop-check

【動作モード】

基本設定モード

【説明】

Next-hop が一致する経路情報に関してのみ、集約する場合に設定します。

【実行例】

Next-hop が一致する経路情報に関してのみ集約します。

```
#configure terminal
(config)#bgp aggregate-nexthop-check
```

【未設定時】

Next-Hop に関係なく経路を集約します。

8.1.3 bgp anvl-dampening-config

【機能】

anvl-dampening-config 動作モードの設定

【入力形式】

bgp anvl-dampening-config

no bgp anvl-dampening-config

【動作モード】

基本設定モード

【説明】

anvl-dampening-config 動作モードを設定します。

【実行例】

anvl-dampening-config 動作モードを設定します。

```
#configure terminal
(config)#bgp anvl-dampening-config
```

【未設定時】

bgp anvl-dampening-config 動作をしません。

8.1.4 no bgp extended-asn-cap

【機能】

4byte AS 機能を off にする設定

【入力形式】

no bgp extended-asn-cap

bgp extended-asn-cap

【動作モード】

基本設定モード

【説明】

4byte AS 機能を off とする場合に設定します。

本コマンドの設定追加時、および削除時には全 BGP ピアを切断します。

【実行例】

4byte AS 機能を off とします。

```
#configure terminal
(config)#no bgp extended-asn-cap
```

【未設定時】

4byte AS 機能は on で動作します。

8.1.5 bgp rfc1771-path-select

【機能】

RFC177 の経路選択メカニズムに準拠する設定

【入力形式】

bgp rfc1771-path-select

no bgp rfc1771-path-select

【動作モード】

基本設定モード

【説明】

RFC1771 の経路選択メカニズムに準拠する場合に設定します。

【実行例】

RFC1771 の経路選択メカニズムに準拠します。

```
#configure terminal
(config)#bgp rfc1771-path-select
```

【未設定時】

RFC1771 の経路選択メカニズムに準拠しません。

8.1.6 bgp rfc1771-strict

【機能】

RFC1771 に完全に準拠する設定

【入力形式】

bgp rfc1771-strict

no bgp rfc1771-strict

【動作モード】

基本設定モード

【説明】

RFC1771 に完全に準拠する場合に設定します。

【実行例】

RFC1771 に完全に準拠します。

```
#configure terminal
(config)#bgp rfc1771-strict
```

【未設定時】

RFC1771 に完全に準拠しません。

8.1.7 ip as-path access-list

【機能】

AS-PATH リストの設定

【入力形式】

ip as-path access-list <アクセスリスト名> {deny | permit} <正規表現>

no ip as-path access-list <アクセスリスト名> [{deny | permit} <正規表現>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アクセスリスト名	アクセスリストの名称を指定します。	254 文字以内の WORD 型	省略不可
deny permit	属性を指定します。	deny: 拒否 permit: 許可	
正規表現	AS 番号を正規表現で指定します。	正規表現：254 文字以内の WORD 型 (*1)	

*1) 1 文字の空白（スペース）は使用可能です。複数の空白（スペース）は 1 文字にまとめられます。

【動作モード】

基本設定モード

【説明】

AS-PATH リストを設定します。AS 番号は正規表現で指定します。

 参照 正規表現については、[「35.1 正規表現について」\(P.968\)](#) を参照してください。

【実行例】

AS-PATH のリストを設定します (アクセスリスト名: access-list-name-A、AS 番号: 100,101,102)。

```
#configure terminal
(config)#ip as-path access-list access-list-name-A permit 100 101 102
```

【未設定時】

AS-PATH リストによるフィルタリングを行いません。

8.1.8 ip community-list

【機能】

コミュニティリストの作成

【入力形式】

ip community-list {<1-99> | standard <コミュニティリスト名>} {deny | permit} <コミュニティ属性>

ip community-list {<100-199> | expanded <コミュニティリスト名>} {deny | permit} <正規表現>

no ip community-list {<1-99> | standard <コミュニティリスト名>} [{deny | permit} <コミュニティ属性>]

no ip community-list {<100-199> | expanded <コミュニティリスト名>} [{deny | permit} <正規表現>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
コミュニティリスト番号	コミュニティリスト番号を指定します。	1～99: 標準コミュニティリスト 100～199: 正規表現コミュニティリスト	省略不可
standard expanded	コミュニティリストが、標準コミュニティリストか、正規表現コミュニティリストかを指定します。	standard: 標準 expanded: 正規表現	
コミュニティリスト名	コミュニティリスト名を指定します。	255 文字以内の WORD 型	
deny permit	設定しているコミュニティリストの属性を指定します。	deny: 拒否 permit: 許可	
コミュニティ属性	コミュニティ属性を指定します。	1～4294967295 AA:NN 書式 internet local-as (=no-export-subconfed) no-advertise no-export	
正規表現	コミュニティ属性を正規表現で指定します。	正規表現: 254 文字以内の WORD 型 (*1)	

*1) 1 文字の空白 (スペース) は使用可能です。複数の空白 (スペース) は 1 文字にまとめられます。

【動作モード】

基本設定モード

【説明】

コミュニティリストを作成します。本コマンドで作成したコミュニティリストは、route-map で使用します。本設定は、設定順にソートされます。

【標準コミュニティリストの場合】

コミュニティリスト番号(1-99)または、standard <コミュニティリスト名>を指定し、コミュニティ属性を指定します。ここで指定したコミュニティ属性と完全に一致するものが対象となります。たとえば"1:1"と指定した場合は、"1:1"のコミュニティ属性を持つ情報のみが対象となります。また、既知のコミュニティ属性については、以下の文字列で指定できます。

- internet
- local-as (=no-export-subconfed)
- no-advertise
- no-export

【正規表現コミュニティリストの場合】

コミュニティ属性は、正規表現で指定を行います。コミュニティリスト番号(100-199)または、expanded <コミュニティリスト名>を指定し、正規表現を指定します。

 参照 正規表現については、[\[35.1 正規表現について\]](#) (P.968) を参照してください。

【実行例】

コミュニティリストを作成します (standard、コミュニティリスト名: community-list-A、deny、コミュニティ属性: 1:1)。

```
#configure terminal
(config)#ip community-list standard community-list-A deny 1:1
```

【未設定時】

コミュニティリストを作成しません。

8.1.9 ip extcommunity-list

【機能】

拡張コミュニティリストの作成

【入力形式】

ip extcommunity-list {<1 - 99> | <拡張コミュニティリスト名>} {permit | deny} rt <拡張コミュニティ属性>

ip extcommunity-list {<100 - 199> | expanded <拡張コミュニティリスト名>} {permit | deny} <正規表現>

no ip extcommunity-list {<1 - 99> | <拡張コミュニティリスト名>} {permit | deny} rt <拡張コミュニティ属性>

no ip extcommunity-list {<100 - 199> | expanded <拡張コミュニティリスト名>} {permit | deny} <正規表現>

no ip extcommunity-list {<拡張コミュニティリスト番号> | <拡張コミュニティリスト名> | expanded <拡張コミュニティリスト名>} *

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
拡張コミュニティリスト番号	拡張コミュニティリスト番号を指定します。	1-99: 標準拡張コミュニティリスト 100-199: 正規表現拡張コミュニティリスト	省略不可
expanded	正規表現拡張コミュニティリストを指定します。	-	
拡張コミュニティリスト名	拡張コミュニティリスト名を指定します。	255文字以内のWORD型	
* deny permit	設定している拡張コミュニティリストの属性を指定します。	*: 一括削除 deny: 拒否 permit: 許可	
拡張コミュニティ属性	拡張コミュニティ属性を指定します。	AA:NN 書式	
正規表現	正規表現を指定します。	254文字以内のWORD型(*1)	

*1) 文字の空白（スペース）は使用可能です。複数の空白（スペース）は1文字にまとめられます。

【動作モード】

基本設定モード

【説明】

拡張コミュニティリストを作成します。本コマンドで作成した拡張コミュニティリストは、route-map で使用します。

"*"を指定することで拡張コミュニティリスト名が一致するすべての行を一括削除します。

本設定は、設定順にソートされます。

【標準拡張コミュニティリストの場合】

拡張コミュニティリスト番号(1-99)または、拡張コミュニティリスト名を指定し、拡張コミュニティ属性を指定します。ここで指定した拡張コミュニティ属性と完全に一致するものが対象となります。たとえば"1:1"と指定した場合は、"1:1"の拡張コミュニティ属性を持つ情報のみが対象となります。

【正規表現拡張コミュニティリストの場合】

拡張コミュニティ属性は正規表現で指定します。拡張コミュニティリスト番号(100-199)または、expanded <拡張コミュニティリスト名>を指定し、正規表現を指定します。

 参照 正規表現については、[「35.1 正規表現について」\(P.968\)](#)を参照してください。

【実行例】

拡張コミュニティリストを作成します（拡張コミュニティリスト名：ext-community-list-A、deny、拡張コミュニティ属性：1:1）。

```
#configure terminal
(config)#ip extcommunity-list ext-community-list-A deny rt 1:1
```

【未設定時】

拡張コミュニティリストを作成しません。

8.1.10 bgp always-compare-med

【機能】

異なる AS に属する複数のピアから受け取った経路の MED の比較

【入力形式】

bgp always-compare-med

no bgp always-compare-med

【動作モード】

BGP サービス設定モード

【説明】

異なる AS に属する複数のピアから受け取った経路の MED の比較を行います。

【実行例】

異なる AS に属する複数のピアから受け取った経路の MED の比較を行います。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#bgp always-compare-med
```

【未設定時】

MED の比較を行いません。

8.1.11 bgp bestpath as-path ignore

【機能】

AS-PATH 長を無視する設定

【入力形式】

bgp bestpath as-path ignore

no bgp bestpath as-path ignore

【動作モード】

BGP サービス設定モード

【説明】

2 つの経路の間で経路選択を行う際、AS-PATH 長を無視する場合に指定します。

【実行例】

AS-PATH 長を無視します。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#bgp bestpath as-path ignore
```

【未設定時】

AS-PATH 長を無視しません。

8.1.12 bgp bestpath compare-routerid

【機能】

ルータ ID を考慮する設定

【入力形式】

bgp bestpath compare-routerid

no bgp bestpath compare-routerid

【動作モード】

BGP サービス設定モード

【説明】

2つの経路の間で経路選択を行う際、ルータ ID を考慮する場合に設定します。

eBGP で学習した経路のベストパス選択処理において、すでに学習済みの経路を優先する処理を抑制し、router id の比較でベストパス選択するための設定となります。

iBGP の場合には本設定は機能しません。

【実行例】

ルータ ID を考慮します。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#bgp bestpath compare-routerid
```

【未設定時】

ルータ ID を考慮しません。

8.1.13 bgp bestpath igp-metric ignore

【機能】

IGP metric を無視する設定

【入力形式】

bgp bestpath igp-metric ignore

no bgp bestpath igp-metric ignore

【動作モード】

BGP サービス設定モード

【説明】

2つの経路の間で経路選択を行う際、IGP metricを無視する場合に設定します。

【実行例】

2つの経路の間で経路選択を行う際、IGP metricを無視します。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#bgp bestpath igp-metric ignore
```

【未設定時】

IGP metricを無視しません。

8.1.14 bgp bestpath med

【機能】

MULTI-EXIT-DISCRIMINATOR 値を考慮する設定

【入力形式】

bgp bestpath med missing-as-worst

no bgp bestpath med missing-as-worst

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
missing-as-worst	MED 属性のない経路を最も適していない経路（MED 値 =4294967295）として扱う場合に指定します。	-	省略不可

【動作モード】

BGP サービス設定モード

【説明】

BGP の最適経路の選択において、MULTI-EXIT-DISCRIMINATOR 値（MED 値）を考慮する場合に設定します。

【BGP の最適経路選択について】

以下の順で最適経路の選択を行います。

優先順位	属性	内容
1	WEIGHT 値	設定された WEIGHT 値の大きい情報が優先されます。
2	LOCAL-PREF 属性	LOCAL-PREF 値の大きい経路が優先されます。

優先順位	属性	内容
3	LOCAL 生成	本装置で生成された BGP 経路について、次のコマンドで生成された順に優先されます。 redistribute connected>redistribute static>network>aggregate-address
4	AS-PATH 属性	AS-PATH 長が短い経路が優先されます。 ただし、bgp bestpath as-path ignore コマンドが設定されている場合は、AS-PATH 長による比較を行いません。
5	ORIGIN 属性	ORIGIN 属性の小さい経路が優先されます。 IGP(0)>EGP(1)>INCOMPLETE(2)の順に優先されます。
6	MED 値	MED 値の小さい経路が優先されます。 bgp always-compare-med コマンドが設定されている場合は、経路種別に関わらず MED 値による比較を行います。設定されていない場合は、比較対象がともに AS-PATH の先頭が同じ値（同一の隣接 AS から受信）、または AS-PATH 長が "0"（Internal 経路）ある場合のみ MED 値による比較を行います。 なお、MED 属性が付加されていない経路については、MED 値を "0" として比較を行います（bgp bestpath med missing-as-worst が設定されていれば、"4294967295" として比較を行います）。
7	ピアタイプ	配布元が eBGP ピアと iBGP ピアである場合、eBGP ピアから学習した経路が優先されます。
8	IGP メトリック値	NEXT-HOP 属性で指定された Next-hop へのメトリック値が小さい経路が優先されます。
9	ルートエイジ	bgp bestpath compare-routerid が設定されていない場合、比較対象が共に eBGP ピアから配布された経路であれば、すでにベストパスとして選択されている経路が優先されます。
10	ROUTER-ID 値	ROUTER-ID 値（ORIGINATOR-ID 属性があれば、ORIGINATOR-ID 値を使用）が小さい経路が優先されます。
11	CLUSTER-LIST 属性	CLUSTER-LIST 属性に含まれる CLUSTER-ID 長の小さい経路が優先されます。 なお、CLUSTER-LIST 属性が付加されていない経路については、CLUSTER-ID 長を "0" として比較を行います。
12	ピアアドレス値	配布元の BGP ピアのアドレス値が小さい経路が優先されます。 なお、ADDRESS-FAMILY が異なる場合は、IPv4>IPv6 の順に優先されます。

* NEXTHOP 属性で指定された Next-Hop への到達性がない場合は、経路が無効となるため比較対象外となります。

【実行例】

MED 値を考慮します (missing-as-worst)。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#bgp bestpath med missing-as-worst
```

【未設定時】

MED 属性のない経路は、MED 値を 0 として扱います。

8.1.15 bgp bundle-time

【機能】

BGP 経路を経路表に登録するまでに待機する時間の設定

【入力形式】

bgp bundle-time <bundle time 値>

no bgp bundle-time [<bundle time 値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
bundle time 値	BGP 経路を経路表に登録するまでに待機する時間（単位：秒）を指定します。	0 ～ 10	省略不可

【動作モード】

BGP サービス設定モード

【説明】

BGP 経路を経路表に登録するまでに待機する時間（単位：秒）を指定します。

【実行例】

BGP 経路を経路表に登録するまでに待機する時間（単位：秒）を指定します（bundle time 値：1 秒）。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#bgp bundle-time 1
```

【未設定時】

bundle time 値は 0 秒で動作します。

8.1.16 no bgp client-to-client reflection

【機能】

他のルータリフレクタクライアントに広告しない設定

【入力形式】

no bgp client-to-client reflection

bgp client-to-client reflection

【動作モード】

BGP サービス設定モード

【説明】

ルータリフレクタとして動作している場合に、ルータリフレクタクライアントから学習した経路情報を、他のルータリフレクタクライアントに広告しない場合に設定します。

【実行例】

他のルータリフレクタクライアントに広告しません。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#no bgp client-to-client reflection
```

【未設定時】

他のルータリフレクタクライアントに広告します。

8.1.17 bgp cluster-id

【機能】

クラスタ ID の設定

【入力形式】

bgp cluster-id <クラスタ ID>

no bgp cluster-id [<クラスタ ID>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
クラスタ ID	BGP クラスタ ID を指定します。	1～4294967295、または、Pv4 アドレス形式	省略不可

【動作モード】

BGP サービス設定モード

【説明】

BGP クラスタが 1 つ以上のルータリフレクタを持つ場合に、クラスタ ID を設定します。

【実行例】

クラスタ ID を設定します（クラスタ ID：1）。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#bgp cluster-id 1
```

【未設定時】

BGP クラスタを使用できません。

8.1.18 bgp dampening

【機能】

ルートフラップダンピングの各種タイマ値の設定

【入力形式】

bgp dampening [<HALFLIFE> [<REUSE> <SUPPRESS> <MAXSUPPRESS>]]

no bgp dampening [<HALFLIFE> <REUSE> <SUPPRESS> <MAXSUPPRESS>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
HALFLIFE	ルートフラップダンピングのペナルティ値が、現在値の 1/2 までに減少する時間（単位：分）を指定します。	1～45	15
REUSE	抑制を解除するルートフラップダンピングのペナルティ下限値を指定します。	1～20000	750
SUPPRESS	抑制を実施するルートフラップダンピングのペナルティ上限値を指定します。	1～20000	2000
MAXSUPPRESS	ルートフラップダンピングによる抑制を行う最大時間（単位：分）を指定します。	1～255	HALFLIFE の 4 倍

【動作モード】

BGP サービス設定モード

【説明】

ルートフラップダンピングの各種タイマ値を設定します。

【実行例】

ルートフラップダンピングの各種タイマ値を設定します（HALFLIFE：20 分、REUSE：800、SUPPRESS：2500、MAXSUPPRESS：80 分）。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)# bgp dampening 20 800 2500 80
```

【未設定時】

ルートフラップダンピング制御を行いません。

8.1.19 no bgp default ipv4-unicast

【機能】

IPv4 経路情報を交換しない設定

【入力形式】

```
no bgp default ipv4-unicast
```

```
bgp default ipv4-unicast
```

【動作モード】

BGP サービス設定モード

【説明】

BGP ピアとの間で、IPv4 経路情報を交換しない場合に設定します。

【実行例】

IPv4 経路情報を交換しません。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#no bgp default ipv4-unicast
```

【未設定時】

IPv4 経路情報を交換します。

8.1.20 bgp default local-preference

【機能】

LOCAL-PREF 属性のデフォルト値の設定

【入力形式】

```
bgp default local-preference <LOCAL-PREFERENCE 値>
```

```
no bgp default local-preference [<LOCAL-PREFERENCE 値>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
LOCAL-PREFERENCE 値	UPDATE メッセージで広告する際に、その LOCAL-PREFERENCE 値を指定します。	0～4294967295	省略不可

【動作モード】

BGP サービス設定モード

【説明】

LOCAL-PREF 属性のデフォルト値を設定します。UPDATE メッセージで通知するすべての経路情報に関して、ここで設定した LOCAL-PREFERENCE 値をつけて通知します。

【LOCAL-PREFERENCE 値とは？】

同一宛先プレフィックスに対する優先度を表します。LOCAL-PREFERENCE 値が大きい経路情報が優先されます。

【実行例】

LOCAL-PREF 属性のデフォルト値を設定します (LOCAL-PREFERENCE 値 : 200)。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#bgp default local-preference 200
```

【未設定時】

LOCAL-PREFERENCE 値は 100 で動作します。

8.1.21 bgp deterministic-med

【機能】

先に同一 AS の経路を比較する設定

【入力形式】

bgp deterministic-med

no bgp deterministic-med

【動作モード】

BGP サービス設定モード

【説明】

最適経路選択において、同一 AS の経路を比較したあとに、異なる AS の経路を比較する場合に設定します。

【実行例】

同一 AS の経路を比較したあとに、異なる AS の経路を比較します。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#bgp deterministic-med
```

【未設定時】

AS に関係なく経路を比較します。

8.1.22 bgp enforce-first-as

【機能】

BGP ピアに設定した AS 番号と同じかどうかをチェックする設定

【入力形式】

bgp enforce-first-as

no bgp enforce-first-as

【動作モード】

BGP サービス設定モード

【説明】

AS-PATH の最初の AS 番号が、BGP ピアに設定した AS 番号と同じかどうかをチェックする場合に設定します。

【実行例】

BGP ピアに設定した AS 番号と同じかどうかをチェックします。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#bgp enforce-first-as
```

【未設定時】

AS-PATH の最初の AS 番号をチェックしません。

8.1.23 no bgp fast-external-failover

【機能】

セッションを切断しない設定

【入力形式】

no bgp fast-external-failover

bgp fast-external-failover

【動作モード】

BGP サービス設定モード

【説明】

BGP セッションを確立しているインタフェースが down しても、セッションを切断しない場合に設定します。

【実行例】

セッションを切断しません。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#no bgp fast-external-failover
```

【未設定時】

セッションを即時に切断します。

8.1.24 bgp listen range

【機能】

動的に BGP 接続を許可するネットワークアドレスの設定

【入力形式】

bgp listen range <ネットワークアドレス> peer-group <peer-group 名>

no bgp listen range <ネットワークアドレス> [peer-group <peer-group 名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ネットワークアドレス	ネットワークアドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
peer-group 名	ピアグループの名称を指定します。	255 文字以内の CDATA 型	

【動作モード】

BGP サービス設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

動的に BGP 接続を許可するネットワークアドレスを設定します。許可した BGP ピアに対して、peer-group 名のポリシーを適用します。

【実行例】

動的に BGP 接続を許可するネットワークアドレスを設定します（ネットワークアドレス：192.0.2.0/24、peer-group 名：peer-group-A）。

```

【BGP サービス設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#bgp listen range 192.0.2.0/24 peer-group peer-group-A

```

【未設定時】

動的に BGP 接続を許可するネットワークアドレスを設定しません。

8.1.25 bgp log-neighbor-changes

【機能】

ログ情報の出力

【入力形式】

bgp log-neighbor-changes

no bgp log-neighbor-changes

【動作モード】

BGP サービス設定モード

【説明】

以下の場合に、ログ情報を出力します。

- BGP ピアとの間でセッションが確立された場合

- BGP ピアとの間でセッションが切断された場合
- BGP NOTIFICATION メッセージを送信した場合
- BGP NOTIFICATION メッセージを受信した場合

【実行例】

ログ情報を出力します。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#bgp log-neighbor-changes
```

【未設定時】

ログ情報を出力しません。

8.1.26 bgp log-update-error

【機能】

ログ情報の出力

【入力形式】

bgp log-update-error

no bgp log-update-error

【動作モード】

BGP サービス設定モード

【説明】

以下の場合に、ログ情報を出力します。

- 受信した UPDATE メッセージ内で Treat-as-withdraw を行う不正を発見した場合
- 受信した UPDATE メッセージ内で Attribute discard を行う不正を発見した場合

【実行例】

ログ情報を出力します。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#bgp log-update-error
```

【未設定時】

ログ情報を出力しません。

8.1.27 bgp multi-path

【機能】

BGP のマルチパス機能の設定

【入力形式】

```
bgp multi-path [relax]
```

```
no bgp multi-path [relax]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
relax	条件の 2. を無効とする場合に指定します。	-	条件 1.、条件 2. とも有効

【動作モード】

BGP サービス設定モード

【説明】

BGP のマルチパス機能を有効にします (IPv4/IPv4 VRF/IPv6/IPv6 VRF 経路をサポートしています)。

BGP のマルチパスとして登録される経路は、以下の 2 つの条件を満たした経路です。

1. ベストパス選択の優先度において、"BGP ネクストホップまでの IGP メトリック値が小さい経路"までの比較が同一であること
2. 最終的に選択されたベストパスとピアの AS が同一であること

"relax" を指定した場合には、条件 2. は無効となります。



参照 ベストパス選択の優先度については、[\[8.1.14 bgp bestpath med\]](#) (P.274) の『BGP の最適経路選択について』の一覧表を参照してください。

【実行例】

BGP のマルチパス機能を有効にします。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#bgp multi-path
```

【未設定時】

BGP のマルチパス機能が有効となりません。

8.1.28 bgp network import-check

【機能】

IGP を通過できる経路かどうかのチェック

【入力形式】

```
bgp network import-check
```

```
no bgp network import-check
```


【動作モード】

BGP サービス設定モード

【説明】

IGP を通過できる経路かどうかをチェックします。

【実行例】

IGP を通過できる経路かどうかをチェックします。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#bgp network import-check
```

【未設定時】

GP を通過できる経路かどうかをチェックしません。

8.1.29 bgp nexthop-validation-timer

【機能】

経路選択処理を始めるまでの時間の設定

【入力形式】

bgp nexthop-validation-timer <wait-time 値>

no bgp nexthop-validation-timer [<wait-time 値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
wait-time 値	nexthop への到達性の変化を検知してから、経路選択処理を始めるまでの時間（単位：秒）を指定します。	1～3600	省略不可

【動作モード】

BGP サービス設定モード

【説明】

nexthop への到達性の変化を検知してから、経路選択処理を始めるまでの時間（単位：秒）を設定します。経路フラップにより nexthop への到達性が一時的に変化した際に、wait timer が動作することで経路選択処理の実行を抑制し、装置に負荷がかかるのを防ぐことができます。設定投入時点ですでに wait timer が動いていた場合、動いている wait timer は破棄して、新しい timer 値で再度 wait timer を動作させます。

【実行例】

経路選択処理を始めるまでの時間（単位：秒）を設定します（wait-time 値：10 秒）。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#bgp nexthop-validation-timer 10
```

【未設定時】

wait-time 値は 0 秒で動作します。

8.1.30 bgp router-id

【機能】

BGP のルータ ID の設定

【入力形式】

bgp router-id <ルータ ID>

no bgp router-id [<ルータ ID>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ルータ ID	BGP のルータ ID を指定します。	IPv4 アドレス形式	省略不可

【動作モード】

BGP サービス設定モード

【説明】

BGP のルータ ID を設定します。

【ルータ ID とは？】

BGP で使用する装置の ID です。通常は、本装置のインタフェースの中から任意の IPv4 アドレスを割り当てます。ルータ ID が指定されていない場合は、ルータの全インタフェースアドレスのうち、最大のものを BGP ルータ ID とします。

【実行例】

BGP のルータ ID を設定します（ルータ ID：192.0.2.1）。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#bgp router-id 192.0.2.1
```

【未設定時】

全インタフェースアドレスのうち、最大のものを BGP ルータ ID とします。

8.1.31 distance

【機能】

経路のディスタンス値の設定

【入力形式】

distance <ディスタンス値> <ネットワークアドレス> <ネットマスク> [<アクセスリスト番号>]

no distance <ディスタンス値> <ネットワークアドレス> <ネットマスク> [<アクセスリスト番号>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ディスタンス値	設定している経路のディスタンス値を指定します。	1～255	省略不可
ネットワークアドレス	ディスタンス値を設定する送信元ネットワークアドレスを指定します。	IPv4 アドレス形式	
ネットマスク	ディスタンス値を設定する送信元ネットマスクを指定します。	IPv4 アドレス形式	
アクセスリスト番号	ディスタンス値を設定する経路をアクセスリスト番号で指定します。	-	全経路が対象

【動作モード】

BGP サービス設定モード

【説明】

特定の BGP ピアから広告された経路のディスタンス値を設定します。ディスタンス値は、値が小さいほど優先度が高くなります。指定したアクセスリスト番号に合致する経路のみディスタンス値を設定します。

【実行例】

経路のディスタンス値を設定します（ディスタンス値：1、ネットワークアドレス：192.0.2.0、ネットマスク：255.255.255.0、アクセスリスト番号：1）。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#distance 1 192.0.2.0 255.255.255.0 1
```

【未設定時】

distance bgp コマンドの設定に従います。

8.1.32 distance bgp

【機能】

経路のディスタンス値の設定

【入力形式】

distance bgp <EBGP ディスタンス値> <IBGP ディスタンス値> <local ディスタンス値>

no distance bgp [<EBGP ディスタンス値> <IBGP ディスタンス値> <local ディスタンス値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
EBGP ディスタンス値	EBGP のディスタンス値を指定します。	1 ～ 255	省略不可
IBGP ディスタンス値	IBGP のディスタンス値を指定します。	1 ～ 255	
local ディスタンス値	local のディスタンス値を指定します。	1 ～ 255	

【動作モード】

BGP サービス設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

External BGP(EBGP)経路、Internal BGP(IBGP)経路、ローカル経路のディスタンス値を設定します。ディスタンス値は小さいほど優先度が高くなります。

【実行例】

ローカル経路のディスタンス値を設定します (EBGP ディスタンス値 : 30、IBGP ディスタンス値 : 210、local ディスタンス値 250)。

```

【BGP サービス設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#distance bgp 30 210 250

```

【未設定時】

以下の値で動作します。

EBGP ディスタンス値 : 20

IBGP ディスタンス値 : 200

local ディスタンス値 : 200

8.1.33 neighbor advertisement-interval

【機能】

タイマ満了時間の設定

【入力形式】

neighbor <BGP ピア> advertisement-interval <interval>

no neighbor <BGP ピア> advertisement-interval [<interval>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名(*1):255 文字以内の CDATA 型	省略不可
interval	UPDATE メッセージ送信タイマの満了時間（単位：秒）を指定します。	0 ～ 600	

*1) address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モードでは指定できません。

【動作モード】

BGP サービス設定モード、address-family ipv4VRF 設定モード、address-family ipv6VRF 設定モード

【説明】

UPDATE メッセージ送信タイマの満了時間（単位：秒）を設定します。

UPDATE の事象が発生した場合は、本コマンドで設定されたタイマ満了時間以内に UPDATE メッセージを送信します（タイマは設定時間で定期的に満了します）。

"0" を設定した場合は、UPDATE の事象が発生しだい、即時に送信を行います。

経路が無効になったことを広告する場合 (withdraw) は、即時に UPDATE メッセージを送信します。

UPDATE の事象が発生してから本コマンドで指定した時間経過後に UPDATE メッセージを送信するものではありません。

なお、1 以上の値を設定した場合、タイマ満了時に送信される経路数の上限は 2000 です。

【実行例】

タイマ満了時間を設定します（BGP ピア：192.0.2.1、interval：100）。

```

【BGP サービス設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor 192.0.2.1 advertisement-interval 100

```

【未設定時】

以下の値で動作します。

IBGP： 0 秒

EBGP： 30 秒（INET の場合）

0 秒（VRF の場合）

8.1.34 neighbor advertisement-limit

【機能】

メッセージ送信用キューサイズの設定

【入力形式】

neighbor <BGP ピア> advertisement-limit <limit-value>

no neighbor <BGP ピア> advertisement-limit [<limit-value>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名 (*1):255 文字以内の CDATA 型	省略不可
limit-value	BGP ピアに対する update/withdraw メッセージ送信キューのサイズを指定します。	10 ～ 20000	

*1) address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モードでは指定できません。

【動作モード】

BGP サービス設定モード、address-family ipv4VRF 設定モード、address-family ipv6VRF 設定モード

【説明】

BGP ピアに対する NLRI update/withdraw メッセージ送信用キューのサイズを設定します。

指定した数の NLRI update/withdraw メッセージを、送信キューで保持することが可能となります。

キューのサイズを大きくすることで BGP ピアに対する経路送信は速くなりますが、大きくしすぎると経路送信以外の処（keepalive など）が滞る可能性があります。

【実行例】

NLRI update/withdraw メッセージ送信用キューのサイズを設定します（BGP ピア：192.0.2.1、limit-value：20000）。

```

【BGP サービス設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor 192.0.2.1 advertisement-limit 20000

```

【未設定時】

送信用キューのサイズは 10000 で動作します。

8.1.35 neighbor capability route-refresh

【機能】

route-refresh ケイパビリティを送信するかどうかの設定

【入力形式】

neighbor <BGP ピア> capability route-refresh {enable | disable}

no neighbor <BGP ピア> capability route-refresh [enable | disable]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可
enable disable	route-refresh ケイパビリティの送信有無を指定します。	enable：送信する disable：送信しない	

【動作モード】

BGP サービス設定モード

【説明】

OPEN メッセージのオプションパラメタとして、route-refresh ケイパビリティを送信するかどうかを設定します。

【実行例】

route-refresh ケイパビリティを送信するかどうかを設定します（BGP ピア：192.0.2.1、disable）。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor 192.0.2.1 capability route-refresh disable
```

【未設定時】

enable で動作します。

8.1.36 neighbor description

【機能】

BGP ピアに対する名前や説明の文字列の設定

【入力形式】

neighbor <BGP ピア> description <名称>

no neighbor <BGP ピア> description

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可
名称	BGP ピアの名称を設定します。	254 文字以内の WORD 型 (*1)	

*1) 1 文字の空白（スペース）は使用可能です。複数の空白（スペース）は 1 文字にまとめられます。

【動作モード】

BGP サービス設定モード、address-family ipv4VRF 設定モード、address-family ipv6VRF 設定モード

【説明】

BGP ピアに名前や説明のための文字列を設定します。

【実行例】

BGP ピアに文字列を設定します (BGP ピア : 192.0.2.1、名称 : description-A)。

```
【BGP サービス設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor 192.0.2.1 description description-A
```

【未設定時】

名称や説明を設定しません。

8.1.37 neighbor dont-capability-negotiate

【機能】

ケイパビリティ交渉を行わない設定

【入力形式】

neighbor <BGP ピア> dont-capability-negotiate

no neighbor <BGP ピア> dont-capability-negotiate

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名 : 255 文字以内の CDATA 型	省略不可

【動作モード】

BGP サービス設定モード、address-family ipv4VRF 設定モード、address-family ipv6VRF 設定モード

【説明】

OPEN メッセージのオプションによる、ケイパビリティ交渉を行わない場合に設定します。

【実行例】

ケイパビリティ交渉を行いません (BGP ピア : 192.0.2.1)。

```
【BGP サービス設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor 192.0.2.1 dont-capability-negotiate
```


【未設定時】

ケイパビリティ交渉を行います。

8.1.38 neighbor ebgp-multihop

【機能】

EBGP ピアと最大ホップ数の設定

【入力形式】

neighbor <BGP ピア> ebgp-multihop <最大ホップ数>

no neighbor <BGP ピア> ebgp-multihop [<最大ホップ数>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名 (*1) : 255 文字以内の CDATA 型	省略不可
最大ホップ数	BGP ピアとしてセッションを確立するための最大ホップ数を指定します。	2～255	

*1) address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モードでは指定できません。

【動作モード】

BGP サービス設定モード、address-family ipv4VRF 設定モード、address-family ipv6VRF 設定モード

【説明】

直接接続されていないネットワーク上の EBGP ピアと最大ホップ数を設定します。

【実行例】

EBGP ピアと最大ホップ数を設定します (BGP ピア : 192.0.2.1、最大ホップ数 : 255)。

```

【BGP サービス設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor 192.0.2.1 ebgp-multihop 255

```

【未設定時】

直接接続されているピアのみ許可します。

8.1.39 neighbor enforce-multihop

【機能】

EBGP ピアとのセッションの確立

【入力形式】

```
neighbor <BGP ピア> enforce-multihop
```

```
no neighbor <BGP ピア> enforce-multihop
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可

【動作モード】

BGP サービス設定モード

【説明】

直接接続されていないネットワーク上の EBGP ピアとのセッションを確立する場合に設定します。

【実行例】

EBGP ピアとのセッションを確立します（BGP ピア：192.0.2.1）。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor 192.0.2.1 enforce-multihop
```

【未設定時】

直接接続されているピアのみ許可します。

8.1.40 neighbor interface

【機能】

BGP ピアのインタフェースの設定

【入力形式】

```
neighbor <BGP ピア> interface <インタフェース名> <インタフェース番号>
```

```
no neighbor <BGP ピア> interface <インタフェース名> <インタフェース番号>
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
インタフェース名	インタフェース名を指定します。	-	
インタフェース番号	インタフェース番号を指定します。	-	

【動作モード】

BGP サービス設定モード

【説明】

BGP ピアのインタフェースを設定します。

【実行例】

BGP ピアのインタフェースを設定します (BGP ピア : 192.0.2.1、インタフェース名 : port-channel、インタフェース番号 : 1)。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor 192.168.0.1 interface port-channel 1
```

【未設定時】

BGP ピアのインタフェースを特定しません。

8.1.41 neighbor override-capability

【機能】

自身のケイパビリティで上書きする設定

【入力形式】

neighbor <BGP ピア> override-capability

no neighbor <BGP ピア> override-capability

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名 : 255 文字以内の CDATA 型	省略不可

【動作モード】

BGP サービス設定モード

【説明】

OPEN メッセージのオプションによるケイパビリティ交渉の結果を、自身のケイパビリティで上書きする場合に設定します。neighbor strict-capability-match コマンドと同時に設定できません。

【実行例】

自身のケイパビリティで上書きします (BGP ピア : 192.0.2.1)。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor 192.0.2.1 override-capability
```

【未設定時】

自身のケイパビリティで上書きしません。

8.1.42 neighbor passive

【機能】

BGP セッション接続要求の設定

【入力形式】

neighbor <BGP ピア> passive

no neighbor <BGP ピア> passive

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可

【動作モード】

BGP サービス設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP セッション接続要求を待ちます。本装置から BGP セッション接続要求を送信しません。

【実行例】

BGP セッション接続要求を待ちます（BGP ピア：192.0.2.1）。

```

【BGP サービス設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor 192.0.2.1 passive

```

【未設定時】

BGP セッション接続要求を送信します。

8.1.43 neighbor password

【機能】

TCP MD5 認証オプションの設定

【入力形式】

neighbor <BGP ピア> password <パスワード>

no neighbor <BGP ピア> password

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 (*1) IPv6 アドレス形式 (*2)	省略不可
パスワード	TCP MD5 認証オプションで使用するパスワードを指定します。	25 文字以内の STRING 型	

*1) address-family ipv6 VRF 設定モードでは指定できません。

*2) address-family ipv4 VRF 設定モードでは指定できません。

【動作モード】

BGP サービス設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

TCP MD5 認証オプション (RFC2385:Protection of BGP Sessions via the TCP MD5 Signature Option) を有効にします。また、パスワード文字列として使用する文字列を設定します。

【実行例】

TCP MD5 認証オプションを有効にします (BGP ピア : 192.0.2.1、パスワード : authkey)。

```
【BGP サービス設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor 192.0.2.1 password authkey
```

【未設定時】

TCP MD5 認証オプションは有効となりません。

8.1.44 neighbor peer-group

【機能】

ピアグループの設定

【入力形式】

neighbor <BGP ピア> peer-group <peer-group 名>

no neighbor <BGP ピア> peer-group [<peer-group 名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
peer-group 名	ピアグループの名称を指定します。	255 文字以内の CDATA 型	

【動作モード】

BGP サービス設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

同じ BGP ポリシーを持つ複数の BGP ピアを、ピアグループとして設定します。同じ BGP ポリシーを持つグループに対して、設定を行うことができます。

【実行例】

ピアグループとして設定します（BGP ピア：192.0.2.1/192.0.2.2、peer-group 名：peer-group-A）。

```
【BGP サービス設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor 192.0.2.1 peer-group peer-group-A
(config-bgp)#neighbor 192.0.2.2 peer-group peer-group-A
```

【未設定時】

ピアグループを設定しません。

8.1.45 neighbor peer-group

【機能】

ピアグループ名称の設定

【入力形式】

neighbor <peer-group 名> peer-group

no neighbor <peer-group 名> peer-group

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
peer-group 名	ピアグループの名称を指定します。	255 文字以内の CDATA 型	省略不可

【動作モード】

BGP サービス設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

ピアグループの名称を設定します。

【実行例】

ピアグループの名称を設定します（peer-group 名：peer-group-A）。

```
【BGP サービス設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor peer-group-A peer-group
```

【未設定時】

ピアグループの名称を設定しません。

8.1.46 neighbor port

【機能】

TCP ポート番号の設定

【入力形式】

neighbor <BGP ピア> port <ポート番号>

no neighbor <BGP ピア> port [<ポート番号>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
ポート番号	BGP ピアとの通信に使用する、 TCP ポート番号を指定します。	1～65535	

【動作モード】

BGP サービス設定モード

【説明】

TCP ポート番号を設定します。

【実行例】

TCP ポート番号を設定します（BGP ピア：192.0.2.1、TCP ポート番号：1025）。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor 192.0.2.1 port 1025
```

【未設定時】

TCP ポート番号は 179 で動作します。

8.1.47 neighbor remote-as

【機能】

BGP ピアの AS 番号の設定

【入力形式】

neighbor <BGP ピア> remote-as <AS 番号>

no neighbor <BGP ピア> remote-as <AS 番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：254 文字以内の WORD 型	省略不可
AS 番号	BGP ピアの AS 番号を指定します。	1～4294967295	

【動作モード】

BGP サービス設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP ピアの AS 番号を設定します。

【実行例】

BGP ピアの AS 番号を設定します（BGP ピア：192.0.2.1、AS 番号：64497）。

```

【BGP サービス設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor 192.0.2.1 remote-as 64497

```

【未設定時】

BGP セッションを確立できません。

8.1.48 neighbor retain-stale time

【機能】

BGP ピアから受信した経路情報を保持しておく時間の設定

【入力形式】

neighbor <BGP ピア> retain-stale time <経路情報保持時間>

no neighbor <BGP ピア> retain-stale time [<経路情報保持時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可
経路情報保持時間	BGP ピアが無効になったあと、BGP ピアから受信した経路情報を保持しておく時間（単位：秒）を指定します。	1～65535	

【動作モード】

BGP サービス設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP ピアが無効になったあと、BGP ピアから受信した経路情報を保持しておく時間（単位：秒）を設定します。

【実行例】

BGP ピアから受信した経路情報を保持しておく時間を設定します（BGP ピア：192.0.2.1、経路情報保持時間：100 秒）。

```
【BGP サービス設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor 192.0.2.1 retain-stale time 100
```

【未設定時】

経路情報保持時間は 300 秒で動作します。

8.1.49 neighbor shutdown

【機能】

BGP ピアを一時的に無効にする設定

【入力形式】

neighbor <BGP ピア> shutdown

no neighbor <BGP ピア> shutdown

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可

【動作モード】

BGP サービス設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP ピアを一時的に無効にします。

【実行例】

BGP ピアを一時的に無効にします（BGP ピア：192.0.2.1）。

```
【BGP サービス設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor 192.0.2.1 shutdown
```

【未設定時】

BGP ピアは有効となります。

8.1.50 neighbor start-interval

【機能】

再接続を行うまでの時間の設定

【入力形式】

neighbor <BGP ピア> start-interval <再接続待ち時間>

no neighbor <BGP ピア> start-interval [<再接続待ち時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可
再接続待ち時間	BGP セッションが切れたあと、再接続を行うまでの時間（単位：秒）を指定します。	1～65535	

【動作モード】

BGP サービス設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP セッションが切れたあとに、再接続を行うまでの時間（単位：秒）を設定します。

【実行例】

再接続を行うまでの時間を設定します（BGP ピア：192.0.2.1、再接続待ち時間：100 秒）。

```

【BGP サービス設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor 192.0.2.1 start-interval 100

```

【未設定時】

再接続待ち時間は 5 秒で動作します。

8.1.51 neighbor strict-capability-match

【機能】

BGP セッションを確立しない設定

【入力形式】

neighbor <BGP ピア> strict-capability-match

no neighbor <BGP ピア> strict-capability-match

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

【動作モード】

BGP サービス設定モード

【説明】

OPEN メッセージのオプションによるネイパビリティ交渉の際に、ピアから未サポートのオプションを受信した場合や、自身の指定するオプションをピアが受け入れなかった場合に、BGP セッションを確立しない場合に設定します。neighbor override-capability コマンドと同時に設定できません。

【実行例】

BGP セッションを確立しません (BGP ピア : 192.0.2.1)。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor 192.0.2.1 strict-capability-match
```

【未設定時】

BGP セッションを確立します。

8.1.52 neighbor timers

【機能】

BGP ピア、または、ピアグループで使用する各種タイマの設定

【入力形式】

neighbor <BGP ピア> timers {<Keepalive-interval> <Holdtime> | connect <Connect-timer>}

no neighbor <BGP ピア> timers [<Keepalive-interval> <Holdtime> | connect <Connect-timer>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名 : 255 文字以内の CDATA 型	省略不可
Keepalive-interval	Keepalive パケットの送信間隔 (単位 : 秒) を指定します。	0 ~ 65535	
Holdtime	指定した時間 (単位 : 秒) KeepAlive パケットを受信しなかった場合は、BGP セッションを切断します。	0,3 ~ 65535	
Connect-timer	TCP コネクションの再送間隔 (単位 : 秒) を指定します。	5 ~ 65535 省略不可	

【動作モード】

BGP サービス設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP ピア、または、ピアグループで使用する各種タイマを設定します。Holdtime で "1" または "2" を指定した場合は設定が無効となり、デフォルトの値で動作します。

【実行例】

BGP ピア、または、ピアグループで使用する各種タイマを設定します (BGP ピア : 192.0.2.1、Keepalive-interval : 30 秒、Holdtime : 90 秒)。

```

【BGP サービス設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor 192.0.2.1 timers 30 90

```

【未設定時】

以下の内容で動作します。

```

Keepalive-interval: 60 秒
Holdtime:           180 秒
Connect-timer:      120 秒

```

8.1.53 neighbor update-source

【機能】

BGP セッション確立の際の送信元アドレスの設定

【入力形式】

```
neighbor <BGP ピア> update-source {<インタフェース名> <インタフェース番号> | <送信元アドレス>}
```

```
no neighbor <BGP ピア> update-source [<インタフェース名> [<インタフェース番号>] | <送信元アドレス>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名 : 255 文字以内の CDATA 型	省略不可
インタフェース名	インタフェース名を指定します。	-	
インタフェース番号	インタフェース番号を指定します。	-	
送信元アドレス	送信元アドレスを指定します。	IPv4 アドレス形式 (*1) IPv6 アドレス形式 (*2)	

*1) BGP ピアが IPv4、または peer-group 名の場合に指定できます。

*2) BGP ピアが IPv6、または peer-group 名の場合に指定できます。

【動作モード】

BGP サービス設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP セッション確立の際、送信元アドレスを指定する場合に設定します。インタフェースを指定した場合には、そのインタフェースのアドレスを送信元アドレスとします。送信元アドレスにリンクローカルアドレスは指定できません。

【実行例】

任意のインタフェースアドレスを使用します (BGP ピア : 192.0.2.1、インタフェース名 : port-channel、インタフェース番号 : 1)。

```

【BGP サービス設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor 192.0.2.1 update-source port-channel 1

```

【未設定時】

実際に送信するインタフェースのアドレスを使用します。

8.1.54 neighbor version

【機能】

ピアとの間で使用する BGP のプロトコルバージョンの設定

【入力形式】

```
neighbor <BGP ピア> version {4 | draft}
```

```
no neighbor <BGP ピア> version [4 | draft]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
4 draft	BGP のプロトコルバージョンを指定します。	4 : BGP4 draft : マルチプロトコル拡張ドラフト	

【動作モード】

BGP サービス設定モード

【説明】

ピアとの間で使用する BGP のプロトコルバージョンを設定します。

【実行例】

ピアとの間で使用する BGP のプロトコルバージョンを設定します (BGP ピア : 192.0.2.1、4)。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor 192.0.2.1 version 4
```

【未設定時】

プロトコルバージョンは 4 で動作します。

8.1.55 neighbor weight

【機能】

BGP ピアからの経路情報の優先度の設定

【入力形式】

neighbor <BGP ピア> weight <weight 値>

no neighbor <BGP ピア> weight [<weight 値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名 : 255 文字以内の CDATA 型	省略不可
weight 値	BGP ピアからの経路情報の優先度を指定します。	0 ~ 65535	

【動作モード】

BGP サービス設定モード

【説明】

BGP ピアからの経路情報の優先度を設定します。

【実行例】

BGP ピアからの経路情報の優先度を設定します (BGP ピア : 192.0.2.1、weight 値 : 1)。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor 192.0.2.1 weight 1
```

【未設定時】

以下の値で動作します。

BGP ピア : 0

ローカルルータ : 32768

8.1.56 timers bgp

【機能】

KeepAlive のタイマ値の設定

【入力形式】

timers bgp <Keepalive interval> <Holdtime>

no timers bgp [<Keepalive interval> <Holdtime>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
Keepalive interval	KeepAlive パケットの送信間隔 (単位 : 秒) を指定します。	0 ~ 65535	省略不可
Holdtime	指定した時間 (単位 : 秒) KeepAlive パケットを受信しなかった場合は、BGP セッションを解放します。	0,3 ~ 65535	

【動作モード】

BGP サービス設定モード

【説明】

KeepAlive のタイマ値を設定します。BGP ピアごとに設定する場合は、neighbor timers コマンドを実行します。

Holdtime で "1" または "2" を指定した場合は、設定が無効となり、デフォルトの値で動作します。

VRF に対しては無効なコマンドとなります。VRF 側のピアに対してタイマの設定を行う場合には、address-family ipv4 VRF 設定モード、および address-family ipv6 VRF 設定モード配下で neighbor timers コマンドを設定する必要があります。

【実行例】

KeepAlive のタイマ値を設定します (KeepAlive interval:100 秒、Holdtime : 300 秒)。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#timers bgp 100 300
```

【未設定時】

以下の値で動作します。

Keepalive interval: 60 秒

Holdtime: 180 秒

8.2 IPv4 経路交換の設定

8.2.1 address-family ipv4 unicast

【機能】

address-family ipv4 設定モードへの移行

【入力形式】

address-family ipv4 unicast

no address-family [ipv4 unicast]

【動作モード】

BGP サービス設定モード

【説明】

address-family ipv4 設定モードに移行します。コマンドの先頭に "no" を指定することで、address-family ipv4 設定モードの内容がすべて消去されます。

【実行例】

address-family ipv4 設定モードに移行します。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#
```

8.2.2 aggregate-address

【機能】

経路情報の集約

【入力形式】

aggregate-address {<ネットワークアドレス> <ネットマスク> | <ネットワークアドレス> <プレフィックス長>} [as-set] [summary-only]

no aggregate-address {<ネットワークアドレス> <ネットマスク> | <ネットワークアドレス> <プレフィックス長>} [as-set] [summary-only]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ネットワークアドレス	集約後のネットワークアドレスを指定します。	IPv4 アドレス形式 (*1) IPv6 アドレス形式 (*2)	省略不可
ネットマスク	集約後のネットマスクを指定します。	IPv4 アドレス形式 (*1)	
プレフィックス長	集約後のプレフィックス長を指定します。	0 ~ 128 (*2)	

パラメタ	設定内容	設定範囲	省略時
as-set	AS set path information を生成する場合に指定します。	-	集約前の経路情報の AS-PATH 情報を含めない
summary-only	集約後の経路情報のみを広告する場合に指定します。	-	集約前の経路情報もすべて広告

*1) address-family ipv6 設定モード、address-family ipv6 VRF 設定モードでは指定できません。

*2) address-family ipv4 設定モード、address-family ipv4 VRF 設定モードでは指定できません。

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

経路情報を集約し、その情報を BGP で広告します。通知する際には、PATH 属性に ATOMIC-AGGREGATE 属性、AGGREGATOR 属性を付与して広告します。"summary-only" を指定した場合は、集約後の経路情報のみを広告し、集約された他の情報は広告しません。

【実行例】

経路情報を集約します（ネットワークアドレス：192.0.2.0、ネットマスク：255.255.255.0）。

```

【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#aggregate-address 192.0.2.0 255.255.255.0

```

【未設定時】

経路情報を集約しません。

8.2.3 default-information originate

【機能】

スタティック登録したデフォルトルートの情報を広告する設定

【入力形式】

default-information originate

no default-information originate

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

スタティック登録したデフォルトルートの情報を広告する場合に設定します。

【実行例】

スタティック登録したデフォルトルート情報を広告します。

```
【BGP サービス設定の場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#default-information originate
```

【未設定時】

デフォルトルートを広告しません。

8.2.4 neighbor activate

【機能】

経路を交換する設定

【入力形式】

neighbor <BGP ピア> activate

no neighbor <BGP ピア> activate

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

経路の交換を行う場合に設定します。

【実行例】

経路の交換を行います (BGP ピア：192.0.2.1)。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 activate
```

【未設定時】

経路の交換を行いません。IPv4 経路は、本コマンドを設定しなくとも、デフォルトで交換を行います。

8.2.5 neighbor allowas-in

【機能】

自身の AS 番号が含まれる経路の受信の許可

【入力形式】

neighbor <BGP ピア> allowas-in [<許可数>]

no neighbor <BGP ピア> allowas-in [<許可数>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可
許可数	経路情報内の自身の AS 番号の重複許可数を指定します。	1～10	3

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

自身の AS 番号が含まれる経路の受信を許可します。

【実行例】

自身の AS 番号が含まれる経路の受信を許可します（BGP ピア：192.0.2.1、許可数：3）。

```

【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 allowas-in 3

```

【未設定時】

自身の AS 番号が含まれる経路の受信を許可しません。

8.2.6 neighbor attribute-unchanged

【機能】

UPDATE メッセージを BGP ピアに送信する際に変換しない Attribute 情報の設定

【入力形式】

neighbor <BGP ピア> attribute-unchanged [as-path] [med] [next-hop]

no neighbor <BGP ピア> attribute-unchanged [as-path] [med] [next-hop]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名 : 255 文字以内の CDATA 型	省略不可
as-path	AS-PATH 属性を変換しない場合に指定します。	-	AS-PATH 属性を変換する
med	MED 属性を変換しない場合に指定します。	-	MED 属性を変換する
next-hop	NEXT-HOP 属性を変換しない場合に指定します。	-	NEXT-HOP 属性を変換する
属性の指定なし	「AS-PATH 属性」、「MED 属性」、「NEXT-HOP 属性」すべてを変換しません。	-	-

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

UPDATE メッセージを BGP ピアに送信する際に、変換しない Attribute 情報を設定します。

【実行例】

変換しない Attribute 情報を設定します (BGP ピア : 192.0.2.1、as-path、med、next-hop)。

```

【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 attribute-unchanged as-path med next-hop

```

【未設定時】

UPDATE メッセージを送信する際に、Attribute 情報を変換します。

8.2.7 neighbor capability graceful-restart

【機能】

Graceful-restart ケイパビリティの送信

【入力形式】

neighbor <BGP ピア> capability graceful-restart

no neighbor <BGP ピア> capability graceful-restart

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

OPEN メッセージのオプションパラメタとして、Graceful-restart ケイパビリティを送信します。

【実行例】

Graceful-restart ケイパビリティを送信します (BGP ピア：192.0.2.1)。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 capability graceful-restart
```

【未設定時】

Graceful-restart ケイパビリティを送信しません。

8.2.8 neighbor default-originate

【機能】

デフォルトルートを BGP ピアに広告する設定

【入力形式】

neighbor <BGP ピア> default-originate [route-map <route-map 名>]

no neighbor <BGP ピア> default-originate [route-map <route-map 名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可
route-map 名	適用する route-map 名を指定します。	254 文字以内の WORD 型	route-map を適用しない

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP スピーカ（ローカルルータ）をデフォルトルートとして使うために、デフォルトルートを BGP ピアに広告する場合に設定します。

【実行例】

デフォルトルートを BGP ピアに広告します（IPv4 アドレス：192.0.2.1）。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 default-originate
```

【未設定時】

デフォルトルートを広告しません。

8.2.9 neighbor disable-nexthop-validation

【機能】

経路を有効と判定する設定

【入力形式】

neighbor <BGP ピア> disable-nexthop-validation

no neighbor <BGP ピア> disable-nexthop-validation

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP ピアから学習した経路の Nexthop 到達性チェックを行わず、経路を有効と判定する場合に設定します。

本設定が変更された場合、すでに確立されている BGP セッションは再確立が行われます。

【実行例】

Nexthop 到達性チェックを行いません（BGP ピア：192.0.2.1）。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 disable-nexthop-validation
```

【未設定時】

Nexthop 到達性チェックを行います。

8.2.10 neighbor distribute-list

【機能】

フィルタリングの設定

【入力形式】

neighbor <BGP ピア> distribute-list <アクセスリスト番号> {in | out}

no neighbor <BGP ピア> distribute-list <アクセスリスト番号> {in | out}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可
アクセスリスト番号	BGP ピアに対して、送信する／送信しない経路情報を指定するために、アクセスリスト番号を指定します。	-	
in out	受信時に適用するか／送信時に適用するかを指定します。	in: 受信時 out: 送信時	

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP の送受信に対して、フィルタリングの設定を行います。アクセスリストで指定した宛先経路情報のみを受信する／しない、または、送信する／しないといった制御を行うことができます。

【実行例】

フィルタリングの設定を行いません (BGP ピア：192.0.2.1、アクセスリスト番号：1、in)。

```

【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 distribute-list 1 in

```

【未設定時】

フィルタリングを行いません。

8.2.11 neighbor filter-list

【機能】

UPDATE メッセージで送受信する際のフィルタリングの設定

【入力形式】

neighbor <BGP ピア> filter-list <アクセスリスト名> {in | out}

no neighbor <BGP ピア> filter-list [<アクセスリスト名> [in | out]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可
アクセスリスト名	アクセスリスト名を指定します。	254 文字以内の WORD 型	
in out	受信時に適用するか／送信時に適用するかを指定します。	in: 受信時 out: 送信時	

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

UPDATE メッセージで送受信する際のフィルタリングを設定します。

【実行例】

UPDATE メッセージで送受信する際のフィルタリングを設定します (BGP ピア：192.0.2.1、アクセスリスト名：accesslist-name-A、out)。

```

【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 filter-list accesslist-name-A out

```

【未設定時】

フィルタリングを設定しません。

8.2.12 neighbor maximum-prefix

【機能】

BGP ピアから受け付けるプレフィックス数の最大値、および警告を発行する割合の設定

【入力形式】

neighbor <BGP ピア> maximum-prefix <プレフィックス数> {<割合> | warning-only}

no neighbor <BGP ピア> maximum-prefix [<プレフィックス数> [warning-only]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可
プレフィックス数	BGP ピアから受信するプレフィックス数の最大数を指定します。	1～4294967295	
割合 warning-only	警告を発行する割合（単位：%）を指定します。	1～100 warning-only: 警告のみを行う場合	

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP ピアから受け付けるプレフィックス数の最大値、および警告を発行する割合を設定します。警告値、および最大値となった場合にはログ情報を出力します。

【実行例】

BGP ピアから受け付けるプレフィックス数の最大値、および警告を発行する割合を設定します（BGP ピア：192.0.2.1、プレフィックス数：1000、割合：90%）。

```

【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 maximum-prefix 1000 90

```

【未設定時】

受け付けるプレフィックス数を制限しません。

8.2.13 neighbor next-hop-self

【機能】

Next-hop を、このピア自身とする設定

【入力形式】

neighbor <BGP ピア> next-hop-self

no neighbor <BGP ピア> next-hop-self

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP ピアから受信した経路に対する Next-hop を、このピア自身とする場合に設定します。

【実行例】

Next-hop をこのピア自身とします（BGP ピア：192.0.2.1）。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 next-hop-self
```

【未設定時】

Next-hop をこのピア自身としません。

8.2.14 neighbor prefix-list

【機能】

BGP で送受信するプレフィックスをリストに従いフィルタリングする設定

【入力形式】

neighbor <BGP ピア> prefix-list <プレフィックスリスト名> {in | out}

no neighbor <BGP ピア> prefix-list [<プレフィックスリスト名> [in | out]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名 : 255 文字以内の CDATA 型	省略不可
プレフィックスリスト名	参照するプレフィックスリスト名を指定します。	254 文字以内の WORD 型	
in out	受信時に適用するか／送信時に適用するかを指定します。	in: 受信時 out: 送信時	

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP で送受信するプレフィックスを、リストに従いフィルタリングします。

【実行例】

リストに従いフィルタリングします (BGP ピア : 192.0.2.1、プレフィックスリスト名 : prefix-list-name-A、out)。

```

【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 prefix-list prefix-list-name-A out

```

【未設定時】

フィルタリングを行いません。

8.2.15 neighbor remove-private-as

【機能】

AS-PATH 属性からプライベート AS 番号の情報を削除する設定

【入力形式】

neighbor <BGP ピア> remove-private-as

no neighbor <BGP ピア> remove-private-as

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名 : 255 文字以内の CDATA 型	省略不可

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

経路を広告する際に、AS-PATH 属性からプライベート AS 番号（64512～65534, 4200000000～4294967294）の情報を削除する場合に設定します。グローバル AS 番号とプライベート AS 番号の両方が含まれている場合は、プライベート AS 番号の情報を削除しません。

【実行例】

プライベート AS 番号の情報を削除します（BGP ピア：192.0.2.1）。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 remove-private-as
```

【未設定時】

プライベート AS 番号の情報を削除しません。

8.2.16 neighbor route-map

【機能】

BGP ピアに route-map を適用する設定

【入力形式】

neighbor <BGP ピア> route-map <route-map 名> {in | out}

no neighbor <BGP ピア> route-map <route-map 名> {in | out}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可
route-map 名	適用する route-map 名を指定します。	254 文字以内の WORD 型	
in out	受信時に適用するか／送信時に適用するかを指定します。	in: 受信時 out: 送信時	

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP ピアに route-map を適用します。

【実行例】

BGP ピアに route-map を適用します (BGP ピア : 192.0.2.1、route-map 名 : route-map-A、in)。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 route-map route-map-A in
```

【未設定時】

route-map を適用しません。

8.2.17 neighbor route-server-client

【機能】

BGP ピアをルートサーバクライアントとする設定

【入力形式】

neighbor <BGP ピア> route-server-client

no neighbor <BGP ピア> route-server-client

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名 : 255 文字以内の CDATA 型	省略不可

【動作モード】

address-family ipv4 設定モード、address family-ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP ピアをルートサーバクライアントとする場合に設定します。

【実行例】

BGP ピアをルートサーバクライアントに設定します (BGP ピア : 192.0.2.1)。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 route-server-client
```

【未設定時】

BGP ピアをルートサーバクライアントとしません。

8.2.18 neighbor send-community

【機能】

UPDATE メッセージで送信する際のコミュニティ属性の設定

【入力形式】

neighbor <BGP ピア> send-community {both | extended | standard}

no neighbor <BGP ピア> send-community [both | extended | standard]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可
both extended standard	コミュニティ属性を指定します。	both: 標準、および拡張コミュニティ extended: 拡張コミュニティ standard: 標準コミュニティ	

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

UPDATE メッセージで送信する際のコミュニティ属性を設定します。

【実行例】

UPDATE メッセージで送信する際のコミュニティ属性を設定します (BGP ピア：192.0.2.1、extended)。

```

【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 send-community extended

```

【未設定時】

コミュニティ属性を設定しません。

8.2.19 neighbor soft-reconfiguration inbound

【機能】

BGP ピアから受信した経路情報をキャッシュする設定

【入力形式】

neighbor <BGP ピア> soft-reconfiguration inbound

no neighbor <BGP ピア> soft-reconfiguration inbound

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP ピアから受信した経路情報をキャッシュする場合に設定します。

【実行例】

BGP ピアから受信した経路情報をキャッシュします（BGP ピア：192.0.2.1）。

```

【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 soft-reconfiguration inbound

```

【未設定時】

受信した経路情報をキャッシュしません。

8.2.20 neighbor soo

【機能】

BGP ピアの SOO 値の設定

【入力形式】

neighbor <BGP ピア> soo <SOO 値>

no neighbor <BGP ピア> soo

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
SOO 値	Site of Origin (SOO) 値を指定します。	A:B 型式	

【動作モード】

address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

extended community 属性に設定する、BGP ピアの SOO 値を設定します。

【実行例】

BGP ピアの SOO 値を設定する (BGP ピア：192.0.2.1、SOO 値：1:1000)

```

【address-family ipv4 VRF 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 vrf vrf-A
(config-af ipv4 vrf vrf-A)#neighbor 192.168.0.1 soo 1:1000

```

【未設定時】

SOO 値を設定しません。

8.2.21 network

【機能】

BGP で広告するネットワークの設定

【入力形式】

network {<ネットワークアドレス> <ネットマスク> | <ネットワークアドレス> <プレフィックス長>}
[backdoor]

no network {<ネットワークアドレス> <ネットマスク> | <ネットワークアドレス> <プレフィックス長>}
[backdoor]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ネットワークアドレス	BGP で広告するネットワークアドレスを指定します。	IPv4 アドレス形式 (*1) IPv6 アドレス形式 (*2)	省略不可
ネットマスク	BGP で広告するネットマスクを指定します。	IPv4 アドレス形式 (*1)	
プレフィックス長	BGP で広告するプレフィックス長を指定します。	0 ~ 128 (*2)	
backdoor	本経路をローカル BGP 経路として扱う場合に指定します。	-	External 経路または Internal 経路として扱う

- *1) address-family ipv6 VRF 設定モードでは指定できません。
- *2) address-family ipv4 VRF 設定モードでは指定できません。

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード

【説明】

BGP で広告するネットワークを設定します。

【実行例】

BGP で広告するネットワークを設定します（ネットワークアドレス：192.0.2.0、ネットマスク：255.255.255.0）。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#network 192.0.2.0 255.255.255.0
```

【未設定時】

本装置の経路情報を広告します。

8.2.22 no bgp lookup default-information

【機能】

デフォルトルートを除外する設定

【入力形式】

no bgp lookup default-information

bgp lookup default-information

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP の nexthop validation check において、デフォルトルートを除外する場合に設定します。なお、本コマンドは refresh 後に即時有効となります。

【実行例】

デフォルトルートを除外します。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#no bgp lookup default-information
```

【未設定時】

BGP の nexthop validation check において、デフォルトルートを使用します。

8.2.23 redistribute

【機能】

経路情報を再広告する設定

【入力形式】

```
redistribute { <再広告する経路情報> | isakmp sa-up { local-prot1 | local-prot2 } } [route-map <route-map 名>]
```

```
no redistribute { <再広告する経路情報> | isakmp sa-up { local-prot1 | local-prot2 } } [route-map <route-map 名>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
再広告する経路情報	BGP 以外の手段で取得した経路情報のうち、BGP で広告するものを指定します。	connected:connected 経路 kernel(*1、*3、*4):kernel にセットされた経路 ospf(*1、*3):OSPF で学習した経路 ospf6(*2、*3、*4):OSPF6 で学習した経路 rip(*1、*3、*4):RIP で学習した経路 static:スタティック経路	省略不可
isakmp sa-up	SA-UP ルートを BGP で広告する場合に指定します。	-	
local-prot1 local-prot2	SA-UP ルートを管理するプロトコル名を指定します。	-	
route-map 名	適用する route-map 名を指定します。	254 文字以内の WORD 型	route-map を適用しない

- *1) address-family ipv6 設定モードでは指定できません。
- *2) address-family ipv4 設定モードでは指定できません。
- *3) address-family ipv6 VRF 設定モードでは指定できません。
- *4) address-family ipv4 VRF 設定モードでは指定できません。

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

異なるルートドメインに対して、経路情報の再広告を行う場合に設定します。

【実行例】

経路情報の再広告を行います（再広告する経路情報：static）。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#redistribute static
```

【未設定時】

再広告を行いません。

8.2.24 table-map

【機能】

BGP 経路を RIB に登録するときに指定された Route-Map の適用

【入力形式】

table-map <route-map 名> [filter]

no table-map <route-map 名> [filter]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
route-map 名	route-map 名を指定します。	254 文字以内の WORD 形式	省略不可
filter	Route-Map に MATCH しない経路を RIB に登録しない場合に指定します。	-	コマンド概要参照

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード

【説明】

BGP 経路を RIB に登録するときに指定された Route-Map を適用します。

filter オプションが指定されていない場合、Route-Map に MATCH した BGP 経路は Route-Map 適用後の経路情報が RIB に登録され、MATCH しない場合は元の BGP 経路情報が RIB に登録されます。

【実行例】

Route Reflector 用途で使用するなど、すべての BGP 経路の RIB 登録を抑制する場合、以下のように存在しない Route-Map bgp-to-rib を指定します。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 650016
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)# neighbor 192.168.1.1 remote-as 65002
(config-af ipv4 unicast)# table-map bgp-to-rib filter
(config-af ipv4 unicast)# exit
(config-bgp)#exit
```

一部の BGP 経路に対して Metric を変更して登録する場合、以下の Route-Map を指定します。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 650016
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)# neighbor 192.168.1.1 remote-as 65002
(config-af ipv4 unicast)# table-map bgp-to-rib MAP
(config-af ipv4 unicast)# exit
(config-bgp)#exit
(config)#
(config)#access-list 1 permit 172.16.1.0 0.0.255.255
(config)#route-map MAP permit 1
(config-rmap MAP permit 1)#match ip address 1
(config-rmap MAP permit 1)#set metric 9999
(config-rmap MAP permit 1)#exit
(config)#
```

【未設定時】

BGP 経路はすべて RIB に登録されます。

8.3 IPv6 経路交換の設定

8.3.1 address-family ipv6 unicast

【機能】

address-family ipv6 設定モードへの移行

【入力形式】

address-family ipv6 unicast

no address-family [ipv6 unicast]

【動作モード】

BGP サービス設定モード

【説明】

address-family ipv6 設定モードに移行します。コマンドの先頭に "no" を指定することで、address-family ipv6 設定モードの内容がすべて消去されます。

【実行例】

address-family ipv6 設定モードに移行します。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv6 unicast
(config-af ipv6 unicast)#
```

8.3.2 aggregate-address

【機能】

経路情報の集約

【入力形式】

aggregate-address {<ネットワークアドレス> <ネットマスク> | <ネットワークアドレス> <プレフィックス長>} [as-set] [summary-only]

no aggregate-address {<ネットワークアドレス> <ネットマスク> | <ネットワークアドレス> <プレフィックス長>} [as-set] [summary-only]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ネットワークアドレス	集約後のネットワークアドレスを指定します。	IPv4 アドレス形式 (*1) IPv6 アドレス形式 (*2)	省略不可
ネットマスク	集約後のネットマスクを指定します。	IPv4 アドレス形式 (*1)	
プレフィックス長	集約後のプレフィックス長を指定します。	0 ~ 128 (*2)	

パラメタ	設定内容	設定範囲	省略時
as-set	AS set path information を生成する場合に指定します。	-	集約前の経路情報の AS-PATH 情報を含めない
summary-only	集約後の経路情報のみを広告する場合に指定します。	-	集約前の経路情報もすべて広告

*1) address-family ipv6 設定モード、address-family ipv6 VRF 設定モードでは指定できません。

*2) address-family ipv4 設定モード、address-family ipv4 VRF 設定モードでは指定できません。

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

経路情報を集約し、その情報を BGP で広告します。通知する際には、PATH 属性に ATOMIC-AGGREGATE 属性、AGGREGATOR 属性を付与して広告します。"summary-only" を指定した場合は、集約後の経路情報のみを広告し、集約された他の情報は広告しません。

【実行例】

経路情報を集約します（ネットワークアドレス：192.0.2.0、ネットマスク：255.255.255.0）。

```

【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#aggregate-address 192.0.2.0 255.255.255.0

```

【未設定時】

経路情報を集約しません。

8.3.3 default-information originate

【機能】

スタティック登録したデフォルトルートの情報を広告する設定

【入力形式】

default-information originate

no default-information originate

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

スタティック登録したデフォルトルートの情報を広告する場合に設定します。

【実行例】

スタティック登録したデフォルトルート情報を広告します。

```
【BGP サービス設定の場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#default-information originate
```

【未設定時】

デフォルトルートを広告しません。

8.3.4 neighbor activate

【機能】

経路を交換する設定

【入力形式】

neighbor <BGP ピア> activate

no neighbor <BGP ピア> activate

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

経路の交換を行う場合に設定します。

【実行例】

経路の交換を行います（BGP ピア：192.0.2.1）。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 activate
```

【未設定時】

経路の交換を行いません。IPv4 経路は、本コマンドを設定しなくとも、デフォルトで交換を行います。

8.3.5 neighbor allowas-in

【機能】

AS 番号が重複した経路情報の受信の許可

【入力形式】

neighbor <BGP ピア> allowas-in [<許可数>]

no neighbor <BGP ピア> allowas-in [<許可数>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可
許可数	AS 番号が重複した経路情報の重複許可数を指定します。	1～10	重複を許可しない

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

AS 番号が重複した経路情報の受信を許可します。

【実行例】

AS 番号が重複した経路情報の受信を許可します (BGP ピア：192.0.2.1、許可数：3)。

```

【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 allowas-in 3

```

【未設定時】

AS 番号が重複した経路情報の受信を許可しません。

8.3.6 neighbor attribute-unchanged

【機能】

変換しない Attribute 情報の設定

【入力形式】

neighbor <BGP ピア> attribute-unchanged [as-path] [med] [next-hop]

no neighbor <BGP ピア> attribute-unchanged [as-path] [med] [next-hop]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名 : 255 文字以内の CDATA 型	省略不可
as-path	AS-PATH 属性を変換しない場合に指定します。	-	AS-PATH 属性を変換する
med	MED 属性を変換しない場合に指定します。	-	MED 属性を変換する
next-hop	NEXT-HOP 属性を変換しない場合に指定します。	-	NEXT-HOP 属性を変換する
属性の指定なし	「AS-PATH 属性」、「MED 属性」、「NEXT-HOP 属性」すべてを変換しません。	-	-

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

UPDATE メッセージを BGP ピアに送信する際に、変換しない Attribute 情報を設定します。

【実行例】

変換しない Attribute 情報を設定します (BGP ピア : 192.0.2.1、as-path、med、next-hop)。

```

【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 attribute-unchanged as-path med next-hop

```

【未設定時】

UPDATE メッセージを送信する際に、Attribute 情報を変換します。

8.3.7 neighbor capability graceful-restart

【機能】

Graceful-restart ケイパビリティの送信

【入力形式】

neighbor <BGP ピア> capability graceful-restart

no neighbor <BGP ピア> capability graceful-restart

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

OPEN メッセージのオプションパラメタとして、Graceful-restart ケイパビリティを送信します。

【実行例】

Graceful-restart ケイパビリティを送信します (BGP ピア：192.0.2.1)。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 capability graceful-restart
```

【未設定時】

Graceful-restart ケイパビリティを送信しません。

8.3.8 neighbor default-originate

【機能】

デフォルトルートをも BGP ピアに広告する設定

【入力形式】

neighbor <BGP ピア> default-originate [route-map <route-map 名>]

no neighbor <BGP ピア> default-originate [route-map <route-map 名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可
route-map 名	適用する route-map 名を指定します。	254 文字以内の WORD 型	route-map を適用しない

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP スピーカ（ローカルルータ）をデフォルトルートとして使うために、デフォルトルートを BGP ピアに広告する場合に設定します。

【実行例】

デフォルトルートを BGP ピアに広告します（IPv4 アドレス：192.0.2.1）。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 default-originate
```

【未設定時】

デフォルトルートを広告しません。

8.3.9 neighbor disable-nexthop-validation

【機能】

Nexthop 到達性チェックを行わずに経路を有効と判定する設定

【入力形式】

neighbor <BGP ピア> disable-nexthop-validation

no neighbor <BGP ピア> disable-nexthop-validation

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP ピアから学習した経路の Nexthop 到達性チェックを行わず、経路を有効と判定する場合に設定します。

本設定が変更された場合、すでに確立されている BGP セッションは再確立が行われます。

【実行例】

Nexthop 到達性チェックを行いません（BGP ピア：192.0.2.1）。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 disable-nexthop-validation
```

【未設定時】

Nexthop 到達性チェックを行います。

8.3.10 neighbor distribute-list

【機能】

フィルタリングの設定

【入力形式】

neighbor <BGP ピア> distribute-list <アクセスリスト番号> {in | out}

no neighbor <BGP ピア> distribute-list <アクセスリスト番号> {in | out}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可
アクセスリスト番号	BGP ピアに対して、送信する／送信しない経路情報を指定するために、アクセスリスト番号を指定します。	-	
in out	受信時に適用するか／送信時に適用するかを指定します。	in: 受信時 out: 送信時	

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP の送受信に対して、フィルタリングの設定を行います。アクセスリストで指定した宛先経路情報のみを受信する／しない、または、送信する／しないといった制御を行うことができます。

【実行例】

フィルタリングの設定を行います（BGP ピア：192.0.2.1、アクセスリスト番号：1、in）。

```

【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 distribute-list 1 in

```

【未設定時】

フィルタリングを行いません。

8.3.11 neighbor filter-list

【機能】

UPDATE メッセージで送受信する際のフィルタリングの設定

【入力形式】

neighbor <BGP ピア> filter-list <アクセスリスト名> {in | out}

no neighbor <BGP ピア> filter-list [<アクセスリスト名> [in | out]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可
アクセスリスト名	アクセスリスト名を指定します。	254 文字以内の WORD 型	
in out	受信時に適用するか／送信時に適用するかを指定します。	in: 受信時 out: 送信時	

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

UPDATE メッセージで送受信する際のフィルタリングを設定します。

【実行例】

UPDATE メッセージで送受信する際のフィルタリングを設定します (BGP ピア：192.0.2.1、アクセスリスト名：accesslist-name-A、out)。

```

【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 filter-list accesslist-name-A out

```

【未設定時】

フィルタリングを設定しません。

8.3.12 neighbor maximum-prefix

【機能】

BGP ピアから受け付けるプレフィックス数の最大値、警告を発行する割合の設定

【入力形式】

neighbor <BGP ピア> maximum-prefix <プレフィックス数> {<割合> | warning-only}

no neighbor <BGP ピア> maximum-prefix [<プレフィックス数> [warning-only]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可
プレフィックス数	BGP ピアから受信するプレフィックス数の最大数を指定します。	1～4294967295	
割合 warning-only	警告を発行する割合（単位：%）を指定します。	1～100 warning-only：警告のみを行う場合	

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP ピアから受け付けるプレフィックス数の最大値、および警告を発行する割合を設定します。警告値、および最大値を超えた場合にはログ情報を出力します。

【実行例】

BGP ピアから受け付けるプレフィックス数の最大値、および警告を発行する割合を設定します（BGP ピア：192.0.2.1、プレフィックス数：1000、割合：90%）。

```

【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 maximum-prefix 1000 90

```

【未設定時】

受け付けるプレフィックス数を制限しません。

8.3.13 neighbor next-hop-self

【機能】

Next-hop を、このピア自身とする設定

【入力形式】

neighbor <BGP ピア> next-hop-self

no neighbor <BGP ピア> next-hop-self

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名 : 255 文字以内の CDATA 型	省略不可

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP ピアから受信した経路に対する Next-hop を、このピア自身とする場合に設定します。

【実行例】

Next-hop をこのピア自身とします (BGP ピア : 192.0.2.1)。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 next-hop-self
```

【未設定時】

Next-hop をこのピア自身としません。

8.3.14 neighbor prefix-list

【機能】

リストに従いフィルタリングする設定

【入力形式】

neighbor <BGP ピア> prefix-list <プレフィックスリスト名> {in | out}

no neighbor <BGP ピア> prefix-list [<プレフィックスリスト名> [in | out]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名 : 255 文字以内の CDATA 型	省略不可
プレフィックスリスト名	参照するプレフィックスリスト名を指定します。	254 文字以内の WORD 型	
in out	受信時に適用するか／送信時に適用するかを指定します。	in: 受信時 out: 送信時	

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP で送受信するプレフィックスを、リストに従いフィルタリングします。

【実行例】

リストに従いフィルタリングします (BGP ピア : 192.0.2.1、プレフィックスリスト名 : prefix-list-name-A、out)。

```

【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 prefix-list prefix-list-name-A out

```

【未設定時】

フィルタリングを行いません。

8.3.15 neighbor remove-private-as

【機能】

プライベート AS 番号の情報を削除する設定

【入力形式】

neighbor <BGP ピア> remove-private-as

no neighbor <BGP ピア> remove-private-as

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名 : 255 文字以内の CDATA 型	省略不可

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

経路を広告する際に、AS-PATH 属性からプライベート AS 番号（64512～65534, 4200000000～4294967294）の情報を削除する場合に設定します。グローバル AS 番号とプライベート AS 番号の両方が含まれている場合は、プライベート AS 番号の情報を削除しません。

【実行例】

プライベート AS 番号の情報を削除します（BGP ピア：192.0.2.1）。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 remove-private-as
```

【未設定時】

プライベート AS 番号の情報を削除しません。

8.3.16 neighbor route-map

【機能】

BGP ピアに route-map を適用する設定

【入力形式】

neighbor <BGP ピア> route-map <route-map 名> {in | out}

no neighbor <BGP ピア> route-map <route-map 名> {in | out}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可
route-map 名	適用する route-map 名を指定します。	254 文字以内の WORD 型	
in out	受信時に適用するか／送信時に適用するかを指定します。	in: 受信時 out: 送信時	

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP ピアに route-map を適用します。

【実行例】

BGP ピアに route-map を適用します (BGP ピア : 192.0.2.1、route-map 名 : route-map-A、in)。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 route-map route-map-A in
```

【未設定時】

route-map を適用しません。

8.3.17 neighbor route-reflector-client

【機能】

BGP ピアをルータリフレクタクライアントとする設定

【入力形式】

neighbor <BGP ピア> route-reflector-client

no neighbor <BGP ピア> route-reflector-client

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名 : 255 文字以内の CDATA 型	省略不可

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP ピアをルータリフレクタクライアントとする場合に設定します。

【実行例】

BGP ピアをルータリフレクタクライアントとします (BGP ピア : 192.0.2.1)。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 route-reflector-client
```

【未設定時】

BGP ピアをルータリフレクタクライアントとしません。

8.3.18 neighbor route-server-client

【機能】

BGP ピアをルートサーバクライアントとする設定

【入力形式】

neighbor <BGP ピア> route-server-client

no neighbor <BGP ピア> route-server-client

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可

【動作モード】

address-family ipv4 設定モード、address family-ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP ピアをルートサーバクライアントとする場合に設定します。

【実行例】

BGP ピアをルートサーバクライアントに設定します（BGP ピア：192.0.2.1）。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 route-server-client
```

【未設定時】

BGP ピアをルートサーバクライアントとしません。

8.3.19 neighbor send-community

【機能】

UPDATE メッセージで送信する際のコミュニティ属性の設定

【入力形式】

neighbor <BGP ピア> send-community {both | extended | standard}

no neighbor <BGP ピア> send-community [both | extended | standard]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可
both extended standard	コミュニティ属性を指定します。	both：標準、および拡張コミュニティ extended：拡張コミュニティ standard：標準コミュニティ	

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

UPDATE メッセージで送信する際のコミュニティ属性を設定します。

【実行例】

UPDATE メッセージで送信する際のコミュニティ属性を設定します (BGP ピア：192.0.2.1、extended)。

```

【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 send-community extended

```

【未設定時】

コミュニティ属性を設定しません。

8.3.20 neighbor soft-reconfiguration inbound

【機能】

BGP ピアから受信した経路情報をキャッシュする設定

【入力形式】

neighbor <BGP ピア> soft-reconfiguration inbound

no neighbor <BGP ピア> soft-reconfiguration inbound

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP ピアから受信した経路情報をキャッシュする場合に設定します。

【実行例】

BGP ピアから受信した経路情報をキャッシュします (BGP ピア：192.0.2.1)。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 soft-reconfiguration inbound
```

【未設定時】

受信した経路情報をキャッシュしません。

8.3.21 neighbor soo

【機能】

BGP ピアの SOO 値の設定

【入力形式】

neighbor <BGP ピア> soo <SOO 値>

no neighbor <BGP ピア> soo

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
SOO 値	Site of Origin (SOO) 値を指定します。	A:B 型式	

【動作モード】

address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

extended community 属性に設定する、BGP ピアの SOO 値を設定します。

【実行例】

BGP ピアの SOO 値を設定する (BGP ピア：192.0.2.1、SOO 値：1:1000)

```
【address-family ipv4 VRF 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 vrf vrf-A
(config-af ipv4 vrf vrf-A)#neighbor 192.168.0.1 soo 1:1000
```

【未設定時】

SOO 値を設定しません。

8.3.22 network

【機能】

BGP で広告するネットワークの設定

【入力形式】

network {<ネットワークアドレス> <ネットマスク> | <ネットワークアドレス> / <プレフィックス長>}
[backdoor]

no network {<ネットワークアドレス> <ネットマスク> | <ネットワークアドレス> / <プレフィックス長>}
[backdoor]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ネットワークアドレス	BGP で広告するネットワークアドレスを指定します。	IPv4 アドレス形式 (*1) IPv6 アドレス形式 (*2)	省略不可
ネットマスク	BGP で広告するネットマスクを指定します。	IPv4 アドレス形式 (*1)	
プレフィックス長	BGP で広告するプレフィックス長を指定します。	0 ~ 128 (*2)	
backdoor	本経路をローカル BGP 経路として扱う場合に指定します。	-	External 経路または Internal 経路として扱う

*1) address-family ipv6 設定モードでは指定できません。

*2) address-family ipv4 設定モードでは指定できません。

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード

【説明】

BGP で広告するネットワークを設定します。

【実行例】

BGP で広告するネットワークを設定します (ネットワークアドレス : 192.0.2.0、ネットマスク : 255.255.255.0)。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#network 192.0.2.0 255.255.255.0
```

【未設定時】

本装置の経路情報を広告します。

8.3.23 no bgp lookup default-information

【機能】

デフォルトルートを除外する設定

【入力形式】

no bgp lookup default-information

bgp lookup default-information

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP の nexthop validation check において、デフォルトルートを除外する場合に設定します。なお、本コマンドは refresh 後に即時有効となります。

【実行例】

デフォルトルートを除外します。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#no bgp lookup default-information
```

【未設定時】

BGP の nexthop validation check において、デフォルトルートを使用します。

8.3.24 redistribute

【機能】

経路情報を再広告する設定

【入力形式】

redistribute { <再広告する経路情報> | isakmp sa-up { local-prot1 | local-prot2 } } [route-map <route-map 名>]

no redistribute { <再広告する経路情報> | isakmp sa-up { local-prot1 | local-prot2 } } [route-map <route-map 名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
再広告する経路情報	BGP 以外の手段で取得した経路情報のうち、BGP で広告するものを指定します。	connected: connected 経路 kernel(*1、*3、*4): kernel にセットされた経路 ospf(*1、*3): OSPF で学習した経路 ospf6(*2、*3、*4): OSPF6 で学習した経路 rip (*1、*3、*4) : RIP で学習した経路 static: スタティック経路	省略不可
isakmp sa-up	SA-UP ルートを BGP で広告する場合に指定します。	-	
local-prot1 local-prot2	SA-UP ルートを管理するプロトコル名を指定します。	-	
route-map 名	適用する route-map 名を指定します。	254 文字以内の WORD 型	route-map を適用しない

- *1) address-family ipv6 設定モードでは指定できません。
 *2) address-family ipv4 設定モードでは指定できません。
 *3) address-family ipv6 VRF 設定モードでは指定できません。
 *4) address-family ipv4 VRF 設定モードでは指定できません。

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

異なるルートドメインに対して、経路情報の再広告を行う場合に設定します。

【実行例】

経路情報の再広告を行います（再広告する経路情報：static）。

```

【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#redistribute static

```

【未設定時】

再広告を行いません。

8.3.25 table-map

【機能】

BGP 経路を RIB に登録するときに指定された Route-Map の適用

【入力形式】

```
table-map <route-map 名> [filter]
```

```
no table-map <route-map 名> [filter]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
route-map 名	route-map 名を指定します。	254 文字以内の WORD 形式	省略不可
filter	Route-Map に MATCH しない経路を RIB に登録しない場合に指定します。	-	コマンド概要参照

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード

【説明】

BGP 経路を RIB に登録するときに指定された Route-Map を適用します。

filter オプションが指定されていない場合、Route-Map に MATCH した BGP 経路は Route-Map 適用後の経路情報が RIB に登録され、MATCH しない場合は元の BGP 経路情報が RIB に登録されます。

【実行例】

Route Reflector 用途で使用するなど、すべての BGP 経路の RIB 登録を抑制する場合、以下のように存在しない Route-Map bgp-to-rib を指定します。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 650016
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)# neighbor 192.168.1.1 remote-as 65002
(config-af ipv4 unicast)# table-map bgp-to-rib filter
(config-af ipv4 unicast)# exit
(config-bgp)#exit
```

一部の BGP 経路に対して Metric を変更して登録する場合、以下の Route-Map を指定します。

```
【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 650016
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)# neighbor 192.168.1.1 remote-as 65002
(config-af ipv4 unicast)# table-map bgp-to-rib MAP
(config-af ipv4 unicast)# exit
(config-bgp)#exit
(config)#
(config)#access-list 1 permit 172.16.1.0 0.0.255.255
(config)#route-map MAP permit 1
(config-rmap MAP permit 1)#match ip address 1
(config-rmap MAP permit 1)#set metric 9999
(config-rmap MAP permit 1)#exit
(config)#
```

【未設定時】

BGP 経路はすべて RIB に登録されます。

8.4 IPv4VRF 経路交換の設定

8.4.1 address-family ipv4 vrf

【機能】

address-family ipv4 VRF 設定モードへの移行

【入力形式】

address-family ipv4 vrf <VRF 名>

no address-family [ipv4 vrf <VRF 名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VRF 名	VRF 名を指定します。	63 文字以内の WORD 型	省略不可

【動作モード】

BGP サービス設定モード

【説明】

address-family ipv4 VRF 設定モードに移行します。address-family ipv4 VRF 設定モードでは、VRF インタフェースの BGP ピアとの間で IPv4 ユニキャストの BGP 通信をする場合の設定を行います。コマンドの先頭に "no" を指定することで、該当 address-family ipv4 VRF 設定モードの内容がすべて消去されます。

【実行例】

address-family ipv4 VRF 設定モードに移行します (VRF 名 : vrf-A)。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 vrf vrf-A
(config-af ipv4 vrf vrf-A)#
```

8.5 IPv6VRF 経路交換の設定

8.5.1 address-family ipv6 vrf

【機能】

address-family ipv6 VRF 設定モードへの移行

【入力形式】

address-family ipv6 vrf <VRF 名>

no address-family [ipv6 vrf <VRF 名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VRF 名	VRF 名を指定します。	63 文字以内の WORD 型	省略不可

【動作モード】

BGP サービス設定モード

【説明】

address-family ipv6 VRF 設定モードに移行します。address-family ipv6 VRF 設定モードでは、VRF インタフェースの BGP ピアとの間で IPv6 ユニキャストの BGP 通信をする場合の設定を行います。コマンドの先頭に "no" を指定することで、該当 address-family ipv6 VRF 設定モードの内容がすべて消去されます。

【実行例】

address-family ipv6 VRF 設定モードに移行します (VRF 名 : vrf-A)。

```
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv6 vrf vrf-A
(config-af ipv6 vrf vrf-A)#
```

第9章 route-mapの設定



この章では、route-mapの設定に関するコマンドについて説明します。

9.1 route-map の設定

9.1.1 route-map

【機能】

route-map 設定モードへの移行

【入力形式】

route-map <route-map 名> {permit | deny} <シーケンス番号>

no route-map <route-map 名> {{permit | deny} <シーケンス番号> | *}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
route-map 名	route-map 名を指定します。	254 文字以内の WORD 型	省略不可
permit deny	属性を指定します。	permit: 許可 deny: 拒否	
シーケンス番号	シーケンス番号を指定します。	1～65535	

【動作モード】

基本設定モード

【説明】

route-map 設定モードに移行します。route-map では、ルート情報の送受信条件や送受信先を詳細に規定します。ルート情報の送受信条件や送受信対象を "match" で特定し、送受信するルート情報を "set" で編集します。no で "*" を指定した場合には、該当 route-map 設定モードの内容がすべて消去されます。

【実行例】

route-map 設定モードに移行します (route-map 名: route-map-A、許可、シーケンス番号: 1)。

```
#configure terminal
(config)#route-map map-A permit 1
(config-rmap map-A permit 1)#
```

9.1.2 continue

【機能】

次に評価したいroute-mapのシーケンス番号の設定

【入力形式】

continue [<シーケンス番号>]

no continue [<シーケンス番号>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
シーケンス番号	シーケンス番号を指定します。	1～65535	次に見つかった route-map

【動作モード】

route-map 設定モード

【説明】

route-map にマッチした場合に、次に評価したい route-map のシーケンス番号を設定します。シーケンス番号を省略した場合、次に見つかった route-map を評価します。

対象プロトコル：RIP、OSPF、BGP、OSPF6

【実行例】

次に評価したい route-map のシーケンス番号を設定します（次に見つかった route-map）。

```
#configure terminal
(config)#route-map route-map-A permit 1
(config-rmap route-map-A permit 1)#continue
```

【未設定時】

route-map にマッチした場合、route-map の評価を終了します。

9.1.3 match as-path

【機能】

AS-PATH アクセスリストにマッチさせる設定

【入力形式】

match as-path <アクセスリスト名>

no match as-path [<アクセスリスト名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アクセスリスト名	アクセスリスト名を指定します。	254 文字以内の WORD 型	省略不可

【動作モード】

route-map 設定モード

【説明】

AS-PATH アクセスリストにマッチさせる場合に設定します。

対象プロトコル：BGP

【実行例】

AS-PATH アクセスリストにマッチさせます (AS アクセスリスト名: asacclist-A)。

```
#configure terminal
(config)#route-map route-map-A permit 1
(config-rmap route-map-A permit 1)#match as-path asacclist-A
```

【未設定時】

AS-PATH アクセスリストにマッチさせません。

9.1.4 match community

【機能】

コミュニティリストにマッチさせる設定

【入力形式】

match community <コミュニティリスト名>

no match community [<コミュニティリスト名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
コミュニティリスト名	コミュニティリスト名を指定します。	254 文字以内の WORD 型	省略不可

【動作モード】

route-map 設定モード

【説明】

コミュニティリストにマッチさせる場合に指定します。

対象プロトコル: BGP

【実行例】

コミュニティリストにマッチさせます (コミュニティリスト名: community-list-A)。

```
#configure terminal
(config)#route-map route-map-A permit 1
(config-rmap route-map-A permit 1)#match community community-list-A
```

【未設定時】

コミュニティリストにマッチさせません。

9.1.5 match interface

【機能】

インタフェースの比較

【入力形式】

match interface <インタフェース名> <インタフェース番号>

no match interface <インタフェース名> [<インタフェース番号>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース名	インタフェース名を指定します。	-	省略不可
インタフェース番号	インタフェース番号を指定します。	-	

【動作モード】

route-map 設定モード

【説明】

インタフェースを比較します。

対象プロトコル：RIP、OSPF

【実行例】

インタフェースを比較します（インタフェース名：port-channel、インタフェース番号：1）。

```
#configure terminal
(config)#route-map route-map-A permit 1
(config-rmap route-map-A permit 1)#match interface port-channel 1
```

【未設定時】

インタフェースを比較しません。

9.1.6 match ip address

【機能】

アクセスリスト、プレフィックスリストにマッチさせる設定

【入力形式】

match ip address {<アクセスリスト番号> | prefix-list <プレフィックスリスト名>}

no match ip address [<アクセスリスト番号> | prefix-list [<プレフィックスリスト名>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アクセスリスト番号	アクセスリスト番号を指定します。	-	省略不可
プレフィックスリスト名	プレフィックスリスト名を指定します。	254 文字以内の WORD 型	

【動作モード】

route-map 設定モード

【説明】

アクセスリストまたはプレフィックスリストにマッチさせる場合に設定します。

対象プロトコル：RIP、OSPF、BGP

【実行例】

アクセスリストにマッチさせます（アクセスリスト番号：20）。

```
#configure terminal
(config)#route-map route-map-A permit 1
(config-rmap route-map-A permit 1)#match ip address 20
```

【未設定時】

アクセスリストまたはプレフィックスリストにマッチさせません。

9.1.7 match ip next-hop

【機能】

アクセスリスト、プレフィックスリストにマッチさせる設定

【入力形式】

match ip next-hop [<アクセスリスト番号> | prefix-list <プレフィックスリスト名>]

no match ip next-hop [<アクセスリスト番号> | prefix-list [<プレフィックスリスト名>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アクセスリスト番号	アクセスリスト番号を指定します。	-	省略不可
プレフィックスリスト名	プレフィックスリスト名を指定します。	254 文字以内の WORD 型	

【動作モード】

route-map 設定モード

【説明】

アクセスリストまたはプレフィックスリストにマッチさせる場合に設定します。

対象プロトコル：RIP、OSPF、BGP

【実行例】

アクセスリストにマッチさせます（アクセスリスト番号：1）。

```
#configure terminal
(config)#route-map route-map-A permit 1
(config-rmap route-map-A permit 1)#match ip next-hop 1
```

【未設定時】

アクセスリストまたはプレフィックスリストにマッチさせません。

9.1.8 match ipv6 address

【機能】

アクセスリスト、プレフィックスリストにマッチさせる設定

【入力形式】

match ipv6 address {<アクセスリスト番号> | prefix-list <プレフィックスリスト名>}

no match ipv6 address {<アクセスリスト番号> | prefix-list <プレフィックスリスト名>}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アクセスリスト番号	アクセスリスト番号を指定します。	-	省略不可
プレフィックスリスト名	プレフィックスリスト名を指定します。	254文字以内のWORD型	

【動作モード】

route-map 設定モード

【説明】

アクセスリストまたはプレフィックスリストにマッチさせる場合に設定します。

対象プロトコル：OSPF6（プレフィックスリストのみ使用可能）、BGP

【実行例】

アクセスリストにマッチさせます（アクセスリスト番号：3000）。

```
#configure terminal
(config)#route-map route-map-A permit 1
(config-rmap route-map-A permit 1)#match ipv6 address 3000
```

【未設定時】

アクセスリストまたはプレフィックスリストにマッチさせません。

9.1.9 match ipv6 next-hop

【機能】

経路情報の Next-hop アドレスと設定した Next-hop アドレスとの比較

【入力形式】

match ipv6 next-hop <Next-hop アドレス>

no match ipv6 next-hop <Next-hop アドレス>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
Next-hop アドレス	Next-hop アドレスを指定します。	IPv6 アドレス形式	省略不可

【動作モード】

route-map 設定モード

【説明】

経路情報の Next-hop アドレスと設定した Next-hop アドレスとを比較します。

対象プロトコル：BGP

【実行例】

Next-hop アドレスを比較します（Next-hop アドレス：2001:db8::1）。

```
#configure terminal
(config)#route-map route-map-A permit 1
(config-rmap route-map-A permit 1)#match ipv6 next-hop 2001:db8::1
```

【未設定時】

Next-hop アドレスを比較しません。

9.1.10 match metric

【機能】

経路情報のメトリック値と設定したメトリック値との比較

【入力形式】

match metric <メトリック値>

no match metric [<メトリック値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
メトリック値	メトリック値を指定します。	0～4294967295	省略不可

【動作モード】

route-map 設定モード

【説明】

経路情報のメトリック値と設定したメトリック値とを比較します。

対象プロトコル：RIP、OSPF、BGP

【実行例】

経路情報のメトリック値と設定したメトリック値を比較します（メトリック値：12）。

```
#configure terminal
(config)#route-map route-map-A permit 1
(config-rmap route-map-A permit 1)#match metric 12
```

【未設定時】

メトリック値を比較しません。

9.1.11 match origin

【機能】

経路情報の ORIGIN 属性と設定した ORIGIN 属性との比較

【入力形式】

match origin <ORIGIN 属性>

no match origin [<ORIGIN 属性>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ORIGIN 属性	ORIGIN 属性を指定します。	egp igp incomplete	省略不可

【動作モード】

route-map 設定モード

【説明】

経路情報の ORIGIN 属性と設定した ORIGIN 属性とを比較します。

対象プロトコル：BGP

【実行例】

経路情報の ORIGIN 属性と設定した ORIGIN 属性を比較します（ORIGIN 属性：egp）。

```
#configure terminal
(config)#route-map route-map-A permit 1
(config-rmap route-map-A permit 1)#match origin egp
```

【未設定時】

ORIGIN 属性を比較しません。

9.1.12 match route-type external

【機能】

経路情報のメトリックタイプと設定したメトリックタイプとの比較

【入力形式】

match route-type external {type-1 | type-2}

no match route-type external [type-1 | type-2]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
type-1 type-2	メトリックタイプを指定します。	type-1 type-2	省略不可

【動作モード】

route-map 設定モード

【説明】

経路情報のメトリックタイプと設定したメトリックタイプとを比較します。

対象プロトコル：OSPF

【実行例】

経路情報のメトリックタイプと設定したメトリックタイプを比較します (type-1)。

```
#configure terminal
(config)#route-map route-map-A permit 1
(config-rmap route-map-A permit 1)#match route-type external type-1
```

【未設定時】

メトリックタイプを比較しません。

9.1.13 match tag

【機能】

タグ値と設定したタグ値との比較

【入力形式】

match tag <タグ値>

no match tag [<タグ値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
タグ値	タグ値を指定します。	1～2147483647	省略不可

【動作モード】

route-map 設定モード

【説明】

タグ値と設定したタグ値とを比較します。

対象プロトコル：OSPF、BGP

【実行例】

タグ値を比較します（タグ値：10）。

```
#configure terminal
(config)#route-map route-map-A permit 1
(config-rmap route-map-A permit 1)#match tag 10
```

【未設定時】

タグ値を比較しません。

9.1.14 set aggregator

【機能】

route-map に該当する経路情報の AGGREGATOR 属性の設定

【入力形式】

set aggregator as <AS 番号> <AGGREGATOR 属性>

no set aggregator as [<AS 番号> <AGGREGATOR 属性>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
AS 番号	AS 番号を指定します。	1～4294967295	省略不可
AGGREGATOR 属性	AGGREGATOR 属性を指定します。	IPv4 アドレス形式	

【動作モード】

route-map 設定モード

【説明】

route-map に該当する経路情報の AGGREGATOR 属性を設定します。

対象プロトコル：BGP

【実行例】

route-map に該当する経路情報の AGGREGATOR 属性を設定します（AS 番号：100、AGGREGATOR 属性：192.0.2.1）。

```
#configure terminal
(config)#route-map route-map-A permit 1
(config-rmap route-map-A permit 1)#set aggregator as 100 192.0.2.1
```

【未設定時】

AGGREGATOR 属性を設定しません。

9.1.15 set as-path prepend

【機能】

route-map に該当する経路情報の AS-PATH 属性の付加

【入力形式】

set as-path prepend <AS 番号>

no set as-path prepend [<AS 番号>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
AS 番号	AS-PATH 属性に付加する AS 番号を指定します。	1 ～ 4294967295	省略不可

【動作モード】

route-map 設定モード

【説明】

route-map に該当する経路情報の AS-PATH 属性に付加します。

対象プロトコル：BGP

【実行例】

AS-PATH 属性に付加します（AS 番号：16）。

```
#configure terminal
(config)#route-map route-map-A permit 1
(config-rmap route-map-A permit 1)#set as-path prepend 16
```

【未設定時】

AS-PATH 属性に付加しません。

9.1.16 set atomic-aggregate

【機能】

route-map に該当する経路情報の ATOMIC-AGGREGATE 属性の設定

【入力形式】

set atomic-aggregate

no set atomic-aggregate

【動作モード】

route-map 設定モード

【説明】

route-map に該当する経路情報の ATOMIC-AGGREGATE 属性を設定します。

対象プロトコル：BGP

【実行例】

ATOMIC-AGGREGATE 属性を設定します。

```
#configure terminal
(config)#route-map route-map-A permit 1
(config-rmap route-map-A permit 1)#set atomic-aggregate
```

【未設定時】

ATOMIC-AGGREGATE 属性を設定しません。

9.1.17 set community

【機能】

コミュニティ属性の設定

【入力形式】

set community [additive] <コミュニティ属性値>

no set community [additive] [<コミュニティ属性値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
additive	コミュニティ属性を追加する場合に指定します。	-	コミュニティ属性を置換
コミュニティ属性値	コミュニティ属性値を指定します。	local-as:NO-EXPORT- SUBCONFED 属性 no-advertise:NO- ADVERTISE 属性 no-export:NO- EXPORT 属性 none:NONE 属性 A:B: コミュニティ値	省略不可

【動作モード】

route-map 設定モード

【説明】

route-map に該当する経路情報のコミュニティ属性を設定します。additive を指定した場合には、コミュニティ属性を追加します。

対象プロトコル：BGP

【実行例】

コミュニティ属性を設定します（コミュニティ属性値：no-advertise）。

```
#configure terminal
(config)#route-map map-A permit 1
(config-rmap map-A permit 1)#set community no-advertise
```

【未設定時】

コミュニティ属性を設定・追加しません。

9.1.18 set extcommunity

【機能】

EXT-COMMUNITIES 属性の設定

【入力形式】

set extcommunity {rt | soo} [additive] [<RT 値> | <SOO 属性値>]

no set extcommunity {rt | soo} [additive] [<RT 値> | <SOO 属性値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
rt soo	RouteTarget か、SOO かを指定します。	rt:RT 値 soo:SOO 値	省略不可
additive	指定された RT 値を追加します。	-	EXT-COMMUNITIES 属性を置換
RT 値	RouteTarget 値を指定します。	A:B 形式	省略不可
SOO 属性値	SOO 属性値を指定します。	A:B 形式	

【動作モード】

route-map 設定モード

【説明】

route-map に該当する経路情報の EXT-COMMUNITIES 属性を設定します。additive を指定した場合には、EXT-COMMUNITIES 属性を追加します。

対象プロトコル：BGP

【実行例】

EXT-COMMUNITIES 属性を設定します（rt、RT 値：1:1000）。

```
#configure terminal
(config)#route-map map-A permit 1
(config-rmap map-A permit 1)#set extcommunity rt 1:1000
```

【未設定時】

EXT-COMMUNITIES 属性を設定／追加しません。

9.1.19 set ip next-hop

【機能】

Next-hop アドレスの設定

【入力形式】

set ip next-hop <Next-hop アドレス>

no set ip next-hop [<Next-hop アドレス>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
Next-hop アドレス	Next-hop アドレスを指定します。	IPv4 アドレス形式	省略不可

【動作モード】

route-map 設定モード

【説明】

route-map に該当する経路情報の Next-hop アドレスを設定します。BGP の場合には、NEXT-HOP 属性として設定値を広告します。

対象プロトコル：RIP、BGP

【実行例】

Next-hop アドレスを設定します（Next-hop アドレス：192.0.2.1）。

```
#configure terminal
(config)#route-map map-A permit 1
(config-rmap map-A permit 1)#set ip next-hop 192.0.2.1
```

【未設定時】

Next-hop アドレスを設定しません。

9.1.20 set ipv6 next-hop

【機能】

Next-hop アドレスの設定

【入力形式】

set ipv6 next-hop {global | local} <Next-hop アドレス>

no set ipv6 next-hop {global | local} [<Next-hop アドレス>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
global local	グローバルアドレスかリンクローカルアドレスかを指定します。	global: グローバルアドレス local: リンクローカルアドレス	省略不可
Next-hop アドレス	Next-hop アドレスを指定します。	IPv6 アドレス形式	

【動作モード】

route-map 設定モード

【説明】

route-map に該当する経路情報の Next-hop アドレスを設定します。

対象プロトコル：BGP

【実行例】

Next-hop アドレスを設定します (global、Next-hop アドレス：2001:db8::1)。

```
#configure terminal
(config)#route-map map-A permit 1
(config-rmap map-A permit 1)#set ipv6 next-hop global 2001:db8::1
```

【未設定時】

Next-hop アドレスを設定しません。

9.1.21 set local-preference

【機能】

route-map に該当する経路情報の LOCAL-PREF 値の設定

【入力形式】

set local-preference <LOCAL-PREF 値>

no set local-preference [<LOCAL-PREF 値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
LOCAL-PREF 値	LOCAL-PREF 値を設定します。	0～4294967295	省略不可

【動作モード】

route-map 設定モード

【説明】

route-map に該当する経路情報の LOCAL-PREF 値を設定します。

対象プロトコル：BGP

【実行例】

LOCAL-PREF 値を設定します (LOCAL-PREF 値 : 95)。

```
#configure terminal
(config)#route-map map-A permit 1
(config-rmap map-A permit 1)#set local-preference 95
```

【未設定時】

LOCAL-PREF 値を設定しません。

9.1.22 set metric

【機能】

メトリック値の設定

【入力形式】

set metric <メトリック値>

no set metric [<メトリック値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
メトリック値	メトリック値を指定します。	0 ~ 4294967295	省略不可

【動作モード】

route-map 設定モード

【説明】

route-map に該当する経路情報のメトリック値を設定します。BGP の場合は、MULTI-EXIT-DISCRIMINATOR 属性として設定値を広告します。

対象プロトコル : RIP、OSPF、BGP、OSPF6

【実行例】

メトリック値を設定します (メトリック値 : 12)。

```
#configure terminal
(config)#route-map route-map-A permit 1
(config-rmap route-map-A permit 1)#set metric 12
```

【未設定時】

メトリック値を設定しません。

9.1.23 set metric-type

【機能】

メトリックタイプの設定

【入力形式】

set metric-type {type-1 | type-2}

no set metric-type [type-1 | type-2]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
type-1 type-2	メトリックタイプを指定します。	type-1 type-2	省略不可

【動作モード】

route-map 設定モード

【説明】

route-map に該当する経路情報のメトリックタイプを設定します。

対象プロトコル：OSPF、OSPF6

【実行例】

メトリックタイプを設定します（メトリックタイプ：type-1）。

```
#configure terminal
(config)#route-map route-map-A permit 1
(config-rmap route-map-A permit 1)#set metric-type type-1
```

【未設定時】

メトリックタイプはtype-2で動作します。

9.1.24 set next-hop

【機能】

AS-external-LSAのNext-hopアドレスの設定

【入力形式】

set next-hop <Next-hop アドレス>

no set next-hop [<Next-hop アドレス>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
Next-hop アドレス	Next-hop アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

【動作モード】

route-map 設定モード

【説明】

route-map に該当する経路情報について、AS-external-LSA の Next-hop アドレスを設定します。

対象プロトコル：OSPF、OSPF6

【実行例】

AS-external-LSA の Next-hop アドレスを設定します（Next-hop アドレス：192.0.2.1）。

```
#configure terminal
(config)#route-map route-map-A permit 1
(config-rmap route-map-A permit 1)#set next-hop 192.0.2.1
```

【未設定時】

AS-external-LSA の Next-hop アドレスを設定しません。

9.1.25 set origin

【機能】

ORIGIN 属性の設定

【入力形式】

set origin <ORIGIN 属性>

no set origin [<ORIGIN 属性>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ORIGIN 属性	ORIGIN 属性を指定します。	egp igp incomplete	省略不可

【動作モード】

route-map 設定モード

【説明】

route-map に該当する経路情報の ORIGIN 属性を設定します。

対象プロトコル：BGP

【実行例】

ORIGIN 属性を設定します（ORIGIN 属性：egp）。

```
#configure terminal
(config)#route-map route-map-A permit 1
(config-rmap route-map-A permit 1)#set origin egp
```

【未設定時】

ORIGIN 属性を設定しません。

9.1.26 set originator-id

【機能】

ORIGINATOR-ID 属性の設定

【入力形式】

set originator-id <ORIGINATOR-ID 属性>

no set originator-id [<ORIGINATOR-ID 属性>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ORIGINATOR-ID 属性	ORIGINATOR-ID 属性を指定します。	IPv4 アドレス形式	省略不可

【動作モード】

route-map 設定モード

【説明】

route-map に該当する経路情報の ORIGINATOR-ID 属性を設定します。

対象プロトコル：BGP

【実行例】

ORIGINATOR-ID 属性を設定します（ORIGINATOR-ID 属性：192.0.2.1）。

```
#configure terminal
(config)#route-map route-map-A permit 1
(config-rmap route-map-A permit 1)#set originator-id 192.0.2.1
```

【未設定時】

ORIGINATOR-ID 属性を設定しません。

9.1.27 set tag

【機能】

route-map に該当するタグ値の設定

【入力形式】

set tag <タグ値>

no set tag [<タグ値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
タグ値	タグ値を指定します。	0 ～ 4294967295	省略不可

【動作モード】

route-map 設定モード

【説明】

route-map に該当するタグ値を設定します。

対象プロトコル：OSPF

【実行例】

route-map に該当するタグ値を設定します（タグ値：10）。

```
#configure terminal
(config)#route-map route-map-A permit 1
(config-rmap route-map-A permit 1)#set tag 10
```

【未設定時】

タグ値を設定しません。

9.1.28 set weight

【機能】

weight 値の設定

【入力形式】

set weight <weight 値>

no set weight [<weight 値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
weight 値	weight 値を指定します。	0 ～ 65535	省略不可

【動作モード】

route-map 設定モード

【説明】

route-map に該当する経路情報の weight 値を設定します。

対象プロトコル：BGP

【実行例】

weight 値を設定します (weight 値 : 64)。

```
#configure terminal
(config)#route-map route-map-A permit 1
(config-rmap route-map-A permit 1)#set weight 64
```

【未設定時】

weight 値を設定しません。

第10章 アクセスリストの設定



この章では、アクセスリストの設定に関するコマンドについて説明します。

10.1 アクセスリスト／アクセスグループの設定

各種フィルタ機能では、アクセスリストが利用されます。

アクセスリストにパケットの種類を登録し、各フィルタコマンドで登録したアクセスリストを指定する形で設定を行います。

10.1.1 access-list

【機能】

SPI 登録 (spi) ／許可 (permit) ／拒否 (deny) の属性を与える設定

パケットの種類を登録を行います。ここで登録したものを各モジュールが参照することで、パケットフィルタリング、ルーティング相手の特定など、幅広く利用できます。

access-list 設定は常に基本設定モードで行われます。そのフォーマットは、access-list コマンドの次にくる数字（アクセスリスト番号）で変化します。

1-99,1300-1999,10000-19999,100000-199999	IPv4 標準設定
100-199,2000-2699,20000-29999,200000-299999	IPv4 拡張設定
3000-3999,30000-39999,300000-399999	IPv6 標準設定
4000-4999,40000-49999,400000-499999	IPv6 拡張設定
500-599,5000-5999,50000-59999,500000-599999	MAC アドレス設定

アクセスリストのエントリ消費量は、show traffic-manager network resources コマンドで確認できます。

10.1.2 access-list (IPv4 標準設定)

【機能】

SPI 登録 (spi) ／許可 (permit) ／拒否 (deny) の設定

【入力形式】

access-list <アクセスリスト番号> {spi | permit | deny} {any | <src-address> [<src-wildcard>]}

no access-list <アクセスリスト番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アクセスリスト番号	アクセスリスト番号を指定します。	-	省略不可
spi permit deny	SPI 登録／許可／拒否を指定します。	spi: SPI 登録 permit: 許可 deny: 拒否	
any <src-address>	送信元 IPv4 アドレスを指定します。	any: すべて src-address: IPv4 アドレス形式	
src-wildcard	送信元 IPv4 アドレスのワイルドカードを指定します。	IPv4 アドレス形式	ワイルドカードなし

【動作モード】

基本設定モード

【説明】

送信元 IPv4 アドレスを指定し、SPI 登録 (spi)／許可 (permit)／拒否 (deny) を設定します。アクセスリスト番号が同一の設定は、設定順にソートされます。

spi が指定されている場合は out 方向で指定された場合のみ有効となり、in 方向で指定されても無効となります。

【実行例】

IPv4 標準アクセスリストを設定します（アクセスリスト番号：1、permit、src-address：192.0.2.0、src-wildcard：0.0.0.255）。

```
#configure terminal
(config)#access-list 1 permit 192.0.2.0 0.0.0.255
```

10.1.3 access-list (IPv4 拡張設定)

【機能】

SPI 登録 (spi)／許可 (permit)／拒否 (deny) の設定

【入力形式】

```
access-list <アクセスリスト番号> {spi | permit | deny}
{<protocol-number> | <protocol-name>}
{any | host <src-address> | <src-address> [<src-wildcard>]}
[{eq | gt | lt} <port-number> | range <port-no-min> <port-no-max>]
{any | host <dst-address> | <dst-address> <dst-wildcard>}
[{eq | gt | lt} <port-number> | range <port-no-min> <port-no-max>]
[established] [<icmp-type> [<icmp-code>]] [precedence <precedence-value>]
[tos <tos-value>] [dscp <dscp-level>]
[fragments] [802.1p-priority <802.1p-priority>]

no access-list <アクセスリスト番号>
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アクセスリスト番号	アクセスリスト番号を指定します。	-	省略不可
spi permit deny	SPI 登録／許可／拒否を指定します。	spi: SPI 登録 permit: 許可 deny: 拒否	
<protocol-number> <protocol-name>	プロトコル番号／プロトコル名を指定します。	protocol-number: 0～255 protocol-name: ip, icmp, tcp, udp	
any host <src-address>	送信元 IPv4 アドレスを指定します。	any: すべて src-address: IPv4 アドレス形式	
src-wildcard	送信元 IPv4 アドレスのワイルドカードを指定します。	IPv4 アドレス形式	ワイルドカードなし
eq gt lt range	TCP または UDP 指定時のみ、 "eq"、"gt"、"lt"、"range" を指定できます。	eq: 等しい gt: より大きい (値は含まず) lt: より小さい (値は含まず) range: 以上から、以下まで (値は含む)	特定しない
<port-number> <port-no-min> port-no-max>	ポート番号を指定します。	<port-number> <port-no-min> <port-no-max>: 0～65535	
any host <dst-address>	宛先 IPv4 アドレスを指定します。	any: すべて dst-address: IPv4 アドレス形式	省略不可
dst-wildcard	宛先 IPv4 アドレスのワイルドカードを指定します。	IPv4 アドレス形式	ワイルドカードなし
established	establish 状態の TCP セッション上のパケットを指定します。	-	特定しない
icmp-type	icmp-type を指定します。	0～255	特定しない
icmp-code	icmp-code を指定します。	0～255	
precedence-value	Precedence 値を指定します。	0～7	特定しない
tos-value	TOS 値を指定します。	0～255	特定しない
dscp-level	DSCP 値を指定します。	0～63	
fragments	IP フラグメントパケットを指定します。	-	
802.1p-priority	802.1p-priority 値を指定します。	0～7	

【動作モード】

基本設定モード

【説明】

送信元 IPv4 アドレスと宛先 IPv4 アドレス（さらに必要であれば TCP または UDP のポート番号）を指定し、SPI 登録 (spi)／許可 (permit)／拒否 (deny) を設定します。アクセスリスト番号が同一の設定は、設定順にソートされます。

spi が指定されている場合は out 方向で指定された場合のみ有効となり、in 方向で指定されても無効となります。

【実行例】

IPv4 拡張アクセスリストを設定します（アクセスリスト番号：102、permit、protocol-name:tcp、src-address:any、dst-address:192.0.2.0、dst-wildcard:0.0.0.255、eq、port-number:25）。

```
#configure terminal
(config)#access-list 102 permit tcp any 192.0.2.0 0.0.0.255 eq 25
```

10.1.4 access-list (IPv6 標準設定)

【機能】

SPI 登録 (spi) / 許可 (permit) / 拒否 (deny) の設定

【入力形式】

access-list <アクセスリスト番号> {spi | permit | deny} {any | <src-prefix>}

no access-list <アクセスリスト番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アクセスリスト番号	アクセスリスト番号を指定します。	-	省略不可
spi permit deny	SPI 登録 / 許可 / 拒否を指定します。	spi: SPI 登録 permit: 許可 deny: 拒否	
any <src-prefix>	送信元 IPv6 プレフィックスを指定します。	any: すべて src-prefix: IPv6 アドレス形式	

【動作モード】

基本設定モード

【説明】

送信元 IPv6 プレフィックスを指定し、SPI 登録 (spi) / 許可 (permit) / 拒否 (deny) を設定します。アクセスリスト番号が同一の設定は、設定順にソートされます。

spi が指定されている場合は out 方向で指定された場合のみ有効となり、in 方向で指定されても無効となります。

【実行例】

IPv6 標準アクセスリストを設定します（アクセスリスト番号：3000、permit、src-prefix:2001e:db8::1/48）。

```
#configure terminal
(config)#access-list 3000 permit 2001:db8::1/48
```

10.1.5 access-list (IPv6 拡張設定)

【機能】

SPI 登録 (spi) / 許可 (permit) / 拒否 (deny) の設定

【入力形式】

access-list <アクセスリスト番号> {spi | permit | deny}

{<nexthead-number> | <nexthead-name>}

{any | <src-prefix>}

[{eq | gt | lt} <port-number> | range <port-no-min> <port-no-max>]

{any | <dst-prefix>}

[{eq | gt | lt} <port-number> | range <port-no-min> <port-no-max>]

[established] [<icmp-type> [<icmp-code>]] [traffic-class <0-255>]

[dscp <dscp-level>] [flow-label <0-1048575>] [fragments] [802.1p-priority <0-7>]

no access-list <アクセスリスト番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アクセスリスト番号	アクセスリスト番号を指定します。	-	省略不可
spi permit deny	SPI 登録 / 許可 / 拒否を指定します。	spi: SPI 登録 permit: 許可 deny: 拒否	
<nexthead-number> <nexthead-name>	プロトコル番号 / プロトコル名を指定します。	nexthead-number: 0 ~ 255 nexthead-name: ipv6, tcp, udp, icmp6	
any src-prefix	送信元 IPv6 プレフィックスを指定します。	any: すべて src-prefix: IPv6 アドレス形式	
eq gt lt range	TCP または UDP 指定時のみ、 "eq"、"gt"、"lt"、"range" を指定できます。	eq: 等しい gt: より大きい (値は含まず) lt: より小さい (値は含まず) range: 以上、以下まで (値は含む)	特定しない
<port-number> <port-no-min> <port-no-max>	ポート番号を指定します。	<port-number> <port-no-min> <port-no-max>: 0 ~ 65535	
any dst-prefix	宛先 IPv6 プレフィックスを指定します。	any: すべて dst-prefix: IPv6 アドレス形式	
established	establish 状態の TCP セッション上の パケットを指定します。	-	特定しない
icmp-type	icmp-type を指定します。	0 ~ 255	特定しない
icmp-code	icmp-code を指定します。	0 ~ 255	

パラメタ	設定内容	設定範囲	省略時
traffic-class	Traffic-Class 値を指定します。	0 ～ 255	特定しない
dscp-level	DSCP 値を指定します。	0 ～ 63	
flow-label	flow-label を指定します。	0 ～ 1048575	特定しない
fragments	IPv6 フラグメントパケットを指定します。	-	
802.1p-priority	802.1p priority 値を指定します。	0 ～ 7	

【動作モード】

基本設定モード

【説明】

送信元 IPv6 プレフィックスと宛先 IPv6 プレフィックス（さらに必要であれば TCP または UDP のポート番号）を指定し、SPI 登録 (spi) / 許可 (permit) / 拒否 (deny) を設定します。アクセスリスト番号が同一の設定は、設定順にソートされます。

spi が指定されている場合は out 方向で指定された場合のみ有効となり、in 方向で指定されても無効となります。

【実行例】

IPv6 拡張アクセスリストを設定します（アクセスリスト番号：4000、permit、protocol-name:tcp、src-prefix:2001:db8::1/48、dst-prefix:any、eq、port-no:23）。

```
#configure terminal
(config)#access-list 4000 permit tcp 2001:db8::1/48 any eq 23
```

10.1.6 access-list (MAC アドレス設定)

【機能】

許可 (permit) / 拒否 (deny) の設定

【入力形式】

access-list <アクセスリスト番号> {permit | deny} <src_mac> <dst_mac> [ether-type {<ether-type-value> | ip [<src-address> [<src-wildcard> <dst-address> [<dst-wildcard>]]] [tos <tos-value>] | ipv6 [traffic-class <traffic-class-value>]]]

no access-list <アクセスリスト番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アクセスリスト番号	アクセスリスト番号を指定します。	500 ～ 599、5000 ～ 5999、50000 ～ 59999、500000 ～ 599999	省略不可
permit deny	許可 / 拒否を指定します。	permit: 許可 deny: 拒否	省略不可

パラメタ	設定内容	設定範囲	省略時
src_mac	送信元 MAC アドレスを指定します。	any: すべて multicast: マルチキャスト MAC アドレス broadcast: ブロードキャスト MAC アドレス 0000.0000.0000 ~ ffff.ffff.ffff	省略不可
dst_mac	宛先 MAC アドレスを指定します。	any: すべて multicast: マルチキャスト MAC アドレス broadcast: ブロードキャスト MAC アドレス 0000.0000.0000 ~ ffff.ffff.ffff	省略不可
ether-type-value	イーサタイプフィールドの値を指定します。	0 ~ ffff ipv4(0x0800) ipv6(0x86dd)	すべてのイーサタイプフィールド
src-address	送信元 IPv4 アドレスを指定します。	IPv4 アドレス形式	すべての送信元アドレス
src-wildcard	送信元 IPv4 アドレスのワイルドカードを指定します。	IPv4 アドレス形式	ワイルドカードなし
dst-address	宛先 IPv4 アドレスを指定します。	IPv4 アドレス形式	すべての宛先アドレス
dst-wildcard	宛先 IPv4 アドレスのワイルドカードを指定します。	IPv4 アドレス形式	ワイルドカードなし
tos-value	IPv4 TOS 値を指定します。	0 ~ 255	特定しない
traffic-class-value	IPv6 TRAFFIC-CLASS 値を指定します。	0 ~ 255	特定しない

【動作モード】

基本設定モード

【説明】

送信元 MAC アドレスと宛先 MAC アドレスを指定し、許可 (permit) / 拒否 (deny) を設定します。

<src_mac> または <dst_mac> に ffff.ffff.ffff を指定すると、show access-lists コマンドでは broadcast と表示されます。

<src-wildcard> または <dst-wildcard> に 255.255.255.255 を指定すると、show access-lists コマンドでは、アドレスが any と表示されます。

【実行例】

MAC アドレス設定の access-list を設定します (アクセスリスト番号 : 500、deny、src_mac : any、dst_mac : broadcast)。

```
#configure terminal
(config)#access-list 500 deny any broadcast
```

10.1.7 access-list description

【機能】

アクセスリストの説明書き

【入力形式】

access-list <アクセスリスト番号> description <説明>

no access-list <アクセスリスト番号> [description [<説明>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アクセスリスト番号	アクセスリスト番号を指定します。	-	省略不可
説明	説明を指定します。	254 文字以内の WORD 型 (*1)	省略不可

*1) 文字の空白（スペース）は使用可能です。複数の空白（スペース）は 1 文字にまとめられます。また、最大 60 ワードまで設定できます。

【動作モード】

基本設定モード

【説明】

アクセスリストの説明書きを設定します。この説明書きは、データの中継には影響しません。

【実行例】

説明書きを設定します（アクセスリスト番号：1、説明：customer-A）。

```
#configure terminal
(config)#access-list 1 description customer-A
```

【未設定時】

説明書きは設定されません。

10.1.8 ip access-group

【機能】

受信時に適用するか／送信時に適用するかの設定

【入力形式】

ip access-group {<アクセスリスト番号>} {in | out} [<シーケンス番号>] [count]

no ip access-group {<アクセスリスト番号>} {in | out}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アクセスリスト番号	アクセスリスト番号を指定します。	-	省略不可
in out	受信時に適用するか／送信時に適用するかを指定します。	in: 受信時 out: 送信時	
シーケンス番号	検索順序を指定します。	1～1000000	アクセスリスト番号順
count	このフィルタが適用された回数をカウントする場合に指定します。	-	カウントしない

【動作モード】

gigaethernet インタフェース設定モード、gigaethernet サブインタフェース設定モード、tunnel インタフェース設定モード、trunk-channel インタフェース設定モード、trunk-channel サブインタフェース設定モード、USB Ethernet インタフェース設定モード

【説明】

access-list コマンドで指定したアクセスリストに対して、受信時に適用するか／送信時に適用するかを設定します。本コマンドは、telnet-server access-class、ftp-server access-class、ssh-server accessclass、dns-server access-class、snmp-server community コマンドによるフィルタリングより優先して動作します。

アクセスリストが input 側に設定されたインタフェースでは、アクセスリストにヒットしなかったトラフィックは拒絶します。

アクセスリストが output 側に設定されたインタフェースでは、アクセスリストにヒットしなかったトラフィックは許可します。

本コマンドは、service-policy コマンドによるポリシーより先に動作します。

count オプションを指定していない場合は、show access-lists statistics で統計情報が表示されません。

フィルタ／QoS／データコネク ト QoS／DVPN ACL／ポリシールーティングのクラシファイエントリはすべて共用です。各機能でエントリを使用していると、データコネク ト QoS のエントリが入らないことがあります。

【実行例】

受信時に適用するか／送信時に適用するかを設定します（アクセスリスト番号：1、in）。

```

【gigaethernet インタフェース設定モードの場合】
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#ip access-group 1 in

```

【未設定時】

アクセスリストが設定されていないインタフェースでは、全トラフィックを許可します。

10.1.9 ipv6 access-group

【機能】

受信時に適用するか／送信時に適用するかの設定

【入力形式】

```
ipv6 access-group <アクセスリスト番号> {in | out} [<シーケンス番号>] [count]
```

```
no ipv6 access-group <アクセスリスト番号> {in | out}
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アクセスリスト番号	アクセスリスト番号を指定します。	-	省略不可
in out	受信時に適用するか／送信時に適用するかを指定します。	in: 受信時 out: 送信時	
シーケンス番号	検索順序を指定します。	1～1000000	アクセスリスト番号順
count	このフィルタが適用された回数をカウントする場合に指定します。	-	カウントしない

【動作モード】

gigaethernet インタフェース設定モード、gigaethernet サブインタフェース設定モード、tunnel インタフェース設定モード、trunk-channel インタフェース設定モード、trunk-channel サブインタフェース設定モード、USB Ethernet インタフェース設定モード

【説明】

access-list コマンドで指定したアクセスリストに対して、受信時に適用するか／送信時に適用するかを設定します。本コマンドは、telnet-server access-class、ftp-server access-class、ssh-server accessclass、dns-server access-class、snmp-server community コマンドによるフィルタリングより優先して動作します。

アクセスリストが input 側に設定されたインタフェースでは、アクセスリストにヒットしなかったトラフィックは拒絶します。

アクセスリストが output 側に設定されたインタフェースでは、アクセスリストにヒットしなかったトラフィックは許可します。

本コマンドは、service-policy コマンドによるポリシーより先に動作します。

count オプションを指定していない場合は、show access-lists statistics で統計情報が表示されません。

フィルタ／QoS／データコネクト QoS／DVPN ACL／ポリシールーティングのクラシファイエントリはすべて共用です。各機能でエントリを使用していると、データコネクト QoS のエントリが入らないことがあります。

【実行例】

受信時に適用するか／送信時に適用するかを設定します（アクセスリスト番号：4000、in）。

```
【gigaethernet インタフェース設定モードの場合】
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#ipv6 access-group 4000 in
```

【未設定時】

アクセスリストが設定されていないインタフェースでは、全トラフィックを許可します。

10.1.10 ip access-group default spi

【機能】

インタフェースごとの IPv4 パケットに対する SPI の動作の設定

【入力形式】

ip access-group default spi

no ip access-group default spi

【動作モード】

gigaethernet インタフェース設定モード、gigaethernet サブインタフェース設定モード、tunnel インタフェース設定モード、trunk-channel インタフェース設定モード、trunk-channel サブインタフェース設定モード、USB Ethernet インタフェース設定モード

【説明】

インタフェースにて送信する IPv4 パケットが、どの IPv4 フィルタリングテーブルにも一致しなかった場合に、そのパケットに対して SPI を動作（SPI テーブルエントリを作成して、パケットを送信）する場合に設定します。

【実行例】

どの IPv4 フィルタリングテーブルにも一致しなかった場合に、そのパケットに対して SPI を動作させます。

```
【gigaethernet インタフェース設定モードの場合】
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#ip access-group default spi
```

【未設定時】

未設定のインタフェースから送信する IPv4 パケットに対して、SPI は動作しません。

access-list にて SPI の指定があれば、その設定に従います。

10.1.11 ipv6 access-group default spi

【機能】

インタフェースごとの IPv6 パケットに対する SPI の動作の設定

【入力形式】

ipv6 access-group default spi

no ipv6 access-group default spi

【動作モード】

gigaethernet インタフェース設定モード、gigaethernet サブインタフェース設定モード、tunnel インタフェース設定モード、trunk-channel インタフェース設定モード、trunk-channel サブインタフェース設定モード、USB Ethernet インタフェース設定モード

【説明】

インタフェースにて送信する IPv6 パケットが、どの IPv6 フィルタテーブルにも一致しなかった場合に、そのパケットに対して SPI を動作（SPI テーブルエントリを作成して、パケットを送信）する場合に設定します。

【実行例】

どの IPv6 フィルタリングテーブルにも一致しなかった場合に、そのパケットに対して SPI を動作させます。

```
【gigaetherne インタフェース設定モードの場合】
#configure terminal
(config)#interface gigaetherne 1/1
(config-if-ge 1/1)#ipv6 access-group default spi
```

【未設定時】

未設定のインタフェースから送信する IPv6 パケットに対して、SPI は動作しません。
access-list にて SPI の指定があれば、その設定に従います。

10.1.12 ip access-group spi ftp-data enable

【機能】

IPv4 通信に対するダイナミックフィルタリング機能の設定

【入力形式】

```
ip access-group spi ftp-data enable
no ip access-group spi ftp-data enable
```

【動作モード】

gigaetherne インタフェース設定モード、gigaetherne サブインタフェース設定モード、tunnel インタフェース設定モード、trunk-channel インタフェース設定モード、trunk-channel サブインタフェース設定モード、USB Ethernet インタフェース設定モード

【説明】

設定したインタフェースにおいて、IPv4 通信に対してダイナミックフィルタリング機能を有効にします。
ダイナミックフィルタリング機能とは、FTP 通信をフィルタリングで透過する場合において、コントロールコネクションの透過設定を行うとデータコネクションの透過ルールを自動的に追加する機能です。

【実行例】

IPv4 通信に対してダイナミックフィルタリング機能を有効にします。

```
【gigaetherne インタフェース設定モードの場合】
#configure terminal
(config)#interface gigaetherne 1/1
(config-if-ge 1/1)#ip access-group spi ftp-data enable
```

【未設定時】

設定したインタフェースにおいて、IPv4 通信に対してダイナミックフィルタリング機能は動作しません。

10.1.13 ipv6 access-group spi ftp-data enable

【機能】

IPv6 通信に対するダイナミックフィルタリング機能の設定

【入力形式】

ipv6 access-group spi ftp-data enable

no ipv6 access-group spi ftp-data enable

【動作モード】

gigaethernet インタフェース設定モード、gigaethernet サブインタフェース設定モード、tunnel インタフェース設定モード、trunk-channel インタフェース設定モード、trunk-channel サブインタフェース設定モード、USB Ethernet インタフェース設定モード

【説明】

設定したインタフェースにおいて、IPv6 通信に対してダイナミックフィルタリング機能を有効にします。ダイナミックフィルタリング機能とは、FTP 通信をフィルタリングで透過する場合において、コントロールコネクションの透過設定を行うとデータコネクションの透過ルールを自動的に追加する機能です。

【実行例】

IPv6 通信に対してダイナミックフィルタリング機能を有効にします。

```
【gigaethernet インタフェース設定モードの場合】
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#ipv6 access-group spi ftp-data enable
```

【未設定時】

設定したインタフェースにおいて、IPv6 通信に対してダイナミックフィルタリング機能は動作しません。

10.1.14 ip access-group spi timeout

【機能】

IPv4 パケット中継時の SPI の無通信監視時間の設定

【入力形式】

ip access-group spi timeout [tcp-syn <SYN 無通信監視時間>] [tcp-fin <FIN 無通信監視時間>] [tcp-idle <TCP 無通信監視時間>] [udp-idle <UDP 無通信監視時間>] [icmp <ICMP 無通信監視時間>] [others <無通信監視時間>]

no ip access-group spi timeout [tcp-syn <SYN 無通信監視時間>] [tcp-fin <FIN 無通信監視時間>] [tcp-idle <TCP 無通信監視時間>] [udp-idle <UDP 無通信監視時間>] [icmp <ICMP 無通信監視時間>] [others <無通信監視時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
SYN 無通信監視時間	TCP の SYN フラグが設定されたパケットの無通信監視時間（単位：秒）を指定します。	5～86400	省略不可
FIN 無通信監視時間	TCP の FIN フラグが設定されたパケットの無通信監視時間（単位：秒）を指定します。	5～86400	省略不可
TCP 無通信監視時間	TCP の SYN フラグ、FIN フラグ以外の TCP パケットの無通信監視時間（単位：秒）を指定します。	5～86400	省略不可
UDP 無通信監視時間	UDP パケットの無通信監視時間（単位：秒）を指定します。	5～86400	省略不可
ICMP 無通信監視時間	ICMP パケットの無通信監視時間（単位：秒）を指定します。	5～86400	省略不可
無通信監視時間	TCP／UDP／ICMP 以外のパケットの無通信監視時間（単位：秒）を指定します。	5～86400	省略不可

【動作モード】

gigaethernet インタフェース設定モード、gigaethernet サブインタフェース設定モード、tunnel インタフェース設定モード、trunk-channel インタフェース設定モード、trunk-channel サブインタフェース設定モード、USB Ethernet インタフェース設定モード

【説明】

IPv4 パケット中継時の SPI の無通信監視時間（単位：秒）を設定します。

無通信監視時間経過後、SPI テーブルエントリを解放します。

【実行例】

IPv4 中継時の SPI の無通信監視時間を設定します（SYN 無通信監視時間：60 秒）。

```

【gigaethernet インタフェース設定モードの場合】
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#ip access-group spi timeout tcp-syn 60

```

【未設定時】

無通信監視時間は、以下のとおりとなります。

SYN 無通信監視時間 : 60 秒

FIN 無通信監視時間 : 60 秒

TCP 無通信監視時間 : 3600 秒

UDP 無通信監視時間 : 300 秒

ICMP 無通信監視時間 : 60 秒

TCP／UDP／ICMP 以外の無通信監視時間：86400 秒

10.1.15 ipv6 access-group spi timeout

【機能】

IPv6 パケット中継時の SPI の無通信監視時間を設定

【入力形式】

```
ipv6 access-group spi timeout [tcp-syn <SYN 無通信監視時間>] [tcp-fin <FIN 無通信監視時間>] [tcp-idle <TCP 無通信監視時間>] [udp-idle <UDP 無通信監視時間>] [icmp <ICMP 無通信監視時間>] [others <無通信監視時間>]
```

```
no ipv6 access-group spi timeout [tcp-syn <SYN 無通信監視時間>] [tcp-fin <FIN 無通信監視時間>] [tcp-idle <TCP 無通信監視時間>] [udp-idle <UDP 無通信監視時間>] [icmp <ICMP 無通信監視時間>] [others <無通信監視時間>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
SYN 無通信監視時間	TCP の SYN フラグが設定されたパケットの無通信監視時間（単位：秒）を指定します。	5～86400	省略不可
FIN 無通信監視時間	TCP の FIN フラグが設定されたパケットの無通信監視時間（単位：秒）を指定します。	5～86400	省略不可
TCP 無通信監視時間	TCP の SYN フラグ、FIN フラグ以外の TCP パケットの無通信監視時間（単位：秒）を指定します。	5～86400	省略不可
UDP 無通信監視時間	UDP パケットの無通信監視時間（単位：秒）を指定します。	5～86400	省略不可
ICMP 無通信監視時間	ICMP パケットの無通信監視時間（単位：秒）を指定します。	5～86400	省略不可
無通信監視時間	TCP／UDP／ICMP 以外のパケットの無通信監視時間（単位：秒）を指定します。	5～86400	省略不可

【動作モード】

gigaethernet インタフェース設定モード、gigaethernet サブインタフェース設定モード、tunnel インタフェース設定モード、trunk-channel インタフェース設定モード、trunk-channel サブインタフェース設定モード、USB Ethernet インタフェース設定モード

【説明】

IPv6 中継時の SPI の無通信監視時間（単位：秒）を設定します。

無通信監視時間経過後、SPI テーブルエントリを解放します。

【実行例】

IPv6 中継時の SPI の無通信監視時間を設定します（SYN 無通信監視時間：60 秒）。

```
【gigaethernet インタフェース設定モードの場合】
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#ipv6 access-group spi timeout tcp-syn 60
```

【未設定時】

無通信監視時間は、以下のとおりとなります。

SYN 無通信監視時間 : 60 秒

FIN 無通信監視時間 : 60 秒

TCP 無通信監視時間 : 3600 秒

UDP 無通信監視時間 : 300 秒

ICMP 無通信監視時間 : 60 秒

TCP／UDP／ICMP 以外の無通信監視時間：86400 秒

10.1.16 ip spi entry tcp-syn-timeout

【機能】

TCP の SYN フラグが設定された IPv4 パケットの SPI の無通信監視時間の設定

【入力形式】

ip spi entry tcp-syn-timeout <無通信監視時間>

no ip spi entry tcp-syn-timeout [<無通信監視時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
無通信監視時間	TCP の SYN フラグが設定されたパケットの無通信監視時間（単位：秒）を指定します。	5～86400	省略不可

【動作モード】

基本設定モード

【説明】

TCP の SYN フラグが設定された IPv4 パケットの SPI の無通信監視時間（単位：秒）を設定します。

インタフェースに ip access-group spi timeout コマンドによる設定がある場合は、そちらが優先されます。

無通信監視時間経過後、SPI テーブルエントリを解放します。

【実行例】

TCP の SYN フラグが設定された IPv4 パケットの SPI の無通信監視時間を設定します（無通信監視時間：600 秒）。

```
#configure terminal
(config)#ip spi entry tcp-syn-timeout 600
```

【未設定時】

無通信監視時間は 60 秒となります。

10.1.17 ipv6 spi entry tcp-syn-timeout

【機能】

TCP の SYN フラグが設定された IPv6 パケットの SPI の無通信監視時間の設定

【入力形式】

ipv6 spi entry tcp-syn-timeout <無通信監視時間>

no ipv6 spi entry tcp-syn-timeout [<無通信監視時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
無通信監視時間	TCP の SYN フラグが設定されたパケットの無通信監視時間（単位：秒）を指定します。	5～86400	省略不可

【動作モード】

基本設定モード

【説明】

TCP の SYN フラグが設定された IPv6 パケットの SPI の無通信監視時間（単位：秒）を設定します。

インタフェースに `ipv6 access-group spi timeout` コマンドによる設定がある場合は、そちらが優先されます。

無通信監視時間経過後、SPI テーブルエントリを解放します。

【実行例】

TCP の SYN フラグが設定された IPv6 パケットの SPI の無通信監視時間を設定します（無通信監視時間：600 秒）。

```
#configure terminal
(config)#ipv6 spi entry tcp-syn-timeout 600
```

【未設定時】

無通信監視時間は 60 秒となります。

10.1.18 ip spi entry tcp-fin-timeout

【機能】

TCP の FIN フラグが設定された IPv4 パケットの SPI の無通信監視時間の設定

【入力形式】

`ip spi entry tcp-fin-timeout <無通信監視時間>`

`no ip spi entry tcp-fin-timeout [<無通信監視時間>]`

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
無通信監視時間	TCP の FIN フラグが設定されたパケットの SPI の無通信監視時間（単位：秒）を指定します。	5～86400	省略不可

【動作モード】

基本設定モード

【説明】

TCP の FIN フラグが設定された IPv4 パケットの SPI の無通信監視時間（単位：秒）を設定します。

インタフェースに `ip access-group spi timeout` コマンドによる設定がある場合は、そちらが優先されます。

無通信監視時間経過後、SPI テーブルエントリを解放します。

【実行例】

TCP の FIN フラグが設定された IPv4 パケットの SPI の無通信監視時間を設定します（無通信監視時間：600 秒）。

```
#configure terminal
(config)#ip spi entry tcp-fin-timeout 600
```

【未設定時】

無通信監視時間は 60 秒となります。

10.1.19 ipv6 spi entry tcp-fin-timeout

【機能】

TCP の FIN フラグが設定された IPv6 パケットの SPI の無通信監視時間の設定

【入力形式】

ipv6 spi entry tcp-fin-timeout <無通信監視時間>

no ipv6 spi entry tcp-fin-timeout [<無通信監視時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
無通信監視時間	TCP の FIN フラグの TCP パケットの無通信監視時間（単位：秒）を指定します。	5～86400	省略不可

【動作モード】

基本設定モード

【説明】

TCP の FIN フラグが設定された IPv6 パケットの SPI の無通信監視時間（単位：秒）を設定します。

インタフェースに ipv6 access-group spi timeout コマンドによる設定がある場合は、そちらが優先されます。

無通信監視時間経過後、SPI テーブルエントリを解放します。

【実行例】

TCP の FIN フラグが設定された IPv6 パケットの SPI の無通信監視時間を設定します（無通信監視時間：600 秒）。

```
#configure terminal
(config)#ipv6 spi entry tcp-fin-timeout 600
```

【未設定時】

無通信監視時間は 60 秒となります。

10.1.20 ip spi entry tcp-idle-timeout

【機能】

TCP パケット (IPv4) の SPI の無通信監視時間の設定

【入力形式】

ip spi entry tcp-idle-timeout <無通信監視時間>

no ip spi entry tcp-idle-timeout [<無通信監視時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
無通信監視時間	TCP パケットの無通信監視時間（単位：秒）を指定します。	5～86400	省略不可

【動作モード】

基本設定モード

【説明】

TCP パケット (IPv4) の SPI の無通信監視時間（単位：秒）を設定します。

インタフェースに ip access-group spi timeout コマンドによる設定がある場合は、そちらが優先されます。

無通信監視時間経過後、SPI テーブルエントリを解放します。

【実行例】

TCP パケットの SPI の無通信監視時間を設定します（無通信監視時間：600 秒）。

```
#configure terminal
(config)#ip spi entry tcp-idle-timeout 600
```

【未設定時】

無通信監視時間は 3600 秒となります。

10.1.21 ipv6 spi entry tcp-idle-timeout

【機能】

TCP パケット (IPv6) の SPI の無通信監視時間

【入力形式】

ipv6 spi entry tcp-idle-timeout <無通信監視時間>

no ipv6 spi entry tcp-idle-timeout [<無通信監視時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
無通信監視時間	TCP パケットの無通信監視時間（単位：秒）を指定します。	5～86400	省略不可

【動作モード】

基本設定モード

【説明】

TCP パケット (IPv6) の SPI の無通信監視時間（単位：秒）を設定します。

インタフェースに ipv6 access-group spi timeout コマンドによる設定がある場合は、そちらが優先されます。

無通信監視時間経過後、SPI テーブルエントリを解放します。

【実行例】

TCP パケットの SPI の無通信監視時間を設定します（無通信監視時間：600 秒）。

```
#configure terminal
(config)#ipv6 spi entry tcp-idle-timeout 600
```

【未設定時】

無通信監視時間は 3600 秒となります。

10.1.22 ip spi entry udp-idle-timeout

【機能】

UDP パケット (IPv4) の SPI の無通信監視時間の設定

【入力形式】

ip spi entry udp-idle-timeout <無通信監視時間>

no ip spi entry udp-idle-timeout [<無通信監視時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
無通信監視時間	UDP パケットの無通信監視時間（単位：秒）を指定します。	5～86400	省略不可

【動作モード】

基本設定モード

【説明】

UDP パケット (IPv4) の SPI の無通信監視時間（単位：秒）を設定します。

インタフェースに ip access-group spi timeout コマンドによる設定がある場合は、そちらが優先されます。

無通信監視時間経過後、SPI テーブルエントリを解放します。

【実行例】

UDP パケット (IPv4) の SPI の無通信監視時間を設定します（無通信監視時間：600 秒）。

```
#configure terminal
(config)#ip spi entry udp-idle-timeout 600
```

【未設定時】

無通信監視時間は 300 秒となります。

10.1.23 ipv6 spi entry udp-idle-timeout

【機能】

UDP パケット (IPv6) の SPI の無通信監視時間の設定

【入力形式】

ipv6 spi entry udp-idle-timeout <無通信監視時間>

no ipv6 spi entry udp-idle-timeout [<無通信監視時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
無通信監視時間	UDP パケットの無通信監視時間（単位：秒）を指定します。	5～86400	省略不可

【動作モード】

基本設定モード

【説明】

UDP パケット (IPv6) の SPI の無通信監視時間（単位：秒）を設定します。

インタフェースに ipv6 access-group spi timeout コマンドによる設定がある場合は、そちらが優先されます。

無通信監視時間経過後、SPI テーブルエントリを解放します。

【実行例】

UDP パケット (IPv6) の SPI の無通信監視時間を設定します（無通信監視時間：600 秒）。

```
#configure terminal
(config)#ipv6 spi entry udp-idle-timeout 600
```

【未設定時】

無通信監視時間は 300 秒となります。

10.1.24 ip spi entry icmp-timeout

【機能】

ICMP パケットの SPI の無通信監視時間の設定

【入力形式】

ip spi entry icmp-timeout <無通信監視時間>

no ip spi entry icmp-timeout [<無通信監視時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
無通信監視時間	ICMP パケットの無通信監視時間（単位：秒）を指定します。	5～86400	省略不可

【動作モード】

基本設定モード

【説明】

ICMP パケットの SPI の無通信監視時間（単位：秒）を設定します。

インタフェースに ip access-group spi timeout コマンドによる設定がある場合は、そちらが優先されます。

無通信監視時間経過後、SPI テーブルエントリを解放します。

【実行例】

ICMP パケット (IPv4) の SPI の無通信監視時間を設定します（無通信監視時間：600 秒）。

```
#configure terminal
(config)#ip spi entry icmp-timeout 600
```

【未設定時】

無通信監視時間は 60 秒となります。

10.1.25 ipv6 spi entry icmp-timeout

【機能】

ICMPv6 パケット中継時の SPI の無通信監視時間の設定

【入力形式】

ipv6 spi entry icmp-timeout <無通信監視時間>

no ipv6 spi entry icmp-timeout [<無通信監視時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
無通信監視時間	ICMPv6 パケットの無通信監視時間（単位：秒）を指定します。	5～86400	省略不可

【動作モード】

基本設定モード

【説明】

ICMPv6 パケットの SPI の無通信監視時間（単位：秒）を設定します。

インタフェースに `ipv6 access-group spi timeout` コマンドによる設定がある場合は、そちらが優先されます。

無通信監視時間経過後、SPI テーブルエントリを解放します。

【実行例】

ICMPv6 パケットの SPI の無通信監視時間を設定します（無通信監視時間：600 秒）。

```
#configure terminal
(config)#ipv6 spi entry icmp-timeout 600
```

【未設定時】

無通信監視時間は 60 秒となります。

10.1.26 ip spi entry others-timeout

【機能】

TCP / UDP / ICMP 以外の IPv4 パケットの SPI の無通信監視時間の設定

【入力形式】

`ip spi entry others-timeout <無通信監視時間>`

`no ip spi entry others-timeout [<無通信監視時間>]`

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
無通信監視時間	TCP / UDP / ICMP 以外のパケットの無通信監視時間（単位：秒）を指定します。	5～86400	省略不可

【動作モード】

基本設定モード

【説明】

TCP / UDP / ICMP 以外の IPv4 パケットの SPI の無通信監視時間（単位：秒）を指定します。

インタフェースに `ip access-group spi timeout` コマンドによる設定がある場合は、そちらが優先されます。

無通信監視時間経過後、SPI テーブルエントリを解放します。

【実行例】

TCP / UDP / ICMP 以外の IPv4 パケットの SPI の無通信監視時間を設定します（無通信監視時間：600 秒）。

```
#configure terminal
(config)#ip spi entry others-timeout 600
```

【未設定時】

無通信監視時間は 86400 秒となります。

10.1.27 ipv6 spi entry others-timeout

【機能】

TCP / UDP / ICMP 以外の IPv6 パケットの SPI の無通信監視時間の設定

【入力形式】

ipv6 spi entry others-timeout <無通信監視時間>

no ipv6 spi entry others-timeout [<無通信監視時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
無通信監視時間	TCP / UDP / ICMPv6 以外のパケットの無通信監視時間（単位：秒）を指定します。	5～86400	省略不可

【動作モード】

基本設定モード

【説明】

TCP / UDP / ICMPv6 以外の IPv6 パケットの SPI の無通信監視時間（単位：秒）を指定します。

インタフェースに ipv6 access-group spi timeout コマンドによる設定がある場合は、そちらが優先されます。

無通信監視時間経過後、SPI テーブルエントリを解放します。

【実行例】

TCP / UDP / ICMPv6 以外の IPv6 パケットの SPI の無通信監視時間を設定します（無通信監視時間：600 秒）。

```
#configure terminal
(config)#ipv6 spi entry others-timeout 600
```

【未設定時】

無通信監視時間は 86400 秒となります。

10.1.28 mac access-group

【機能】

受信時に適用するか／送信時に適用するかの設定

【入力形式】

mac access-group <アクセスリスト番号> { in | out } [<シーケンス番号> [count]]

no mac access-group <アクセスリスト番号> { in | out }

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アクセスリスト番号	アクセスリスト番号を指定します。	500～599、 5000～5999、 50000～59999、 500000～599999	省略不可
in out	受信時に適用するか／送信時に適用するかを指定します。	in：受信時 out：送信時	省略不可
シーケンス番号	検索順序を指定します。	1～1000000	アクセスリスト番号順
count	このフィルタが適用された回数をカウントする場合に指定します。	-	カウントしない

【動作モード】

gigaethernet インタフェース設定モード、gigaethernet サブインタフェース設定モード、tunnel インタフェース設定モード（EtherIP と L2TPv3 のみ）、trunk-channel インタフェース設定モード、trunk-channel サブインタフェース設定モード

【説明】

access-list コマンド（MAC アドレス設定）で指定したアクセスリストに対して、受信時に適用するか／送信時に適用するかを設定します。

シーケンス番号は service-policy コマンドと共有しており、フィルタリングとサービスポリシーで任意の検索順序を指定できます。

count オプションを指定していない場合は、show access-lists statistics で統計情報が表示されません。

【実行例】

受信時に適用するか／送信時に適用するかを設定します（アクセスリスト番号：500、in）。

```

【gigaethernet インタフェース設定モードの場合】
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)# mac access-group 500 in

```

【未設定時】

アクセスリストが設定されていないインタフェースでは、全トラフィックを許可します。

本コマンドが input に設定されたインタフェースでは、アクセスリストにヒットしなかった L2 中継パケットは拒絶されます。

一方、output に設定されたインタフェースでは、アクセスリストにヒットしなかった L2 中継パケットは許可されます。

第11章 IPv4 の設定



この章では、IPv4 の設定に関するコマンドについて説明します。

11.1	ARP キャッシュの設定	402
11.2	DNS の設定	406
11.3	ICMP の設定	408
11.4	アドレスプールの設定 (IPv4)	410
11.5	IPv4 プレフィックスリストの設定	411
11.6	IPv4 スタティックルートの設定	414
11.7	IPv4 インタフェースアドレスの設定	416
11.8	Proxy-ARP の設定	417
11.9	送信元 IPv4 アドレスの設定	418
11.10	DHCPv4 クライアント／サーバ／リレーエージェント機能設定	419

11.1 ARP キャッシュの設定

11.1.1 arp

【機能】

ARP エントリの登録

【入力形式】

arp <IPv4 アドレス> <MAC アドレス> <インタフェース名> <インタフェース番号>

no arp <IPv4 アドレス> [<MAC アドレス> <インタフェース名> <インタフェース番号>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
IPv4 アドレス	IPv4 アドレスを指定します。	IPv4 アドレス形式	省略不可
MAC アドレス	MAC アドレスを指定します。	HHHH.HHHH.HHHH 型式	
インタフェース名	インタフェース名を指定します。	-	
インタフェース番号	インタフェース番号を指定します。	-	

【動作モード】

基本設定モード

【説明】

ARP エントリを登録します。

【実行例】

ARP エントリを登録します (IPv4 アドレス：192.0.2.1、MAC アドレス：2ed4:4401:2345、インタフェース名：gigaetherent、インタフェース番号：1/1)。

```
#configure terminal
(config)#arp 192.0.2.1 2ed4.4401.2345 gigaetherent 1/1
```

【未設定時】

ARP エントリを登録しません。

11.1.2 ip arp packet-hold

【機能】

パケット数の設定

【入力形式】

ip arp packet-hold <装置最大数> <1 エントリ最大数>

no ip arp packet-hold [<装置最大数> <1 エントリ最大数>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
装置最大数	装置の最大数を指定します。	1～2048	省略不可
1 エントリ最大数	1 エントリの最大数を指定します。	1～32	

【動作モード】

基本設定モード

【説明】

ARP 解決中に滞留させるパケット数を設定します。

【実行例】

ARP 解決中に滞留させるパケット数を設定します（装置最大数：1024、1 エントリ最大数：16）。

```
#configure terminal
(config)#ip arp packet-hold 1024 16
```

【未設定時】

以下の値で動作します。

装置最大数： 2048

1 エントリ最大数： 32

11.1.3 ip arp polling disable

【機能】

ARP の維持のためのポーリングの送信の停止

【入力形式】

ip arp polling disable

no ip arp polling disable

【動作モード】

基本設定モード

【説明】

本装置は、ARP 解決済みのネイバーに対し、ARP の維持を目的とし、ポーリングを行うことがありますが、そのポーリングの送信を停止します。

ARP 解決済みのネイバー宛に通信が発生しているとき、または ARP 解決済みのネイバー向きの経路が存在しているとき、ポーリングを行います。

【実行例】

ARP の維持のためのポーリングの送信を停止します。

```
#configure terminal
(config)#ip arp polling disable
```

【未設定時】

ARP 解決済みのネイバーに対し、ポーリングを行うことがあります。

11.1.4 ip arp pre-solution disable

【機能】

経路登録時ゲートウェイに対する ARP リクエストの送信の抑制

【入力形式】

ip arp pre-solution disable

no ip arp pre-solution disable

【動作モード】

基本設定モード

【説明】

本装置は、経路登録時にゲートウェイに対し ARP リクエストを送信することがありますが、その送信を停止します。

【実行例】

経路登録時ゲートウェイに対する ARP リクエストの送信を抑制します。

```
#configure terminal
(config)# ip arp pre-solution disable
```

【未設定時】

経路登録時にゲートウェイに対し ARP リクエストを送信することがあります。

11.1.5 ip arp max-request

【機能】

ARP リクエストの最大送信回数の設定

【入力形式】

ip arp max-request <ARP リクエスト最大送信回数>

no ip arp max-request [<ARP リクエスト最大送信回数>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ARP リクエスト最大送信回数	ARP リクエスト最大送信回数を指定します。	1～30	省略不可

【動作モード】

基本設定モード

【説明】

ARP リクエストの最大送信回数を設定します。

【実行例】

ARP リクエストの最大送信回数を設定します (ARP リクエスト最大送信回数：15)。

```
#configure terminal
(config)#ip arp max-request 15
```

【未設定時】

ARP リクエスト最大送信回数は5回で動作します。

11.2 DNS の設定

11.2.1 ip domain-name

【機能】

補完するドメイン名の設定

【入力形式】

ip domain-name <ドメイン名>

no ip domain-name <ドメイン名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ドメイン名	ドメイン名を指定します。	254 文字以内の WORD 型	省略不可

【動作モード】

基本設定モード

【説明】

補完するドメイン名を設定します。

【実行例】

補完するドメイン名を設定します（ドメイン名：example.com）。

```
#configure terminal
(config)#ip domain-name example.com
```

【未設定時】

ドメイン名を登録しません。

11.2.2 ip host

【機能】

ホスト名と IPv4 アドレスの登録

【入力形式】

ip host <ホスト名> <IPv4 アドレス>

no ip host <ホスト名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ホスト名	ホスト名を指定します。	64 文字以内の WORD 型	省略不可
IPv4 アドレス	IPv4 アドレスを指定します。	IPv4 アドレス形式	

【動作モード】

基本設定モード

【説明】

ホスト名と IPv4 アドレスを登録します。

【実行例】

ホスト名と IPv4 アドレスを登録します（ホスト名：host-A、IPv4 アドレス：192.0.2.1）。

```
#configure terminal
(config)#ip host host-A 192.0.2.1
```

【未設定時】

ホスト名と IPv4 アドレスを登録しません。

11.3 ICMP の設定

11.3.1 ip icmp disable-sending-errors

【機能】

ICMP エラーを送信しない ICMP タイプの設定

【入力形式】

ip icmp disable-sending-errors [<ICMP タイプ>]

no ip icmp disable-sending-errors [<ICMP タイプ>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ICMP タイプ	ICMP エラーを送信しない ICMP タイプを指定します。 複数指定が可能です。	port-unreach: Unreach(Port) unreach: ICMP Unreach (Need fragment を除く) ttl-exceeded:TTL Exceeded redirect:Redirect	echo/ reply,unreach(Need fragment) を除く ICMP エラーの送信をしない

【動作モード】

基本設定モード、management インタフェース設定モード、port-channel インタフェース設定モード、
tunnel インタフェース設定モード

【説明】

ICMP エラーを送信しない ICMP タイプを設定します。

【実行例】

ICMP エラーを送信しない ICMP タイプを設定します。

```
【基本設定モードの場合】
#configure terminal
(config)#ip icmp disable-sending-errors
```

【未設定時】

すべての ICMP エラーを送信します。

11.3.2 ip icmp source

【機能】

ICMP 送信の際の送信元アドレスの設定

【入力形式】

```
ip icmp [vrf <VRF 名>] source {interface <インタフェース名> <インタフェース番号> | address <送信元  
アドレス>}
```

```
no ip icmp [vrf <VRF 名>] source [interface <インタフェース名> <インタフェース番号> | address <送信  
元アドレス>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VRF 名	VRF 名を指定します。	63 文字以内の WORD 型	VRF を指定しない
インタフェース名	送信元アドレスとして使用するインタフェース名を指定します。	-	省略不可
インタフェース番号	送信元アドレスとして使用するインタフェース番号を指定します。	-	
送信元アドレス	送信元アドレスとして使用するアドレスを指定します。	IPv4 アドレス形式	

【動作モード】

基本設定モード

【説明】

ICMP 送信の際の送信元アドレスを設定します。

【実行例】

ICMP 送信の際の送信元アドレスを設定します（インタフェース名：port-channel、インタフェース番号：1）。

```
#configure terminal
(config)#ip icmp source interface port-channel 1
```

【未設定時】

送信元アドレスは送信インタフェースのアドレスで動作します。

11.4 アドレスプールの設定 (IPv4)

11.4.1 ip local pool

【機能】

IPsec や L2TP/PPP により通知するアドレス範囲の設定

【入力形式】

ip local pool <アドレスプール名> <割り当て開始アドレス> <割り当て最終アドレス>

no ip local pool <アドレスプール名> <割り当て開始アドレス> <割り当て最終アドレス>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アドレスプール名	アドレスプール名を指定します。	63 文字以内の CDATA 型	省略不可
割り当て開始アドレス	Mode-config/ConfigPayload で通知する IPv4 アドレスの割り当て開始アドレスを指定します。	IPv4 アドレス形式	
割り当て最終アドレス	Mode-config/ConfigPayload で通知する IPv4 アドレスの割り当て最終アドレスを指定します。	IPv4 アドレス形式	

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

IPsec(Mode-config/Config Payload) により通知するアドレス範囲を設定します。本設定は、設定順にソートされます。

【実行例】

IPsec(Mode-config/Config Payload) により通知するアドレス範囲を設定します (アドレスプール名 : pool-A、割り当て開始アドレス : 192.0.2.1、割り当て最終アドレス : 192.0.2.16)。

```
#configure terminal
(config)#ip local pool pool-A 192.0.2.1 192.0.2.16
```

【未設定時】

IPv4 アドレス割り当てを行いません。

11.5 IPv4 プレフィックスリストの設定

11.5.1 ip prefix-list

【機能】

IPv4 プレフィックスリスト情報の設定

【入力形式】

```
ip prefix-list <プレフィックスリスト名> seq <シーケンス番号> {permit | deny} [<プレフィックス> [ge
<0-32>] [le <0-32>] | any]
```

```
no ip prefix-list <プレフィックスリスト名> [seq <シーケンス番号> {permit | deny} [<プレフィックス>
[ge <0-32>] [le <0-32>] | any]]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プレフィックスリスト名	プレフィックスリスト名を指定します。BGP/OSPF/RIP でプレフィックスリストを指定する場合は、この名称を使用します。	254 文字以内の WORD 型	省略不可
シーケンス番号	シーケンス番号を指定します。	1～4294967295	
permit deny	このプレフィックスリストの属性（許可／拒否）を指定します。	permit: 許可 deny: 拒否	
any	すべての IPv4 プレフィックスを対象とします。	-	
プレフィックス	プレフィックスを指定します。	IPv4 アドレス形式	
ge	このプレフィックスリストを使用するために、最小限ヒットしなければならないビット数を指定します。	0～32	すべてヒットする必要あり
le	このプレフィックスリストを使用するために、最大限ヒットしなければならないビット数を指定します。	0～32	

【動作モード】

基本設定モード

【説明】

IPv4 プレフィックスリスト情報を設定します。設定した IPv4 プレフィックスリストは、BGP/OSPF/RIP で通知するプレフィックス情報のフィルタリングに使用します。本設定は、設定順にソートされます。

ge、le を指定することにより、プレフィックス長を範囲で指定することができます。範囲指定する場合は、それぞれの値が次の条件を満たす必要があります。

プレフィックス長 < ge ≤ le

【実行例】

プレフィックスリスト情報を設定します（プレフィックスリスト名：prefix-list-A、シーケンス番号：1、属性：許可、プレフィックス：192.0.2.0/24）。

```
#configure terminal
(config)#ip prefix-list prefix-list-A seq 1 permit 192.0.2.0/24
```

プレフィックスリスト情報を設定します（プレフィックスリスト名：prefix-list-A、シーケンス番号：1、属性：許可、プレフィックス：上位24bitsは192.0.2で固定、下位8bitsは不定、かつプレフィックス長25bits以上）。

```
#configure terminal
(config)#ip prefix-list prefix-list-A seq 1 permit 192.0.2.0/24 ge 25
```

【未設定時】

プレフィックスリスト情報は設定されません。

11.5.2 ip prefix-list description

【機能】

IPv4 プレフィックスリスト名の設定

【入力形式】

ip prefix-list <プレフィックスリスト名> description <名称>

no ip prefix-list <プレフィックスリスト名> description [<名称>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プレフィックスリスト名	プレフィックスリスト名を指定します。BGP/OSPF/RIPでプレフィックスリストを指定する場合は、この名称を使用します。	254文字以内のWORD型	省略不可
名称	このプレフィックスリストにわかりやすい名称を指定します。	254文字以内のWORD型(*1)	

*1) 1文字の空白（スペース）は使用可能です。複数の空白（スペース）は1文字にまとめられます。

【動作モード】

基本設定モード

【説明】

IPv4 プレフィックスリスト名に名称を設定します。

【実行例】

IPv4 プレフィックスリスト名に名称を設定します（プレフィックスリスト名：prefix-list-A、名称：prefix-list-NAME）。

```
#configure terminal
(config)#ip prefix-list prefix-list-A description prifix-list-NAME
```


【未設定時】

IPv4 プレフィックスリスト名に名称を設定しません。

11.6 IPv4 スタティックルートの設定

11.6.1 ip route

【機能】

スタティック経路情報の設定

【入力形式】

ip route <ネットワークアドレス> <ネットマスク> <Next-hop> [<ディスタンス値>]

no ip route <ネットワークアドレス> <ネットマスク> <Next-hop> [<ディスタンス値>]

ip route <ネットワークアドレス> <ネットマスク> <インタフェース名> <インタフェース番号>
[<ディスタンス値>]

no ip route <ネットワークアドレス> <ネットマスク> <インタフェース名> <インタフェース番号>
[<ディスタンス値>]

ip route <ネットワークアドレス> <ネットマスク> dhcp <DHCP クライアントインタフェース名>
<DHCP クライアントインタフェース番号> [<ディスタンス値>]

no ip route <ネットワークアドレス> <ネットマスク> dhcp <DHCP クライアントインタフェース名>
<DHCP クライアントインタフェース番号> [<ディスタンス値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ネットワークアドレス	ネットワークアドレスを指定します。	IPv4 アドレス形式	省略不可
ネットマスク	ネットマスクを指定します。	IPv4 アドレス形式	
Next-hop	Next-hop アドレスを指定します。	IPv4 アドレス形式	
インタフェース名	インタフェース名を指定します。	-	
インタフェース番号	インタフェース番号を指定します。	-	
dhcp	DHCP 機能で配布された DHCP オプション (3):Router アドレスを使用します。	-	
DHCP クライアントインタフェース名	DHCPv4 クライアントが動作するインタフェース名を指定します。	-	省略不可
DHCP クライアントインタフェース番号	DHCPv4 クライアントが動作するインタフェース番号を指定します。	-	
ディスタンス値	ディスタンス値を指定します。	2～255	1

【動作モード】

基本設定モード

【説明】

スタティック経路情報を設定します。Next-hop にはアドレスまたはインタフェースを指定します。

dhcp を指定した場合は、配布された DHCP オプション (3):Router をゲートウェイアドレスとして登録します。アドレスが複数配布された場合は最初の 1 つを登録します。

宛先プレフィックスの同じ経路情報が複数存在した場合の優先度（小さい方が優先）をディスタンス値で設定します。

 参照 survey 連携機能を使用する場合は、[\[29.1.2 ip route survey\]](#) (P.871) を参照してください。

【実行例】

スタティック経路情報を設定します（ネットワークアドレス：192.0.2.128、ネットマスク：255.255.255.128、Next-hop：192.0.2.1）。

```
#configure terminal
(config)#ip route 192.0.2.128 255.255.255.128 192.0.2.1
```

DHCP で配布された router アドレスでスタティック経路情報を設定します（ネットワークアドレス：192.168.1.0、ネットマスク：255.255.255.0、DHCP クライアントが動作するインタフェース：port-channel 1）。

```
#configure terminal
(config)#ip route 192.168.1.0 255.255.255.0 dhcp port-channel 1
```

【未設定時】

スタティック経路を登録しません。

11.7 IPv4 インタフェースアドレスの設定

11.7.1 ip address

【機能】

IPv4 アドレスとネットマスクの設定

【入力形式】

ip address [secondary] <IPv4 アドレス> [<ネットマスク>]

no ip address [secondary] [<IPv4 アドレス> [<ネットマスク>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
secondary(*1)	Secondary Address を指定します。	-	Primary Address
IPv4 アドレス (*2)	IPv4 アドレスを指定します。	IPv4 アドレス形式	省略不可
ネットマスク (*2)(*3)	ネットマスクを指定します。	IPv4 アドレス形式	省略不可 (ただし、loopback インタフェース設定モードのみ入力不可)

*1) loopback インタフェース設定モード、port-channel インタフェース設定モードのみ指定可能

*2) management インタフェース設定モード、tunnel インタフェースの設定削除では指定不可

*3) loopback インタフェース設定モードのみ指定可能

【動作モード】

management インタフェース設定モード、loopback インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

IPv4 アドレスとネットマスクを設定します。

"secondary" を指定した場合には、Secondary Address を付与します。DHCP 機能などで動的にアドレスを取得している場合に、取得アドレスとプレフィックスが重複するアドレスを設定すると、重複元・重複先のインタフェースで正しく動作しません。

また、動作保証可能な"secondary"設定は3アドレスまでとなります。

プレフィックスが重複するアドレスを設定する場合は、いったんコンフィグから重複するインタフェースを削除してrefreshしてください。そのあとで改めてアドレスを設定する必要があります。

【実行例】

IPv4 アドレスとネットマスクを設定します (IPv4 アドレス: 192.0.2.1、ネットマスク 255.255.255.0)。

```

【port-channel の場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ip address 192.0.2.1 255.255.255.0

```

【未設定時】

IPv4 通信を行うことができません。

11.8 Proxy-ARP の設定

11.8.1 ip proxy-arp

【機能】

proxy-arp 動作を行う設定

【入力形式】

ip proxy-arp

no ip proxy-arp

【動作モード】

port-channel インタフェース設定モード

【説明】

proxy-arp 動作を行う場合に設定します。

【実行例】

proxy-arp 動作を行います。

```
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ip proxy-arp
```

【未設定時】

proxy-arp 動作を行いません。

11.9 送信元 IPv4 アドレスの設定

11.9.1 ip unnumbered

【機能】

送信元として使用する IPv4 アドレスのインタフェースの設定

【入力形式】

ip unnumbered <インタフェース名> <インタフェース番号>

no ip unnumbered

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース名	インタフェース名を指定します。	-	省略不可
インタフェース番号	インタフェース番号を指定します。	-	

【動作モード】

tunnel インタフェース設定モード

【説明】

tunnel インタフェースに IPv4 アドレスを設定していない場合、送信元として使用する IPv4 アドレスをインタフェースで設定します。ip address コマンドで IPv4 アドレスが指定されている場合は無効になります。

【実行例】

送信元として使用する IPv4 アドレスをインタフェースで設定します（インタフェース名：loopback、インタフェース番号：1）。

```
#configure terminal
(config)#interface tunnel 1
(config-if-tun 1)#ip unnumbered loopback 1
```

【未設定時】

ip unnumbered コマンドも ip address コマンドも設定していない場合には、management インタフェース以外の任意のインタフェースのアドレスを送信元とします。

11.10 DHCPv4 クライアント／サーバ／リレーエージェント機能設定

11.10.1 ip dhcp service

【機能】

DHCPv4 クライアント／サーバ／リレーエージェント機能の設定

【入力形式】

```
ip dhcp service {client | server | relay <アドレス 1> [<アドレス 2>] [source <送信元インタフェース名>
<送信元インタフェース番号>]}
```

```
no ip dhcp service [{client | server | relay <アドレス 1> [<アドレス 2>] [source <送信元インタフェース
名> <送信元インタフェース番号>]}]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
client server relay	DHCPv4 機能を指定します。	client: クライアント機能 server: サーバ機能 relay: リレーエージェント機能	省略不可
アドレス 1	DHCPv4 リレーエージェント機能でリレーする際の、1 目目のリレー先 DHCP サーバの IP アドレスを指定します。	IPv4 アドレス形式	省略不可
アドレス 2	DHCPv4 リレーエージェント機能でリレーする際の、2 目目のリレー先 DHCP サーバの IP アドレスを指定します。	IPv4 アドレス形式	リレー先 DHCP サーバはアドレス 1 で設定したものだけとなる。
送信元インタフェース名	DHCPv4 リレーする際の送信元 IP アドレスに使用するインタフェース名を指定します。	-	実際に送信するインタフェースの IP アドレス
送信元インタフェース番号	DHCPv4 リレーする際の送信元 IP アドレスに使用するインタフェース番号を指定します。	-	実際に送信するインタフェースの IP アドレス

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

DHCPv4 クライアント／サーバ／リレーエージェント機能を有効にします。インタフェースごとに 1 エントリのみ設定でき、クライアント／サーバ／リレーエージェント機能のどれかで動作します。

【実行例】

DHCPv4 クライアント機能を有効にします（インタフェース名：port-channel、インタフェース番号：1）。

```
(config)#interface port-channel 1
(config-if-ch 1)#ip dhcp service client
```

【未設定時】

DHCPv4 クライアント／サーバ／リレーエージェント機能が無効となります。

11.10.2 ip dhcp client-profile

【機能】

DHCPv4 クライアント機能の client プロファイル設定モードへの移行

【入力形式】

ip dhcp client-profile <client プロファイル名>

no ip dhcp client-profile <client プロファイル名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
client プロファイル名	client プロファイル名を指定します。	16 文字以内の WORD 型	省略不可

【動作モード】

基本設定モード

【説明】

DHCPv4 クライアント機能の client プロファイル設定モードに移行します。

【実行例】

client プロファイル設定モードに移行します（プロファイル名：PROF1）。

```
#configure terminal
(config)#ip dhcp client-profile PROF1
(config-dhcp PROF1)#
```

11.10.3 ip dhcp server-profile

【機能】

DHCPv4 サーバ機能の ip dhcp server プロファイル設定モードへの移行

【入力形式】

ip dhcp server-profile <server プロファイル名>

no ip dhcp server-profile <server プロファイル名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
server プロファイル名	server プロファイル名を設定します。	16 文字以内の WORD 型	省略不可

【動作モード】

基本設定モード

【説明】

DHCPv4 サーバ機能の ip dhcp server プロファイル設定モードに移行します。

【実行例】

DHCPv4 サーバ機能の ip dhcp server プロファイル設定モードに移行します (server プロファイル名: prof01)。

```
#configure terminal
(config)#ip dhcp server-profile prof01
(config-dhcps prof01)#
```

11.10.4 ip dhcp host-database

【機能】

ip dhcp host-database 設定モードへの移行

【入力形式】

ip dhcp host-database

no ip dhcp host-database

【動作モード】

基本設定モード

【説明】

DHCPv4 サーバ機能の ip dhcp host-database 設定モードに移行します。

【実行例】

DHCPv4 サーバ機能の ip dhcp host-database 設定モードに移行します。

```
#configure terminal
(config)#ip dhcp host-database
(config-dhcp-host)#
```

11.10.5 ip dhcp client-profile

【機能】

使用する DHCPv4 クライアント機能の client プロファイル名の設定

【入力形式】

ip dhcp client-profile <client プロファイル名>

no ip dhcp client-profile [<client プロファイル名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
client プロファイル名	client プロファイル名を指定します。	16 文字以内の WORD 型	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

使用する DHCPv4 クライアント機能の client プロファイル名を設定します。

client プロファイル名は、ip dhcp client-profile コマンドで設定した名称を指定します。

【実行例】

使用する client プロファイル名を設定します（プロファイル名：PROF1）。

```
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ip dhcp client-profile PROF1
```

【未設定時】

DHCPv4 クライアント機能の詳細設定はすべてデフォルトの動作となります。

11.10.6 client-id

【機能】

クライアント ID で使用する ID の設定

【入力形式】

client-id {ascii <クライアント ID> | hex <クライアント ID>}

no client-id [ascii <クライアント ID> | hex <クライアント ID>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ascii <クライアント ID>	DHCP オプション (61): クライアント ID で使用する ID を指定します	63 文字以内の WORD 型	省略不可
hex <クライアント ID>	DHCP オプション (61): クライアント ID で使用する ID を指定します	最大 126 桁の 16 進数	省略不可

【動作モード】

ip dhcp client プロファイル設定モード

【説明】

DHCP オプション (61): クライアント ID で使用する ID を指定します。

【実行例】

使用するクライアント ID を設定します（クライアント ID：client-12345678）。

```
#configure terminal
(config)#ip dhcp client-profile PROF1
(config-dhcp PROF1)#client-id ascii client-12345678
```

【未設定時】

送信する DHCP メッセージに DHCP オプション(61): クライアント ID をセットしません。

11.10.7 retries infinity

【機能】

DHCP メッセージの返信があるまで再送する設定

【入力形式】

retries infinity

no retries infinity

【動作モード】

ip dhcp client プロファイル設定モード

【説明】

DHCP メッセージの返信があるまで再送します。

無限再送中は 64sec 間隔で再送します。

DHCP クライアント機能を使用する場合、本設定を推奨します。

【実行例】

DHCP メッセージの返信があるまで再送を無限に設定します。

```
#configure terminal
(config)#ip dhcp client-profile PROF1
(config-dhcp PROF1)#retries infinity
```

【未設定時】

最大再送回数を超えた場合に DHCP クライアントを停止します。

11.10.8 ip dhcp server-profile

【機能】

DHCPv4 サーバ機能の server プロファイル名の設定

【入力形式】

ip dhcp server-profile <server プロファイル名>

no ip dhcp server-profile [<server プロファイル名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
server プロファイル名	server プロファイル名を設定します。	16 文字以内の WORD 型	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

使用する DHCPv4 サーバ機能の server プロファイル名を設定します。

server プロファイル名は、ip dhcp server-profile コマンドで設定した名称を指定します。

【実行例】

使用する DHCPv4 サーバ機能の server プロファイル名を設定します (server プロファイル名: prof01)。

```
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ip dhcp server-profile prof01
```

【未設定時】

DHCPv4 サーバ機能が無効となります。

11.10.9 address

【機能】

DHCPv4 クライアントに配布する IPv4 アドレス情報の設定

【入力形式】

address <IPv4 アドレスの先頭アドレス> <IPv4 アドレスの最終アドレス>

no address [<IPv4 アドレスの先頭アドレス> <IPv4 アドレスの最終アドレス>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
IPv4 アドレスの先頭アドレス	配布する IPv4 アドレスの先頭アドレスを指定します。	IPv4 アドレス形式	省略不可
IPv4 アドレスの最終アドレス	配布する IPv4 アドレスの最終アドレスを指定します。	IPv4 アドレス形式	省略不可

【動作モード】

ip dhcp server プロファイル設定モード

【説明】

DHCPv4 クライアントに配布する IPv4 アドレス情報を設定します。なお、アドレスは最終アドレスから払い出されます。

先頭から 4 件までの設定を有効とし、配布する最大アドレス数は 253 個です。

【実行例】

DHCPv4 クライアントに配布する IPv4 アドレス情報を設定します（配布する IPv4 アドレス範囲：192.168.1.100～192.168.1.110）。

```
#configure terminal
(config)#ip dhcp server-profile prof01
(config-dhcp prof01)#address 192.168.1.100 192.168.1.110
```

【未設定時】

DHCPv4 サーバ機能が無効となります。

11.10.10 dns

【機能】

DHCPv4 クライアントに配布する DNS サーバアドレスの設定

【入力形式】

dns <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>]

no dns [<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>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プライマリ DNS サーバアドレス	配布するプライマリ DNS サーバアドレスを指定します。	IPv4 アドレス形式	省略不可
セカンダリ DNS サーバアドレス	配布するセカンダリ DNS サーバアドレスを指定します。	IPv4 アドレス形式	プライマリ DNS サーバアドレスのみ配布

【動作モード】

ip dhcp server プロファイル設定モード

【説明】

DHCPv4 クライアントに配布する DNS サーバアドレスを設定します。

【実行例】

DHCPv4 クライアントに配布する DNS サーバアドレスを設定します（プライマリ DNS サーバアドレス：192.168.1.10、セカンダリ DNS サーバアドレス：192.168.1.11）。

```
#configure terminal
(config)#ip dhcp server-profile prof01
(config-dhcp prof01)#dns 192.168.1.10 192.168.1.11
```

【未設定時】

DNS サーバアドレスを配布しません。

11.10.11 domain

【機能】

DHCPv4 クライアントに配布する DNS ドメイン名の設定

【入力形式】

domain <DNS ドメイン名>

no domain [<DNS ドメイン名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
DNS ドメイン名	配布する DNS ドメイン名を指定します。	80 文字以内の DOMAINWORD 型	省略不可

【動作モード】

ip dhcp server プロファイル設定モード

【説明】

DHCPv4 クライアントに配布する DNS ドメイン名を設定します。

【実行例】

DHCPv4 クライアントに配布する DNS ドメイン名を設定します (DNS ドメイン名: example.com)。

```
#configure terminal
(config)#ip dhcp server-profile prof01
(config-dhcps prof01)#domain example.com
```

【未設定時】

DNS ドメイン名を配布しません。

11.10.12 gateway

【機能】

DHCPv4 クライアントに配布するデフォルトルータアドレスの設定

【入力形式】

gateway <デフォルトルータアドレス>

no gateway [<デフォルトルータアドレス>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
デフォルトルータアドレス	配布するデフォルトルータアドレスを指定します。	IPv4 アドレス形式	省略不可

【動作モード】

ip dhcp server プロファイル設定モード

【説明】

DHCPv4 クライアントに配布するデフォルトルータアドレスを設定します。

【実行例】

DHCPv4 クライアントに配布するデフォルトルータアドレスを設定します（デフォルトルータアドレス：192.168.1.50）。

```
#configure terminal
(config)#ip dhcp server-profile prof01
(config-dhcps prof01)#gateway 192.168.1.50
```

【未設定時】

デフォルトルータアドレスを配布しません。

11.10.13 lease-time

【機能】

DHCP クライアントに配布する情報の有効時間の設定

【入力形式】

lease-time <DHCP リース期間>

no lease-time [<DHCP リース期間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
DHCP リース期間	配布する IPv4 アドレスの DHCP リース期間（単位：秒）を指定します。	1～31536000 infinity: 無制限	省略不可

【動作モード】

ip dhcp server プロファイル設定モード

【説明】

DHCP クライアントに配布する情報の有効時間（単位：秒）を設定します。

infinity を指定した場合、無制限になります。

【実行例】

DHCP クライアントに配布する情報の有効時間を設定します（DHCP リース期間：3600 秒）。

```
#configure terminal
(config)#ip dhcp server-profile prof01
(config-dhcps prof01)#lease-time 3600
```

【未設定時】

無制限で動作します。

11.10.14 ntp-server

【機能】

DHCPv4 クライアントに配布する NTP サーバアドレスの設定

【入力形式】

ntp-server <NTP サーバアドレス>

no ntp-server [<NTP サーバアドレス>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
NTP サーバアドレス	配布する NTP サーバアドレスを指定します。	IPv4 アドレス形式	省略不可

【動作モード】

ip dhcp server プロファイル設定モード

【説明】

DHCPv4 クライアントに配布する NTP サーバアドレスを設定します。

【実行例】

DHCPv4 クライアントに配布する NTP サーバアドレスを設定します（NTP サーバアドレス：192.168.1.50）。

```
#configure terminal
(config)#ip dhcp server-profile prof01
(config-dhcp prof01)#ntp-server 192.168.1.50
```

【未設定時】

NTP サーバアドレスを配布しません。

11.10.15 option

【機能】

任意の DHCP オプションを配布する設定

【入力形式】

option <DHCP オプション番号> hex <DHCP オプション内容>

no option <DHCP オプション番号> [hex <DHCP オプション内容>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
DHCP オプション番号	配布する DHCP オプション番号を指定します。	1～254	省略不可
DHCP オプション内容	配布する DHCP オプションデータを指定します。	最大 127 桁の 16 進数	省略不可

【動作モード】

ip dhcp server プロファイル設定モード

【説明】

DHCP オプション番号とオプション内容を設定することにより、任意の DHCP オプションを配布することができます。

DHCP オプション番号でソートされ、DHCP オプション番号が一番小さいエントリから 4 件までが有効となります。

【実行例】

任意の DHCP オプションを配布する設定をします（DHCP オプション番号：100、DHCP オプション内容：1234567890）。

```
#configure terminal
(config)#ip dhcp server-profile prof01
(config-dhcps prof01)# option 100 hex 1234567890
```

【未設定時】

任意オプションを配布しません。

11.10.16 sip-server

【機能】

DHCPv4 クライアントに配布する SIP サーバの IP アドレスまたはドメイン名の設定

【入力形式】

sip-server {address <プライマリ SIP サーバアドレス> [<セカンダリ SIP サーバアドレス>] | domain <プライマリ SIP サーバドメイン名> [<セカンダリ SIP サーバドメイン名>]}

no sip-server [{address [<プライマリ SIP サーバアドレス> [<セカンダリ SIP サーバアドレス>]] | domain [<プライマリ SIP サーバドメイン名> [<セカンダリ SIP サーバドメイン名>]]}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プライマリ SIP サーバアドレス	配布する SIP サーバアドレスを指定します。	IPv4 アドレス形式	省略不可
セカンダリ SIP サーバアドレス	配布するセカンダリ SIP サーバアドレスを指定します。	IPv4 アドレス形式	セカンダリ SIP サーバアドレスを配布しない
プライマリ SIP サーバドメイン名	配布する SIP サーバドメイン名を指定します。	80 文字以内の SIP サーバドメイン名	省略不可
セカンダリ SIP サーバドメイン名	配布するセカンダリ SIP サーバドメイン名を指定します。	80 文字以内のセカンダリ SIP サーバドメイン名	セカンダリ SIP サーバドメイン名を配布しない

【動作モード】

ip dhcp server プロファイル設定モード

【説明】

DHCPv4 クライアントに配布する SIP サーバの IP アドレスまたはドメイン名を設定します。

【実行例】

DHCPv4 クライアントに配布する SIP サーバの IP アドレスを設定します（プライマリ SIP サーバアドレス：192.168.1.50）。

```
#configure terminal
(config)#ip dhcp server-profile prof01
(config-dhcp prof01)#sip-server address 192.168.1.50
```

【未設定時】

SIP サーバの IP アドレスまたはドメイン名を配布しません。

11.10.17 time-server

【機能】

DHCPv4 クライアントに配布する TIME サーバアドレスの設定

【入力形式】

time-server <TIME サーバアドレス>

no time-server [<TIME サーバアドレス>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
TIME サーバアドレス	配布する TIME サーバアドレスを指定します。	IPv4 アドレス形式	省略不可

【動作モード】

ip dhcp server プロファイル設定モード

【説明】

DHCPv4 クライアントに配布する TIME サーバアドレスを設定します。

【実行例】

DHCPv4 クライアントに配布する TIME サーバアドレスを設定します（TIME サーバアドレス：192.168.1.50）。

```
#configure terminal
(config)#ip dhcp server-profile prof01
(config-dhcp prof01)#time-server 192.168.1.50
```

【未設定時】

TIME サーバアドレスを配布しません。

11.10.18 wins-server

【機能】

DHCPv4 クライアントに配布する WINS サーバアドレスの設定

【入力形式】

wins-server <WINS サーバアドレス>

no wins-server [<WINS サーバアドレス>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
WINS サーバアドレス	配布する WINS サーバアドレスを指定します。	IPv4 アドレス形式	省略不可

【動作モード】

ip dhcp server プロファイル設定モード

【説明】

DHCPv4 クライアントに配布する WINS サーバアドレスを設定します。

【実行例】

DHCPv4 クライアントに配布する WINS サーバアドレスを設定します（WINS サーバアドレス：192.168.1.50）。

```
#configure terminal
(config)#ip dhcp server-profile prof01
(config-dhcp prof01)#wins-server 192.168.1.50
```

【未設定時】

WINS サーバアドレスを配布しません。

11.10.19 host

【機能】

特定ホストに配布する IPv4 アドレスと MAC アドレスの設定

【入力形式】

host <定義番号> <配布する IP アドレス> <配布先ホストの MAC アドレス>

no host <定義番号> [<配布する IP アドレス> <配布先ホストの DMAC アドレス>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
定義番号	ホストデータベースの定義番号を指定します。	1～64	省略不可
配布する IPv4 アドレス	固定配布する IPv4 アドレスを指定します。	IPv4 アドレス形式	省略不可
配布先ホストの MAC アドレス	配布先ホストの MAC アドレスを指定します。	MAC アドレス形式	省略不可

【動作モード】

ip dhcp host-database 設定モード

【説明】

特定ホストに配布する IP アドレスと MAC アドレスを設定します。

【実行例】

特定ホストに配布する IP アドレスと MAC アドレスを設定します（定義番号：1、配布する IPv4 アドレス：192.168.1.251、配布先ホストの MAC アドレス：XXXX.XXXX.XXXX）。

```
(config)#ip dhcp host-database
(config-dhcp-host)# host 1 192.168.1.251 XXXX.XXXX.XXXX
```

【未設定時】

特定ホストに対し、固定の IP アドレスを割り当てません。

第12章 IPv6 の設定



この章では、IPv6 の設定に関するコマンドについて説明します。

12.1	DNS の設定	434
12.2	ICMP の設定	435
12.3	アドレスプールの設定 (IPv6)	437
12.4	IPv6 プレフィックスリストの設定	438
12.5	IPv6 スタティックルートの設定	441
12.6	IPv6 インタフェースアドレスの設定	443
12.7	DHCPv6 クライアント／サーバ／リレーエージェント機能設定	446
12.8	IPv6 アドレス有効設定	463
12.9	IPv6 Neighbor Discovery Protocol 設定	464
12.10	送信元 IPv6 アドレスの設定	481

12.1 DNS の設定

12.1.1 ipv6 host

【機能】

ホスト名と IPv6 アドレスの登録

【入力形式】

ipv6 host <ホスト名> <IPv6 アドレス>

no ipv6 host <ホスト名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ホスト名	ホスト名を指定します。	64 文字以内の WORD 型	省略不可
IPv6 アドレス	IPv6 アドレスを指定します。	IPv6 アドレス形式	

【動作モード】

基本設定モード

【説明】

ホスト名と IPv6 アドレスを登録します。設定されているホストへのアクセス（TELNET/RADIUS/NTP など）では、DNS サーバへの問い合わせを行いません。設定されていないホストへのアクセスでは、必ず DNS サーバへ問い合わせを行います。

【実行例】

ホスト名と IPv6 アドレスを登録します（ホスト名：host-A、IPv6 アドレス：2001:db8::1）。

```
#configure terminal
(config)#ipv6 host host-A 2001:db8::1
```

【未設定時】

ホスト名と IPv6 アドレスを登録しません。

12.2 ICMP の設定

12.2.1 ipv6 icmp disable-sending-errors

【機能】

ICMPv6 エラーを送信しない ICMPv6 タイプの設定

【入力形式】

ipv6 icmp disable-sending-errors [<ICMPv6 タイプ>]

no ipv6 icmp disable-sending-errors [<ICMPv6 タイプ>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ICMPv6 タイプ	ICMPv6 エラーを送信しない ICMPv6 タイプを指定します。 複数指定が可能です。	port-unreach: Unreach(Port) unreach:ICMP Unreach hop-limitexceeded: Hop Limit Exceeded redirect:Redirect	echo/reply,packet too big を除く ICMPv6 エラーの送信をしない

【動作モード】

基本設定モード、management インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

ICMPv6 エラーを送信しない ICMPv6 タイプを設定します。

【実行例】

ICMPv6 エラーを送信しない ICMPv6 タイプを設定します。

```
【基本設定モードの場合】
#configure terminal
(config)#ipv6 icmp disable-sending-errors
```

【未設定時】

すべての ICMPv6 エラーを送信します。

12.2.2 ipv6 icmp source

【機能】

ICMPv6 送信の際の送信元アドレスの設定

【入力形式】

```
ipv6 icmp [vrf <VRF 名>] source {interface <インタフェース名> <インタフェース番号> | address <送信元アドレス>}
```

```
no ipv6 icmp [vrf <VRF 名>] source [interface <インタフェース名> <インタフェース番号> | address <送信元アドレス>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VRF 名	VRF 名を指定します。	63 文字以内の WORD 型	VRF を指定しない
インタフェース名	送信元アドレスとして使用するインタフェース名を指定します。	-	省略不可
インタフェース番号	送信元アドレスとして使用するインタフェース番号を指定します。	-	
送信元アドレス	送信元アドレスとして使用するアドレスを指定します。	IPv6 アドレス形式	

【動作モード】

基本設定モード

【説明】

ICMPv6 送信の際の送信元アドレスを設定します。

【実行例】

ICMPv6 送信の際の送信元アドレスを設定します（インタフェース名：port-channel、インタフェース番号：1）。

```
#configure terminal
(config)#ipv6 icmp source interface port-channel 1
```

【未設定時】

送信元アドレスは送信インタフェースのアドレスで動作します。

12.3 アドレスプールの設定 (IPv6)

12.3.1 ipv6 local pool

【機能】

IPsec や L2TP/PPP により通知するアドレス範囲の設定

【入力形式】

ipv6 local pool <アドレスプール名> <割り当て開始アドレス> <割り当て最終アドレス>

no ipv6 local pool <アドレスプール名> <割り当て開始アドレス> <割り当て最終アドレス>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アドレスプール名	アドレスプール名を指定します。	63 文字以内の CDATA 型	省略不可
割り当て開始アドレス	Mode-config/ConfigPayload で通知する IPv6 アドレスの割り当て開始アドレスを指定します。	IPv6 アドレス形式	
割り当て最終アドレス	Mode-config/ConfigPayload で通知する IPv6 アドレスの割り当て最終アドレスを指定します。	IPv6 アドレス形式	

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

IPsec(Mode-config/Config Payload) により通知するアドレス範囲を設定します。本設定は、設定順にソートされます。

【実行例】

IPsec(Mode-config/Config Payload) により通知するアドレス範囲を設定します (アドレスプール名 : pool-A、割り当て開始アドレス : 2001:db8::1、割り当て最終アドレス : 2001:db8::16)。

```
#configure terminal
(config)#ipv6 local pool pool-A 2001:db8::1 2001:db8::16
```

【未設定時】

IPv6 アドレス割り当てを行いません。

12.4 IPv6 プレフィックスリストの設定

12.4.1 ipv6 prefix-list

【機能】

IPv6 プレフィックスリスト情報の設定

【入力形式】

```
ipv6 prefix-list <プレフィックスリスト名> seq <シーケンス番号> {permit | deny} [<プレフィックス>
[ge <0-128>] [le <0-128>] | any]
```

```
no ipv6 prefix-list <プレフィックスリスト名> [seq <シーケンス番号> {permit | deny} [<プレフィックス>
[ge <0-32>] [le <0-32>] | any]]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プレフィックスリスト名	プレフィックスリスト名を指定します。BGP/OSPF6でプレフィックスリストを指定する場合は、この名称を使用します。	254 文字以内の WORD 型	省略不可
シーケンス番号	シーケンス番号を指定します。	1～4294967295	
permit deny	このプレフィックスリストの属性（許可／拒否）を指定します。	permit: 許可 deny: 拒否	
any	すべてのIPv6プレフィックスを対象とします。	-	
プレフィックス	プレフィックスを指定します。	IPv6 アドレス形式：	
ge	このプレフィックスリストを使用するために、最小限ヒットしなければならないビット数を指定します。	0～128	すべてヒットする必要あり
le	このプレフィックスリストを使用するために、最大限ヒットしなければならないビット数を指定します。	0～128	

【動作モード】

基本設定モード

【説明】

IPv6 プレフィックスリスト情報を設定します。設定した IPv6 プレフィックスリストは、BGP/OSPF6 で通知するプレフィックス情報のフィルタリングに使用します。本設定は、設定順にソートされます。

ge、le を指定することにより、プレフィックス長を範囲で指定することができます。範囲指定する場合は、それぞれの値が次の条件を満たす必要があります。

プレフィックス長 < ge ≤ le

【実行例】

IPv6 プレフィックスリスト情報を設定します（プレフィックスリスト名：prefix-list-A、シーケンス番号：1、許可、プレフィックス：2001:db8::/48）。

```
#configure terminal
(config)#ipv6 prefix-list prefix-list-A seq 1 permit 2001:db8::/48
```

プレフィックスリスト情報を設定します（プレフィックスリスト名：prefix-list-A、シーケンス番号：1、属性：許可、プレフィックス：上位 48bit は 2001:db8:: で固定、下位 80bit は不定、かつプレフィックス長 49 以上）。

```
#configure terminal
(config)#ipv6 prefix-list prefix-list-A seq 1 permit 2001:db8::/48 ge 49
```

【未設定時】

プレフィックスリスト情報は設定されません。

12.4.2 ipv6 prefix-list description

【機能】

IPv6 プレフィックスリスト名の設定

【入力形式】

ipv6 prefix-list <プレフィックスリスト名> description <名称>

no ipv6 prefix-list <プレフィックスリスト名> description [<名称>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プレフィックスリスト名	プレフィックスリスト名を指定します。BGP/OSPF6 でプレフィックスリストを指定する場合は、この名称を使用します。	254 文字以内の WORD 型	省略不可
名称	このプレフィックスリストにわかりやすい名称を指定します。	254 文字以内の WORD 型 (*1)	

*1) 1 文字の空白（スペース）は使用可能です。複数の空白（スペース）は 1 文字にまとめられます。

【動作モード】

基本設定モード

【説明】

IPv6 プレフィックスリスト名に名称を設定します。

【実行例】

プレフィックスリスト名に名称を設定します（プレフィックスリスト名：prefix-list-A、名称：prefix-list-NAME）。

```
#configure terminal
(config)#ipv6 prefix-list prefix-list-A description prifix-list-NAME
```

【未設定時】

プレフィックスリストに名称を設定しません。

12.5 IPv6 スタティックルートの設定

12.5.1 ipv6 route

【機能】

スタティック経路情報の設定

【入力形式】

ipv6 route <ネットワークアドレス>/<プレフィックス長> <Next-hop> [<ディスタンス値>]

no ipv6 route <ネットワークアドレス>/<プレフィックス長> <Next-hop> [<ディスタンス値>]

ipv6 route <ネットワークアドレス>/<プレフィックス長> <インタフェース名> <インタフェース番号> [<リンクローカルアドレス>] [<ディスタンス値>]

no ipv6 route <ネットワークアドレス>/<プレフィックス長> <インタフェース名> <インタフェース番号> [<リンクローカルアドレス>] [<ディスタンス値>]

ipv6 route <ネットワークアドレス>/<プレフィックス長> dhcp <DHCPクライアントインタフェース名> <DHCPクライアントインタフェース番号> [<ディスタンス値>]

no ipv6 route <ネットワークアドレス>/<プレフィックス長> dhcp <DHCPクライアントインタフェース名> <DHCPクライアントインタフェース番号> [<ディスタンス値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ネットワークアドレス	ネットワークアドレスを指定します。	IPv6 アドレス形式	省略不可
プレフィックス長	プレフィックス長を指定します。	0～128	
Next-hop	Next-hop アドレスを指定します。	IPv6 アドレス形式	
インタフェース名	インタフェース名を指定します。	-	
インタフェース番号	インタフェース番号を指定します。	-	
リンクローカルアドレス(*1)	リンクローカルアドレスを指定します。	IPv6 アドレス形式	リンクローカルアドレスを指定しない
dhcp	DHCPv6 サーバのアドレスを使用する場合に指定します。	-	省略不可
DHCP クライアントインタフェース名	DHCPv6 クライアントが動作するインタフェース名を指定します。	-	
DHCP クライアントインタフェース番号	DHCPv6 クライアントが動作するインタフェース番号を指定します。	-	
ディスタンス値	ディスタンス値を指定します。	2～255	1

*1) インタフェース名に "port-channel"、"management" を指定した場合のみ、"リンクローカルアドレス" を指定できます。

【動作モード】

基本設定モード

【説明】

スタティック経路情報を設定します。Next-hop にはアドレスまたはインタフェースを指定します。Next-hop がリンクローカルアドレスの場合は、インタフェース名を指定します。

"dhcp" を指定した場合は、DHCPv6 サーバアドレスをゲートウェイアドレスとして登録します。

宛先プレフィックスの同じ経路情報が複数存在した場合の優先度（小さい方が優先）をディスタンス値で設定します。

 参照 survey 連携機能を使用する場合は、[\[29.1.4 ipv6 route survey\]](#) (P.873) を参照してください。

【実行例】

スタティック経路情報を設定します（ネットワークアドレス：2001:db8:2::、プレフィックス長：48、Next-hop:2001:db8:1::1、ディスタンス値：2）。

```
#configure terminal
(config)#ipv6 route 2001:db8:2::/48 2001:db8:1::1 2
```

DHCPv6 サーバアドレスをゲートウェイアドレスとして登録するデフォルトルートの設定をします（DHCPv6 クライアントが動作するインタフェース：port-channel 1）。

```
#configure terminal
(config)#ipv6 route ::/0 dhcp port-channel 1
```

【未設定時】

スタティック経路を登録しません。

12.6 IPv6 インタフェースアドレスの設定

12.6.1 ipv6 address

【機能】

該当インタフェースで IPv6 通信を可能にする設定

【入力形式】

```
ipv6 address {{<IPv6 アドレス>/<プレフィックス長> [{eui-64 | anycast}] | <IPv6 アドレス> link-local} |
autoconfig [interface-id <インタフェース ID>]}
```

```
no ipv6 address {<IPv6 アドレス>/<プレフィックス長> [{eui-64 | anycast}]] | autoconfig [interface-id
<インタフェース ID>]}
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
IPv6 アドレス	IPv6 アドレスを指定します。	IPv6 アドレス形式	省略不可
プレフィックス長(*1)	プレフィックス長を指定します。	0 ～ 128	
eui-64(*1)	グローバルアドレスを EUI-64 型式とします。EUI-64 とは、IPv6 のインタフェース識別子を、インタフェースの MAC アドレスから割り出す方式です。	-	EUI-64 型式としない
anycast(*2)	設定している IPv6 アドレスをユニキャストアドレスとする場合に指定します。	-	ユニキャストアドレス
link-local(*1)	設定している IPv6 アドレスをリンクローカルアドレスとする場合に指定します。	-	グローバルアドレス
autoconfig(*2)	Stateless Address Autoconfiguration を使用してアドレスを設定する場合に指定します。	-	-
インタフェース ID	Stateless Address Autoconfiguration において使用するインタフェース ID を指定します。	IPv6 アドレス形式	EUI-64 形式

*1) loopback インタフェース設定モードでは指定できません。

*2) loopback インタフェース設定モード、tunnel インタフェース設定モードでは指定できません。

【動作モード】

management インタフェース設定モード、loopback インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

IPv6 アドレスを登録し、該当インタフェースで IPv6 通信を可能にします。"eui-64" を指定した場合には、<IPv6 アドレス> の下位 64bit を EUI-64 インタフェース識別子に置き換えたアドレスを登録します（プレフィックス長が 64bit を超える場合はプレフィックスを優先します）。"anycast" の設定を行ったアドレスは送信元アドレスとしては使用できません。"link-local" を指定した場合には、自動生成されるリンクローカルアドレスを指定されたアドレスで上書きします。

autoconfig の設定を行うことで、インタフェースで Stateless Address Autoconfiguration を使用し、IPv6 アドレスを自動設定します。本設定を行う場合は、ipv6 nd receive-ra コマンドの設定が必要です。DHCP 機能などで動的にアドレスを取得している場合に、取得アドレスとプレフィックスが重複するアドレスを設定すると、重複元・重複先のインタフェースで正しく動作しません。

プレフィックスが重複するアドレスを設定する場合は、いったんコンフィグから重複するインタフェースを削除して refresh してください。そのあとで改めてアドレスを設定する必要があります。

【実行例】

該当インタフェースで IPv6 通信を可能にします (IPv6 アドレス : fe80::1、リンクローカルアドレス)。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 address fe80::1 link-local
```

【未設定時】

IPv6 通信を行うことができません。

12.6.2 ipv6 address dhcp

【機能】

DHCPv6 クライアント機能で取得したプレフィックスを使用する IPv6 アドレスのインタフェースの設定

【入力形式】

ipv6 address dhcp <DHCP クライアントインタフェース名> <DHCP クライアントインタフェース番号>
<インタフェース ID> / <プレフィックス長>

no ipv6 address dhcp [<DHCP クライアントインタフェース名> <DHCP クライアントインタフェース番号> <インタフェース ID> / <プレフィックス長>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
DHCP クライアントインタフェース名	DHCPv6 クライアント機能が有効なインタフェース名を指定します。	-	省略不可
DHCP クライアントインタフェース番号	DHCPv6 クライアント機能が有効なインタフェース番号を指定します。	-	省略不可
インタフェース ID	DHCPv6 クライアントで取得したプレフィックスと合わせるインタフェース ID を指定します。	IPv6 アドレス形式	省略不可
プレフィックス長	作成した IPv6 アドレスのプレフィックス長を指定します。	0 ～ 128	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード、
tunnel インタフェース設定モード

【説明】

DHCPv6 クライアント機能で取得したプレフィックスを使用し、インタフェースに IPv6 アドレスを設定します。

指定した下位 80bit と DHCPv6 クライアント機能で取得したプレフィックスの有数のビットが重なる指定はできません。

interface tunnel は PPPoE モードのみ有効です。

【実行例】

DHCPv6 クライアント機能で取得したプレフィックスを使用し、インタフェースに IPv6 アドレスを設定します (DHCPv6 クライアント機能が有効なインタフェース名 番号 : port-channel 1、IPv6 アドレスを設定するインタフェース名 番号 : port-channel 2、プレフィックスと合わせるインタフェース ID : 1::1、プレフィックス長 / 64)。

```
#configure terminal
(config)#interface port-channel 2
(config-if-ch 2)#ipv6 address dhcp port-channel 1 ::1/64
```

【未設定時】

DHCPv6 クライアント機能で取得したプレフィックスを使用した IPv6 アドレスの設定はしません。

12.7 DHCPv6 クライアント／サーバ／リレーエージェント機能設定

12.7.1 ipv6 dhcp service

【機能】

DHCPv6 クライアント／サーバ／リレーエージェント機能の設定

【入力形式】

```
ipv6 dhcp service {client [auto] | server | relay <DHCPv6 サーバアドレス> | dest <送信先インタフェース>} [source <送信元インタフェース>]
```

```
no ipv6 dhcp service [client [auto] | server | relay <DHCPv6 サーバアドレス> | dest <送信先インタフェース>] [source <送信元インタフェース>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
client server relay	DHCPv6 機能を設定します。	client: クライアント機能 server: サーバ機能 relay: リレー機能	省略不可
auto	RA 連携を行う場合に指定します。	-	RA 連携を行いません
DHCPv6 サーバアドレス	DHCPv6 リレーエージェント機能でリレーする際の、リレー先 DHCP サーバのアドレスを指定します。設定されたサーバのアドレスがグローバルアドレスではない場合、設定は無効となります。	IPv6 アドレス形式	FF05::1:3宛に送信する。送信先インタフェースの設定が必要。
送信元インタフェース	DHCPv6 サーバへ送信する際の送信元アドレスとして使用するインタフェースを指定します。	-	実際に送信するインタフェースの IP アドレス
送信先インタフェース	FF05::1:3宛に送信する場合の送信インタフェースを指定します。	-	経路情報に従う

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

DHCPv6 クライアント／サーバ／リレーエージェント機能を有効にします。

インタフェースごとに 1 エントリのみ設定でき、クライアント機能とサーバ機能、リレーエージェント機能のどれかで動作します。

"auto" を指定した場合は、RA(RouterAdvertisement)の M フラグと O フラグに連携します。

tunnel インタフェースでは、PPPoE モードで DHCPv6 クライアント機能を動作させる場合のみ対応しています。

ipv6 enable または ipv6 address 設定がない場合は無効になります。

【実行例】

DHCPv6 クライアント機能を有効にします（対象インタフェース：port-channel 1）。

```
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 dhcp service client
```

【未設定時】

DHCPv6 クライアント／サーバ／リレーエージェント機能が無効となります。

12.7.2 ipv6 dhcp client-profile

【機能】

DHCPv6 クライアント機能の client プロファイル名設定モードへの移行

【入力形式】

ipv6 dhcp client-profile <client プロファイル名>

no ipv6 dhcp client-profile <client プロファイル名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
client プロファイル名	client プロファイル名を指定します。	16 文字以内の WORD 型	省略不可

【動作モード】

基本設定モード

【説明】

DHCPv6 クライアント機能の client プロファイル名設定モードに移行します。

【実行例】

client プロファイル名設定モードに移行します（client プロファイル名：PROF1）。

```
#configure terminal
(config)#ipv6 dhcp client-profile PROF1
(config-dhcp6 PROF1)#
```

12.7.3 ipv6 dhcp server-profile

【機能】

DHCPv6 サーバ機能の server プロファイル設定モードへの移行

【入力形式】

ipv6 dhcp server-profile <server プロファイル名>

no ipv6 dhcp server-profile <server プロファイル名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
server プロファイル名	server プロファイル名を指定します。	16 文字以内の WORD 型	省略不可

【動作モード】

基本設定モード

【説明】

ipv6 dhcp server プロファイル設定モードに移行します。

【実行例】

DHCPv6 サーバ機能の ipv6 dhcp server プロファイル設定モードに移行します (server プロファイル名 : prof1)。

```
#configure terminal
(config)#ipv6 dhcp server-profile prof1
(config-dhcp6 prof1)#
```

12.7.4 ipv6 dhcp host-database

【機能】

ipv6 dhcp host-database 設定モードへの移行

【入力形式】

ipv6 dhcp host-database

no ipv6 dhcp host-database

【動作モード】

基本設定モード

【説明】

ipv6 dhcp host-database 設定モードに移行します。

【実行例】

ipv6 dhcp host-database 設定モードに移行します。

```
#configure terminal
(config)#ipv6 dhcp host-database
(config-dhcp6-host)#
```

12.7.5 ipv6 dhcp client-profile

【機能】

使用する DHCPv6 クライアント機能の client プロファイル名の設定

【入力形式】

ipv6 dhcp client-profile <client プロファイル名>

no ipv6 dhcp client-profile [<client プロファイル名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
client プロファイル名	client プロファイル名を指定します。	16 文字以内の WORD 型	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード、
tunnel インタフェース設定モード

【説明】

使用する DHCPv6 クライアント機能の client プロファイル名を設定します。

client プロファイル名は、ipv6 dhcp client-profile コマンドで設定した名称を指定します。

【実行例】

使用する client プロファイル名を設定します（プロファイル名：PROF1）。

```
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 dhcp client-profile PROF1
```

【未設定時】

DHCPv6 クライアント機能が無効となります。

12.7.6 iaaid

【機能】

IAID 値の設定

【入力形式】

iaaid <IAID 値>

no iaaid <IAID 値>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
IAID 値	IAID 値を指定します。	1 ～ 4294967295	省略不可

【動作モード】

ipv6 dhcp client プロファイル設定モード

【説明】

IAID 値を設定します。

インタフェースごとに異なる IAID が必要なため、本設定をしたプロファイルを複数のインタフェースで指定できません。

【実行例】

IAID 値を設定します (IAID 値: 12345678)。

```
#configure terminal
(config)#ipv6 dhcp client-profile PROF1
(config-dhcp6 PROF1)#iaid 12345678
```

【未設定時】

MIB の ifIndex 値を設定します。

12.7.7 option-request

【機能】

DHCPv6 サーバへの情報取得要求

【入力形式】

option-request <要求情報名>

no option-request [要求情報名]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
要求情報名	DHCPv6 サーバに取得要求を行う情報を指定します。	prefix-delegation: アドレスプレフィックス (*1) dns-server: DNS サーバ dns-server-domain: DNS サーバドメイン名 snmp-server: SNMP サーバ sip-server: SIP サーバ sip-server-domain: SIP サーバドメイン名	省略不可

*1) "prefix-delegation" を指定した場合、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。リジェクト経路宛の送信者に対して応答しません。

【動作モード】

ipv6 dhcp client プロファイル設定モード

【説明】

DHCPv6 サーバに情報取得要求を行います。

【実行例】

DHCPv6 サーバに情報取得要求を行うように設定します（要求情報名：dns-server）。

```
#configure terminal
(config)#ipv6 dhcp client-profile PROF1
(config-dhcp6 PROF1)#option-request dns-server
```

【未設定時】

各種情報要求を行いません。

12.7.8 retries infinity

【機能】

DHCPv6 メッセージの返信があるまで再送する設定

【入力形式】

retries infinity

no retries infinity

【動作モード】

ipv6 dhcp client プロファイル設定モード

【説明】

DHCPv6 メッセージの返信があるまで再送します。

無限再送中は 64sec 間隔で再送します。

DHCPv6 クライアント機能を使用する場合、本設定を推奨します。

【実行例】

DHCPv6 メッセージの返信があるまで再送するように設定します。

```
#configure terminal
(config)#ipv6 dhcp client-profile PROF1
(config-dhcp6 PROF1)#retries infinity
```

【未設定時】

最大再送回数を超えた場合に DHCP クライアントを停止します。

12.7.9 ipv6 dhcp server-profile

【機能】

DHCPv6 サーバ機能の server プロファイル名の設定

【入力形式】

ipv6 dhcp server-profile <server プロファイル名>

no ipv6 dhcp server-profile [<server プロファイル名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
server プロファイル名	server プロファイル名を指定します。	16 文字以内の WORD 型	省略不可

【動作モード】

port-channel インタフェース設定モード、management インタフェース設定モード

【説明】

使用する DHCPv6 サーバ機能の server プロファイル名を設定します。

server プロファイル名は、ipv6 dhcp server-profile コマンドで設定した名称を指定します。

【実行例】

使用する DHCPv6 サーバ機能の server プロファイル名を設定します (server プロファイル名: prof1)。

```
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 dhcp server-profile prof1
```

【未設定時】

DHCPv6 サーバ機能が無効となります。

12.7.10 address

【機能】

DHCPv6 クライアントに配布する IPv6 アドレス情報の設定

【入力形式】

address {<IPv6 アドレスの先頭アドレス> <IPv6 アドレスの最終アドレス> <Valid lifetime> <Preferred lifetime> | <DHCP クライアントインタフェース名> <DHCP クライアントインタフェース番号> <先頭インタフェース ID> <最終インタフェース ID>}

no address [{<IPv6 アドレスの先頭アドレス> <IPv6 アドレスの最終アドレス> <Valid lifetime> <Preferred lifetime> | <DHCP クライアントインタフェース名> <DHCP クライアントインタフェース番号> <先頭インタフェース ID> <最終インタフェース ID>}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
IPv6 アドレスの先頭アドレス	配布する IPv6 アドレスの先頭アドレスを指定します。	IPv6 アドレス形式	省略不可
IPv6 アドレスの最終アドレス	配布する IPv6 アドレスの最終アドレスを指定します。	IPv6 アドレス形式	省略不可
Valid lifetime	Valid Lifetime 値 (単位: 秒) を指定します。	1 ~ 31536000 infinity: 無制限	省略不可
Preferred lifetime	Preferred lifetime 値 (単位: 秒) を指定します。	1 ~ 31536000 infinity: 無制限	省略不可
DHCP クライアントインタフェース名	連携する DHCPv6 クライアント機能が動作するインタフェース名を指定します。	-	省略不可

パラメタ	設定内容	設定範囲	省略時
DHCP クライアントインタフェース番号	連携する DHCPv6 クライアント機能が動作するインタフェース番号を指定します。	-	省略不可
先頭インタフェース ID	配布する IPv6 アドレスの先頭インタフェース ID を指定します。	IPv6 アドレスの下位 80bit	省略不可
最終インタフェース ID	配布する IPv6 アドレスの最終インタフェース ID を指定します。	IPv6 アドレスの下位 80bit	省略不可

【動作モード】

ipv6 dhcp server プロファイル設定モード

【説明】

DHCPv6 クライアントに配布する IPv6 アドレス情報を設定します。

DHCPv6 クライアント機能と連携する場合は、DHCPv6 クライアントが機能しているインタフェースと配布する IPv6 アドレスのインタフェース ID を設定します。

先頭から 4 件までの設定を有効とし、配布する最大アドレス数は 253 個です。

【実行例】

DHCPv6 クライアントに配布する IPv6 アドレス情報を設定します (IPv6 アドレス配布範囲 : 2001:db8:1001::100 ~ 2001:db8:1001::200、Valid lifetime : 86400、Preferred lifetime : 72000)。

```
#configure terminal
(config)#ipv6 dhcp server-profile prof1
(config-dhcps6 prof1)# address 2001:db8:1001::100 2001:db8:1001::200 86400 72000
```

DHCPv6 クライアント機能と連携して配布する IPv6 アドレス情報を設定します (インタフェース : port-channel 101、配布する IPv6 アドレスのインタフェース ID 範囲 : ::1:100 ~ ::1:200)。

```
#configure terminal
(config)#ipv6 dhcp server-profile prof1
(config-dhcps6 prof1)# address port-channel 101 ::1:100 ::1:200
```

【未設定時】

IPv6 アドレスを配布しません。

12.7.11 dns

【機能】

DHCPv6 クライアントに配布する DNS サーバアドレス情報の設定

【入力形式】

dns [<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>] | <DHCP クライアントインタフェース名> <DHCP クライアントインタフェース番号>]

no dns [[<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>] | <DHCP クライアントインタフェース名> <DHCP クライアントインタフェース番号>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プライマリ DNS サーバアドレス	配布するプライマリ DNS サーバアドレスを指定します。	IPv6 アドレス形式	省略不可
セカンダリ DNS サーバアドレス	配布するセカンダリ DNS サーバアドレスを指定します。	IPv6 アドレス形式	プライマリ DNS サーバアドレスのみ配布
DHCP クライアントインタフェース名	連携する DHCPv6 クライアント機能が動作するインタフェース名を指定します。	-	省略不可
DHCP クライアントインタフェース番号	連携する DHCPv6 クライアント機能が動作するインタフェース番号を指定します。	-	省略不可

【動作モード】

ipv6 dhcp server プロファイル設定モード

【説明】

DHCPv6 クライアントに配布する DNS サーバアドレス情報を設定します。

DHCPv6 クライアント機能で取得した DNS サーバアドレスを配布する場合、DHCPv6 クライアント機能が動作するインタフェースを設定します。

【実行例】

DHCPv6 クライアントに配布する DNS サーバアドレス情報を設定します（プライマリ DNS サーバアドレス：2001:db8:1001::10、セカンダリ DNS サーバアドレス：2001:db8:1001::20）。

```
#configure terminal
(config)#ipv6 dhcp server-profile prof1
(config-dhcpv6 prof1)# dns 2001:db8:1001::10 2001:db8:1001::20
```

DHCPv6 クライアント機能で取得した DNS サーバアドレスを配布する設定をします（連携する DHCPv6 クライアント機能が動作するインタフェース：port-channel 101）。

```
#configure terminal
(config)#ipv6 dhcp server-profile prof1
(config-dhcpv6 prof1)# dns port-channel 101
```

【未設定時】

DNS サーバアドレスを配布しません。

12.7.12 domain

【機能】

DHCPv6 クライアントに配布する DNS ドメイン名情報の設定

【入力形式】

domain {<DNS ドメイン名> | <DHCP クライアントインタフェース名> <DHCP クライアントインタフェース番号>}

no domain [{<DNS ドメイン名> | <DHCP クライアントインタフェース名> <DHCP クライアントインタフェース番号>}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
DNS ドメイン名	配布する DNS ドメイン名を指定します。	80 文字以内の DOMAINWORD 型	省略不可
DHCP クライアント インタフェース名	連携する DHCPv6 クライアント機能が動作するインタフェース名を指定します。	-	省略不可
DHCP クライアント インタフェース番号	連携する DHCPv6 クライアント機能が動作するインタフェース番号を指定します。	-	省略不可

【動作モード】

ipv6 dhcp server プロファイル設定モード

【説明】

DHCPv6 クライアントに配布する DNS ドメイン名情報を設定します。

DHCPv6 クライアント機能で取得した DNS ドメイン名を配布する場合、DHCPv6 クライアント機能が動作するインタフェースを設定します。

【実行例】

DHCPv6 クライアントに配布する DNS ドメイン名情報を設定します (DNS ドメイン名: example.com)。

```
#configure terminal
(config)#ipv6 dhcp server-profile prof1
(config-dhcps6 prof1)# domain example.com
```

DHCPv6 クライアント機能で取得した DNS ドメイン名を配布する設定をします (連携する DHCPv6 クライアント機能が動作するインタフェース: port-channel 101)。

```
#configure terminal
(config)#ipv6 dhcp server-profile prof1
(config-dhcps6 prof1)# domain port-channel 101
```

【未設定時】

DNS ドメイン名を配布しません。

12.7.13 duid

【機能】

DHCP オプション (2): サーバ ID で使用する ID の設定

【入力形式】

duid <DUID 値>

no duid [<DUID 値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
DUID 値	DHCPv6 サーバの DUID 値を指定します。	最大 127 桁の 16 進数	省略不可

【動作モード】

ipv6 dhcp server プロファイル設定モード

【説明】

DHCP オプション (2): サーバ ID で使用する ID 値を設定します。

【実行例】

DHCP オプション (2): サーバ ID で使用する ID 値を設定します (DUID 値: 12345678901234567890)。

```
#configure terminal
(config)#ipv6 dhcp server-profile prof1
(config-dhcpv6 prof1)#duid 12345678901234567890
```

【未設定時】

DHCP オプション (2): サーバ ID に MAC アドレスを使用します。

12.7.14 option

【機能】

任意の DHCP オプションを配布する設定

【入力形式】

option <DHCP オプション番号> hex <DHCP オプション内容>

no option <DHCP オプション番号> [hex <DHCP オプション内容>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
DHCP オプション番号	配布する DHCP オプション番号を指定します。	1 ~ 254	省略不可
DHCP オプション内容	配布する DHCP オプションデータを指定します。	最大 127 桁の 16 進数	省略不可

【動作モード】

ipv6 dhcp server プロファイル設定モード

【説明】

DHCP オプション番号とオプション内容を設定することにより、任意の DHCP オプションを配布することができます。

DHCP オプション番号でソートされ、DHCP オプション番号が一番小さいエントリから 4 件までが有効となります。

【実行例】

任意の DHCP オプションを配布する設定をします (DHCP オプション番号: 100、DHCP オプション内容: 1234567890)。

```
#configure terminal
(config)#ipv6 dhcp server-profile prof1
(config-dhcpv6 prof1)# option 100 hex 1234567890
```

【未設定時】

任意の DHCP オプションを配布しません。

12.7.15 preference

【機能】

DHCP オプション (7): サーバ優先度で使用する優先度の設定

【入力形式】

preference <サーバ優先度>

no preference <サーバ優先度>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
サーバ優先度	DHCPv6 サーバの優先度を指定します。	0～255	省略不可

【動作モード】

ipv6 dhcp server プロファイル設定モード

【説明】

DHCP オプション (7): サーバ優先度で使用する優先度を設定します。

大きい値ほど優先度が高くなります。

【実行例】

DHCP オプション (7): サーバ優先度で使用する優先度を設定します (サーバ優先度: 50)。

```
#configure terminal
(config)#ipv6 dhcp server-profile prof1
(config-dhcps6 prof1)# preference 50
```

【未設定時】

サーバ優先度は 0 で動作します。

12.7.16 prefix

【機能】

DHCPv6 クライアントに配布するプレフィックス情報の設定

【入力形式】

prefix {<プレフィックス> <Valid lifetime> <Preferred lifetime> <経路の自動登録> <DUID 値> | <DHCP クライアントインタフェース名> <DHCP クライアントインタフェース番号> <プレフィックス下位 80bit> <経路の自動登録> <DUID 値>}

no prefix [{<プレフィックス> <Valid lifetime> <Preferred lifetime> <経路の自動登録> <DUID 値> |
<DHCP クライアントインタフェース名> <DHCP クライアントインタフェース番号> <プレフィックス
下位 80bit> <経路の自動登録> <DUID 値>}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プレフィックス	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。	IPv6 アドレス形式	省略不可
Valid lifetime	Valid lifetime 値（単位：秒）を指定します。	1～31536000	省略不可
Preferred lifetime	Preferred lifetime 値（単位：秒）を指定します。	1～31536000 infinity: 無制限	省略不可
経路の自動登録	配布プレフィックスへの経路を自動登録の動作を指定します。	on: 配布プレフィックスへの経路の登録を行う off: 配布プレフィックスへの経路の登録を行わない	省略不可
DUID 値	プレフィックスを配布するクライアントの DUID を指定します。	最大 127 桁の 16 進数	省略不可
DHCP クライアントインタフェース名	連携する DHCPv6 クライアント機能が動作するインタフェース名を指定します。	-	省略不可
DHCP クライアントインタフェース番号	連携する DHCPv6 クライアント機能が動作するインタフェース番号を指定します。	-	省略不可
プレフィックス下位 80bit	配布するプレフィックスの下位 80bit/ プレフィックス長を指定します。	プレフィックスの下位 80bit/ プレフィックス長	省略不可

【動作モード】

ipv6 dhcp server プロファイル設定モード

【説明】

DHCPv6 クライアントに配布するプレフィックス情報を設定します。

DHCPv6 クライアント機能で取得したプレフィックスを配布する場合、DHCPv6 クライアント機能が動作するインタフェースを設定します。

DHCPv6 クライアント機能と連動する場合、プレフィックスは下位 80bit を設定します。

経路の自動登録に on を指定した場合、クライアントへの経路登録を行います。

【実行例】

DHCPv6 クライアントに配布するプレフィックス情報を設定します（プレフィックス：2001:db8:1001::/64、Valid lifetime: 無制限、Preferred lifetime: 無制限、経路の自動登録：on、DUID 値：001234）。

```
#configure terminal
(config)#ipv6 dhcp server-profile prof1
(config-dhcpv6 prof1)# prefix 2001:db8:1001::/64 infinity infinity on 001234
```

DHCPv6 クライアント機能と連動して DHCPv6 クライアントに配布するプレフィックス情報を設定します（インタフェース：port-channel 101、プレフィックス下位 80bit：:1000::/64、経路の自動登録：off、DUID 値：12345678901234567890）。

```
#configure terminal
(config)#ipv6 dhcp server-profile prof1
(config-dhcpv6 prof1)# prefix port-channel 101 :1000::/64 off 12345678901234567890
```

【未設定時】

プレフィックスを配布しません。

12.7.17 sip-server address

【機能】

DHCPv6 クライアントに配布する SIP サーバアドレス情報の設定

【入力形式】

sip-server address {<プライマリ SIP サーバアドレス> [<セカンダリ SIP サーバアドレス>] | <DHCP クライアントインタフェース名> <DHCP クライアントインタフェース番号>}

no sip-server address [{<プライマリ SIP サーバアドレス> [<セカンダリ SIP サーバアドレス>] | <DHCP クライアントインタフェース名> <DHCP クライアントインタフェース番号>}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プライマリ SIP サーバアドレス	配布するプライマリ SIP サーバアドレスを指定します。	IPv6 アドレス形式	省略不可
セカンダリ SIP サーバアドレス	配布するセカンダリ SIP サーバアドレスを指定します。	IPv6 アドレス形式	プライマリ SIP サーバアドレスのみ配布
DHCP クライアントインタフェース名	連携する DHCPv6 クライアント機能が動作するインタフェース名を指定します。	-	省略不可
DHCP クライアントインタフェース番号	連携する DHCPv6 クライアント機能が動作するインタフェース番号を指定します。	-	省略不可

【動作モード】

ipv6 dhcp server プロファイル設定モード

【説明】

DHCPv6 クライアントに配布する SIP サーバアドレス情報を設定します。

DHCPv6 クライアント機能で取得した SIP サーバアドレスを配布する場合、DHCPv6 クライアント機能が動作するインタフェースを設定します。

【実行例】

DHCPv6 クライアントに配布する SIP サーバアドレス情報を設定します（プライマリ SIP サーバアドレス：2001:db8:1001::10、セカンダリ SIP サーバアドレス：2001:db8:1001::20）。

```
#configure terminal
(config)#ipv6 dhcp server-profile prof1
(config-dhcps6 prof1)# sip-server address 2001:db8:1001::10 2001:db8:1001::20
```

DHCPv6 クライアント機能で取得した SIP サーバアドレスを配布する設定をします（連携する DHCPv6 クライアント機能が動作するインタフェース：port-channel 101）。

```
#configure terminal
(config)#ipv6 dhcp server-profile prof1
(config-dhcps6 prof1)# sip-server address port-channel 101
```

【未設定時】

SIP サーバアドレスを配布しません。

12.7.18 sip-server domain

【機能】

DHCPv6 クライアントに配布する SIP ドメイン名情報の設定

【入力形式】

sip-server domain {<プライマリ SIP ドメイン名> [<セカンダリ SIP ドメイン名>] | <DHCP クライアントインタフェース名> <DHCP クライアントインタフェース番号>}

no sip-server domain [{<プライマリ SIP ドメイン名> [<セカンダリ SIP ドメイン名>] | <DHCP クライアントインタフェース名> <DHCP クライアントインタフェース番号>}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プライマリ SIP ドメイン名	配布するプライマリ SIP ドメイン名を指定します。	80 文字以内のドメイン名	省略不可
セカンダリ SIP ドメイン名	配布するセカンダリ SIP ドメイン名を指定します。	80 文字以内のドメイン名	プライマリ SIP ドメイン名のみ配布
DHCP クライアントインタフェース名	連携する DHCPv6 クライアント機能が動作するインタフェース名を指定します。	-	省略不可
DHCP クライアントインタフェース番号	連携する DHCPv6 クライアント機能が動作するインタフェース番号を指定します。	-	省略不可

【動作モード】

ipv6 dhcp server プロファイル設定モード

【説明】

DHCPv6 クライアントに配布する SIP ドメイン名情報を設定します。

DHCPv6 クライアント機能で取得した SIP ドメイン名を配布する場合、DHCPv6 クライアント機能が動作するインタフェースを設定します。

【実行例】

DHCPv6 クライアントに配布する SIP ドメイン名情報を設定します（プライマリ SIP ドメイン名：example-first.com、セカンダリ SIP ドメイン名：example-2nd.com）。

```
#configure terminal
(config)#ipv6 dhcp server-profile prof1
(config-dhcps6 prof1)# sip-server domain example-first.com example-2nd.com
```

DHCPv6 クライアント機能で取得した SIP ドメイン名情報を配布する設定をします（連携する DHCPv6 クライアント機能が動作するインタフェース：port-channel 101）。

```
#configure terminal
(config)#ipv6 dhcp server-profile prof1
(config-dhcps6 prof1)# sip-server domain port-channel 101
```


【未設定時】

SIP ドメイン名を配布しません。

12.7.19 sntp-server

【機能】

DHCPv6 クライアントに配布する SNTP サーバアドレス情報の設定

【入力形式】

sntp-server {<プライマリ SNTP サーバアドレス> [<セカンダリ SNTP サーバアドレス>] | <DHCP クライアントインタフェース名> <DHCP クライアントインタフェース番号>}

no sntp-server [[<プライマリ SNTP サーバアドレス> [<セカンダリ SNTP サーバアドレス>] | <DHCP クライアントインタフェース名> <DHCP クライアントインタフェース番号>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プライマリ SNTP サーバアドレス	配布するプライマリ SNTP サーバアドレスを指定します。	IPv6 アドレス形式	省略不可
セカンダリ SNTP サーバアドレス	配布するセカンダリ SNTP サーバアドレスを指定します。	IPv6 アドレス形式	プライマリ SNTP サーバアドレスのみ配布
DHCP クライアントインタフェース名	連携する DHCPv6 クライアント機能が動作するインタフェース名を指定します。	-	省略不可
DHCP クライアントインタフェース番号	連携する DHCPv6 クライアント機能が動作するインタフェース番号を指定します。	-	省略不可

【動作モード】

ipv6 dhcp server プロファイル設定モード

【説明】

DHCPv6 クライアントに配布する SNTP サーバアドレス情報を設定します。

DHCPv6 クライアント機能で取得した SNTP サーバアドレスを配布する場合、DHCPv6 クライアント機能が動作するインタフェースを設定します。

【実行例】

DHCPv6 クライアントに配布する SNTP サーバアドレス情報を設定します（プライマリ SNTP サーバアドレス：2001:db8:1001::10、セカンダリ SNTP サーバアドレス：2001:db8:1001::20）。

```
#configure terminal
(config)#ipv6 dhcp server-profile prof1
(config-dhcps6 prof1)# sntp-server 2001:db8:1001::10 2001:db8:1001::20
```

DHCPv6 クライアント機能で取得した SNTP サーバアドレス情報を配布する設定をします（連携する DHCPv6 クライアント機能が動作するインタフェース：port-channel 101）。

```
#configure terminal
(config)#ipv6 dhcp server-profile prof1
(config-dhcps6 prof1)# sntp-server port-channel 101
```

【未設定時】

SNTP サーバアドレスを配布しません。

12.7.20 host

【機能】

特定ホストに配布する IPv6 アドレスと DUID の設定

【入力形式】

host <定義番号> <配布する IPv6 アドレス> <配布先ホストの DUID>

no host <定義番号> [<配布する IPv6 アドレス> <配布先ホストの DUID>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
定義番号	ホストデータベースの定義番号を指定します。	1～64	省略不可
配布する IPv6 アドレス	固定配布する IPv6 アドレスを指定します。	IPv6 アドレス形式	省略不可
配布先ホストの DUID	配布先ホストの DUID を指定します。	最大 127 桁の 16 進数	省略不可

【動作モード】

ipv6 dhcp host-database 設定モード

【説明】

特定ホストに配布する IPv6 アドレスと DUID を設定します。

【実行例】

特定ホストに配布する IPv6 アドレスと DUID を設定します（定義番号：1、配布する IPv6 アドレス：2001:db8:1001::100、配布先ホストの DUID：1234567890）。

```
(config)#ipv6 dhcp host-database
(config-dhcp6-host)# host 1 2001:db8:1001::100 1234567890
```

【未設定時】

特定ホストに対し、固定の IPv6 アドレスを割り当てません。

12.8 IPv6 アドレス有効設定

12.8.1 ipv6 enable

【機能】

リンクローカルアドレスの付与

【入力形式】

ipv6 enable

no ipv6 enable

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

IPv6 アドレスが明示的に設定されていないインタフェースに、リンクローカルアドレスのみ付与します。

【実行例】

リンクローカルアドレスのみ付与します。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 enable
```

【未設定時】

IPv6 アドレスを明示的に設定しない場合、リンクローカルアドレスも割り当てられません。

12.9 IPv6 Neighbor Discovery Protocol 設定

12.9.1 ipv6 hop-limit

【機能】

IPv6 ヘッダにつける最大 HOP 数の設定

【入力形式】

ipv6 hop-limit <最大 HOP 数>

no ipv6 hop-limit

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
最大 HOP 数	IPv6 の最大 HOP 数を指定します。 この値以上のルータを経由したデータは、廃棄されます。	1 ～ 255	省略不可

【動作モード】

基本設定モード

【説明】

本装置から IPv6 データを送信する際に、IPv6 ヘッダにつける最大 HOP 数を設定します。また、Router Advertisement(RA)を送信する際に使用する最大 HOP 数の値も設定します。

【実行例】

IPv6 ヘッダにつける最大 HOP 数を設定します（最大 HOP 数：15）。

```
#configure terminal
(config)#ipv6 hop-limit 15
```

【未設定時】

本装置が送信する IPv6 パケットには 64 を使用し、ルータ通知には 0 の値を含めます。

12.9.2 ipv6 nd max-solicit

【機能】

NS の最大送信回数の設定

【入力形式】

ipv6 nd max-solicit <NS 最大送信回数>

no ipv6 nd max-solicit [<NS 最大送信回数>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
NS 最大送信回数	NS 最大送信回数を指定します。	1 ～ 30	省略不可

【動作モード】

基本設定モード

【説明】

NS の最大送信回数を設定します。

【実行例】

NS の最大送信回数を設定します (NS 最大送信回数：15)。

```
#configure terminal
(config)#ipv6 nd max-solicit 15
```

【未設定時】

NS 最大送信回数は 3 回で動作します。

12.9.3 ipv6 nd packet-hold

【機能】

NDP 解決中に滞留させるパケット数の設定

【入力形式】

ipv6 nd packet-hold <装置最大数> <1 エントリ最大数>

no ipv6 nd packet-hold [<装置最大数> <1 エントリ最大数>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
装置最大数	装置の最大数を指定します。	1 ～ 2048	省略不可
1 エントリ最大数	1 エントリの最大数を指定します。	1 ～ 32	

【動作モード】

基本設定モード

【説明】

NDP 解決中に滞留させるパケット数を設定します。

【実行例】

NDP 解決中に滞留させるパケット数を設定します (装置最大数：1024、1 エントリ最大数：16)。

```
#configure terminal
(config)#ipv6 nd packet-hold 1024 16
```

【未設定時】

以下の値で動作します。

装置最大数： 2048

1 エントリ最大数： 32

12.9.4 ipv6 neighbor

【機能】

スタティックでの Neighbor Discovery(ND) の登録

【入力形式】

ipv6 neighbor <IPv6 アドレス> <インタフェース名> <インタフェース番号> <MAC アドレス>

no ipv6 neighbor <IPv6 アドレス> [<インタフェース名> <インタフェース番号> <MAC アドレス>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
IPv6 アドレス	スタティックで ND を登録する IPv6 アドレスを指定します。	IPv6 アドレス型式	省略不可
インタフェース名	インタフェース名を指定します。	-	
インタフェース番号	インタフェース番号を指定します。	-	
MAC アドレス	指定する IPv6 アドレスを持つノードの MAC アドレスを指定します。	HHHH.HHHH.HHHH 形式	

【動作モード】

基本設定モード

【説明】

スタティックで Neighbor Discovery(ND) を登録します。

【実行例】

スタティックで ND を登録します (IPv6 アドレス：2001:db8::1、インタフェース名：gigaethernet、インタフェース番号：1/1、MAC アドレス：2ed4:4401:2345)。

```
#configure terminal
(config)#ipv6 neighbor 2001:db8::1 gigaethernet 1/1 2ed4.4401.2345
```

【未設定時】

NDP を使用して学習します。

12.9.5 ipv6 hoplimit-receive-enable

【機能】

受信した RA で指定されている CurHopLimit を有効とする設定

【入力形式】

ipv6 hoplimit-receive-enable

no ipv6 hoplimit-receive-enable

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

受信した RA で指定されている CurHopLimit を有効とする場合に設定します。有効とする場合、受信した CurHopLimit と設定されているホップリミットを比較し、小さい値を実際のインタフェースのホップリミットとします。

【実行例】

受信した RA で指定されている CurHopLimit を有効とします。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 hoplimit-receive-enable
```

【未設定時】

CurHopLimit 情報を無視します。

12.9.6 ipv6 mtu-receive-enable

【機能】

受信した RA の MTU オプションで指定されている MTU 値を有効とする設定

【入力形式】

ipv6 mtu-receive-enable

no ipv6 mtu-receive-enable

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

受信した RA の MTU オプションで指定されている MTU 値を有効とする場合に設定します。有効とする場合、受信した MTU 長と設定されている MTU 長を比較し、小さい値を実際のインタフェースの MTU 長とします。

受信した RA の MTU オプションで指定されている MTU は、IPv6 の自局送信パケットにのみ反映されます。

【実行例】

受信した RA の MTU オプションで指定されている MTU 値を有効とします。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 mtu-receive-enable
```

【未設定時】

MTU オプションを受信しても無視します。

12.9.7 ipv6 nd managed-config-flag

【機能】

RA 内の M フラグのセット

【入力形式】

ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

RA 内の M フラグをセットします。M フラグがセットされた RA をホストが受信した場合、ホストはアドレスの自動設定のためにステートフルプロトコルを利用します。

【実行例】

RA 内の M フラグをセットします。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 nd managed-config-flag
```

【未設定時】

RA 内の M フラグをセットしません。

12.9.8 ipv6 nd ns-interval

【機能】

Neighbor Solicitation を送信する間隔の設定

【入力形式】

ipv6 nd ns-interval <NS 送信間隔>

no ipv6 nd ns-interval [<NS 送信間隔>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
NS 送信間隔	NS の送信間隔（単位：ミリ秒）を指定します。	1000～4294967295	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

Neighbor Solicitation(NS)を送信する間隔を設定します。設定値を RA の Retrans Timer フィールドに含め、かつ、本装置自身もこの値を使用します。

【実行例】

NS を送信する間隔を設定します（NS 送信間隔：1000 ミリ秒）。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 nd ns-interval 1000
```

【未設定時】

以下の値で動作します。

RA の Retrans Timer フィールド :0（未指定）

本装置自身： 1000

12.9.9 ipv6 nd other-config-flag

【機能】

RA 内の O フラグのセット

【入力形式】

ipv6 nd other-config-flag

no ipv6 nd other-config-flag

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

RA 内の O フラグをセットします。O フラグがセットされた RA をホストが受信した場合、ホストはアドレス以外の情報を自動設定するためにステートフルプロトコルを使用します。

【実行例】

RA 内の O フラグをセットします。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 nd other-config-flag
```

【未設定時】

RA内のOフラグをセットしません。

12.9.10 ipv6 nd prefix-advertisement

【機能】

RAに含まれるIPv6プレフィックスの設定

【入力形式】

```
ipv6 nd prefix-advertisement <プレフィックス> <Valid Lifetime> <Preferred Lifetime> [onlink]
[autoconfig]
```

```
no ipv6 nd prefix-advertisement <プレフィックス> [<Valid Lifetime> <Preferred Lifetime> [onlink]
[autoconfig]]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プレフィックス	RAで通知するIPv6プレフィックスを指定します。	IPv6アドレス形式	省略不可
Valid Lifetime	Valid Lifetime 値（単位：秒）を指定します。	0～4294967295	
Preferred Lifetime	Preferred Lifetime 値（単位：秒）を指定します。	0～4294967295	
onlink	Onlink フラグを立てる場合に指定します。	-	Onlink フラグを立てない
autoconfig	Autoconfig フラグを立てる場合に指定します。	-	Autoconfig フラグを立てない

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

RAに含まれるIPv6プレフィックスを設定します。"onlink"、"autoconfig"はそれぞれ、プレフィックスオプション内のLフラグ、Aフラグをセットします。本設定は、設定順にソートされます。

Valid Lifetime	このプレフィックスをノードが使用する場合に、使用可能な時間（単位：秒）
Preferred Lifetime	このプレフィックスをノードが使用する場合に、正当な使用が問題ない時間（単位：秒）
onlink フラグ	同一リンク上に存在することを表すフラグ
Autoconfig フラグ	ノードがプレフィックスを受信した場合に、Stateless Auto Configuration でアドレスを使用してよいかどうかを表すフラグ

【実行例】

RAに含まれるIPv6プレフィックスを設定します（プレフィックス：2001:db8::/32、Valid Lifetime：500秒、Preferred Lifetime：400秒、Autoconfigフラグ）。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 nd prefix-advertisement 3ffe:1::/48 500 400 autoconfig
```

【未設定時】

以下の値で動作します。

```
sValid Lifetime:    2592000 秒 (30 日)
sPreferred Lifetime: 604800 秒 (7 日)
sonlink:            あり
sautoconfig:        あり
```

12.9.11 ipv6 nd pre-solution disable

【機能】

経路登録時ゲートウェイに対する Neighbor Solicitation の送信の抑制

【入力形式】

ipv6 nd pre-solution disable

no ipv6 nd pre-solution disable

【動作モード】

基本設定モード

【説明】

本装置は、経路登録時にゲートウェイに対し Neighbor Solicitation を送信することがありますが、その送信を停止します。

【実行例】

経路登録時ゲートウェイに対する Neighbor Solicitation の送信を抑制します。

```
#configure terminal
(config)# ipv6 nd pre-solution disable
```

【未設定時】

経路登録時にゲートウェイに対し Neighbor Solicitation を送信することがあります。

12.9.12 ipv6 nd ra-delay

【機能】

Router Advertisement の初回送信までの遅延時間の設定

【入力形式】

```
ipv6 nd ra-delay <RS 初回送信遅延時間>
```

```
no ipv6 nd ra-delay [<RS 初回送信遅延時間>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
RA 初回送信遅延時間	RA の初回送信までの遅延時間（単位：秒）を指定します。	0 ～ 3600	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

Router Advertisement(RA) の初回送信までの遅延時間の設定をします。

【実行例】

RA 送信を開始します。

```

【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 nd ra-delay 5

```

【未設定時】

RA の初回送信までの遅延時間は、1 秒で動作します。

12.9.13 ipv6 nd ra-interval

【機能】

Router Advertisement を送信する間隔の設定

【入力形式】

```
ipv6 nd ra-interval <RA 送信間隔>
```

```
no ipv6 nd ra-interval [<RA 送信間隔>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
RA 送信間隔	RA を定期送信する際の送信間隔（単位：秒）を指定します。	4 ～ 1800	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

Router Advertisement(RA) を送信する間隔（単位：秒）を設定します。

【実行例】

RAを送信する間隔を設定します（RA送信間隔：300秒）。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 nd ra-interval 300
```

【未設定時】

RA送信間隔は200秒で動作します。

12.9.14 ipv6 nd ra-lifetime

【機能】

Router Advertisementに含まれるルータ有効時間の設定

【入力形式】

ipv6 nd ra-lifetime <ルータ有効時間>

no ipv6 nd ra-lifetime [<ルータ有効時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ルータ有効時間	RAに含まれる、ルータ有効時間 (単位：秒) を指定します。	0～65535	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

Router Advertisement(RA)に含まれるルータ有効時間（単位：秒）を設定します。ルータ自身がデフォルトルータとして有効な時間を意味します。0秒を設定した場合には、デフォルトルータとなりません。

【実行例】

ルータ有効時間を設定します（ルータ有効時間：3600秒）。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 nd ra-lifetime 3600
```

【未設定時】

ルータ有効時間は1800秒で動作します。

12.9.15 ipv6 nd reachable-time

【機能】

ノードを到達可能とみなす時間の設定

【入力形式】

ipv6 nd reachable-time <Reachable Time 値>

no ipv6 nd reachable-time [<Reachable Time 値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
Reachable Time 値	Reachable Time 値（単位：ミリ秒）を指定します。	0～3600000	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

リモート IPv6 ノードに対してなんらかの到達確認イベントが発生したあとに、そのノードを到達可能とみなす時間（単位：ミリ秒）を設定します。0 を設定した場合には、本装置によって指定しない（unspecified）ことを示します。

【実行例】

ノードを到達可能とみなす時間（単位：ミリ秒）を設定します（Reachable Time 値：1700000 ミリ秒）。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 nd reachable-time 1700000
```

【未設定時】

以下の値で動作します。

RA: 0 ミリ秒

NS: 30000 ミリ秒

12.9.16 ipv6 reachable-time-receive-enable

【機能】

受信した RA で指定されている Reachable time を有効とする設定

【入力形式】

ipv6 reachable-time-receive-enable

no ipv6 reachable-time-receive-enable

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

受信した RA で指定されている Reachable time を有効とする場合に設定します。有効とする場合、受信した Reachable time と設定されている Reachable time を比較し、小さい値を実際のインタフェースの Reachable time とします。

【実行例】

受信した RA で指定されている Reachable time を有効とします。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 reachable-time-receive-enable
```

【未設定時】

Reachable time の情報を受信しても無視します。

12.9.17 ipv6 nd receive-ra

【機能】

RA を受信する設定

【入力形式】

ipv6 nd receive-ra

no ipv6 nd receive-ra

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

RA を受信する場合に設定します。Stateless Auto Configuration の設定を行っている場合には、アドレスを付与させることができます。

【実行例】

RA を受信します。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 nd receive-ra
```

【未設定時】

RA を受信しません。

12.9.18 ipv6 nd rs-delay

【機能】

RS の初回送信までの遅延時間と初回送信以降の送信間隔の設定

【入力形式】

ipv6 nd rs-delay <RS 初回送信遅延時間> <RS 送信間隔>

no ipv6 nd rs-delay [<RS 初回送信遅延時間> <RS 送信間隔>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
RS 初回送信遅延時間	インタフェースが有効になってから、RS の初回送信までの遅延時間（単位：秒）を指定します。	0 ～ 3600	省略不可
RS 送信間隔	RS 初回送信以降の送信間隔（単位：秒）を指定します。	4 ～ 3600	

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

インタフェースが有効になってから、RS の初回送信までの遅延時間と、初回送信以降の送信間隔を設定します。

【実行例】

RS の初回送信までの遅延時間と、初回送信以降の送信間隔を設定します（RS 初回送信遅延時間：5 秒、RS 送信間隔：10 秒）。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 nd rs-delay 5 10
```

【未設定時】

以下の値で動作します。

RS 初回送信遅延時間： 0 秒

RS 送信間隔： 4 秒

12.9.19 ipv6 nd rs-times

【機能】

RS 送信開始後、RA が受信できない場合の RS 送信回数の設定

【入力形式】

ipv6 nd rs-times <RS 送信回数>

no ipv6 nd rs-times [<RS 送信回数>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
RS 送信回数	RS 送信開始後、RA が受信できない場合の RS 送信回数を指定します。	0 ～ 65535	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

RS 送信開始後、RA が受信できない場合の RS 送信回数を設定します。

なお、"0" を設定した場合、RA が受信できるまで RS を送信し続けます。

【実行例】

RA が受信できない場合の RS 送信回数を設定します (RS 送信回数 : 5 回)。

【port-channel インタフェース設定モードの場合】

```
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 nd rs-times 5
```

【未設定時】

RS 送信回数は 3 回で動作します。

12.9.20 ipv6 nd send-ra

【機能】

Router Advertisement の送信を開始する設定

【入力形式】

ipv6 nd send-ra [vrrp]

no ipv6 nd send-ra [vrrp]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
vrrp	vrrp との連携を行う場合に指定します。	-	vrrp との連携を行わない

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

Router Advertisement(RA) の送信を開始します。

ルータが RA を送信することにより、ネットワーク上のホストが自身のプレフィックスを知ることができます。

ホストが Stateless Auto Configuration で動作する場合は、この設定を行ってください。
vrrp のオプションを指定した場合は、vrrp の状態が Master の場合のみ、RA 送信を行います。

【実行例】

RA 送信を開始します。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 nd send-ra
```

【未設定時】

RA を送信しません。

12.9.21 ipv6 nd curhoplimit

【機能】

Router Advertisemet に含まれる最大 hop 数の設定

【入力形式】

ipv6 nd curhoplimit <最大 hop 数>

no ipv6 nd curhoplimit [<最大 hop 数>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
最大 hop 数	RA に含まれる、IPv6 の最大 hop 数を指定します。	1～255	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

Router Advertisemet(RA) に含まれる最大 hop 数を設定します。

【実行例】

Router Advertisemet(RA) に含まれる最大 hop 数を設定します（最大 hop 数：255）。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-port 1)#ipv6 nd curhoplimit 255
```

【未設定時】

RA で、curhoplimit を "0" で通知します。

12.9.22 ipv6 nd mtu

【機能】

Router Advertisemetに含まれる MTU 長の設定

【入力形式】

ipv6 nd mtu <MTU 長>

no ipv6 nd mtu [<MTU 長>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
MTU 長	RAに含まれる、MTU 長（単位：bytes）を指定します。	1280～9100	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

Router Advertisemet(RA)に含まれる MTU 長（単位：bytes）を設定します。

【実行例】

Router Advertisemet(RA)に含まれる MTU 長を設定します（MTU 長：1280byte）。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-port 1)#ipv6 nd mtu 1280
```

【未設定時】

RA で、MTU を通知しません。

12.9.23 ipv6 ns-interval-receive-enable

【機能】

受信した RA で指定されている RetransTimer を有効とする設定

【入力形式】

ipv6 ns-interval-receive-enable

no ipv6 ns-interval-receive-enable

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

受信した RA で指定されている RetransTimer を有効とする場合に設定します。有効とする場合、受信した RetransTimer と設定されている RetransTimer を比較し、小さい値を実際のインタフェースの RetransTimer とします。

【実行例】

受信した RA で指定されている RetransTimer を有効とします。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 ns-interval-receive-enable
```

【未設定時】

RetransTimer の情報を受信しても無視します。

12.9.24 ipv6 router-lifetime-receive-enable

【機能】

受信した RA で指定されている Router time を有効とする設定

【入力形式】

ipv6 router-lifetime-receive-enable

no ipv6 router-lifetime-receive-enable

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

受信した RA で指定されている Router time を有効とする場合に設定します。有効とする場合、受信した Router time で RA を送信したルータを nexthop とする default 経路を登録します。

【実行例】

受信した RA で指定されている Router time を有効とします。

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 router-lifetime-receive-enable
```

【未設定時】

Router time 情報を受信しても無視します。

12.10 送信元 IPv6 アドレスの設定

12.10.1 ipv6 unnumbered

【機能】

送信元として使用する IPv6 アドレスのインタフェースの設定

【入力形式】

ipv6 unnumbered <インタフェース名> <インタフェース番号>

no ipv6 unnumbered

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース名	インタフェース名を指定します。	-	省略不可
インタフェース番号	インタフェース番号を指定します。	-	

【動作モード】

tunnel インタフェース設定モード

【説明】

tunnel インタフェースに IPv6 アドレスを設定していない場合、送信元として使用する IPv6 アドレスをインタフェースで設定します。ipv6 address コマンドで IPv6 アドレスが指定されている場合は、どちらのアドレスも有効となります。

【実行例】

送信元として使用する IPv6 アドレスをインタフェースで設定します（インタフェース名：loopback、インタフェース番号：1）。

```
#configure terminal
(config)#interface tunnel 1
(config-if-tun 1)#ipv6 unnumbered loopback 1
```

【未設定時】

ipv6 unnumbered コマンドも ipv6 address コマンドも設定していない場合には、management インタフェース以外からロングストマッチで送信元アドレスを決定します。

第13章 NAT の設定



この章では、NAT の設定に関するコマンドについて説明します。

13.1 NAT の設定

13.1.1 ip nat pool

【機能】

NAT/NAT+ 変換で変換後アドレスとして利用可能範囲の設定

【入力形式】

ip nat pool <pool 番号> <変換後のアドレス：開始> <変換後のアドレス：終了>

no ip nat pool <pool 番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
pool 番号	pool 番号を指定します。	1～8	省略不可
変換後のアドレス：開始	NAT/NAT+ 変換後アドレスを範囲指定する場合の先頭のアドレスを指定します。	IPv4 アドレス形式	省略不可
変換後のアドレス：終了	NAT/NAT+ 変換後アドレスを範囲指定する場合の最後のアドレスを指定します。	IPv4 アドレス形式	省略不可

【動作モード】

基本設定モード

【説明】

NAT/NAT+ 変換で変換後のアドレスとして利用可能なアドレスの範囲を指定します。

アドレスは、<変換後のアドレス：開始>から順に払い出していきます。

【実行例】

NAT/NAT+ 変換で変換後のアドレスとして利用可能なアドレスの範囲を指定します（pool 番号：2、変換後アドレス範囲：10.0.0.2～10.0.0.254）。

```
#configure terminal
(config)#ip nat pool 2 10.0.0.2 10.0.0.254
```

【未設定時】

当該 pool 番号を利用する ip nat inside source の設定が無効となります。

13.1.2 ip nat list

【機能】

NAT 変換の対象アドレスの設定

【入力形式】

ip nat list <NAT リスト番号> {any | <送信元アドレス> <ワイルドカードマスク>}

no ip nat list <NAT リスト番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
NAT リスト番号	NAT リスト番号を指定します。	1～8	省略不可
any	すべてのアドレスを NAT 変換の対象に指定します。	-	省略不可
送信元アドレス	NAT 変換の対象にする送信元アドレスを指定します。	IPv4 アドレス形式	省略不可
ワイルドカードマスク	送信元アドレスのワイルドカードマスクを指定します。	IPv4 アドレス形式	省略不可

【動作モード】

基本設定モード

【説明】

NAT 変換の対象アドレスを設定します。

【実行例】

NAT 変換の対象アドレスを設定します (NAT リスト番号：1、NAT 変換対象アドレス：192.168.0.0/24)。

```
#configure terminal
(config)#ip nat list 1 192.168.0.0 0.0.0.255
```

【未設定時】

当該 NAT リスト番号を利用する ip nat inside source の設定が無効となります。

13.1.3 ip nat inside source list pool

【機能】

設定のあるインタフェースから送信するパケットの送信元アドレスに対する NAT/NAT+ 変換ルールの設定 (pool のアドレスを利用)

【入力形式】

```
ip nat inside source list <NAT リスト番号> [<変換前ポート：開始> <変換前ポート：終了>] pool <pool 番号> [<変換後ポート：開始> <変換後ポート：終了>] [overload]
```

```
no ip nat inside source list <NAT リスト番号> [<変換前ポート：開始> <変換前ポート：終了>] pool <pool 番号> [<変換後ポート：開始> <変換後ポート：終了>] [overload]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
NAT リスト番号	NAT/NAT+ 変換前パケットの送信元アドレスを規定した NAT リストを指定します。	1～8	省略不可
変換前ポート：開始 変換前ポート：終了	NAT+ 変換前のパケットの TCP/UDP の送信元ポート番号の範囲を指定します。 本設定を入れると TCP/UDP パケットのみが NAT 変換対象になります。	1～65535	自動ポート変換

パラメタ	設定内容	設定範囲	省略時
pool 番号	NAT/NAT+ 変換後の IP アドレスを払い出す pool を指定します。	1～8	省略不可
変換後ポート：開始 変換後ポート：終了	NAT+ 変換後のパケットの TCP/UDP の送信元ポート番号の範囲を指定します。	1～65535	自動ポート変換
overload	この設定がある場合 NAT+ 変換を行う際に、TCP/UDP の送信元ポート番号を、必ず変換します。	-	ポート番号を基本的には変換しない すでにそのポート番号が使用されている場合に限り、別のポート番号に変換

【動作モード】

port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

設定のあるインタフェースから送信するパケットの送信元アドレスに対する NAT/NAT+ 変換ルールを設定します。

変換後のアドレスは pool のアドレスを使用します。

アドレス、ポート番号に余りがない場合は廃棄します。

1つのインタフェースに同一 pool 番号を複数設定した場合、NAT テーブル作成ができない場合があります。

- ポート、overload の設定を省略した場合
払い出すアドレスが pool からなくなるまでは、NAT 変換を行います（TCP/UDP の送信元ポート番号は変更しません）。
パケットの送信元アドレスが異なる場合は、pool より新しいアドレスを払い出します。
pool にアドレスの余りがなくなった場合は、最後に払い出したアドレスを使って NAT+ 変換を行います。
- ポート、overload の設定を行った場合
NAT+ 変換を行います。
空いているポート番号がある限り、pool より新しいアドレスは払い出しを行いません。

【実行例】

pool で指定したアドレス範囲で、送信元アドレスを NAT 変換する場合のルールを設定します（pool 番号：2、変換後アドレス範囲：10.0.0.2～10.0.0.254、NAT リスト：1、NAT 変換対象アドレス：192.168.0.0/24）。

```

【port-channel の場合】
#configure terminal
(config)#ip nat pool 2 10.0.0.2 10.0.0.254
(config)#ip nat list 1 192.168.0.0 0.0.0.255
(config)#
(config)#interface port-channel 2
(config-if-ch 2)#ip nat inside source list 1 pool 2

```

pool で指定したアドレス範囲で、送信元アドレスを NAT+ 変換する場合のルールを設定します（NAT リスト：1、NAT 変換対象アドレス：192.168.0.0/24、NAT 変換対象ポート番号範囲：1～1024、pool 番号：2、変換後アドレス範囲：10.0.0.2～10.0.0.254、変換後ポート番号範囲：1～65535、overload：TCP/UDP の送信元ポート番号を必ず変換する）。

```

【port-channel の場合】
#configure terminal
(config)#ip nat list 1 192.168.0.0 0.0.0.255
(config)#ip nat pool 2 10.0.0.2 10.0.0.254
(config)#
(config)#interface port-channel 2
(config-if-ch 2)#ip nat inside source list 1 1024 60000 pool 2 1 65535 overload

```

【未設定時】

アドレス変換は行いません。

13.1.4 ip nat inside source list interface

【機能】

設定のあるインタフェースから送信するパケットの送信元アドレスに対する NAT/NAT+ 変換ルールの設定 (インタフェースのアドレスを利用)

【入力形式】

```
ip nat inside source list <NAT リスト番号> [<変換前ポート：開始> <変換前ポート：終了>] interface
[<変換後ポート：開始> <変換後ポート：終了>] [overload]
```

```
no ip nat inside source list <NAT リスト番号> [<変換前ポート：開始> <変換前ポート：終了>] interface
[<変換後ポート：開始> <変換後ポート：終了>] [overload]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
NAT リスト番号	NAT/NAT+ 変換前パケットの送信元アドレスを規定した NAT リストを指定します。	1～8	省略不可
変換前ポート：開始 変換前ポート：終了	NAT+ 変換前のパケットの TCP/UDP の送信元ポート番号の範囲を指定します。 本設定を入れると TCP/UDP パケットのみが NAT 変換対象になります。	1～65535	自動ポート変換
変換後ポート：開始 変換後ポート：終了	NAT+ 変換後のパケットの TCP/UDP の送信元ポート番号の範囲を指定します。	1～65535	自動ポート変換
overload	この設定がある場合 NAT+ 変換を行う際に、TCP/UDP の送信元ポート番号を、必ず変換します。	-	ポート番号を基本的には変換しない すでにそのポート番号が使用されている場合に限り、別のポート番号に変換

【動作モード】

port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

設定のあるインタフェースから送信するパケットの送信元アドレスに対する NAT/NAT+ 変換ルールを設定します。

変換後のアドレスはインタフェースのアドレスを使用します。

アドレス、ポート番号に余りがない場合は廃棄します。

1つのインタフェースに複数設定した場合、NAT テーブル作成ができない場合があります。



secondary アドレス設定時の動作

- primary アドレスを優先的に利用します。
- primary アドレスがない場合、secondary アドレスのどれかを利用します。

【実行例】

送信するインタフェースのアドレスで、送信元アドレスを NAT+ 変換する場合のルールを設定します
(NAT リスト：1、変換後アドレス:10.0.0.1)。



TCP/UDP/ICMP 以外のプロトコルは NAT 変換します。

```
【port-channel の場合】
#configure terminal
(config)#interface port-channel 2
(config-if-ch 2)#ip address 10.0.0.1 255.255.255.0
(config-if-ch 2)#ip nat inside source list 1 interface
```

【未設定時】

アドレス変換は行いません。

13.1.5 ip nat inside source static

【機能】

設定のあるインタフェースから送信するパケットの送信元アドレスに対する NAT 変換ルールの設定
(スタティック登録)

【入力形式】

ip nat inside source static <変換前アドレス> <変換後アドレス> [proto <プロトコル番号>]

no ip nat inside source static <変換前アドレス> <変換後アドレス> [proto <プロトコル番号>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
変換前アドレス	NAT 変換前のパケットの送信元アドレスを指定します。	IPv4 アドレス形式	省略不可
変換後アドレス	NAT 変換後のアドレスを指定します。	IPv4 アドレス形式	省略不可
プロトコル番号	NAT 変換を行うパケットのプロトコル番号を指定します。	0 ~ 255	すべてのプロトコル

【動作モード】

port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

設定のあるインタフェースから送信するパケットの送信元アドレスに対する NAT 変換ルールを設定します。

変更前と変換後のアドレスを一对一で固定変換します。

プロトコルにはスタティック NAT の対象となるプロトコル番号を指定します。

【実行例】

変換前と変換後のアドレスを固定で、送信元アドレスを NAT 変換する場合のルールを設定します（変換前アドレス：192.168.0.2、変換後アドレス 10.0.0.2）。

```
【port-channel の場合】
#configure terminal
(config)#interface port-channel 2
(config-if-ch 2)#ip nat inside source static 192.168.0.2 10.0.0.2
```

【未設定時】

アドレス変換は行いません。

13.1.6 ip nat inside source static-subnet

【機能】

設定のあるインタフェースから送信するパケットの送信元アドレスに対する NAT 変換ルールの設定（ステューク一括変換登録）。

【入力形式】

```
ip nat inside source static-subnet <変換前ネットワークアドレス> <変換後ネットワークアドレス> <サブネットマスク>
```

```
no ip nat inside source static-subnet <変換前ネットワークアドレス> <変換後ネットワークアドレス> <サブネットマスク>
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
変換前ネットワークアドレス	NAT 変換前のパケットの送信元ネットワークアドレスを指定します。	IPv4 アドレス形式	省略不可
変換後ネットワークアドレス	NAT 変換後のネットワークアドレスを指定します。	IPv4 アドレス形式	省略不可
サブネットマスク	変換前、変換後のネットワークアドレスをサブネットマスク単位で一括指定します。	IPv4 アドレス形式	省略不可

【動作モード】

port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

設定のあるインタフェースから送信するパケットの送信元ネットワークアドレスに対する NAT 変換ルールを設定します。

変更前と変換後のアドレスをネットワークアドレス単位で変換します。

【実行例】

変更前と変換後のアドレスをネットワークアドレス単位で、送信元アドレスを NAT 変換する場合のルールを設定します（変換前ネットワークアドレス：192.168.0.0/24、変換後ネットワークアドレス 10.0.0.0/24）。

アドレスは以下のように NAT 変換されます。

```
192.168.0.0 → 10.0.0.0
192.168.0.1 → 10.0.0.1
      :      :
192.168.0.255 → 10.0.0.255
```

```
【port-channel の場合】
#configure terminal
(config)#interface port-channel 2
(config-if-ch 2)#ip nat inside source static-subnet 192.168.0.0 10.0.0.0 255.255.255.0
```

【未設定時】

アドレス変換は行いません。

13.1.7 ip nat inside destination static

【機能】

設定のあるインタフェースで受信するパケットの宛先アドレスに対する NAT/NAT+ 変換ルールの設定（ステティック登録）

【入力形式】

```
ip nat inside destination static <変換前アドレス> [<変換前ポート：開始> <変換前ポート：終了>] <変換後アドレス> [ポート番号] [proto <プロトコル番号>]
```

```
no ip nat inside destination static <変換前アドレス> [<変換前ポート：開始> <変換前ポート：終了>]
<変換後アドレス> [ポート番号] [proto <プロトコル番号>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
変換前アドレス	NAT 変換前のパケットの宛先アドレスを指定します。	IPv4 アドレス形式	省略不可
変換前ポート：開始 変換前ポート：終了	NAT+ 変換前のパケットの TCP/UDP の宛先ポート番号の範囲を指定します。 本設定を入れると TCP/UDP パケットのみが NAT 変換対象になります。	1～65535	ポート変換しない
変換後アドレス	NAT 変換後のアドレスを指定します。	IPv4 アドレス形式	省略不可
ポート番号	NAT+ 変換後の TCP/UDP のポート番号を指定します。変換前のポート番号で範囲指定をしていた場合は NAT+ 変換後ポート番号のベース値となります。	1～65535	ポート変換しない
プロトコル番号	NAT 変換を行うパケットのプロトコル番号を指定します。変換前ポートを指定した場合、6, 17 以外のプロトコル番号を指定した設定は無視されます。	0～255	すべてのプロトコル

【動作モード】

port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

設定のあるインタフェースで受信するパケットの宛先アドレスに対する NAT/NAT+ 変換ルールを設定します。

変更前と変換後のアドレスを一對一で固定変換します。

プロトコルにはスタティック NAT の対象となるプロトコル番号を指定します。

【実行例】

変換前と変換後のアドレスを固定で、宛先アドレスを NAT 変換する場合のルールを設定します（変換前アドレス：10.0.0.2、変換前ポート：2000～3000、変換後アドレス：192.168.0.2、変換後ポート：5000～6000）。

```
【port-channel の場合】
#configure terminal
(config)#interface port-channel 2
(config-if-ch 2)#ip nat inside destination static 10.0.0.2 2000 3000 192.168.0.2 5000
```

【未設定時】

アドレス変換は行いません。

13.1.8 ip nat inside destination static-subnet

【機能】

設定のあるインタフェースで受信するパケットの宛先アドレスに対する NAT/NAT+ 変換ルールの設定（スタティック一括変換登録）

【入力形式】

ip nat inside destination static-subnet <変換前ネットワークアドレス> <変換後ネットワークアドレス>
<サブネットマスク>

no ip nat inside destination static-subnet <変換前ネットワークアドレス> <変換後ネットワークアドレス>
<サブネットマスク>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
変換前ネットワークアドレス	NAT 変換前のパケットの宛先ネットワークアドレスを指定します。	IPv4 アドレス形式	省略不可
変換後ネットワークアドレス	NAT 変換後のネットワークアドレスを指定します。	IPv4 アドレス形式	省略不可
サブネットマスク	変換前、変換後のネットワークアドレスをサブネットマスク単位で一括指定します。	IPv4 アドレス形式	省略不可

【動作モード】

port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

設定のあるインタフェースで受信するパケットの宛先アドレスに対する NAT 変換ルールを設定します。

変更前と変換後のアドレスをネットワークアドレス単位で変換します。

【実行例】

変換前と変換後のアドレスをネットワークアドレス単位で、宛先アドレスをNAT変換する場合のルールを設定します（変換前アドレス：10.0.0.0/24、変換後アドレス：192.168.0.0/24）。

アドレスは以下のようにNAT変換されます。

```
10.0.0.0 → 192.168.0.0
10.0.0.1 → 192.168.0.1
      :      :
10.0.0.255 → 192.168.0.255
```

```
【port-channel の場合】
#configure terminal
(config)#interface port-channel 2
(config-if-ch 2)#ip nat inside destination static-subnet 10.0.0.0 192.168.0.0 255.255.255.0
```

【未設定時】

アドレス変換は行いません。

13.1.9 ip nat outside source static

【機能】

設定のあるインタフェースで受信するパケットの送信元アドレスに対するNAT変換ルールの設定（スタティック登録）

【入力形式】

```
ip nat outside source static <変換前アドレス> <変換後アドレス> [proto <プロトコル番号>]
```

```
no ip nat outside source static <変換前アドレス> <変換後アドレス> [proto <プロトコル番号>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
変換前アドレス	NAT変換前のパケットの送信元アドレスを指定します。	IPv4 アドレス形式	省略不可
変換後アドレス	NAT変換後のアドレスを指定します。	IPv4 アドレス形式	省略不可
プロトコル番号	NAT変換を行うパケットのプロトコル番号を指定します。	0～255	すべてのプロトコル

【動作モード】

port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

設定のあるインタフェースで受信するパケットの送信元アドレスに対するNAT変換ルールを設定します。

変更前と変換後のアドレスを一对一で固定変換します。

プロトコルにはスタティックNATの対象となるプロトコル番号を指定します。

【実行例】

変換前と変換後のアドレスを固定で、送信元アドレスを NAT 変換する場合のルールを設定します（変換前アドレス：172.16.0.100、変換後アドレス：192.168.100.100）。

```

【port-channel の場合】
#configure terminal
(config)#interface port-channel 2
(config-if-ch 2)#ip nat outside source static 172.16.0.100 192.168.100.100

```

【未設定時】

アドレス変換は行いません。

13.1.10 ip nat outside source static-subnet

【機能】

設定のあるインタフェースで受信するパケットの送信元アドレスに対する NAT 変換ルールの設定（ステューク一括変換登録）

【入力形式】

ip nat outside source static-subnet <変換前ネットワークアドレス> <変換後ネットワークアドレス> <サブネットマスク>

no ip nat outside source static-subnet <変換前ネットワークアドレス> <変換後ネットワークアドレス> <サブネットマスク>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
変換前ネットワークアドレス	NAT 変換前のパケットの送信元ネットワークアドレスを指定します。	IPv4 アドレス形式	省略不可
変換後ネットワークアドレス	NAT 変換後のネットワークアドレスを指定します。	IPv4 アドレス形式	省略不可
サブネットマスク	変換前、変換後のネットワークアドレスをサブネットマスク単位で一括指定します。	IPv4 アドレス形式	省略不可

【動作モード】

port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

設定のあるインタフェースで受信するパケットの送信元アドレスに対する NAT 変換ルールを設定します。
変更前と変換後のアドレスをネットワークアドレス単位で変換します。

【実行例】

変換前と変換後のアドレスをネットワークアドレス単位で、送信元アドレスを NAT 変換する場合のルールを設定します（変換前アドレス：172.16.0.0/24、変換後アドレス：192.168.100.0/24）。

アドレスは以下のように NAT 変換されます。

```
172.16.0.0 → 192.168.100.0
172.16.0.1 → 192.168.100.1
      :      :
172.16.0.255 → 192.168.100.255
```

```
【port-channel の場合】
#configure terminal
(config)#interface port-channel 2
(config-if-ch 2)#ip nat outside source static-subnet 172.16.0.0 192.168.100.0 255.255.255.0
```

【未設定時】

アドレス変換は行いません。

13.1.11 ip nat outside destination static

【機能】

設定のあるインタフェースから送信するパケットの宛先アドレスの変換ルールの設定（スタティック登録）

【入力形式】

```
ip nat outside destination static <変換前アドレス> <変換後アドレス> [proto <プロトコル番号>]
```

```
no ip nat outside destination static <変換前アドレス> <変換後アドレス> [proto <プロトコル番号>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
変換前アドレス	NAT 変換前のパケットの宛先アドレスを指定します。	IPv4 アドレス形式	省略不可
変換後アドレス	NAT 変換後のアドレスを指定します。	IPv4 アドレス形式	省略不可
プロトコル番号	NAT 変換を行うパケットのプロトコル番号を指定します。	0～255	すべてのプロトコル

【動作モード】

port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

設定のあるインタフェースから送信するパケットの宛先アドレスに対する NAT 変換ルールを設定します。

変更前と変換後のアドレスを一对一で固定変換します。

プロトコルにはスタティック NAT の対象となるプロトコル番号を指定します。

【実行例】

変換前と変換後のアドレスを固定で、宛先アドレスを NAT 変換する場合のルールを設定します（変換前アドレス：100.0.0.100、変換後アドレス：172.16.0.100）。

```
【port-channel の場合】
#configure terminal
(config)#interface port-channel 2
(config-if-ch 2)#ip nat outside destination static 100.0.0.100 172.16.0.100
```

【未設定時】

アドレス変換は行いません。

13.1.12 ip nat outside destination static-subnet

【機能】

設定のあるインタフェースで送信するパケットの宛先アドレスに対する NAT 変換ルールの設定（ステイクー括変換登録）

【入力形式】

ip nat outside destination static-subnet <変換前ネットワークアドレス> <変換後ネットワークアドレス>
<サブネットマスク>

no ip nat outside destination static-subnet <変換前ネットワークアドレス> <変換後ネットワークアドレス>
<サブネットマスク>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
変換前ネットワークアドレス	NAT 変換前のパケットの送信元ネットワークアドレスを指定します。	IPv4 アドレス形式	省略不可
変換後ネットワークアドレス	NAT 変換後のネットワークアドレスを指定します。	IPv4 アドレス形式	省略不可
サブネットマスク	変換前、変換後のネットワークアドレスをサブネットマスク単位で一括指定します。	IPv4 アドレス形式	省略不可

【動作モード】

port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

設定のあるインタフェースで送信するパケットの宛先アドレスに対する NAT 変換ルールを設定します。
変更前と変換後のアドレスをネットワークアドレス単位で変換します。

【実行例】

変換前と変換後のアドレスをネットワークアドレス単位で、送信元アドレスを NAT 変換する場合のルールを設定します（変換前アドレス：192.168.100.0/24、変換後アドレス：172.16.0.0/24）。

アドレスは以下のように NAT 変換されます。

```
192.168.100.0 → 172.16.0.0
192.168.100.1 → 172.16.0.1
      :           :
192.168.100.255 → 172.16.0.255
```

```
【port-channel の場合】
#configure terminal
(config)#interface port-channel 2
(config-if-ch 2)#ip nat outside destination static-subnet 192.168.100.0 172.16.0.0 2
55.255.255.0
```

【未設定時】

アドレス変換は行いません。

13.1.13 ip nat acl

【機能】

NAT 対象パケットのフィルタリングの設定

【入力形式】

```
ip nat acl <NAT アクセスリスト番号> {any | <送信元アドレス> <送信元ワイルドカードマスク>} {any | <宛先アドレス> <宛先ワイルドカードマスク>} [プロトコル番号]
```

```
no ip nat acl <NAT アクセスリスト番号>
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
NAT アクセスリスト番号	NAT アクセスリスト番号を指定します。	1～255	省略不可
any <送信元アドレス>	送信元アドレスを指定します。	any: すべて (IPv4) 送信元アドレス: IPv4 アドレス形式	省略不可
送信元ワイルドカードマスク	送信元ワイルドカードマスクを指定します。	IPv4 アドレス形式	省略不可
any <宛先アドレス>	宛先アドレスを指定します。	any: すべて (IPv4) 宛先アドレス: IPv4 アドレス形式	省略不可
宛先ワイルドカードマスク	宛先ワイルドカードマスクを指定します。	IPv4 アドレス形式	省略不可
プロトコル番号	プロトコル番号を指定します。	0～255	すべてのプロトコル

【動作モード】

基本設定モード

【説明】

NAT 対象パケットのフィルタリングの設定をします。

【実行例】

NAT 対象のパケットのフィルタリングの設定をします（送信元アドレス：192.168.0.0/24、宛先アドレス：10.0.0.0/24）。

```
#configure terminal
(config)#ip nat acl 1 192.160.0.0 0.0.0.255 10.0.0.0 0.0.0.255
```

【未設定時】

当該 NAT アクセスリスト番号を利用する ip nat acl permit コマンドが無効となります。

13.1.14 ip nat acl permit

【機能】

インタフェースにて扱う NAT 対象パケットに対してのフィルタリングの適用

【入力形式】

```
ip nat acl <NAT アクセスリスト番号> permit {in | out | reverse}
```

```
no ip nat acl <NAT アクセスリスト番号>
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
NAT アクセスリスト番号	NAT 対象パケットの設定をした NAT アクセスリスト番号を指定します。	1 ～ 255	省略不可
in	受信パケットに対してフィルタリングを行う場合に指定します。	-	省略不可
out	送信パケットに対してフィルタリングを行う場合に指定します。	-	省略不可
reverse	送信／受信両方向に対してフィルタリングを行う場合に指定します。受信パケットに対しては指定された NAT アクセスリストをそのまま適用します。送信パケットに対しては指定された NAT アクセスリストの宛先／送信元アドレスを逆転させ適用します。	-	省略不可

【動作モード】

port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

インタフェースにて扱う NAT 対象パケットに対してのフィルタリングを適用します。

NAT テーブルを作る前に、設定した内容に適合するかの判定を行い、適合した場合は NAT テーブルを作成し NAT 変換を行います。適合しなかった場合は、パケットは NAT 変換を行うことなく転送されます。すでに NAT テーブルが作成されているケースでは、NAT 対象であるかの判定は行いません。

in だけ設定した場合、out 側では NAT 対象であるかの判定は行いません。out だけの設定だった場合も同様に動作します。

【実行例】

NAT 対象パケットに対してのフィルタリングを適用します (NAT アクセスリスト番号：1、送信元アドレス：192.168.0.0/24、宛先アドレス：10.0.0.0/24、out: 送信パケットだけフィルタリングを行う)。

```
【port-channel の場合】
#configure terminal
(config)#ip nat acl 1 192.160.0.0 0.0.0.255 10.0.0.0 0.0.0.255
(config)#
(config)#interface port-channel 2
(config-if-ch 2)#ip nat acl 1 permit out
```

【未設定時】

すべてのパケットが NAT 変換の対象パケットとなります。

13.1.15 ip nat translation finrst-timeout

【機能】

TCP の FIN フラグまたは RST フラグが設定されたパケットについての NAT テーブルタイムアウト時間の設定

【入力形式】

ip nat translation finrst-timeout <タイムアウト時間>

no ip nat translation finrst-timeout

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
タイムアウト時間	NAT/NAT+ 変換テーブルのタイムアウト時間（単位：秒）を指定します。	1 ～ 86400	省略不可

【動作モード】

基本設定モード

【説明】

TCP の FIN フラグまたは RST フラグが設定されたパケットについて NAT/NAT+ 変換する場合に、装置の内部テーブルにデータをエージアウトする時間を設定します。

【実行例】

FIN/RST フラグが設定されたパケットの NAT 変換タイムアウト時間を設定します（タイムアウト時間：1000 秒）。

```
#configure terminal
(config)#ip nat translation finrst-timeout 1000
```

【未設定時】

60 秒でタイムアウトします。

13.1.16 ip nat translation icmp-timeout

【機能】

ICMP についての NAT テーブルタイムアウト時間の設定

【入力形式】

ip nat translation icmp-timeout <タイムアウト時間>

no ip nat translation icmp-timeout

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
タイムアウト時間	NAT/NAT+ 変換テーブルのタイムアウト時間（単位：秒）を指定します。	1 ～ 86400	省略不可

【動作モード】

基本設定モード

【説明】

ICMP を NAT/NAT+ 変換する場合に、装置の内部テーブルにデータをエージアウトする時間を設定します。

【実行例】

ICMP パケットの NAT 変換タイムアウト時間を設定します（タイムアウト時間：1000 秒）。

```
#configure terminal
(config)#ip nat translation icmp-timeout 1000
```

【未設定時】

60 秒でタイムアウトします。

13.1.17 ip nat translation tcp-timeout

【機能】

TCP についての NAT テーブルタイムアウト時間の設定

【入力形式】

ip nat translation tcp-timeout <タイムアウト時間>

no ip nat translation tcp-timeout

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
タイムアウト時間	NAT/NAT+ 変換テーブルのタイムアウト時間 (単位：秒) を指定します。	1 ～ 86400	省略不可

【動作モード】

基本設定モード

【説明】

TCP について NAT/NAT+ 変換する場合に、装置の内部テーブルにデータをエージアウトする時間を設定します。

【実行例】

TCP パケットの NAT 変換タイムアウト時間を設定します（タイムアウト時間：6000 秒）。

```
#configure terminal
(config)#ip nat translation tcp-timeout 6000
```

【未設定時】

3600 秒でタイムアウトします。

13.1.18 ip nat translation udp-timeout

【機能】

UDP についての NAT テーブルタイムアウト時間の設定

【入力形式】

ip nat translation udp-timeout <タイムアウト時間>

no ip nat translation udp-timeout

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
タイムアウト時間	NAT/NAT+ 変換テーブルのタイムアウト時間 (単位: 秒) を指定します。	1 ~ 86400	省略不可

【動作モード】

基本設定モード

【説明】

UDP について NAT/NAT+ 変換する場合に、装置の内部テーブルにデータをエージアウトする時間を設定します。

【実行例】

UDP パケットの NAT 変換タイムアウト時間を設定します (タイムアウト時間: 4000 秒)。

```
#configure terminal
(config)#ip nat translation udp-timeout 4000
```

【未設定時】

300 秒でタイムアウトします。

13.1.19 ip nat translation timeout

【機能】

TCP/UDP/ICMP を除くパケットについての NAT テーブルタイムアウト時間の設定

【入力形式】

ip nat translation timeout <タイムアウト時間>

no ip nat translation timeout

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
タイムアウト時間	NAT/NAT+ 変換テーブルのタイムアウト時間 (単位: 秒) を指定します。	1 ~ 86400	省略不可

【動作モード】

基本設定モード

【説明】

TCP/UDP/ICMP を除くパケットについて NAT/NAT+ 変換する場合に、装置の内部テーブルにデータをエージアウトする時間を設定します。

TCP/UDP/ICMP は以下のコマンドで設定を行います。

TCP(FIN/RST):ip nat translation finrst-timeout コマンド

TCP:ip nat translation tcp-timeout コマンド

UDP:ip nat translation udp-timeout コマンド

ICMP:ip nat translation icmp-timeout コマンド

【実行例】

TCP/UDP/ICMP を除くパケットの NAT 変換タイムアウト時間を設定します（タイムアウト時間：80000 秒）。

```
#configure terminal
(config)#ip nat translation timeout 80000
```

【未設定時】

86400 秒でタイムアウトします。

13.1.20 ip nat wellknown

【機能】

プライベートポート番号の変換ルールの設定

【入力形式】

ip nat wellknown <id> <ポート番号：開始> <ポート番号：終了> <on | off>

no ip nat wellknown <id>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
id	ポート番号変換定義番号を指定します。	1～100	省略不可
ポート番号：開始 ポート番号：終了	ポート番号の範囲を指定します。	1～65535	省略不可
on off	wellknown として扱うか指定します。	on:wellknown として扱う off:wellknown として扱わない	省略不可

【動作モード】

基本設定モード

【説明】

プライベートポート番号の変換ルールを設定をします。

wellknown で指定したポート番号には、NAT+ では変換しません。

NAT スタティックの設定では、本コマンドに関係なく設定されたポート番号を変換します。

【実行例】

すべてのポート番号を NAT+ で変換するよう設定をします（ポート番号範囲：1～65535、off:wellknown として扱わない）。

```
#configure terminal
(config)#ip nat wellknown 1 1 65535 off
```

【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。

0～1024（本来の well-known ポート番号）

28800～28830(Microsoft Internet Gaming Zone)

13.1.21 ip nat default action

【機能】

NAT 対象外のパケットの取り扱いルールの設定

【入力形式】

ip nat default action <pass | reject>

no ip nat default action

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
pass reject	NAT 対象外のパケットの動作を指定します。	pass:NAT/NAT+ 変換を行うことなく中継します。 reject: 廃棄します。	省略不可

【動作モード】

基本設定モード

【説明】

インタフェースに NAT の設定がある場合に、NAT 対象外のパケットの取り扱いルールを設定します。

自宛、自出しパケットは NAT 対象でないパケットについても受信、送信可能（reject 設定は無効）となります。

【実行例】

NAT 対象外のパケットの取り扱いルールを設定します（pass：NAT/NAT+ 変換を行うことなく中継）。

```
#configure terminal
(config)#ip nat default action pass
```

【未設定時】

NAT 対象外のパケットは廃棄します。

第14章 EtherIP の設定



この章では、EtherIP の設定に関するコマンドについて説明します。

14.1 EtherIP の設定

14.1.1 ether-ip tunnel-profile

【機能】

EtherIP プロファイル設定モードへの移行

【入力形式】

ether-ip tunnel-profile <EtherIP プロファイル名>

no ether-ip tunnel-profile <EtherIP プロファイル名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
EtherIP プロファイル名	EtherIP プロファイル名を指定します。	63 文字以内の CDATA 型	省略不可

【動作モード】

基本設定モード

【説明】

EtherIP の tunnel ポリシーをまとめたプロファイルを作成するために、EtherIP プロファイル設定モードに移行します。

no を指定した場合には、該当 EtherIP プロファイル設定モードの内容がすべて消去されます。

【実行例】

EtherIP プロファイル設定モードに移行します（EtherIP プロファイル名：profile-A）。

```
#configure terminal
(config)#ether-ip tunnel-profile profile-A
(config-ether-ip)#
```

14.1.2 I2-encapsulation map cos-dscp

【機能】

Precedence フィールド、Traffic-Class フィールドへマッピングする値の設定

【入力形式】

I2-encapsulation map cos-dscp {<TOS 値> | <Traffic-Class 値>} {<TOS 値> | <Traffic-Class 値>} {<TOS 値> | <Traffic-Class 値>} {<TOS 値> | <Traffic-Class 値>} {<TOS 値> | <Traffic-Class 値>} {<TOS 値> | <Traffic-Class 値>} {<TOS 値> | <Traffic-Class 値>} {<TOS 値> | <Traffic-Class 値>}

no I2-encapsulation map cos-dscp

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
TOS 値 Traffic-Class 値	TOS 値、または Traffic-Class 値を指定します。	0 ～ 255	省略不可

【動作モード】

基本設定モード

【説明】

EtherIP にてカプセル化を行う際に、ctag（二段目のタグ）の CoS 値（0 ～ 7）を元にカプセル化するヘッダの Precedence フィールド、または Traffic-Class フィールドへマッピングする値を設定します。
ctag がない場合、設定は無視されます。

【実行例】

Precedence フィールド、または Traffic-Class フィールドへマッピングする値を設定します。

```
#configure terminal
(config)#l2-encapsulation map cos-dscp 2 2 2 2 2 2 2 2
```

【未設定時】

TOS 値、または Traffic-Class 値は 0 で動作します。

14.1.3 set mtu

【機能】

EtherIP トンネルインタフェースの MTU 長の設定

【入力形式】

set mtu <MTU 長>

no set mtu

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
MTU 長	MTU 長（単位：bytes）を指定します。	1280 ～ 9100	省略不可

【動作モード】

EtherIP プロファイル設定モード

【説明】

EtherIP トンネルインタフェースの MTU 長（単位：bytes）を設定します。

送信時の MTU 値はカプセル化後のパケットに対して適用されます。

設定変更時は、該当する tunnel インタフェースが一度 Down しますので、ご注意ください。

MTU に従いパケットを分割する場合、基本的に均等な長さにパケットを分割します。しかし、コントロールプレーンから送信する、またはコントロールプレーンを経由して中継する際に分割するケースでは、MTU 長に合わせたパケットの分割を実施します。

【実行例】

EtherIP トンネルインタフェースの MTU 長を設定します (MTU 長：1280bytes)。

```
#configure terminal
(config)#ether-ip tunnel-profile profile-A
(config-ether-ip)#set mtu 1280
```

【未設定時】

MTU 長は 1500bytes で動作します。

14.1.4 tunnel destination

【機能】

EtherIP の通信をする対向装置の IP アドレスの設定

【入力形式】

tunnel destination <IP アドレス>

no tunnel destination [<IP アドレス>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
IP アドレス	EtherIP の通信をする対向装置の IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

【動作モード】

EtherIP プロファイル設定モード

【説明】

EtherIP の通信をする対向装置の IP アドレスを設定します。

【実行例】

EtherIP の通信をする対向装置の IP アドレスを設定します (IP アドレス：192.0.2.2)。

```
#configure terminal
(config)#ether-ip tunnel-profile profile-A
(config-ether-ip)# tunnel destination 192.0.2.2
```

【未設定時】

EtherIP トンネルを確立できません。

14.1.5 tunnel protection

【機能】

EtherIP over IPsec環境下で、EtherIP tunnel インタフェースと紐付ける IPsec tunnel インタフェースの設定

【入力形式】

tunnel protection ipsec tunnel <tunnel 番号 >

no tunnel protection [ipsec tunnel <tunnel 番号 >]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
tunnel 番号	tunnel インタフェースの番号を指定します。	1～16777215	省略不可

【動作モード】

EtherIP プロファイル設定モード

【説明】

EtherIP のパケットを IPsec により保護したい場合に、IPsec で使用している tunnel インタフェースを設定します。

この設定を行った場合、EtherIP でカプセル化したあとのパケットを、経路情報に従わず、指定した tunnel に転送します。また、指定した tunnel 以外から受信した EtherIP のパケットを破棄します。

【実行例】

IPsec で使用している tunnel インタフェースを設定します (tunnel 番号：1)。

```
#configure terminal
(config)#ether-ip tunnel-profile profile-A
(config-ether-ip)#tunnel protection ipsec tunnel 1
```

【未設定時】

経路情報に従って EtherIP のパケットを送信します。

14.1.6 tunnel source

【機能】

EtherIP トンネルを確立する自装置 IP アドレスの設定

【入力形式】

tunnel source <IP アドレス >

no tunnel source [<IP アドレス >]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
IP アドレス	EtherIP トンネルを確立する自装置の IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

【動作モード】

EtherIP プロファイル設定モード

【説明】

EtherIP トンネルを確立する自装置の IP アドレスを設定します。

【実行例】

EtherIP トンネルを確立する自装置の IP アドレスを設定します（送信元アドレス:192.0.2.1）。

```
#configure terminal
(config)#ether-ip tunnel-profile profile-A
(config-ether-ip)# tunnel source 192.0.2.1
```

【未設定時】

EtherIP トンネルを確立できません。

第15章 IPinIP の設定



この章では、IPinIP の設定に関するコマンドについて説明します。

15.1 IPinIP の設定

15.1.1 ipinip tunnel-profile

【機能】

ipinip tunnel プロファイル設定モードへの移行

【入力形式】

ipinip tunnel-profile <IPinIP プロファイル名>

no ipinip tunnel-profile <IPinIP プロファイル名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
IPinIP プロファイル名	IPinIP トンネル設定情報を識別する文字列を指定します。	63 文字以内の WORD 型	省略不可

【動作モード】

基本設定モード

【説明】

ipinip tunnel プロファイル設定モードに移行します。

【実行例】

ipinip tunnel プロファイル設定モードに移行します（プロファイル名：ipinip-profile-A）。

```
#configure terminal
(config)#ipinip tunnel-profile ipinip-profile-A
(config-ipinip-profile)#
```

15.1.2 source address

【機能】

IPinIP カプセリングする IPv4 ヘッダまたは IPv6 ヘッダの送信元アドレスの設定

【入力形式】

source address <IP アドレス>

no source address [<IP アドレス>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
IP アドレス	送信元アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

【動作モード】

ipinip tunnel プロファイル設定モード

【説明】

IPinIP カプセリングする IPv4 ヘッダまたは IPv6 ヘッダの送信元アドレスを設定します。

【実行例】

送信元アドレスを設定します（送信元アドレス：192.168.1.1）。

```
#configure terminal
(config)#ipinip tunnel-profile ipinip-profile-A
(config-ipinip-profile)#source address 192.168.1.1
```

【未設定時】

IPinIP カプセリングを行いません。

15.1.3 destination address

【機能】

宛先アドレスの設定

【入力形式】

destination address <IP アドレス>

no destination address [<IP アドレス>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
IP アドレス	宛先アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

【動作モード】

ipinip tunnel プロファイル設定モード

【説明】

IPinIP カプセリングする IPv4 ヘッダまたは IPv6 ヘッダの宛先アドレスを設定します。

【実行例】

宛先アドレスを設定します（宛先アドレス：192.168.1.2）。

```
#configure terminal
(config)#ipinip tunnel-profile ipinip-profile-A
(config-ipinip-profile)#destination address 192.168.1.2
```

【未設定時】

IPinIP カプセリングを行いません。

15.1.4 ipinip fragment

【機能】

IPinIP カプセリングする際のフラグメント動作の設定

【入力形式】

ipinip fragment {post | pre}

no ipinip fragment [post | pre]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
post pre	IPinIP カプセリングする際のフラグメント動作を指定します。	post:post フラグメント pre:pre フラグメント	省略不可

【動作モード】

ipinip tunnel プロファイル設定モード

【説明】

IPinIP カプセリングする際のフラグメント動作を設定します。

【実行例】

IPinIP カプセリングする際のフラグメント動作を設定します (pre)。

```
#configure terminal
(config)#ipinip tunnel-profile ipinip-profile-A
(config-ipinip-profile)#ipinip fragment pre
```

【未設定時】

post フラグメントで動作します。

15.1.5 profile-mode

【機能】

プロファイルのモードの設定

【入力形式】

profile-mode {ipip | gre}

no profile-mode [ipip | gre]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ipip gre	プロファイルのモードを指定します。 ipip : ip-in-ip tunnelのプロファイルを設定します。 gre : GRE tunnelのプロファイルを設定します。	-	省略不可

【動作モード】

ipinip tunnel プロファイル設定モード

【説明】

プロファイルのモードを設定します。

【注意】

同一のプロファイル設定モード内で profile-mode を ipip、gre で変更した場合、変更後のモードで正しく動作できません。

profile-mode を変更する場合、プロファイルを参照している tunnel インタフェースとプロファイルをコンフィグから削除し refresh 後、改めて変更後の profile-mode で tunnel インタフェースとプロファイルを再設定する必要があります。

【実行例】

プロファイルのモードを設定します（プロファイルモード：gre）。

```
#configure terminal
(config)#ipinip tunnel-profile ipinip-profile-A
(config-ipinip-profile)#profile-mode gre
```

【未設定時】

ip-in-ip tunnel のプロファイルモードで動作します。

15.1.6 set mtu

【機能】

MTU 長の設定

【入力形式】

set mtu <MTU 長>

no set mtu [<MTU 長>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
MTU 長	MTU 長（単位：bytes）を指定します。	1280～9100	省略不可

【動作モード】

ipinip tunnel プロファイル設定モード

【説明】

MTU 長（単位：bytes）を設定します。

MTU に従いパケットを分割する場合、基本的に均等な長さにパケットを分割します。しかし、コントロールプレーンから送信する、またはコントロールプレーンを経由して中継する際に分割するケースでは、MTU 長に合わせたパケットの分割を実施します。

【実行例】

MTU 長を設定します (MTU 長: 1460bytes)。

```
#configure terminal
(config)#ipinip tunnel-profile ipinip-profile-A
(config-ipinip-profile)#set mtu 1460
```

【未設定時】

MTU 長は 1500bytes で動作します。

15.1.7 set ip df-bit

【機能】

Outer (IPv4 パケット) の Don't fragment ビットの設定

【入力形式】

set ip df-bit {0 | 1}

no set ip df-bit [0 | 1]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
0 1	Don't fragment ビットを指定します。	0: フラグメント可 1: フラグメント不可	省略不可

【動作モード】

ipinip tunnel プロファイル設定モード

【説明】

Outer (IPv4 パケット) の Don't fragment ビットを設定します。

【実行例】

Outer (IPv4 パケット) の Don't fragment ビットを設定します (1)。

```
#configure terminal
(config)#ipinip tunnel-profile ipinip-profile-A
(config-ipinip-profile)#set ip df-bit 1
```

【未設定時】

フラグメント可 (0) で動作します。

15.1.8 ipinip propagate-ttl

【機能】

IPinIP カプセリングする際の TTL 値を反映する／しないの設定

【入力形式】

ipinip propagate-ttl {enable | disable [<TTL 値>]}

no ipinip propagate-ttl [enable | disable [<TTL 値>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
enable disable	TTL 値を反映する／しないを指定します。	enable:TTL 値を反映します。 disable:TTL 値を反映せず固定値を指定します。	省略不可
TTL 値	TTL 値を指定します。	1～255	64

【動作モード】

基本設定モード、ipinip tunnel プロファイル設定モード

【説明】

IPinIP カプセリングする際の TTL 値を反映する／しないを指定します。

【実行例】

IPinIP カプセリングする際の TTL 値を反映します (enable)。

```
#configure terminal
(config)#ipinip tunnel-profile ipinip-profile-A
(config-ipinip-profile)#ipinip propagate-ttl enable
```

【未設定時】

以下の値で動作します。

disable

TTL 値 : 64

15.1.9 ipinip propagate-tos

【機能】

IPinIP カプセリングする際の ToS 値を反映する／しないの設定

【入力形式】

ipinip propagate-tos {disable [enable | disable [<ToS 値>]]}

no ipinip propagate-tos [enable | disable [<ToS 値>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
enable disable	ToS(Traffic Class) 値を反映する／しないを指定します。	enable: 反映する disable: 反映しない	省略不可
ToS 値	disable 時の ToS 値を指定します。	0 ～ 255	0

【動作モード】

基本設定モード、ipinip tunnel プロファイル設定モード

【説明】

IPinIP カプセリングする際の ToS 値を反映する／しないを指定します。

【実行例】

IPinIP カプセリングする際の ToS 値を反映します (enable)。

```
#configure terminal
(config)#ipinip tunnel-profile ipinip-profile-A
(config-ipinip-profile)#ipinip propagate-tos enable
```

【未設定時】

以下の値で動作します。

disable

ToS 値 : 0

第16章 BFDの設定



この章では、BFDの設定に関するコマンドについて説明します。

16.1 BFD の設定

16.1.1 bfd-map

【機能】

bfd-map 設定モードへの移行

【入力形式】

bfd-map <bfd-map 名>

no bfd-map <bfd-map 名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
bfd-map 名	bfd-map 名を指定します。	254 文字以内の WORD 型	省略不可

【動作モード】

基本設定モード

【説明】

bfd-map 設定モードに移行します。"no" を指定した場合は、該当 bfd-map 設定モードの内容がすべて消去されます。

【実行例】

bfd-map 設定モードに移行します (bfd-map 名: bfd-map-A)。

```
#configure terminal
(config)#bfd-map bfd-map-A
(config-bfdmap bfd-map-A)#
```

16.1.2 ip route bfd-map

【機能】

BFD 監視による IPv4 経路制御機能の設定

【入力形式】

ip route <ネットワークアドレス> <ネットマスク> <Next-hop> bfd-map <bfd-map 名> [<ディスタンス値>]

no ip route <ネットワークアドレス> <ネットマスク> <Next-hop> bfd-map <bfd-map 名> [<ディスタンス値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ネットワークアドレス	ネットワークアドレスを指定します。	IPv4 アドレス形式	省略不可
ネットマスク	ネットマスクを指定します。	IPv4 アドレス形式	省略不可
Next-hop	Next-hop アドレスを指定します。	IPv4 アドレス形式	省略不可
bfd-map 名	bfd-map 名を指定します。	254 文字以内の WORD 型	省略不可
ディスタンス値	ディスタンス値を指定します。	2～255	1

【動作モード】

基本設定モード

【説明】

BFD 監視による経路制御機能を有効にする場合に設定します。

BFD 監視状態が DOWN の場合、設定したスタティック経路を無効とします。

BFD 監視状態が UP の場合、設定したスタティック経路を有効とします。

なお、設定した bfd-map が存在しない場合、BFD のデフォルト値(interval 1000、min_rx 3000、multiplier 3)で動作します。

【実行例】

BFD 監視による経路制御機能を有効にします（ネットワークアドレス：192.0.2.128、ネットマスク：255.255.255.128、Next-hop：192.0.2.1、bfd-map 名：bfd-map-A）。

```
#configure terminal
(config)#ip route 192.0.2.128 255.255.255.128 192.0.2.1 bfd-map bfd-map-A
```

【未設定時】

BFD 監視による経路制御機能は動作しません。

16.1.3 ipv6 route bfd-map

【機能】

BFD 監視による IPv6 経路制御機能の設定

【入力形式】

ipv6 route <ネットワークアドレス>/<プレフィックス長> <Next-hop> bfd-map <bfd-map 名> [<ディスタンス値>]

no ipv6 route <ネットワークアドレス> <プレフィックス長> <Next-hop> bfd-map <bfd-map 名> [<ディスタンス値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ネットワークアドレス	ネットワークアドレスを指定します。	IPv6 アドレス形式	省略不可
プレフィックス長	プレフィックス長を指定します。	0 ～ 128	省略不可
Next-hop	Next-hop アドレスを指定します。	IPv6 アドレス形式	省略不可
bfd-map 名	bfd-map 名を指定します。	254 文字以内の WORD 型	省略不可
ディスタンス値	ディスタンス値を指定します。	2 ～ 255	1

【動作モード】

基本設定モード

【説明】

BFD 監視による経路制御機能を有効にする場合に設定します。

BFD 監視状態が DOWN の場合、設定したスタティック経路を無効とします。

BFD 監視状態が UP の場合、設定したスタティック経路を有効とします。

なお、設定した bfd-map が存在しない場合、BFD のデフォルト値（interval 1000、min_rx 3000、multiplier 3）で動作します。

【実行例】

BFD 監視による経路制御機能を有効にします（ネットワークアドレス：2001:db8:2::、プレフィックス長：48、Next-hop：2001:db8:1::1、bfd-map 名：bfd-map-A）。

```
#configure terminal
(config)#ipv6 route 2001:db8:2::/48 2001:db8:1::1 bfd-map bfd-map-A
```

【未設定時】

BFD 監視による経路制御機能は動作しません。

16.1.4 ip route vrf bfd-map

【機能】

BFD 監視による IPv4 経路制御機能の設定

【入力形式】

ip route vrf <VRF 名> <ネットワークアドレス> <ネットマスク> <Next-hop> bfd-map <bfd-map 名> [<ディスタンス値>]

no ip route vrf <VRF 名> <ネットワークアドレス> <ネットマスク> <Next-hop> bfd-map <bfd-map 名> [<ディスタンス値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VRF 名	VRF 名を指定します。	63 文字以内の WORD 型	省略不可
ネットワークアドレス	ネットワークアドレスを指定します。	IPv4 アドレス形式	
ネットマスク	ネットマスクを指定します。	IPv4 アドレス形式	
Next-hop	Next-hop アドレスを指定します。	IPv4 アドレス形式	
bfd-map 名	bfd-map 名を指定します。	254 文字以内の WORD 型	
ディスタンス値	ディスタンス値を指定します。	2～255	1

【動作モード】

基本設定モード

【説明】

BFD 監視による経路制御機能を有効にする場合に設定します。

BFD 監視状態が DOWN の場合、設定したスタティック経路を無効とします。

BFD 監視状態が UP の場合、設定したスタティック経路を有効とします。

なお、設定した bfd-map が存在しない場合、BFD のデフォルト値 (interval 1000、min_rx 3000、multiplier 3) で動作します。

【実行例】

BFD 監視による経路制御機能を有効します。

(VRF 名 : vrf-A、ネットワークアドレス : 192.0.2.128、ネットマスク : 255.255.255.128、Next-hop : 192.0.2.1、bfd-map 名 : bfd-map-A)

```
#configure terminal
(config)#ip route vrf vrf-A 192.0.2.128 255.255.255.128 192.0.2.1 bfd-map bfd-map-A
```

【未設定時】

BFD 監視による経路制御機能は動作しません。

16.1.5 ipv6 route vrf bfd-map

【機能】

BFD 監視による IPv6 経路制御機能の設定

【入力形式】

ipv6 route vrf <VRF 名> <ネットワークアドレス> <プレフィックス長> <Next-hop> bfd-map <bfd-map 名> [<ディスタンス値>]

no ipv6 route vrf <VRF 名> <ネットワークアドレス> <プレフィックス長> <Next-hop> bfd-map <bfd-map 名> [<ディスタンス値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VRF 名	VRF 名を指定します。	63 文字以内の WORD 型	省略不可
ネットワークアドレス	ネットワークアドレスを指定します。	IPv6 アドレス形式	
プレフィックス長	プレフィックス長を指定します。	IPv6 アドレス形式	
Next-hop	Next-hop アドレスを指定します。	IPv6 アドレス形式	
bfd-map 名	bfd-map 名を指定します。	254 文字以内の WORD 型	
ディスタンス値	ディスタンス値を指定します。	2 ～ 255	1

【動作モード】

基本設定モード

【説明】

BFD 監視による経路制御機能を有効にする場合に設定します。

BFD 監視状態が DOWN の場合、設定したスタティック経路を無効とします。

BFD 監視状態が UP の場合、設定したスタティック経路を有効とします。

なお、設定した bfd-map が存在しない場合、BFD のデフォルト値 (interval 1000、min_rx 3000、multiplier 3) で動作します。

【実行例】

BFD 監視による経路制御機能を有効します。

(VRF 名 : vrf-A、ネットワークアドレス : 2001:db8:2::、プレフィックス長 : 48、Next-hop : 2001:db8:1::1、bfd-map 名 : bfd-map-A)

```
#configure terminal
(config)#ipv6 route vrf vrf-A 2001:db8:2::/48 2001:db8:1::1 bfd-map bfd-map-A
```

【未設定時】

BFD 監視による経路制御機能は動作しません。

16.1.6 designated-source

【機能】

BFD コントロールパケットの送信元アドレスの設定

【入力形式】

designated-source <送信元アドレス>

no designated-source

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
送信元アドレス	BFD コントロールパケットの送信元アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

【動作モード】

bfd-map 設定モード

【説明】

BFD 監視相手に送信する、BFD コントロールパケットの送信元アドレスを設定します。

【実行例】

BFD コントロールパケットの送信元アドレスを設定します（送信元アドレス：192.0.2.1）。

```
#configure terminal
(config)#bfd-map bfd-map-A
(config-bfdmap bfd-map-A)#designated-source 192.0.2.1
```

【未設定時】

ソースアドレスは送信インタフェースのアドレスで動作します。

16.1.7 interval

【機能】

BFD コントロールパケットの送信間隔の設定

【入力形式】

interval <送信間隔>

no interval

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
送信間隔	BFD コントロールパケットの送信間隔（単位：ミリ秒）を指定します。	100～10000	省略不可

【動作モード】

bfd-map 設定モード

【説明】

BFD コントロールパケットの送信間隔（単位：ミリ秒）を設定します。

本装置では、1000ms 以上の設定を推奨します。

【実行例】

BFD コントロールパケットの送信間隔（単位：ミリ秒）を設定します（送信間隔：5000 ミリ秒）。

```
#configure terminal
(config)#bfd-map bfd-map-A
(config-bfdmap bfd-map-A)#interval 5000
```

【未設定時】

送信間隔は 1000 ミリ秒で動作します。

16.1.8 min_rx

【機能】

BFD コントロールパケットの最小受信間隔の設定

【入力形式】

min_rx <最小受信間隔>

no min_rx

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
最小受信間隔	BFD コントロールパケットの最小受信間隔（単位：ミリ秒）を指定します。	1～10000	省略不可

【動作モード】

bfd-map 設定モード

【説明】

BFD コントロールパケットの最小受信間隔（単位：ミリ秒）を設定します。

本装置では、3000ms 以上の設定を推奨します。

【実行例】

BFD コントロールパケットの最小受信間隔（単位：ミリ秒）を設定します（小受信間隔：5000 ミリ秒）。

```
#configure terminal
(config)#bfd-map bfd-map-A
(config-bfdmap bfd-map-A)#min_rx 5000
```

【未設定時】

最小受信間隔は 3000 ミリ秒で動作します。

16.1.9 multi-hop ttl-drop-threshold

【機能】

受信時にパケットを廃棄する最大 TTL 値の設定

【入力形式】

multi-hop ttl-drop-threshold <最大 TTL 値>

no multi-hop ttl-drop-threshold

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
最大 TTL 値	パケットを廃棄する最大 TTL 値を指定します。	0～254	省略不可

【動作モード】

bfd-map 設定モード

【説明】

BFD パケットを受信した際の、パケットを廃棄する最大 TTL 値を設定します。設定された TTL 値以下の BFD パケットを受信した場合にパケットを廃棄します。

session-mode コマンドで "multi-hop" が指定されている場合のみ動作します。

【実行例】

パケットを廃棄する最大 TTL 値を設定します（最大 TTL 値：128）。

```
#configure terminal
(config)#bfd-map bfd-map-A
(config-bfdmap bfd-map-A)#multi-hop ttl-drop-threshold 128
```

【未設定時】

TTL 値が 255 のパケット以外を廃棄します。

16.1.10 multiplier

【機能】

送信間隔に対する乗算値の設定

【入力形式】

multiplier <乗算値>

no multiplier

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
乗算値	送信間隔に対する乗算値を指定します。	3～50	省略不可

【動作モード】

bfd-map 設定モード

【説明】

送信間隔に対する乗算値を設定します。

【実行例】

送信間隔に対する乗算値を設定します（乗算値：5）。

```
#configure terminal
(config)#bfd-map bfd-map-A
(config-bfdmap bfd-map-A)#multiplier 5
```

【未設定時】

乗算値は 3 で動作します。

16.1.11 neighbor

【機能】

BFD ネイバーのアドレスの設定

【入力形式】

neighbor [{ipv4 | ipv6}] [vrf <VRF 名>] <BFD ネイバー >

no neighbor

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ipv4 ipv6	IPv4 か IPv6 かを指定します。	-	IPv4
VRF 名	VRF 名を指定します。	63 文字以内の WORD 型	VRF を使用しない
BFD ネイバー	BFD ネイバーのアドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

【動作モード】

bfd-map 設定モード

【説明】

BFD ネイバーのアドレスを設定します。

ただし、static 設定時、trunk-group(LAG) 設定時に有効となります。

ipv4、ipv6、ipv4 vrf、ipv6 vrf のそれぞれにユニークな BFD ネイバーのアドレスを設定できます。ほかの bfd-map と重複したネイバーのアドレスを設定した場合はエラーを出力し、入力した設定は無効となります。

【実行例】

BFD ネイバーのアドレスを設定します (BFD ネイバー：192.0.2.1)。

```
#configure terminal
(config)#bfd-map bfd-map-A
(config-bfdmap bfd-map-A)#neighbor 192.0.2.1
```

【未設定時】

ほかのモードの設定に従います。

16.1.12 session-mode

【機能】

BFD の監視相手との接続方法の設定

【入力形式】

session-mode {multi-hop | single-hop}

no session-mode

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
multi-hop single-hop	BFD の監視相手との接続方法を指定します。	-	省略不可

【動作モード】

bfd-map 設定モード

【説明】

BFD の監視相手との接続方法を設定します。

モードの変更を行うと、BFD セッションがダウンします。

trunk-channel インタフェースと紐付けられた場合は、本設定は無効となります。

【実行例】

BFD の監視相手との接続方法を設定します (multi-hop)。

```
#configure terminal
(config)#bfd-map bfd-map-A
(config-bfdmap bfd-map-A)#session-mode multi-hop
```

【未設定時】

single-hop で動作します。

16.1.13 ip ospf bfd

【機能】

OSPF と連携した BFD 監視を行う場合の設定

【入力形式】

ip ospf bfd {disable | bfd-map <bfd-map 名>}

no ip ospf bfd {disable | bfd-map <bfd-map 名>}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
disable	OSPF と連携した BFD 監視を行わない場合に指定します。	-	省略不可
bfd-map 名	bfd-map 名を指定します。	254 文字以内の WORD 型	省略不可

【動作モード】

port-channel インタフェース設定モード

【説明】

OSPF と連携した BFD 監視を行う場合に設定します。

ネイバースタートが FULL のネイバーのみ BFD 監視対象となります。

"disable" を設定した場合には、OSPF と連携した BFD 監視を行いません。

なお、設定した bfd-map が存在しない場合、BFD のデフォルト値（interval 1000、min_rx 3000、multiplier 3）で動作します。

【実行例】

OSPF と連携した BFD 監視を行います（bfd-map 名：bfd-map-A）。

```
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ip ospf bfd bfd-map bfd-map-A
```

【未設定時】

OSPF サービス設定モードの bfd all-interface コマンドの設定に従います。

16.1.14 ipv6 ospf bfd

【機能】

OSPF6 と連携した BFD 監視を行う場合の設定

【入力形式】

ipv6 ospf bfd {disable | bfd-map <bfd-map 名>}

no ipv6 ospf bfd {disable | bfd-map <bfd-map 名>}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
disable	OSPF6 と連携した BFD 監視を行わない場合に指定します。	-	省略不可
bfd-map 名	bfd-map 名を指定します。	254 文字以内の WORD 型	省略不可

【動作モード】

port-channel インタフェース設定モード

【説明】

OSPF6 と連携した BFD 監視を行う場合に設定します。"disable" を設定した場合には、OSPF6 と連携した BFD 監視を行いません。

なお、設定した bfd-map が存在しない場合、BFD のデフォルト値（interval 1000、min_rx 3000、multiplier 3）で動作します。

【実行例】

OSPF6 と連携した BFD 監視を行います（bfd-map 名：bfd-map-A）。

```
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 ospf bfd bfd-map bfd-map-A
```

【未設定時】

OSPF6 サービス設定モードの bfd all-interface コマンドの設定に従います。

16.1.15 bfd all-interface

【機能】

OSPF(OSPF6) ネイバーに対して BFD 監視を行う場合の設定

【入力形式】

```
bfd all-interface bfd-map <bfd-map 名>
```

```
no bfd all-interface bfd-map <bfd-map 名>
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
bfd-map 名	bfd-map 名を指定します。	254 文字以内の WORD 型	省略不可

【動作モード】

OSPF サービス設定モード、OSPF6 サービス設定モード

【説明】

OSPF(OSPF6) ネイバーに対して BFD 監視を行う場合に設定します。

ネイバーステートが FULL のネイバーのみ BFD 監視対象となります。

なお、設定した bfd-map が存在しない場合、BFD のデフォルト値 (interval 1000、min_rx 3000、multiplier 3) で動作します。

port-channel インタフェース設定モードに ip(ipv6) ospf bfd コマンドが設定されている場合は、そちらの設定を優先します。

【実行例】

OSPF ネイバーに対して BFD 監視を行います (bfd-map 名 : bfd-map-A)。

```
【OSPF サービス設定モードの場合】
#configure terminal
(config)#router ospf 1
(config-ospf 1)#bfd all-interface bfd-map bfd-map-A
```

【未設定時】

port-channel インタフェース設定モードに ip(ipv6) ospf bfd コマンドが設定されていない場合は、OSPF(OSPF6) と連携した BFD 監視を行いません。

16.1.16 trunk-group fall-over bfd-map

【機能】

LAG と連携した BFD 監視 (micro BFD) を行う場合の設定

【入力形式】

```
trunk-group fall-over bfd-map <bfd-map 名>
```

```
no trunk-group fall-over bfd-map <bfd-map 名>
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
bfd-map 名	bfd-map 名を指定します。	254 文字以内の WORD 型	省略不可

【動作モード】

trunk-channel インタフェース設定モード

【説明】

LAG と連携した BFD 監視 (micro BFD) を行う場合に設定します。

モードの変更を行うと、trunk-channel インタフェースがダウンします。

なお、設定した bfd-map が存在しない場合、BFD のデフォルト値 (interval 1000、min_rx 3000、multiplier 3) で動作します。

【実行例】

LAG と連携した BFD 監視 (micro BFD) を行います (bfd-map 名 : bfd-map-A)。

```
#configure terminal
(config)#interface trunkchannel 1
(config-if-tr 1)#trunk-group fall-over bfd-map bfd-map-A
```

【未設定時】

LAG と連携した BFD 監視 (micro BFD) を行いません。

第17章 IPsecの設定



この章では、IPsecの設定に関するコマンドについて説明します。

17.1	ISAKMP-SA/IKE SAの設定	531
17.2	IPSEC-SA/CHILD SAの設定	548
17.3	IPSEC セレクタの設定	558
17.4	ISAKMP プロファイルの設定	561
17.5	VPN セレクタの設定	572
17.6	データベースの設定	577
17.7	拡張認証の各種設定	583
17.8	Mode-config/Config Payload の設定	588
17.9	電子証明書の設定	593
17.10	DPD の設定	598
17.11	ESP の設定	604
17.12	SA アップルートの設定	615
17.13	SA 数制限、および IPsec MIB の設定	619
17.14	IPsec の各種設定	632
17.15	ログの設定	658

17.1 ISAKMP-SA/IKE SA の設定

17.1.1 crypto isakmp policy

【機能】

ISAKMP ポリシー設定モードへの移行

【入力形式】

crypto isakmp policy <ISAKMP ポリシー名>

no crypto isakmp policy <ISAKMP ポリシー名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ISAKMP ポリシー名	ISAKMP ポリシー名を指定します。	63 文字以内の CDATA 型	省略不可

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

Internet Key Exchange ポリシー (VPN ピアとの ISAKMP-SA/IKE SA 用のポリシー) のエントリを設定するために、IKE ポリシー設定モードに移行します。コマンドの先頭に "no" を指定することで、該当 IKE ポリシー設定モードの内容がすべて消去されます。

IKE ポリシー設定モードの設定内容は、ISAKMP プロファイル設定モードで参照されます。

【実行例】

IKE ポリシー設定モードに移行します (ISAKMP ポリシー名 : policy-A)。

```
#configure terminal
(config)#crypto isakmp policy policy-A
(config-isakmp)#
```

17.1.2 crypto isakmp keepalive-params no-reconnect

【機能】

DPD メッセージの送信を契機に ISAKMP-SA の再確立動作を行わない設定

【入力形式】

crypto isakmp keepalive-params no-reconnect

no crypto isakmp keepalive-params no-reconnect

【動作モード】

基本設定モード (IKEv1 でのみ有効)

【説明】

DPD メッセージの送信を契機に ISAKMP-SA の再確立動作を行わない場合に設定します。本コマンドを設定しない場合、ISAKMP-SA がない、または ISAKMP-SA の残り lifetime が crypto isakmp negotiation retry 設定の (<再送間隔>×<再送回数>) 秒よりも少ない際に、DPD メッセージの送信を契機に Phase1 ネゴシエーションを開始し、ISAKMP-SA を再確立します。

【実行例】

DPD メッセージの送信を契機に ISAKMP-SA の再確立動作を行いません。

```
#configure terminal
(config)#crypto isakmp keepalive-params no-reconnect
```

【未設定時】

DPD メッセージの送信を契機に ISAKMP-SA の再確立動作を行います。

17.1.3 crypto isakmp rekey continuous-channel

【機能】

IPSEC-SA も同時に再確立する設定

【入力形式】

crypto isakmp rekey continuous-channel

no crypto isakmp rekey continuous-channel

【動作モード】

基本設定モード (IKEv1 でのみ有効)

【説明】

DPD パケットの送信や ISAKMP-SA のソフトライフタイム満了の契機で ISAKMP-SA を再確立する際に、IPSEC-SA も同時に再確立 (IPSEC-SA が存在する場合) する場合に設定します。

【実行例】

ISAKMP-SA を再確立する際に、IPSEC-SA も同時に再確立します。

```
#configure terminal
(config)#crypto isakmp rekey continuous-channel
```

【未設定時】

同様の関連コマンドとして以下の設定があれば、それに従います。

- set rekey continuous-channel

設定がない場合は、ISAKMP-SA の再確立時に IPSEC-SA の再確立は行いません。

17.1.4 crypto isakmp security-association softlimit

【機能】

ISAKMP-SA/IKE SA の生存時間満了からどれくらい前に、新しい SA を確立するかを設定

【入力形式】

crypto isakmp security-association softlimit {initiate | respond} seconds <差動時間>

no crypto isakmp security-association softlimit {initiate | respond} seconds <差動時間>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
initiate respond	ISAKMP-SA/IKE SA を確立した際の接続状態を指定します。	initiate: Initiator respond: Responder	省略不可
差動時間	ISAKMP-SA/IKE SA の生存満了と新しい SA 確立（リキー開始）との差動時間（単位：秒）を指定します。	1 ~ 3600	

【動作モード】

基本設定モード（IKEv1/IKEv2 で有効）

【説明】

ISAKMP-SA/IKE SA の生存時間満了からどれくらい前に、新しい SA を確立するかを設定します。

IPSEC-SA/CHILD SA がない場合は、事前に新しい SA を確立しません。また、差動時間 ≥ ISAKMP-SA/IKE SA の生存時間（ジッタ時間込み）である場合は、差動時間は 1 秒で動作します。

【実行例】

Initiator として確立した ISAKMP-SA/IKE SA の生存時間が満了する 15 秒前に新しい SA の接続を開始します（Initiator、差動時間：15 秒）。

```
#configure terminal
(config)#crypto isakmp security-association softlimit initiate seconds 15
```

【未設定時】

同様の関連コマンドとして以下の設定があれば、それに従います。

- set security-association softlimit

設定がない場合は、ISAKMP-SA/IKE SA の生存時間満了前に新しい SA を確立しません。

17.1.5 crypto isakmp tos

【機能】

ISAKMP パケットの IPv6 ヘッダのトラフィッククラス値の設定

【入力形式】

crypto isakmp tos <TOS フィールド値>

no crypto isakmp tos [<TOS フィールド値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
TOS フィールド値	IPv6 ヘッダのトラフィッククラス値を指定します。	1 ～ 255	省略不可

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

ISAKMP パケットの IPv6 ヘッダのトラフィッククラス値を設定します。

【実行例】

ISAKMP パケットのトラフィッククラス値を設定します (TOS フィールド値：32)。

```
#configure terminal
(config)#crypto isakmp tos 32
```

【未設定時】

ISAKMP パケットのトラフィッククラス値は 0 で動作します。

17.1.6 crypto ipsec udp-encapsulation-force

【機能】

IKE ネゴシエーションの開始と UDP カプセル化

【入力形式】

crypto ipsec udp-encapsulation-force

no crypto ipsec udp-encapsulation-force

【動作モード】

基本設定モード (IKEv2 でのみ有効)

【説明】

装置単位で IKE ネゴシエーションを UDP4500 番ポートで開始し、強制的に UDP カプセル化を行う場合に設定します。

データコネクト機能を使用して IPsec 通信を行う場合は、この設定を有効にしてください。

【実行例】

IKE ネゴシエーションを UDP4500 番ポートで開始し、強制的に UDP カプセル化を行います。

```
#configure terminal
(config)#crypto ipsec udp-encapsulation-force
```

【未設定時】

同様の関連コマンドとして2つ設定がありますが以下の順で適用されます。

- set udp-encapsulation-force
- crypto ipsec udp-encapsulation-force

どの設定もない場合は、IKE ネゴシエーションをUDP500番ポートで開始し、強制的にUDPカプセル化を行いません。

17.1.7 authentication

【機能】

ISAKMP-SA/IKE SA の認証方式の設定

【入力形式】

authentication <認証方式>

no authentication

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
認証方式	認証方式を指定します。	pre-share:Pre-shared key 方式 rsa-sig:RSA-signatures 方式	省略不可

【動作モード】

ISAKMP ポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

ISAKMP-SA/IKE SA の認証方式を設定します。

【実行例】

ISAKMP-SA/IKE SA の認証方式を設定します (RSA-signatures 方式)。

```
#configure terminal
(config)#crypto isakmp policy policy-A
(config-isakmp)#authentication rsa-sig
```

【未設定時】

認証方式は Pre-shared key 方式で動作します。

17.1.8 dont-route

【機能】

経路表を検索せずに IKE パケットを送信する設定

【入力形式】

dont-route

no dont-route

【動作モード】

ISAKMP ポリシー設定モード

【説明】

IKE パケットを経路表を検索せず、同じネットワークのインタフェースに送信する場合に設定します。

【実行例】

IKE パケットを経路表を検索せず、同じネットワークのインタフェースに送信します。

```
#configure terminal
(config)#crypto isakmp policy policy-A
(config-isakmp)#dont-route
```

【未設定時】

経路表を検索して IKE パケットを送信します。

17.1.9 encryption

【機能】

ISAKMP-SA/IKE SA の暗号アルゴリズムの設定

【入力形式】

encryption <暗号化アルゴリズム>

no encryption

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
暗号化アルゴリズム	暗号化アルゴリズムを指定します。 複数指定が可能です。	des:DES 3des:3DES aes:AES	省略不可

【動作モード】

ISAKMP ポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

ISAKMP-SA/IKE SA の暗号アルゴリズムを設定します。本装置の暗号アルゴリズムには、DES(56bit DES-CBC)、3DES(168bit DES)、AESがあります（AES で使用する鍵長は、encryption-keysize aes コマンドで設定します）。

暗号化アルゴリズムは複数指定することができ、複数指定した場合は Initiator 時に複数の提案を行います。

【実行例】

ISAKMP-SA/IKE SA の暗号化アルゴリズムを設定します（暗号化アルゴリズム：AES）。

```
#configure terminal
(config)#crypto isakmp policy policy-A
(config-isakmp)#encryption aes
```

【未設定時】

暗号化アルゴリズムは 3DES で動作します。

17.1.10 encryption-keysize

【機能】

ISAKMP-SA/IKE SA のネゴシエーションで使用する AES の鍵長の設定

【入力形式】

encryption-keysize aes <鍵長の下限值> <鍵長の上限值> <優先する鍵長>

no encryption-keysize

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
鍵長の下限值	鍵長の最小値を指定します。	128 192 256	省略不可
鍵長の上限值	鍵長の最大値を指定します。	128 192 256	
優先する鍵長	Initiator の時の提案で最優先の鍵長を指定します。	128 192 256	

【動作モード】

ISAKMP ポリシー設定モード（IKEv1/IKEv2 で有効）

【説明】

ISAKMP-SA/IKE SA のネゴシエーションで使用する AES の鍵長を設定します。

<鍵長の下限值> ≤ <優先する鍵長> ≤ <鍵長の上限值> となるように設定してください。

【実行例】

ISAKMP-SA/IKE SA のネゴシエーションで使用する AES の鍵長を設定します（鍵長の下限值：128、鍵長の上限值：256、優先する鍵長：192）。

```
#configure terminal
(config)#crypto isakmp policy policy-A
(config-isakmp)#encryption-keysize 128 256 192
```

【未設定時】

以下の値で動作します。

鍵長の下限值：128

鍵長の上限值：256

優先する鍵長：128

17.1.11 group

【機能】

Diffie-Hellman グループ番号の設定

【入力形式】

group <DH グループ番号>

no group

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
DH グループ番号	Diffie-Hellman グループ番号を指定します。 複数指定が可能です。	1,2,5,14,15	省略不可

【動作モード】

ISAKMP ポリシー設定モード（IKEv1/IKEv2 で有効）

【説明】

Diffie-Hellman グループ番号を設定します。Diffie-Hellman グループ番号には、1(768-bit)、2(1024-bit)、5(1536-bit)、14(2048-bit)、15(3072-bit)の5種類があります。

IKEv2 では DH グループ番号は複数指定することができ、複数指定した場合は Initiator 時に複数の提案を行います。

IKEv1 では 1 つだけ提案します。複数の設定が行われた場合には、先頭のグループ番号の提案を行います。

【実行例】

Diffie-Hellman グループ番号を設定します（DH グループ番号：2）。

```
#configure terminal
(config)#crypto isakmp policy policy-A
(config-isakmp)#group 2
```

【未設定時】

DHグループ番号は2で動作します。

17.1.12 hash

【機能】

ISAKMP-SA/IKE SAのハッシュアルゴリズムの設定

【入力形式】

hash <ハッシュアルゴリズム>

no hash

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ハッシュアルゴリズム	ハッシュアルゴリズムを指定します。 複数指定が可能です。	md5:MD5 sha:SHA-1 aes-xcbc:AES-XCBC sha-256:SHA2(256bits) sha-384:SHA2(384bits) sha-512:SHA2(512bits)	省略不可

【動作モード】

ISAKMP ポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

ISAKMP-SA/IKE SAのハッシュアルゴリズムを設定します。本装置のハッシュアルゴリズムには、MD5、SHA-1、AES-XCBC、SHA-2(256bits,384bits,512bits)があります。

ハッシュアルゴリズムは複数指定することができ、複数指定した場合は Initiator 時に複数の提案を行います。

IKEv1 設定時は AES-XCBC を指定できません。IKEv1 設定時に AES-XCBC を指定した場合、AES-XCBC 設定は無効になります。

【実行例】

ISAKMP-SA/IKE SAのハッシュアルゴリズムを設定します (ハッシュアルゴリズム：SHA-1)。

```
#configure terminal
(config)#crypto isakmp policy policy-A
(config-isakmp)#hash sha
```

【未設定時】

ハッシュアルゴリズムは SHA-1 で動作します。

17.1.13 lifetime

【機能】

ISAKMP-SA/IKE SA の生存時間の設定

【入力形式】

lifetime <生存時間> [jitter <ジッタ時間>]

no lifetime

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
生存時間	生存時間（単位：秒）を指定します。	120 ～ 946080000	省略不可
ジッタ時間	生存時間をランダムに短縮する最大時間（単位：秒）を指定します。	1 ～ 30	

【動作モード】

ISAKMP ポリシー設定モード（IKEv1/IKEv2 で有効）

【説明】

ISAKMP-SA/IKE SA の生存時間（単位：秒）を設定します。ここで指定した時間経過したあとに、ISAKMP-SA/IKE SA を解放します。

また IKEv2 の場合では、CHILD SA が存在する場合に Rekey を開始します。Rekey の衝突を回避したい場合は、ジッタ時間を設定することで衝突確率を下げるすることができます。

【実行例】

ISAKMP-SA/IKE SA の生存時間（単位：秒）を設定します（生存時間：3600 秒）。

```
#configure terminal
(config)#crypto isakmp policy policy-A
(config-isakmp)#lifetime 3600
```

【未設定時】

以下の値で動作します。

生存時間： 86400 秒

ジッタ時間： 0 秒（lifetime の短縮を行わない）

17.1.14 crypto keyring

【機能】

Pre-shared Key リング設定モードへの移行

【入力形式】

crypto keyring <キーリング名>

no crypto keyring <キーリング名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
キーリング名	キーリング名を指定します。	63 文字以内の CDATA 型	省略不可

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

Pre-shared Key のキーリング (鍵束) を設定するために、Pre-shared Key リング設定モードに移行します。

コマンドの先頭に "no" を指定することで、該当 Pre-shared Key リング設定モードの内容がすべて消去されます。

【実行例】

Pre-shared Key リング設定モードに移行します (プロファイル名: keyring-A)。

```
#configure terminal
(config)#crypto keyring keyring-A
(config-keyring)#
```

17.1.15 pre-shared-key

【機能】

VPN ピアごとに Pre-shared Key の設定

【入力形式】

```
pre-shared-key {address <VPN ピア> | host <ホスト名> | user <ユーザ名> | key-id {ascii | binary} <キー ID 名> | tel-key-id <TEL キー ID 名> sha-256} key {<Pre-shared Key> | {ascii | binary} <Pre-shared Key> [{secret | private} [encrypted]]}
```

```
no pre-shared-key {address <VPN ピア> | host <ホスト名> | user <ユーザ名> | key-id {ascii | binary} <キー ID 名> | tel-key-id <TEL キー ID 名> sha-256} [key {<Pre-shared Key> | {ascii | binary} <Pre-shared Key> [{secret | private} encrypted]]}
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VPN ピア	VPN ピアの IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
ホスト名	VPN ピアのホスト名を指定します。	128 文字以内の STRING 型	
ユーザ名	VPN ピアのユーザ名を指定します。	128 文字以内の STRING 型	
キー ID 名	VPN ピアのキー ID 名 (ID-TYPE=KEY_ID) として使用する文字列、またはデータを指定します。ASCII の場合は文字列、BINARY の場合は数値 (16 進数) で指定します。	ASCII:128 文字以内の STRING 型 BINARY:64bytes 以内の 16 進数	

パラメタ	設定内容	設定範囲	省略時
TEL キー ID 名	VPN ピアのキー ID 名 (ID-TYPE=KEY_ID) として使用する文字列を指定します。文字列はそのまま使用されず、SHA-256 により HASH 化した結果の 32 バイトを使用します。	128 文字以内の STRING 型	省略不可
ascii binary	Pre-shared Key を、文字列 (ASCII) として登録するか、データ (BINARY) として登録するかを指定します。	-	文字列 (ASCII) として登録
Pre-shared Key	Pre-shared Key として使用する文字列、またはデータを指定します。 ASCII の場合は文字列、BINARY の場合は数値 (16 進数) で指定します。	ASCII: 128 文字以内の STRING 型 BINARY: 64bytes 以内の 16 進数	省略不可
secret/private	Pre-shared Key として使用する文字列の暗号化／復号化に、共通の鍵を使用するか、固有の鍵を使用するかを指定します。	secret: 共通の鍵を使用する private: 固有の鍵を使用する	暗号化せずに保存
encrypted	Pre-shared Key として使用する文字列が暗号化されている場合に指定します。	-	非暗号化文字列として扱う

【動作モード】

Pre-shared Key リング設定モード (IKEv1/IKEv2 で有効)

【説明】

VPN ピアごとに Pre-shared Key を設定します。

Pre-shared Key は、SA を確立する VPN ピアと同じ設定である必要があります。

"binary" 指定時の入力が奇数桁の場合は、先頭に 0 を補完します。

"secret" を指定した場合は、すべての GX500 に共通の鍵を使って暗号化／復号化し、"private" を指定した場合は、装置固有の鍵を使って暗号化／復号化します。

"encrypted" を指定した場合は、文字列を暗号化された文字列と判断しコンフィグに保存します。

show current.cfg(show running.cfg) コマンドなどで内容を確認すると、暗号化されたパスワードの形式で表示されます。

以下の文字列を Pre-shared Key に設定する場合は、"ascii" の指定が必要です。

"a","as","asc","ascii","ascii","b","bi","bin","bina","binar","binary"

【実行例】

VPN ピアごとに Pre-shared Key を設定します (VPN ピア: 192.0.2.1、Pre-shared Key: secret)。

```
#configure terminal
(config)#crypto keyring keyring-A
(config-keyring)#pre-shared-key address 192.0.2.1 key secret
```

【未設定時】

VPN ピアの Pre-shared Key を参照できません。

17.1.16 initiate-mode

【機能】

IKEv1 の Phase1 ネゴシエーションモードの設定

【入力形式】

initiate-mode <ネゴシエーションモード>

no initiate-mode

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ネゴシエーションモード	IKEv1 の Phase1 のネゴシエーションモードを指定します。	main:Main モード aggressive:Aggressive モード	省略不可

【動作モード】

ISAKMP ポリシー設定モード (IKEv1 でのみ有効)

【説明】

IKEv1 の Phase1 ネゴシエーションモードを指定します。Initiator になる場合は指定したモードで行い、Responder となる場合は指定したモードのみ受け付けます。

【実行例】

Phase1 ネゴシエーションモードを指定します (ネゴシエーションモード：Main モード)。

```
#configure terminal
(config)#crypto isakmp policy policy-A
(config-isakmp)#initiate-mode main
```

【未設定時】

Initiator の場合は Main モードで行い、Responder の場合はどちらのモードも受け付けます。

17.1.17 set negotiation expire-time

【機能】

ISAKMP ネゴシエーションのエキスパイア時間の設定

【入力形式】

set negotiation expire-time <エキスパイア時間>

no set negotiation expire-time

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エキスパイア時間	ISAKMP ネゴシエーションのエキスパイア時間 (単位：秒) を指定します。	30 ～ 600	省略不可

【動作モード】

ISAKMP ポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

ISAKMP ネゴシエーションのエキスパイア時間 (単位: 秒) を設定します。

IKEv1 では initiator/responder において、各ネゴシエーションモードの開始から指定された時間内に該当モードが完了しなかった場合、ネゴシエーションを終了します。

IKEv2 では responder において、IKE_SA_INIT から IKE_AUTH 完了までのリクエストパケットを受信 (再送を除く) してから指定された時間内に、次のリクエストを受信しなかった場合、ネゴシエーションを終了します。

【実行例】

ISAKMP ネゴシエーションのエキスパイア時間 (単位: 秒) を設定します (エキスパイア時間: 120 秒)。

```
#configure terminal
(config)#crypto isakmp policy policy-A
(config-isakmp)#set negotiation expire-time 120
```

【未設定時】

同様の関連コマンドとして 3 つの設定がありますが以下の順で適用されます。

- username isakmp negotiation expire-time
- set negotiation expire-time
- crypto isakmp negotiation expire-time

どの設定もない場合は、エキスパイア時間は 60 秒で動作します。

17.1.18 set negotiation retry

【機能】

ISAKMP ネゴシエーションの再送パラメタの設定

【入力形式】

set negotiation retry timer <再送間隔> limit <再送回数> timer-max <最大再送間隔> guard-time <再送ガード時間>

no set negotiation retry

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
再送間隔	ISAKMP ネゴシエーションパケットの再送間隔 (単位: 秒) を指定します。再送を行うごとに間隔は 2 倍に増加していきます。	1 ~ 60	省略不可
再送回数	ISAKMP ネゴシエーションパケットの再送回数を指定します。	0 ~ 5	

パラメタ	設定内容	設定範囲	省略時
最大再送間隔	ISAKMP ネゴシエーションパケットの最大再送間隔（単位：秒）を指定します。再送間隔がこの設定値以上となる場合は、再送間隔をそれ以上増やさず、設定された値の再送間隔で動作します。	1 ～ 60	省略不可
再送ガード時間	ISAKMP ネゴシエーションパケットを送信してから、再送ガード時間（単位：秒）内に受信したパケット（VPN ピアからの再送パケット）を破棄します。	0 ～ 60	

【動作モード】

ISAKMP ポリシー設定モード（IKEv1/IKEv2 で有効）

【説明】

ISAKMP ネゴシエーションの再送パラメタを設定します。

【実行例】

ISAKMP ネゴシエーションの再送パラメタを設定します（再送間隔：5 秒、再送回数：3 回、最大再送間隔：20 秒、再送ガード時間：10 秒）。

```
#configure terminal
(config)#crypto isakmp policy policy-A
(config-isakmp)#set negotiation retry timer 5 limit 3 timer-max 20 guard-time 10
```

【未設定時】

同様の関連コマンドとして 3 つ設定がありますが以下の順で適用されます。

- username isakmp negotiation retry
- set negotiation retry
- crypto isakmp negotiation retry

どの設定もない場合は、以下の値で動作します。

再送間隔： 10 秒
 再送回数： 2 回
 最大再送間隔： 30 秒
 再送ガード時間： 0 秒

17.1.19 set rekey continuous-channel

【機能】

IPSEC-SA も同時に再確立する設定

【入力形式】

set rekey continuous-channel

no set rekey continuous-channel

【動作モード】

ISAKMP ポリシー設定モード (IKEv1 でのみ有効)

【説明】

DPD パケットの送信や ISAKMP-SA のソフトライフタイム満了の契機で ISAKMP-SA を再確立する際に、IPSEC-SA も同時に再確立 (IPSEC-SA が存在する場合) する場合に設定します。

【実行例】

ISAKMP-SA を再確立する際に、IPSEC-SA も同時に再確立します。

```
#configure terminal
(config)#crypto isakmp policy policy-A
(config-isakmp)#set rekey continuous-channel
```

【未設定時】

同様の関連コマンドとして以下の設定があれば、それに従います。

- crypto isakmp rekey continuous-channel

設定がない場合は、ISAKMP-SA の再確立時に IPSEC-SA の再確立は行いません。

17.1.20 set security-association softlimit

【機能】

ISAKMP-SA/IKE SA の生存時間満了からどれくらい前に、新しい SA を確立するかを設定

【入力形式】

set security-association softlimit {initiate | respond} seconds <差動時間>

no set security-association softlimit {initiate | respond} seconds <差動時間>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
initiate respond	ISAKMP-SA/IKE SA を確立した際の接続状態を指定します。	initiate:Initiator respond:Responder	省略不可
差動時間	ISAKMP-SA/IKE SA の生存満了と新しい SA 確立 (リキー開始) との差動時間 (単位: 秒) を指定します。	1 ~ 3600	

【動作モード】

ISAKMP ポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

ISAKMP-SA/IKE SA の生存時間満了からどれくらい前に、新しい SA を確立するかを設定します。

IPSEC-SA/CHILD SA がない場合は、事前に新しい SA を確立しません。また、差動時間 \geq ISAKMP-SA/IKE SA の生存時間 (ジッタ時間込み) である場合は、差動時間は 1 秒で動作します。

【実行例】

Initiator として確立した ISAKMP-SA/IKE SA の生存時間が満了する 15 秒前に新しい SA の接続を開始します (Initiator、差動時間：15 秒)。

```
#configure terminal
(config)#crypto isakmp policy policy-A
(config-isakmp)#set security-association softlimit initiate seconds 15
```

【未設定時】

同様の関連コマンドとして以下の設定があれば、それに従います。

- crypto isakmp security-association softlimit

設定がない場合は、ISAKMP-SA/IKE SA の生存時間満了前に新しい SA を確立しません。

17.1.21 set udp-encapsulation-force

【機能】

IKE ネゴシエーションの開始と UDP カプセル化

【入力形式】

set udp-encapsulation-force

no set udp-encapsulation-force

【動作モード】

IPSEC ポリシー設定モード (IKEv2 でのみ有効)

【説明】

ポリシー設定単位で IKE ネゴシエーションを UDP4500 番ポートで開始し、強制的に UDP カプセル化を行う場合に設定します。

SIP を使用して IPsec 通信を行う場合は、この設定を有効にしてください。

【実行例】

ポリシー設定単位で IKE ネゴシエーションを UDP4500 番ポートで開始し、強制的に UDP カプセル化を行います。

```
#configure terminal
(config)#crypto ipsec policy policy-A
(conf-ipsec)#set udp-encapsulation-force
```

【未設定時】

同様の関連コマンドとして 2 つ設定がありますが以下の順で適用されます。

- set udp-encapsulation-force
- crypto ipsec udp-encapsulation-force

どの設定もない場合は、IKE ネゴシエーションを UDP500 番ポートで開始し、強制的に UDP カプセル化を行いません。

17.2 IPSEC-SA/CHILD SA の設定

17.2.1 crypto ipsec policy

【機能】

IPSEC ポリシーのエントリの設定

【入力形式】

crypto ipsec policy <IPSEC ポリシー名>

no crypto ipsec policy <IPSEC ポリシー名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
IPSEC ポリシー名	IPSEC ポリシー名を指定します。	63 文字以内の CDATA 型	省略不可

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

IPSEC ポリシー (VPN ピアとの IPSEC-SA/CHILD SA 用のポリシー) のエントリを設定するために、IPSEC ポリシー設定モードに移行します。コマンドの先頭に "no" を指定することで、該当 IPSEC ポリシー設定モードの内容がすべて消去されます。

IPSEC ポリシー設定モードの設定内容は、ISAKMP プロファイル設定モードで参照されます。

【実行例】

IPSEC ポリシー設定モードに移行します (IPSEC ポリシー名: policy-A)。

```
#configure terminal
(config)#crypto ipsec policy policy-A
(config-ipsec)#
```

17.2.2 set pfs

【機能】

PFS を使用する際の Diffie-Hellman グループ番号の設定

【入力形式】

set pfs {group1 | group2 | group5 | group14 | group15}

no set pfs

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
group1 group2 group5 group14 group15	PFS を使用する際の Diffie-Hellman グループ番号を指定します。 複数指定が可能です。	-	省略不可

【動作モード】

IPSEC ポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

PFS を使用する際の Diffie-Hellman グループ番号を設定します。

DH グループ番号は複数指定することができ、複数指定した場合、IKEv2 では Initiator 時に複数の提案を行い、IKEv1 では先頭の 1 つのみ提案を行います。

PFS(Perfect Forward Security) を行う際に、Diffie-Hellman 鍵交換を使用した Oakley と呼ばれる暗号化技術を使用します。本コマンドは Oakley Group を指定します。

group1 は 768-bit、group2 は 1024-bit、group5 は 1536-bit、group14 は 2048-bit、group15 は 3072-bit の Diffie-Hellman となります。

【実行例】

PFS を使用する際の Diffie-Hellman グループ番号を設定します (group2)。

```
#configure terminal
(config)#crypto ipsec policy policy-A
(conf-ipsec)#set pfs group2
```

【未設定時】

PFS を使用しません。

17.2.3 set security-association always-up

【機能】

常に SA を確立しておく設定

【入力形式】

set security-association always-up

no set security-association always-up

【動作モード】

IPSEC ポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

常に SA を確立しておく場合に設定します。何らかの原因で SA が解放されてしまった場合には、SA 確立動作を行います。

VPN ピアのアドレスが不定の場合は、SA 確立動作ができませんので、そのようなケースではご使用になれません。

【実行例】

常に SA を確立しておきます。

```
#configure terminal
(config)#crypto ipsec policy policy-A
(config-ipsec)#set security-association always-up
```

【未設定時】

SA は Lifetime 満了時に解放されます。

17.2.4 crypto ipsec security-association lifetime seconds

【機能】

生存時間の設定

【入力形式】

crypto ipsec security-association lifetime seconds <生存時間>

no crypto ipsec security-association lifetime seconds

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
生存時間	IPSEC-SA/CHILD SA の生存時間（単位：秒）を指定します。	120 ～ 946080000	省略不可

【動作モード】

基本設定モード（IKEv1/IKEv2 で有効）

【説明】

IPSEC-SA/CHILD SA の生存時間（単位：秒）を設定します。

IPSEC ポリシー設定モードに set security-association lifetime seconds コマンドの設定がある場合は、そちらの設定を優先します。

【実行例】

IPSEC-SA/CHILD SA の生存時間（単位：秒）を設定します（生存時間：1800 秒）。

```
#configure terminal
(config)#crypto ipsec security-association lifetime seconds 1800
```

【未設定時】

同様の関連コマンドとして 2 つの設定がありますが以下の順で適用されます。

- set security-association lifetime seconds
- crypto ipsec security-association lifetime seconds

どの設定もない場合は、生存時間は 3600 秒で動作します。

17.2.5 set security-association lifetime seconds

【機能】

生存時間の設定

【入力形式】

set security-association lifetime seconds <生存時間>

no set security-association lifetime seconds

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
生存時間	IPSEC-SA/CHILD SAの生存時間（単位：秒）を指定します。	120～946080000	省略不可

【動作モード】

IPSEC ポリシー設定モード（IKEv1/IKEv2 で有効）

【説明】

IPSEC-SA/CHILD SAの生存時間（単位：秒）を設定します。

【実行例】

IPSEC-SA/CHILD SAの生存時間（単位：秒）を設定します（生存時間：1800 秒）。

```
#configure terminal
(config)#crypto ipsec policy policy-A
(config-ipsec)#set security-association lifetime seconds 1800
```

【未設定時】

同様の関連コマンドとして2つの設定がありますが以下の順で適用されます。

- set security-association lifetime seconds
- crypto ipsec security-association lifetime seconds

どの設定もない場合は、生存時間は3600秒で動作します。

17.2.6 crypto ipsec security-association softlimit

【機能】

生存時間満了、またはシーケンス番号の overflow する値からどれくらい前に、新しいSAを確立するかを設定

【入力形式】

crypto ipsec security-association softlimit {seqnum <差動値> | {initiate | respond} seconds <差動時間> [jitter <ジッタ時間>]}

no crypto ipsec security-association softlimit {seqnum | {initiate | respond} seconds}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
差動値	IPSEC-SA/CHILD SA のシーケンス番号が overflow する値からどれくらい前 (単位: シーケンス番号) に、新しい SA を確立 (リキー開始) するかを指定します。	100000 ~ 1000000000	省略不可
initiate respond	IPSEC-SA/CHILD SA を確立した際の接続状態を指定します。	initiate: Initiator respond: Responder	
差動時間	IPSEC-SA/CHILD SA の生存満了と新しい SA 確立 (リキー開始) との差動時間 (単位: 秒) を指定します。	1 ~ 600	
ジッタ時間	差動時間をランダムに延ばす最大時間 (単位: 秒) を指定します。	1 ~ 30	

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

IPSEC-SA/CHILD SA の生存時間満了、またはシーケンス番号の overflow する値からどれくらい前に、新しい SA を確立するかを設定します。

また VPN ピアとの Rekey の衝突を回避したい場合は、ジッタ時間を設定することで衝突確率を下げることもできます。

IPSEC ポリシー設定モードに set security-association softlimit コマンドの設定がある場合は、そちらの設定を優先します。

【実行例】

Initiator として確立した IPSEC-SA/CHILD SA の生存時間が満了する 15 秒前に新しい SA の接続を開始します (Initiator、差動時間: 15 秒)。

```
#configure terminal
(config)#crypto ipsec security-association softlimit initiate seconds 15
```

【未設定時】

IPSEC ポリシー設定モードに set security-association softlimit コマンドの設定がない場合は、以下の値で動作します。

Initiator 時: 90 秒
 Responder 時: 30 秒
 シーケンス番号による Rekey: なし
 ジッタ時間: 0 秒 (softlimit を延ばさない)

17.2.7 set security-association softlimit

【機能】

生存時間満了、またはシーケンス番号の overflow する値からどれくらい前に、新しい SA を確立するかを設定

【入力形式】

```
set security-association softlimit {seqnum <差動値> | {initiate | respond} seconds <差動時間> [jitter <ジッタ時間>]}
```

```
no set security-association softlimit {seqnum | {initiate | respond} seconds}
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
差動値	IPSEC-SA/CHILD SA のシーケンス番号が overflow する値からどれくらい前 (単位: シーケンス番号) に、新しい SA を確立 (リキー開始) するかを指定します。	100000 ~ 1000000000	省略不可
initiate respond	IPSEC-SA/CHILD SA を確立した際の接続状態を指定します。	initiate: Initiator respond: Responder	
差動時間	IPSEC-SA/CHILD SA の生存満了と新しい SA 確立 (リキー開始) との差動時間 (単位: 秒) を指定します。	1 ~ 600	
ジッタ時間	差動時間をランダムに延ばす最大時間 (単位: 秒) を指定します。	1 ~ 30	

【動作モード】

IPSEC ポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

IPSEC-SA/CHILD SA の生存時間満了、またはシーケンス番号の overflow する値からどれくらい前に、新しい SA を確立するかを設定します。

また VPN ピアとの Rekey の衝突を回避したい場合は、ジッタ時間を設定することで衝突確率を下げることができます。

【実行例】

Initiator として確立した IPSEC-SA/CHILD SA の生存時間が満了する 15 秒前に新しい SA の接続を開始します (Initiator、差動時間: 15 秒)。

```
#configure terminal
(config)#crypto ipsec policy policy-A
(conf-ipsec)#set ipsec security-association softlimit initiate seconds 15
```

【未設定時】

crypto ipsec security-association softlimit コマンドの設定に従います。

17.2.8 set security-association transform-keysize aes

【機能】

IPSEC-SA/CHILD SA のネゴシエーションで使用する使用する AES の鍵長を設定

【入力形式】

set security-association transform-keysize aes <鍵長の下限值> <鍵長の上限值> <優先する鍵長>

no set security-association transform-keysize aes

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
鍵長の下限值	Responder時に受け入れる AES 鍵長の最小値を指定します。これより短い鍵長でのネゴシエーションを受けた場合は、エラーとします。	128 192 256	省略不可
鍵長の上限值	Responder時に受け入れる AES 鍵長の最大値を指定します。これより長い鍵長でのネゴシエーションを受けた場合は、エラーとします。	128 192 256	
優先する鍵長	Initiator時の提案で最優先の AES 鍵長を指定します。	128 192 256	

【動作モード】

IPSEC ポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

IPSEC-SA/CHILD SA のネゴシエーションで使用する AES の鍵長を設定します。

<鍵長の下限值> ≤ <優先する鍵長> ≤ <鍵長の上限值> となるように設定してください。

【実行例】

IPSEC-SA/CHILD SA のネゴシエーションで使用する AES の鍵長を設定します (鍵長の下限值：128、鍵長の上限值：256、優先する鍵長：192)。

```
#configure terminal
(config)#crypto ipsec policy policy-A
(conf-ipsec)#set security-association transform-keysize aes 128 256 192
```

【未設定時】

以下の値で動作します。

鍵長の下限值：128

鍵長の上限值：256

優先する鍵長：128

17.2.9 set security-association transform

【機能】

暗号化アルゴリズム、認証アルゴリズムの設定

【入力形式】

set security-association transform [<暗号化アルゴリズム> | <認証アルゴリズム>]

no set security-association transform

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
暗号化アルゴリズム	暗号化アルゴリズムを指定します。 複数指定が可能です。	esp-des:DES esp-3des:3DES esp-aes:AES esp-null : 暗号化しない	3DES
認証アルゴリズム	認証アルゴリズムを指定します。 複数指定が可能です。	esp-md5-hmac:HMAC-MD5 esp-sha-hmac:HMAC-SHA-1 esp-sha256-hmac: HMAC-SHA-2(256bits) esp-sha384-hmac: HMAC-SHA-2(384bits) esp-sha512-hmac: HMAC-SHA-2(512bits) esp-hash-none: 認証なし	HMAC-SHA-1

【動作モード】

IPSEC ポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

IPSEC-SA/CHILD SAのポリシーとして、暗号化アルゴリズム、認証アルゴリズムを設定します。

暗号化アルゴリズム、認証アルゴリズムは複数指定することができ、複数指定した場合はネゴシエーション時に複数の提案を行います。

ただし、esp-hash-noneは他の認証アルゴリズムと一緒に指定できません。一緒に指定した場合、esp-hash-none設定は無視されます。

また、esp-nullとesp-hash-noneのみの設定はできません。

esp-hash-noneには脆弱性(NISCC-004033)が存在するため、使用する際にはご注意ください。

【実行例】

IPSEC-SA/CHILD SAのポリシーとして、暗号化アルゴリズム、認証アルゴリズムを設定します (暗号化アルゴリズム : DES、認証アルゴリズム : HMAC-MD5)。

```
#configure terminal
(config)#crypto ipsec policy policy-A
(conf-ipsec)#set security-association transform esp-des esp-md5-hmac
```

【未設定時】

以下の値で動作します。

暗号化アルゴリズム : 3DES

認証アルゴリズム : HMAC-SHA-1

17.2.10 set esn

【機能】

すべての SA で ESN 機能を有効にする設定

【入力形式】

set esn {enable | disable}

no set esn

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
enable disable	ESN(Extended Sequence Numbers) 機能の有効／無効を指定します。	enable: 有効 disable: 無効	省略不可

【動作モード】

IPSEC ポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

すべての SA で ESN(Extended Sequence Numbers) 機能を有効にする場合に設定します。

なお、ESN 機能を有効にした場合、sequence-overflow 設定に関係なく、シーケンス番号監視機能は無効になります。

【実行例】

すべての SA で ESN(Extended Sequence Numbers) 機能を有効にします。

```
#configure terminal
(config)#crypto ipsec policy policy-A
(conf-ipsec)#set esn enable
```

【未設定時】

同様の関連コマンドとして 2 つ設定がありますが以下の順で適用されます。

- set esn
- crypto ipsec esn

どの設定もない場合は、ESN 機能を使用しません。

17.2.11 set udp-encapsulation

【機能】

ESP パケットの UDP カプセル化を行うポリシー個別の方式の設定

【入力形式】

set udp-encapsulation <UDP カプセル化方式> [keepalive interval <送信間隔> [always-send]]

no set udp-encapsulation [<UDP カプセル化方式> [keepalive interval <送信間隔> [always-send]]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
UDP カプセル化方式	UDP カプセル化を行う方式を指定します。	nat-t:NAT-Traversal を使用します。 spoofed:NAT-Traversal を使用し、常に UDP カプセル化します。	省略不可
送信間隔	NAT-Keepalive メッセージの送信間隔 (単位：秒) を指定します。	10～3600	NAT-Keepalive メッセージを送信しない
always-send	通信の状態によらず、定期的に NAT-Keepalive メッセージを送信する場合に指定します。	-	一定期間通信がなかった場合に、NAT-Keepalive メッセージを送信

【動作モード】

IPSEC ポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

ESP パケットの UDP カプセル化を行うポリシー個別の方式を設定します。NAT-Traversal 機能を使用して動的に UDP カプセル化を行う場合は "nat-t" を指定し、NAT-Traversal 機能を使用して NAT の有無に関係なく常に UDP カプセル化を行う場合は "spoofed" を指定します。

NAT-Traversal は RFC、および draft に準拠しており、RFC 準拠モードの方を優先させて動作します (RFC3947,3948、および draft-ietf-ipsec-nat-t-ike-00.txt,draft-ietf-ipsec-udp-encaps-00.txt,draft-ietf-ipsec-nat-t-ike-03.txt,draft-ietf-ipsec-udp-encaps-03.txt に対応しています)。

また、自装置が NAT の後ろに存在する場合に NAT-Keepalive パケットを送信する場合は、"keepalive" を指定します。IKEv2 で "spoofed" を NAT が存在しない環境で使用する場合、responder 側には crypto ipsec responder udp-encapsulation spoofed の設定も必要です。

【実行例】

ESP パケットの UDP カプセル化を行う方式を設定します (UDP カプセル化方式：nat-t)。

```
#configure terminal
(config)#crypto ipsec policy policy-A
(conf-ipsec)#set udp-encapsulation nat-t
```

【未設定時】

同様の関連コマンドとして 2 つ設定がありますが以下の順で適用されます。

- set udp-encapsulation
- crypto ipsec udp-encapsulation

どちらの設定もない場合は、NAT-Traversal 機能、および UDP カプセル化を行いません。

17.3 IPSEC セレクタの設定

17.3.1 crypto ipsec selector

【機能】

IPSEC-SA/CHILD SA 用のセレクタのエントリの設定

【入力形式】

crypto ipsec selector <IPSEC セレクタ名>

no crypto ipsec selector <IPSEC セレクタ名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
IPSEC セレクタ名	IPSEC セレクタ名を指定します。	63 文字以内の CDATA 型	省略不可

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

IPSEC-SA/CHILD SA 用のセレクタのエントリを設定するために、IPSEC セレクタ設定モードに移行します。コマンドの先頭に "no" を指定することで、該当 IPSEC セレクタ設定モードの内容がすべて消去されます。

IPSEC セレクタ設定モードの設定内容は、VPN セレクタ設定モードで参照されます。

【実行例】

IPSEC セレクタ設定モードに移行します (IPSEC セレクタ名: selector-A)。

```
#configure terminal
(config)#crypto ipsec selector selector-A
(config-ip-selector)#
```

17.3.2 src

【機能】

セレクタの送信元 IP アドレスの設定

【入力形式】

src <セレクタ番号> {ipv4 | ipv6} {any | <src-address> <src-netmask> | <src-prefix>}

no src <セレクタ番号> [{ipv4 | ipv6} {any | <src-address> <src-netmask> | <src-prefix>}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
セレクト番号	セレクトのインデックスを指定します。	1 ～ 46	省略不可
ipv4 ipv6	IPv4 のセレクトか、IPv6 のセレクトかを指定します。	-	
any <src-address> <src-netmask> <src-prefix>	セレクトの送信元アドレス情報を指定します。 any はすべてのアドレスを指定します。	any : すべてのアドレス IPv4 アドレス形式 IPv6 アドレス形式	

【動作モード】

IPSEC セレクト設定モード (IKEv1/IKEv2 で有効)

【説明】

セレクトの送信元 IP アドレスを設定します。

【実行例】

セレクトの送信元 IP アドレスを設定します (セレクト番号 : 1、ipv4、any)。

```
#configure terminal
(config)#crypto ipsec selector selector-A
(config-ip-selector)#src 1 ipv4 any
```

【未設定時】

IPSEC セレクトは無効となります。

17.3.3 dst

【機能】

セレクトの宛先 IP アドレスの設定

【入力形式】

dst <セレクト番号> {ipv4 | ipv6} {any | <dst-address> <dst-netmask> | <dst-prefix>}

no dst <セレクト番号> [{ipv4 | ipv6} {any | <dst-address> <dst-netmask> | <dst-prefix>}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
セレクト番号	セレクトのインデックスを指定します。	1 ～ 46	省略不可
ipv4 ipv6	IPv4 のセレクトか、IPv6 のセレクトかを指定します。	-	
any <dst-address> <dst-netmask> <dst-prefix>	セレクトの宛先アドレス情報を指定します。 any はすべてのアドレスを指定します。	any: すべてのアドレス IPv4 アドレス形式 IPv6 アドレス形式	

【動作モード】

IPSEC セレクタ設定モード (IKEv1/IKEv2 で有効)

【説明】

セレクタの宛先 IP アドレスを設定します。

【実行例】

セレクタの宛先 IP アドレスを設定します (セレクタ番号 : 1、ipv4、any)。

```
#configure terminal
(config)#crypto ipsec selector selector-A
(config-ip-selector)#dst 1 ipv4 any
```

【未設定時】

IPSEC セレクタは無効となります。

17.4 ISAKMP プロファイルの設定

17.4.1 crypto isakmp profile

【機能】

ISAKMP プロファイル設定モードへの移行

【入力形式】

crypto isakmp profile <プロファイル名>

no crypto isakmp profile <プロファイル名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プロファイル名	プロファイル名を指定します。	63 文字以内の CDATA 型	省略不可

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

ISAKMP のポリシーをまとめたプロファイルを作成するために、ISAKMP プロファイル設定モードに移行します。コマンドの先頭に "no" を指定することで、該当 ISAKMP プロファイル設定モードの内容がすべて消去されます。

【実行例】

ISAKMP プロファイル設定モードに移行します (プロファイル名: profile-A)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(config-isa-prof)#
```

17.4.2 accounting

【機能】

アカウント方式名の設定

【入力形式】

accounting <アカウント方式名>

no accounting

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アカウント方式名	アカウント方式名を指定します。	63 文字以内の CDATA 型	省略不可

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

アカウント方式名を設定します。

アカウント方式名は aaa accounting network コマンドで設定した名称を指定します。

本設定を行うことで、aaa accounting network コマンドで指定したサーバグループのポリシーに従い、アカウントリングを行います。

【実行例】

アカウント方式名を設定します (アカウント方式名: account-A)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(conf-isa-prof)#accounting account-A
```

【未設定時】

アカウントリングを行いません。

17.4.3 fvrfr

【機能】

VPN ピアとのネゴシエーションするインタフェースの VRF 名の設定

【入力形式】

fvrfr <VRF 名>

no fvrfr

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VRF 名	VPN ピアとのネゴシエーションを行う際にマッピングする VRF の名称を指定します。	63 文字以内の WORD 型	省略不可

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

VPN ピアとのネゴシエーションを行うインタフェースの VRF 名を設定します。

VRF 名は ip vrf コマンドで設定します。

【実行例】

VPN ピアとのネゴシエーションを行うインタフェースの VRF 名を設定します (VRF 名: vrf-A)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(conf-isa-prof)#fvrfr vrf-A
```

【未設定時】

VRF のマッピングを行いません。

17.4.4 ike-version

【機能】

機能を有効にする IKE のバージョンの設定

【入力形式】

ike-version {1 | 2}

no ike-version

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
1 2	機能を有効にする IKE のバージョンを指定します。	1:IKEv1 のみ 2:IKEv2 のみ	省略不可

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

機能を有効にする IKE のバージョンを設定します。設定を変更した場合には、本プロファイルを使用しているセッションをすべて解放します。

【実行例】

機能を有効にする IKE のバージョンを設定します (2)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(conf-isa-prof)#ike-version 2
```

【未設定時】

IKEv2 のみで動作します。

17.4.5 isakmp authorization list

【機能】

許可方式名の設定

【入力形式】

isakmp authorization list <許可方式名>

no isakmp authorization list

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
許可方式名	許可方式名を指定します。	63 文字以内の CDATA 型	省略不可

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

許可方式名を設定します。

許可方式名は aaa authorization network コマンドで設定した名称を指定します。

【実行例】

許可方式名を設定します (許可方式名: AUTH-A)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(config-isa-prof)#isakmp authorization list AUTH-A
```

【未設定時】

アドレス割り当てを行いません。

17.4.6 keyring

【機能】

キーリング名の設定

【入力形式】

keyring <キーリング名>

no keyring

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
キーリング名	キーリング名を指定します。	63 文字以内の CDATA 型	省略不可

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

キーリング名を設定します。

【実行例】

キーリング名を設定します (キーリング名: keyring-A)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(config-isa-prof)#keyring keyring-A
```


【未設定時】

Pre-shared Key 方式による IPsec 通信を行いません。

17.4.7 local-address

【機能】

本装置の IP アドレスの設定

【入力形式】

local-address {<送信元 IP アドレス> | source-interface <インタフェース名> <インタフェース番号>}

no local-address [{<送信元 IP アドレス> | source-interface <インタフェース名> <インタフェース番号>}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
送信元アドレス	IPsec トンネルを確立する、本装置の IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
インタフェース名	IPsec トンネルを確立する、本装置の送信元 IP アドレスとして使用するインタフェース名を指定します。	-	省略不可
インタフェース番号	IPsec トンネルを確立する、本装置の送信元 IP アドレスとして使用するインタフェース番号を指定します。	-	省略不可

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

IPsec トンネルを確立する、本装置の送信元 IP アドレスまたは送信元 IP アドレスとして使用するインタフェースを設定します。VRRP の仮想アドレスは未サポートとなります。動的 VPN 機能使用時は、本設定は無効になります。

【実行例】

本装置の IP アドレスを設定します (送信元アドレス: 192.0.2.1)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(config-isa-prof)#local-address 192.0.2.1
```

【未設定時】

VPN ピアと通信するインタフェースの IP アドレスを送信元アドレスとします。

17.4.8 local-key

【機能】

本装置の Pre-shared Key の設定

【入力形式】

local-key {<Pre-shared Key> | {ascii | binary} <Pre-shared Key> [{secret | private} [encrypted]] | ngn-sip tunnel-password | dvpn dynamic-key}

no local-key [{<Pre-shared Key> | {ascii | binary} <Pre-shared Key> [{secret | private}] [encrypted] | ngn-sip tunnel-password | dvpn dynamic-key}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ascii binary	Pre-shared Key を、文字列 (ASCII) として登録するか、データ (BINARY) として登録するかを指定します。	-	文字列 (ASCII) として登録
Pre-shared Key	Pre-shared Key として使用する文字列またはデータを指定します。 ASCII の場合は文字列、BINARY の場合は数値 (16 進数) で指定します。	ASCII:128 文字以内の STRING 型 BINARY:64bytes 以内の 16 進数	省略不可
secret/private	Pre-shared Key として使用する文字列の暗号化／復号化に、共通の鍵を使用するか、固有の鍵を使用するかを指定します。	secret: 共通の鍵を使用する private: 固有の鍵を使用する	暗号化せずに保存
encrypted	Pre-shared Key として使用する文字列が暗号化されている場合に指定します。	-	非暗号化文字列として扱う
ngn-sip tunnel-password	データコネクタ機能の Tunnel-Password を使った IKE ネゴシエーションを使用する場合に指定します。	-	データコネクタ機能の Tunnel-Password を使った IKE ネゴシエーションが使用できません。
dvpn dynamic-key	動的 VPN クライアント機能でサーバから通知された共有鍵を IKE ネゴシエーションに使用する場合に指定します。	-	動的 VPN クライアント機能でサーバから通知された共有鍵を IKE ネゴシエーションに使用できません。

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

本装置の Pre-shared Key を設定します。

"binary" 指定時の入力が奇数桁の場合は、先頭に 0 を補完します。

"secret" を指定した場合は、すべての GX500 に共通の鍵を使って暗号化／復号化し、"private" を指定した場合は、装置固有の鍵を使って暗号化／復号化します。

"encrypted" を指定した場合は、文字列を暗号化された文字列と判断しコンフィグに保存します。

show current.cfg(show running.cfg) コマンドなどで内容を確認すると、暗号化されたパスワードの形式で表示されます。

以下の文字列を Pre-shared Key に設定する場合は、"ascii" の指定が必要です。

"a","as","asc","ascii","b","bi","bin","bina","binar","binary"

データコネクト機能で、SIP の RADIUS 認証機能による電話番号認証時の Access-Accept で通知される Tunnel-Password を用いて IKE ネゴシエーションを行う場合、ngn-sip tunnel-password を指定してください。

動的 VPN クライアント機能でサーバから配布された共有鍵を用いて IKE ネゴシエーションを行う場合、dvpn dynamic-key を指定してください。

【実行例】

本装置の Pre-shared Key を設定します (Pre-shared Key:secret)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(conf-isa-prof)#local-key secret
```

【未設定時】

本装置の Pre-shared Key を参照できません。

17.4.9 match identity

【機能】

VPN ピアの識別方法の設定

【入力形式】

match identity {address <VPN ピア> | host <ホスト名> | user <ユーザ名> | key-id {ascii | binary} <キー ID 名> | tel-key-id <TEL キー ID 名> sha-256}

no match identity

パラメタ	設定内容	設定範囲	省略時
VPN ピア	VPN ピアの IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
ホスト名	VPN ピアのホスト名 (ID-TYPE=FQDN) を指定します。	128 文字以内の STRING 型	
ユーザ名	ユーザ名 (ID-TYPE=User-FQDN) を指定します。	128 文字以内の STRING 型	
キー ID 名	VPN ピアのキー ID 名 (ID-TYPE=KEY_ID) として使用する文字列またはデータを指定します。 ASCII の場合は文字列、BINARY の場合は数値 (16 進数) で指定します。	ASCII: 128 文字以内の STRING 型 BINARY: 64bytes 以内の 16 進数	
TEL キー ID 名	VPN ピアのキー ID 名 (ID-TYPE=KEY_ID) として使用する文字列を指定します。文字列はそのまま使用されず、SHA-256 により HASH 化した結果の 32 バイトを使用します。	128 文字以内の STRING 型	

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

VPN ピアの識別方法を設定します。

VPN ピアを識別するために通知される Identity は、IP アドレス形式／FQDN 形式／User-FQDN 形式／キー ID 形式のどれかで通知されます。

IKEv2 では、User-FQDN 形式は ID_RFC822_ADDR に対応します。

【実行例】

VPN ピアの識別方法を設定します（ホスト名：host-A）。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(config-isakmp)#match identity host host-A
```

【未設定時】

VPN ピアの識別方法を参照しません。

17.4.10 self-identity

【機能】

本装置の識別方法の設定

【入力形式】

self-identity {address <本装置のアドレス> | fqdn <ホスト名> | user-fqdn <ユーザ名> | key-id {ascii | binary} <キー ID 名> | tel-key-id <TEL キー ID 名> sha-256}

no self-identity

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
本装置のアドレス	本装置の IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
ホスト名	本装置のホスト名 (ID-TYPE=FQDN) を指定します。	128 文字以内の STRING 型	
ユーザ名	ユーザ名 (ID-TYPE=User-FQDN) を指定します。	128 文字以内の STRING 型	
キー ID 名	本装置のキー ID 名 (ID-TYPE=KEY_ID) として使用する文字列またはデータを指定します。ASCII の場合は文字列、BINARY の場合は数値（16 進数）で指定します。	ASCII：128 文字以内の STRING 型 BINARY：64bytes 以内の 16 進数	
TEL キー ID 名	本装置のキー ID 名 (ID-TYPE=KEY_ID) として使用する文字列を指定します。文字列はそのまま使用されず、SHA-256 により HASH 化した結果の 32 バイトを使用します。	128 文字以内の STRING 型	

【動作モード】

ISAKMP プロファイル設定モード（IKEv1/IKEv2 で有効）

【説明】

本装置の識別方法を設定します。

VPN ピアを識別するために通知される Identity は、IP アドレス形式／FQDN 形式／User-FQDN 形式／キー ID 形式のどれかで通知されます。

Fully Qualified Domain Name(FQDN)形式は "ホスト名.ドメイン名" の形で表記されます。たとえば、host-A.example.com という FQDN 形式の場合、"host-A" がホスト名、"example.com" がドメイン名となります。

User-Fully Qualified Domain Name(User-FQDN)形式は "ユーザ名@ドメイン名" の形で表記されます。たとえば、user-A@example.com という User-FQDN 形式の場合、"user-A" がユーザ名、"example.com" がドメイン名となります。

IKEv2 では、User-FQDN 形式は ID_RFC822_ADDR に対応します。

【実行例】

本装置の識別方法を設定します（ユーザ名：user-A@example.com）。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(conf-isa-prof)#self-identity user-fqdn user-A@example.com
```

【未設定時】

VPN ピアと通信するインタフェースの IP アドレスを利用します。

17.4.11 set ipsec-policy

【機能】

この ISAKMP プロファイルで使用する IPSEC ポリシーの設定

【入力形式】

set ipsec-policy <IPSEC ポリシー名>

no set ipsec-policy

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
IPSEC ポリシー名	IPSEC ポリシー名を指定します。	63 文字以内の CDATA 型	省略不可

【動作モード】

ISAKMP プロファイル設定モード（IKEv1/IKEv2 で有効）

【説明】

この ISAKMP プロファイルで使用する IPSEC ポリシーを設定します。

IPSEC ポリシー名は crypto ipsec policy コマンドで設定した名称を指定します。

【実行例】

この ISAKMP プロファイルで使用する IPSEC ポリシー名を設定します (IPSEC ポリシー名: policy-A)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(config-isa-prof)#set ipsec-policy policy-A
```

【未設定時】

IPSEC ポリシー設定モードの各設定のデフォルト値で動作します。

17.4.12 set isakmp-policy

【機能】

ISAKMP ポリシー名の設定

【入力形式】

set isakmp-policy <ISAKMP ポリシー名>

no set isakmp-policy

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ISAKMP ポリシー名	ISAKMP ポリシー名を指定します。	63 文字以内の CDATA 型	省略不可

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

ISAKMP ポリシー名を設定します。

【実行例】

ISAKMP ポリシー名を設定します (ISAKMP ポリシー名: policy-A)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(config-isa-prof)#set isakmp-policy policy-A
```

【未設定時】

ISAKMP ポリシー設定モードの各設定のデフォルト値で動作します。

17.4.13 set peer

【機能】

VPN ピアの IP アドレスまたはドメイン名の設定

【入力形式】

set peer {<VPN ピアアドレス> | domain <VPN ピアドメイン名> [{v4 | v6}]}sip-profile <SIP プロファイル名> | sip-radius | dvpn-profile <DVPN プロファイル ID>}

no set peer {<VPN ピアアドレス> | domain <VPN ピアドメイン名> [{v4 | v6}]}sip-profile <SIP プロファイル名> | sip-radius | dvpn-profile <DVPN プロファイル ID>}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VPN ピア	VPN ピアの IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
VPN ピアドメイン名	VPN ピアをドメイン名で指定します。	253 文字以内の DOMAIN-WORD 型	省略不可
v4 v6	ドメイン名の名前解決を v4、v6 のどちらで行うか指定します。	v4 v6	local-address で IP アドレスが指定されている場合はその IP バージョンに従います 指定がない場合は v6、v4 の順に名前解決を行います
SIP プロファイル名	SIP 接続用のプロファイル名を指定します。	63 文字以内の CDATA 型	省略不可
sip-radius	データコネクト機能で RADIUS による相手番号認証を行う場合に指定します。	-	RADIUS 認証を用いたデータコネクトが利用できません
DVPN プロファイル ID	動的 VPN クライアント機能での動的 VPN プロファイルの ID を指定します。	1 ～ 3000	省略不可

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

VPN ピアの IP アドレス、またはドメイン名を設定します。

データコネクト機能で IPsec 通信を行う場合は sip profile 名を指定します。

動的 VPN クライアント機能で IPsec 通信を行う場合は、dvpn profile の ID を指定します。

【実行例】

VPN ピアの IP アドレスを設定します (VPN ピア : 192.0.2.1)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(conf-isa-prof)#set peer 192.0.2.1
```

【未設定時】

Initiator として動作しません。

17.5 VPN セレクタの設定

17.5.1 crypto map

【機能】

VPN セレクタ設定モードへの移行

【入力形式】

crypto map <セレクタ名> ipsec-isakmp [dynamic]

no crypto map <セレクタ名> ipsec-isakmp [dynamic]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
セレクタ名	セレクタ名を指定します。	63 文字以内の CDATA 型	省略不可
dynamic	ダイナミックセレクタとして動作する場合に指定します。	-	ダイナミックセレクタとして動作しない

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

VPN ピアとのセレクタ情報のエントリを設定するために、VPN セレクタ設定モードに移行します。コマンドの先頭に "no" を指定することで、該当 VPN セレクタ設定モードの内容がすべて消去されます。

"dynamic" を指定した場合には、ダイナミックセレクタとして動作します。ダイナミックセレクタとは、条件を規定せず相手からの提案に従って通信を行うためのセレクタとなります。

【実行例】

VPN セレクタ設定モードに移行します (セレクタ名: selector-A)。

```
#configure terminal
(config)#crypto map selector-A ipsec-isakmp
(config-crypto-map)#
```

17.5.2 link-state

【機能】

インタフェースの状態を SA 確立に同期させる設定

【入力形式】

link-state sync-sa

no link-state [sync-sa]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
sync-sa	インタフェースの状態を同期させる場合に指定します。	SA 確立に同期	省略不可

【動作モード】

VPN セレクタ設定モード (IKEv1/IKEv2 で有効)

【説明】

インタフェースの状態を SA 確立に同期させる場合に設定します。
survey コマンドによる IPsec tunnel の監視との併用は未サポートとなります。
※Tunnel Down だけでは SA は削除されません。

【sync-sa 設定時】

- SA が確立されていない → tunnel インタフェース DOWN
- SA が確立されている → tunnel インタフェース UP

【実行例】

インタフェースの状態を SA 確立に同期させます。

```
#configure terminal
(config)#crypto map selector-A ipsec-isakmp
(config-crypto-map)#link-state sync-sa
```

【未設定時】

tunnel インタフェース設定モードの link-state 設定に従います。どちらも設定がない場合、スタティックセレクタであれば、SA 確立と同期しません。ダイナミックセレクタであれば、SA 確立に同期します。

17.5.3 match address

【機能】

暗号化するパケットとして IPSEC セレクタ名を設定

【入力形式】

match address <IPSEC セレクタ名>

no match address

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
IPSEC セレクタ名	暗号化するパケットとしてセレクタ名を指定します。	63 文字以内の CDATA 型	IPv4 any, IPv6 any (IKEv2 のダイナミックセレクタ設定時のみ省略可能)

【動作モード】

VPN セレクタ設定モード (IKEv1/IKEv2 で有効)

【説明】

暗号化するパケットとして IPSEC セレクタ名を設定します。

IPSEC セレクタ名は、crypto ipsec selector コマンドで設定した名称を指定します。

パケットの送信元アドレスや宛先アドレスは、IPSEC セレクタ設定モードで設定します。

また、IKEv1 を使用する際に 1 つの VPN ピアに対して複数の IPsec SA を確立したい場合は、tunnel インタフェースで有効にする VPN セレクタを設定し、それぞれ異なる IPSEC セレクタを設定します。この場合、VPN セレクタ設定モードでは match address による IPSEC セレクタの設定は行わないでください。指定した場合、対象 VPN セレクタは無効となります。

【実行例】

暗号化するパケットとして IPSEC セレクタ名を設定します (IPSEC セレクタ名: selector-A)。

```
#configure terminal
(config)#crypto map selector-A ipsec-isakmp
(config-crypto-map)#match address selector-A
```

【未設定時】

IPsec 通信を行うことができません。

17.5.4 set isakmp-profile

【機能】

使用する ISAKMP プロファイル名の設定

【入力形式】

set isakmp-profile <ISAKMP プロファイル名>

no set isakmp-profile

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ISAKMP プロファイル名	ISAKMP プロファイル名を指定します。	63 文字以内の CDATA 型	省略不可

【動作モード】

VPN セレクタ設定モード (IKEv1/IKEv2 で有効)

【説明】

使用する ISAKMP プロファイル名を設定します。

【実行例】

使用する ISAKMP プロファイル名を設定します (ISAKMP プロファイル名: profile-A)。

```
#configure terminal
(config)#crypto map selector-A ipsec-isakmp
(config-crypto-map)#set isakmp-profile profile-A
```

【未設定時】

このVPNセレクトタを使用できません。

17.5.5 tunnel mode

【機能】

VPNセレクトタ、IPinIPトンネルプロファイル、PPPoEプロファイルの設定

【入力形式】

```
tunnel mode {ipsec [map <VPNセレクトタ名>] [match address <IPSECセレクトタ名>]] | ipinip tunnel-  
profile <IPinIPプロファイル名> | pppoe profile <PPPoEプロファイル名>}
```

```
no tunnel mode [ipsec [map <VPNセレクトタ名>] [match address <IPSECセレクトタ名>]] | ipinip tunnel-  
profile <IPinIPプロファイル名> | pppoe profile <PPPoEプロファイル名>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VPNセレクトタ名	VPNセレクトタ名を指定します。	63文字以内のCDATA型	ユーザに固定のインタフェースを使用する
IPSECセレクトタ名	暗号化するパケットとしてセレクトタ名を指定します。	63文字以内のCDATA型	省略不可
IPinIPプロファイル名	IPinIPトンネルプロファイル名を指定します。	63文字以内のWORD型	
PPPoEプロファイル名	PPPoEプロファイル名を指定します。	63文字以内のCDATA型	

【動作モード】

tunnel インタフェース設定モード

【説明】

tunnel インタフェースで有効にするVPNセレクトタ、IPinIPトンネルプロファイル、PPPoEプロファイルを設定します。

VPNセレクトタ名は、crypto map コマンドで設定した名称を指定します。

ダイナミックセレクトタでユーザに固定のインタフェースを使用したい場合は、VPNセレクトタ名を省略します。

また、IKEv1を使用する際に1つのVPNピアに対して複数のIPsec SAを確立したい場合は、tunnel インタフェースで有効にするVPNセレクトタを設定し、それぞれ異なるIPSECセレクトタを設定します。

IPinIPプロファイル名は ipinip tunnel-profile コマンドで設定した名称を指定します。

PPPoEプロファイル名は pppoe profile コマンドで設定した名称を指定します。

【実行例】

tunnel インタフェースで有効にするVPNセレクトタを設定します (VPNセレクトタ名: selector-A)。

```
#configure terminal
(config)#interface tunnel 1
(config-if-tun 1)#tunnel mode ipsec map selector-A
```

【未設定時】

tunnel インタフェースで IPsec、IPinIP 通信、PPPoE 通信の機能が動作しません。

17.5.6 vrf

【機能】

IPsec トンネルにマッピングする VRF 名の設定

【入力形式】

vrf <VRF 名>

no vrf

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VRF 名	IPsec トンネルにマッピングする VRF 名を指定します。	63 文字以内の WORD 型	省略不可

【動作モード】

VPN セレクタ設定モード (IKEv1/IKEv2 で有効)

【説明】

IPsec トンネルにマッピングする VRF 名を設定します。

VRF 名は ip vrf コマンドで設定します。

【実行例】

IPsec トンネルにマッピングする VRF 名を設定します (VRF 名：vrf-A)。

```
#configure terminal
(config)#crypto map selector-A ipsec-isakmp
(config-crypto-map)#vrf vrf-A
```

【未設定時】

VRF のマッピングを行いません。

17.6 データベースの設定

拡張認証を装置に設定したデータベースで行うために、データベースの登録を行います。

17.6.1 aaa local group

【機能】

CLIENT- データベース設定モードへの移行

【入力形式】

aaa local group < 認証グループ名 >

no aaa local group < 認証グループ名 >

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
認証グループ名	認証グループ名を指定します。	63 文字以内の CDATA 型	省略不可

【動作モード】

基本設定モード

【説明】

拡張認証 (Xauth/EAP) を行うデータベースを登録するために、CLIENT- データベース設定モードに移行します。コマンドの先頭に "no" を指定することで、該当 CLIENT- データベース設定モードの内容がすべて消去されます。

【実行例】

CLIENT- データベース設定モードに移行します (認証グループ名: local-A)。

```
#configure terminal
(config)#aaa local group local-A
(config-lg-user)#
```

17.6.2 username

【機能】

拡張認証 (Xauth/EAP) により接続を許可するユーザ名とパスワードの設定

【入力形式】

username < ユーザ名 > password < パスワード > [{secret | private} [encrypted]]

no username < ユーザ名 > [password < パスワード > [{secret | private} encrypted]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ユーザ名	ユーザ名を指定します。	128文字以内の STRING 型	省略不可
パスワード	パスワードを指定します。	128文字以内の STRING 型	
secret/private	パスワードとして使用する文字列の暗号化／復号化に、共通の鍵を使用するか、固有の鍵を使用するかを設定します。	secret: 共通の鍵を使用する private: 固有の鍵を使用する	暗号化せずに保存
encrypted	パスワードとして使用する文字列が暗号化されていることを示します。	-	非暗号化文字列として扱う

【動作モード】

CLIENT- データベース設定モード (IKEv1/IKEv2 で有効)

【説明】

拡張認証 (Xauth/EAP) により接続を許可するユーザ名とパスワードを設定します。

"secret" を指定した場合は、すべての GX500 に共通の鍵を使って暗号化／復号化し、"private" を指定した場合は、装置固有の鍵を使って暗号化／復号化します。

"encrypted" を指定した場合は、文字列を暗号化された文字列と判断しコンフィグに保存します。

"show running.cfg" などで内容を確認すると、暗号化されたパスワードの形式で表示されます。

【実行例】

拡張認証 (Xauth/EAP) により接続を許可するユーザ名とパスワードを設定します (ユーザ名: user-A、パスワード: admin123)。

```
#configure terminal
(config)#aaa local group local-A
(config-lg-user)#username user-A password admin123
```

【未設定時】

この認証グループを利用した IPsec の拡張認証を行いません。

17.6.3 username interface tunnel

【機能】

ダイナミックセレクトを使用したユーザに対して固定のインタフェース番号を使用する設定

【入力形式】

username <ユーザ名> interface tunnel <インタフェース番号>

no username <ユーザ名> interface tunnel <インタフェース番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ユーザ名	ユーザ名を指定します。	128文字以内の STRING 型	省略不可
インタフェース番号	インタフェース番号を指定します。	1 ～ 16777215	

【動作モード】

CLIENT- データベース設定モード (IKEv1/IKEv2 で有効)

【説明】

拡張認証 (Xauth/EAP) による接続時に、ダイナミックセレクトを使用したユーザに対して、固定のインタフェース番号を使用したい場合のインタフェース番号を設定します。

【実行例】

固定のインタフェース番号を使用したい場合のインタフェース番号を設定します (ユーザ名: user-A、インタフェース番号: 200)。

```
#configure terminal
(config)#aaa local group local-A
(config-lg-user)#username user-A interface tunnel 200
```

【未設定時】

ユーザに対して動的にインタフェースを割り付けます。

17.6.4 username isakmp keepalive

【機能】

ユーザに対して個別に KeepAlive 機能として使用する Dead Peer Detection の各種パラメタを設定

【入力形式】

username <ユーザ名> isakmp keepalive [interval <送信間隔>] [always-send | no-send]

no username <ユーザ名> isakmp keepalive [interval <送信間隔>] [always-send | no-send]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ユーザ名	ユーザ名を指定します。	128文字以内の STRING 型	省略不可
送信間隔	DPD メッセージの送信間隔 (単位: 秒) を指定します。	10 ～ 3600	60
always-send no-send	DPD メッセージ送信を制御します。	always-send: 通信の状態によらず、定期的に DPD メッセージを送信 no-send: 一定期間通信がなかった場合に DPD メッセージを送信せず、即時にセッションを解放	一定期間通信がなかった場合に、DPD メッセージを送信

【動作モード】

CLIENT-データベース設定モード (IKEv1/IKEv2 で有効)

【説明】

拡張認証 (Xauth/EAP) による接続時に、ユーザに対して個別に KeepAlive 機能として使用する Dead Peer Detection (DPD) の各種パラメタを設定します。

【実行例】

ユーザに対して個別に KeepAlive 機能として使用する Dead Peer Detection (DPD) の各種パラメタを設定します (ユーザ名: user-A、送信間隔: 60 秒)。

```
#configure terminal
(config)#aaa local group local-A
(config-lg-user)#username user-A isakmp keepalive interval 60
```

【未設定時】

同様の関連コマンドとして 3 つ設定がありますが、以下の順で適用されます。

- username isakmp keepalive
- keepalive
- crypto isakmp keepalive

どの設定もない場合は、DPD の動作を行いませんが、DPD の ACK は返信します。

17.6.5 username isakmp negotiation retry

【機能】

ユーザに対して個別に ISAKMP ネゴシエーションの再送パラメタを設定

【入力形式】

username <ユーザ名> isakmp negotiation retry timer <再送間隔> limit <再送回数> timer-max <最大再送間隔> guard-time <再送ガード時間>

no username <ユーザ名> isakmp negotiation retry timer <再送間隔> limit <再送回数> timer-max <最大再送間隔> guard-time <再送ガード時間>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ユーザ名	ユーザ名を指定します。	128 文字以内の STRING 型	省略不可
再送間隔	ISAKMP ネゴシエーションパケットの再送間隔 (単位: 秒) を指定します。再送を行うごとに間隔は 2 倍に増加していきます。	1 ~ 60	
再送回数	ISAKMP ネゴシエーションパケットの再送回数を指定します。	0 ~ 5	

パラメタ	設定内容	設定範囲	省略時
最大再送間隔	ISAKMP ネゴシエーションパケットの最大再送間隔（単位：秒）を指定します。再送間隔がこの設定値以上となる場合は、再送間隔をそれ以上増やさず、設定された値の再送間隔で動作します。	1 ～ 60	省略不可
再送ガード時間	ISAKMP ネゴシエーションパケットを送信してから、再送ガード時間（単位：秒）内に受信したパケット（VPN ピアからの再送パケット）を破棄します。	0 ～ 60	

【動作モード】

CLIENT- データベース設定モード（IKEv2 でのみ有効）

【説明】

拡張認証 (Xauth/EAP) による接続時に、ユーザに対して個別に ISAKMP ネゴシエーションの再送パラメタを設定します。

IKE_AUTH 交換時以降から適用されます。

【実行例】

ユーザに対して個別に ISAKMP ネゴシエーションの再送パラメタを設定します（ユーザ名：user-A、再送間隔：10 秒、再送回数：5 回、最大再送間隔：30 秒、再送ガード時間：1 秒）。

```
#configure terminal
(config)#aaa local group local-A
(config-lg-user)#username user-A isakmp negotiation retry timer 10 limit 5 timer-max 30 guard-time 1
```

【未設定時】

同様の関連コマンドとして 3 つ設定がありますが以下の順で適用されます。

- username isakmp negotiation retry
- set negotiation retry
- crypto isakmp negotiation retry

どの設定もない場合は、以下の値で動作します。

再送間隔： 10 秒
 再送回数： 2 回
 最大再送間隔： 30 秒
 再送ガード時間： 0 秒

17.6.6 username isakmp negotiation expire-time

【機能】

ユーザに対して個別に ISAKMP ネゴシエーションのエキスパイア時間を設定

【入力形式】

username <ユーザ名> isakmp negotiation expire-time <エキスパイア時間>

no username <ユーザ名> isakmp negotiation expire-time <エキスパイア時間>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ユーザ名	ユーザ名を指定します。	128文字以内の STRING 型	省略不可
エクスパイア時間	ISAKMP ネゴシエーションのエクスパイア時間（単位：秒）を指定します。	30～600	省略不可

【動作モード】

CLIENT-データベース設定モード（IKEv2 でのみ有効）

【説明】

拡張認証(EAP)による接続時に、ユーザに対して個別に ISAKMP ネゴシエーションのエクスパイア時間（単位：秒）を設定します。

IKEv2 の responder において、IKE_SA_INIT から IKE_AUTH 完了までのリクエストパケットを受信（再送を除く）してから指定された時間内に、次のリクエストを受信しなかった場合、ネゴシエーションを終了します。

【実行例】

ユーザに対して個別に ISAKMP ネゴシエーションのエクスパイア時間（単位：秒）を設定します（ユーザ名：user-A、エクスパイア時間：120 秒）。

```
#configure terminal
(config)#aaa local group local-A
(config-lg-user)#username user-A isakmp negotiation expire-time 120
```

【未設定時】

同様の関連コマンドとして3つの設定がありますが以下の順で適用されます。

- username isakmp negotiation expire-time
- set negotiation expire-time
- crypto isakmp negotiation expire-time

どの設定もない場合は、エクスパイア時間は60秒で動作します。

17.7 拡張認証の各種設定

17.7.1 aaa authentication ike-client

【機能】

IPsec の拡張認証 (Xauth/EAP) の認証方式の設定

【入力形式】

aaa authentication ike-client <拡張認証方式名> <認証方式> <認証グループ名>

no aaa authentication ike-client <拡張認証方式名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
拡張認証方式名	拡張認証方式名を指定します。	63 文字以内の CDATA 型	省略不可
認証方式	認証方式を指定します。	group:RADIUS による認証 local-group: 装置内データベースによる認証	
認証グループ名	認証グループ名を指定します。	63 文字以内の CDATA 型	

【動作モード】

基本設定モード

【説明】

IPsec の拡張認証 (Xauth/EAP) の認証方式を設定します。本設定内容は ISAKMP プロファイル設定モードで参照されます。

本装置では拡張認証の認証方式として、装置内に設定したデータベースによる認証と、RADIUS による認証をサポートしています。

装置内データベースによる認証の場合の認証グループ名は、aaa local group コマンドで設定します。

RADIUS による認証の場合の認証グループ名は、aaa group server radius コマンドで設定します。

【実行例】

IPsec の拡張認証 (Xauth/EAP) の認証方式を設定します (拡張認証方式名: XAUTH-RADIUS、認証方式: RADIUS による認証、認証グループ名: radius-A)。

```
#configure terminal
(config)#aaa authentication ike-client XAUTH-RADIUS group radius-A
```

【未設定時】

IPsec の拡張認証を行いません。

17.7.2 client authentication list

【機能】

拡張認証方式名の設定

【入力形式】

client authentication list <拡張認証方式名> [skip]

no client authentication list

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
拡張認証方式名	拡張認証方式名を指定します。	63文字以内のCDATA型	省略不可
skip	skipを指定することで、IKEv1のISAKMP SAの再確立時にXAUTH認証を省略できます。	-	IKEv1のISAKMP SAの再確立時にXAUTH認証を行います。

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

拡張認証 (XAUTH/EAP) を行うための拡張認証方式名を設定します。拡張認証方式名は aaa authentication ike-client コマンドで設定した名称を指定します。IKEv1 の ISAKMP SA の再確立時に XAUTH 認証を行わない端末との接続を行う場合は "skip" を指定することで認証を省略できます。

【実行例】

拡張認証方式名を設定します (拡張認証方式名: radius-A)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(conf-isa-prof)#client authentication list radius-A
```

【未設定時】

拡張認証を行いません。

17.7.3 client authentication my-name

【機能】

拡張認証のクライアントとして動作する際のユーザIDとパスワードの設定

【入力形式】

client authentication my-name <ユーザID> password <パスワード> [{secret | private} [encrypted]]

no client authentication my-name [<ユーザID> password <パスワード> [{secret | private} encrypted]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ユーザ ID	IKEv1 で使用する Xauth のユーザ ID を指定します。IKEv2 の EAP で使用するユーザ ID は IKE ID を使用します。	128 文字以内の STRING 型	省略不可
パスワード	Xauth/EAP で使用するパスワードを指定します。	128 文字以内の STRING 型	
secret/private	パスワードとして使用する文字列の暗号化／復号化に、共通の鍵を使用するか、固有の鍵を使用するかを設定します。	secret: 共通の鍵を使用する private: 固有の鍵を使用する	暗号化せずに保存
encrypted	パスワードとして使用する文字列が暗号化されていることを示します。	-	非暗号化文字列として扱う

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

拡張認証のクライアントとして動作する際のユーザ ID とパスワードを設定します。

"secret" を指定した場合は、すべての GX500 に共通の鍵を使って暗号化／復号化し、"private" を指定した場合は、装置固有の鍵を使って暗号化／復号化します。

"encrypted" を指定した場合は、文字列を暗号化された文字列と判断しコンフィグに保存します。

"show running.cfg" などで内容を確認すると、暗号化されたパスワードの形式で表示されます。

【実行例】

拡張認証のクライアントとして動作する際のユーザ ID とパスワードを設定します (ユーザ ID : user-A、パスワード : admin123)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(conf-isa-prof)#client authentication my-name user-A password admin123
```

【未設定時】

拡張認証のクライアントとして動作しません。

17.7.4 client authentication type

【機能】

拡張認証を行う際の認証タイプの設定

【入力形式】

client authentication type {chap | eap-md5-to-chap | eap-md5 | eap-tls | eap-mschapv2}

no client authentication type {chap | eap-md5-to-chap | eap-md5 | eap-tls | eap-mschapv2}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
chap	chap 認証を指定します (IKEv1 のみ)。	-	省略不可
eap-md5-to-chap	EAP-MD5 認証を CHAP 認証に変換する場合に指定します (IKEv2 のみ)。	-	
eap-md5	EAP-MD5 認証を指定します (IKEv2 のみ)。	-	
eap-tls	EAP-TLS 認証を指定します (responder では IKEv2 の radius 認証時のみ)。	-	
eap-mschapv2	EAP-MSCHAPv2 認証を指定します (IKEv2 のみ)。	-	

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

拡張認証を行う際の認証タイプを設定します。

- chap: IKEv1 で CHAP 認証を行う場合に指定します。
- eap-md5-to-chap: IKEv2 で EAP 認証を行う際に RADIUS に対して CHAP 認証に対応した Access-Request を送信する場合に指定します。
- eap-md5: IKEv2 で EAP-MD5 認証を行う場合に指定します。
- eap-tls: IKEv2 で EAP-TLS 認証を行う場合に指定します。RADIUS による認証時のみ有効となります。
- eap-mschapv2: IKEv2 で EAP-MSCHAPv2 認証を行う場合に指定します。

【実行例】

拡張認証を行う際の認証タイプを設定します (eap-tls、eap-md5)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(conf-isa-prof)#client authentication type eap-tls eap-md5
```

【未設定時】

IKEv1 では PAP 認証で動作し、IKEv2 では EAP-MD5 認証で動作します。

17.7.5 client authentication eap-identity request

【機能】

VPN ピアに対する EAP ID の要求

【入力形式】

client authentication eap-identity request

no client authentication eap-identity request

【動作モード】

ISAKMP プロファイル設定モード (IKEv2 でのみ有効)

【説明】

IKEv2 において、EAP-MSCHAPv2 を使用して VPN ピアを認証する際に VPN ピアに EAP ID を要求します。通常は認証時にユーザ ID として IKE ID を使用しますが、この設定を行っている場合は VPN ピアから受信した EAP ID を使用します。

【実行例】

VPN ピアに EAP ID を要求します。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(config-isa-prof)#client authentication eap-identity request
```

【未設定時】

認証時にユーザ ID として IKE ID を使用します。

17.8 Mode-config/Config Payload の設定

17.8.1 crypto isakmp client configuration group

【機能】

ISAKMP グループポリシー設定モードへの移行

【入力形式】

crypto isakmp client configuration group <ISAKMP グループポリシー名>

no crypto isakmp client configuration group <ISAKMP グループポリシー名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ISAKMP グループポリシー名	ISAKMP グループポリシー名を指定します。	63 文字以内の CDATA 型	省略不可

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

許可方式 (アドレス割り当てなど) を設定するために、ISAKMP グループポリシー設定モードに移行します。コマンドの先頭に "no" を指定することで、該当 ISAKMP グループポリシー設定モードの内容がすべて消去されます。

ISAKMP グループポリシー設定モードの設定内容は、aaa authorization network コマンド設定で参照されます。

本設定モードを使用することで、本装置からの Mode-config/ConfigPayload による割り当てが可能です。

【実行例】

ISAKMP グループポリシー設定モードに移行します (ISAKMP グループポリシー名: group-A)。

```
#configure terminal
(config)#crypto isakmp client configuration group group-A
(config-isakmp-group)#
```

17.8.2 dns

【機能】

VPN ピアに通知する DNS サーバアドレスの設定

【入力形式】

dns <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>]

no dns

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プライマリ DNS サーバアドレス	VPN ピアに通知するプライマリ DNS サーバアドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
セカンダリ DNS サーバアドレス	VPN ピアに通知するセカンダリ DNS サーバアドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	セカンダリ DNS サーバアドレスを通知しない

【動作モード】

ISAKMP グループポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

Mode-config/Config Payload により VPN ピアに通知する DNS サーバアドレスを設定します。

【実行例】

VPN ピアに通知する DNS サーバアドレスを設定します (プライマリ DNS サーバアドレス : 192.0.2.1、セカンダリ DNS サーバアドレス : 192.0.2.2)。

```
#configure terminal
(config)#crypto isakmp client configuration group group-A
(config-isakmp-group)#dns 192.0.2.1 192.0.2.2
```

【未設定時】

DNS サーバアドレスを通知しません。

17.8.3 pool

【機能】

IP アドレス範囲のアドレスプール名の設定

【入力形式】

pool <アドレスプール名>

no pool

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アドレスプール名	アドレスプール名を指定します。	63 文字以内の CDATA 型	省略不可

【動作モード】

ISAKMP グループポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

Mode-config/Config Payload を利用して通知する IP アドレス範囲のアドレスプール名を設定します。IP アドレス範囲は ip(ipv6)local pool コマンドで登録し、ここではそのアドレスプール名を指定します。

【実行例】

アドレスプール名を設定します（アドレスプール名：pool-A）。

```
#configure terminal
(config)#crypto isakmp client configuration group group-A
(config-isakmp-group)#pool pool-A
```

【未設定時】

Mode-config/Config Payload により IP アドレスを通知できません。

17.8.4 aaa authorization network

【機能】

IPsec の許可方式の設定

【入力形式】

aaa authorization network <許可方式名> {local-group <ISAKMP グループポリシー名> | group <認証グループ名> [local-group <ISAKMP グループポリシー名>]}

no aaa authorization network <許可方式名> [{local-group <ISAKMP グループポリシー名> | group <認証グループ名> [local-group <ISAKMP グループポリシー名>]}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
許可方式名	許可方式名を指定します。	63 文字以内の CDATA 型	省略不可
ISAKMP グループポリシー名	ISAKMP グループポリシー名を指定します。	63 文字以内の CDATA 型	
認証グループ名	認証グループ名を指定します。	63 文字以内の CDATA 型	

【動作モード】

基本設定モード（IKEv1/IKEv2 で有効）

【説明】

IPsec の許可方式を設定します。本設定内容は ISAKMP プロファイル設定モードで参照されます。
 本装置は、許可方式として、装置内に設定したデータベースによる許可をサポートしています。
 ISAKMP グループポリシー名は、crypto isakmp client configuration group コマンドで設定します。
 認証グループ名は aaa group server radius コマンドで設定します。

【実行例】

IPsec の許可方式を設定します（許可方式名：AUTH-A、ISAKMP グループポリシー名：GROUP-A）。

```
#configure terminal
(config)#aaa authorization network AUTH-A local-group GROUP-A
```

【未設定時】

許可方式を参照しません。

17.8.5 client configuration address

【機能】

Mode-config/Config Payload のアドレス払い出し動作 (server 側) の設定

【入力形式】

client configuration address {initiate | respond} [{client-mode|skip}]

no client configuration address [{initiate | respond} [{client-mode|skip}]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
initiate respond	Mode-config/Config Payload の動作モードを指定します。	initiate:Set/Ack 方式 respond:Request/Reply 方式	省略不可
client-mode	アドレス払い出しを受ける動作 (client) を行う場合に指定します。	-	アドレス払い出し動作 (server) を行う
skip	skip を指定することで、IKEv1 の ISAKMP SA の再確立時に Mode-config を省略することができます。	-	IKEv1 の ISAKMP-SA の再確立時に Mode-config を行います。

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

Mode-config/Config Payload のアドレス払い出し動作 (server 側) を行います。

client の動作を行う場合は client-mode のオプションを指定します。

IKEv1 の ISAKMP SA の再確立時に Mode-config を行わない端末との接続を行う場合は skip を指定することで Mode-config を省略することができます。

Mode-config/Config Payload のネゴシエーションにおいて、Request/Reply 方式で動作するか Set/Ack 方式で動作するかを設定します。

IKEv1 については Set/Ack 方式と Request/Reply 方式の両方をサポートし、IKEv2 については Request/Reply 方式をサポートします。

1) Request/Response 方式

IKEv1/IKEv2 で有効です。アドレスを割り当てられる側が Mode-config/Config Payload の要求 (Request) を送信し、割り当てる側が応答 (Reply) を送信します。

Request/Reply 方式を使用する場合は、本コマンドで "respond" を指定します。

2) Set/Ack 方式

IKEv1 のみ有効です。アドレスを割り当てる側が Mode-config の通知 (Set) を送信し、割り当てられる側が承認 (Ack) を送信します。

Set/Ack 方式を使用する場合は、本コマンドで "initiate" を指定します。

Radius サーバ側で払い出しアドレスの指定を変更した場合、それを反映するには既存 ISAKMP-SA/IKE SA および IPSEC-SA/CHILD SA を削除する必要がありますのでご注意ください。

【実行例】

Config Payload のアドレス払い出し動作 (server 側) を行います (Request/Reply 方式)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(conf-isa-prof)#client configuration address respond
```

【未設定時】

Mode-config/Config Payload によるアドレス通知を行いません。

17.9 電子証明書の設定

17.9.1 ca trustpoint

【機能】

RSA signatures 認証時に使用する root CA 名の設定

【入力形式】

ca trustpoint <CA 名>

no ca trustpoint

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
CA 名	root CA 名を指定します。	16 文字以内の CDATA-X 型	省略不可

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

RSA signatures 認証時に使用する root CA 名を設定します。

【実行例】

RSA signatures 認証時に使用する root CA 名を設定します (root CA 名 : CA-A)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(config-isa-prof)#ca trustpoint CA-A
```

【未設定時】

root CA の指定なしで動作します。

17.9.2 pki revocation-check

【機能】

revocation-check 方法の設定

【入力形式】

pki revocation-check {crl | crl none | none}

no pki revocation-check

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
crl crl none none	revocation-check の方法を指定します。	crl:CRL を取得し、revocation check を行う crl none:CRL の取得に失敗時、revocation check は行わず証明書を有効とみなす none:revocation check は行わない	省略不可

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

revocation-check の方法を設定します。

【実行例】

revocation-check の方法を設定します (CRL の取得に失敗時、revocation check は行わず証明書を有効とみなします)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(config-isa-prof)#pki revocation-check crl none
```

【未設定時】

crl で動作します。

17.9.3 pki validity-check

【機能】

使用する証明書の有効期限のチェックを行わない場合に設定

【入力形式】

pki validity-check none

no pki validity-check

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

使用する証明書の有効期限のチェックを行わない場合に設定します。

【実行例】

使用する証明書の有効期限のチェックを行いません。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(config-isa-prof)#pki validity-check none
```

【未設定時】

使用する証明書の有効期限のチェックを行います。

17.9.4 crypto pki startup-import store file

【機能】

装置起動時にインポートする鍵ペア・電子証明書（独自フォーマットのファイル）の設定

【入力形式】

```
crypto pki startup-import store file <ファイル名> [force] [password <パスワード> [<private | secret>
[encrypted]]]
```

```
no crypto pki startup-import store file [<ファイル名> [force] [password <パスワード> [<private | secret>
[encrypted]]]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ファイル名	インポートするファイル名を指定します。	255 文字以内の FILE 型	省略不可
force	動作モード（force モード）を指定します。	-	デフォルトのインポートを行う
パスワード	パスワード文字列を指定します。	128 文字以内の CDATA 型 (暗号化されていない場合) 254 文字以内の CDATA 型 (暗号化されている場合)	パスワードなしで動作
private secret	パスワード文字列の暗号化／復号化に、共通の鍵を使用するか、固有の鍵を使用するか指定します。	-	暗号化せずに保存
encrypted	パスワード文字列を暗号化されたものとして扱う場合に指定します。	-	非暗号化文字列として扱う

【動作モード】

基本設定モード（IKEv1/IKEv2 で有効）

【説明】

装置起動時にインポートする鍵ペア・電子証明書（独自フォーマットのファイル）の設定を行います。

force オプションを付けた場合は、装置内に鍵ペア・電子証明書を上書きしてインポートを行います。

force オプションを付けない場合は、鍵ペア・電子証明書の上書きは行いません。

secret オプションを付けた場合は、他の CP モジュールに対して使用可能な鍵を使って暗号化／復号化し、private オプションを付けた場合は、CP モジュール固有の鍵を使って暗号化／復号化します。

encrypted オプションを付けた場合は、入力された文字列を暗号化された文字列と判断しコンフィグに保存します。

【実行例】

装置起動時にインポートする鍵ペア・電子証明書（独自フォーマットのファイル）の設定を行います（ファイル名：/usb1/configuration/pkicert.pki、force、パスワード：pkicert_passwd）。

```
#configure terminal
(config)#crypto pki startup-import store file /usb1/configuration/pkicert.pki force password
pkicert_passwd
```

【未設定時】

装置起動時に鍵ペア・電子証明書をインポートしません。

17.9.5 crypto pki startup-import pkcs12

【機能】

装置起動時にインポートする鍵ペア・電子証明書（PKCS12 フォーマットのファイル）の設定

【入力形式】

crypto pki startup-import pkcs12 <ファイル名> [force] label <鍵ペア名> cert-name <ユーザ証明書名>
ca-name <CA 証明書名> <1 | 2> password <パスワード> [<private | secret> [encrypted]]

no crypto pki startup-import pkcs12 [<ファイル名> [[force] label <鍵ペア名> cert-name <証明書名>
ca-name <CA 証明書名> <1 | 2> password <パスワード> [<private | secret> [encrypted]]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ファイル名	インポートするファイル名を指定します。	255文字以内の filename 型	省略不可
force	動作モード（force モード）を指定します。	-	デフォルトのインポートを行う
鍵ペア名	鍵ペアの名称を指定します。	16文字以内の CDATA-X 型	省略不可
ユーザ証明書名	ユーザ証明書の名称を指定します。	16文字以内の CDATA-X 型	
CA 証明書名	CA 証明書の名称を指定します。	16文字以内の CDATA-X 型	
1 2	CA 証明書の index を指定します。	-	
パスワード	パスワード文字列を指定します。	128文字以内の CDATA 型 (暗号化されていない場合) 254文字以内の CDATA 型 (暗号化されている場合)	暗号化せずに保存
private secret	パスワード文字列の暗号化／復号化に、共通の鍵を使用するか、固有の鍵を使用するか指定します。	-	
encrypted	パスワード文字列を暗号化されたものとして扱う場合に指定します。	-	

【動作モード】

基本設定モード（IKEv1/IKEv2 で有効）

【説明】

装置起動時にインポートする鍵ペア・電子証明書（PKCS12 フォーマットのファイル）の設定を行います。

force オプションを付けた場合は、装置内に鍵ペア・電子証明書を上書きしてインポートを行います。

force オプションを付けない場合は、鍵ペア・電子証明書の上書きは行いません。

secret オプションを付けた場合は、他の CP モジュールに対して使用可能な鍵を使って暗号化／復号化し、private オプションを付けた場合は、CP モジュール固有の鍵を使って暗号化／復号化します。

encrypted オプションを付けた場合は、入力された文字列を暗号化された文字列と判断しコンフィグに保存します。

【実行例】

装置起動時にインポートする鍵ペア・電子証明書（PKCS12 フォーマットのファイル）の設定を行います（ファイル名：/usb1/configuration/pkicert.p12、force、鍵ペア名：PKI_KEY、ユーザ証明書名：PKI_CERT、CA 証明書名：PKI_CA、1、パスワード：pkicert_passwd）。

```
#configure terminal
(config)#crypto pki startup-import pkcs12 /usb1/configuration/pkicert.p12 force label PKI_KEY cert-name PKI_CERT ca-name PKI_CA 1 password pkicert_passwd
```

【未設定時】

装置起動時に鍵ペア・電子証明書をインポートしません。

17.9.6 crypto pki startup-import delete other-certificate

【機能】

装置起動時に鍵ペア・電子証明書を削除する設定

【入力形式】

crypto pki startup-import delete other-certificate

no crypto pki startup-import delete other-certificate

【動作モード】

基本設定モード（IKEv1/IKEv2 で有効）

【説明】

装置起動時に鍵ペア・電子証明書を削除する場合に設定します。

【実行例】

装置起動時に鍵ペア・電子証明書を削除します。

```
#configure terminal
(config)#crypto pki startup-import delete other-certificate
```

【未設定時】

装置起動時に鍵ペア・電子証明書を削除しません。

17.10 DPD の設定

VPN ピアの生存を確認するために、KeepAlive(DPD:Dead Peer Detection)をサポートしています。

17.10.1 crypto isakmp keepalive

【機能】

KeepAlive 機能として使用する Dead Peer Detection の各種パラメタの設定

【入力形式】

crypto isakmp keepalive [interval <送信間隔>] [always-send | no-send]

no crypto isakmp keepalive

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
送信間隔	DPD メッセージの送信間隔 (単位: 秒) を指定します。	10 ~ 3600	60
always-send no-send	DPD メッセージ送信を制御します。	always-send: 通信の状態によらず、定期的に DPD メッセージを送信 no-send: 一定期間通信がなかった場合に DPD メッセージを送信せず、即時にセッションを解放	一定期間通信がなかった場合に、DPD メッセージを送信

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

KeepAlive 機能として使用する Dead Peer Detection(DPD)の各種パラメタを設定します。VPN ピアごとに、異なる KeepAlive のタイマ値で運用する場合は、ISAKMP プロファイル設定モードの keepalive コマンドで設定を行います。また、再送パラメタは crypto isakmp negotiation retry コマンドにより、ISAKMP パケット全体の再送パラメタとして設定可能です。

設定は次の IKE SA 確立時から有効となります。

【実行例】

KeepAlive 機能として使用する Dead Peer Detection(DPD)の各種パラメタを設定します (送信間隔: 60 秒、一定期間通信がなかった場合に DPD メッセージを送信)。

```
#configure terminal
(config)#crypto isakmp keepalive
```

【未設定時】

同様の関連コマンドとして 3 つ設定がありますが、以下の順で適用されます。

- username isakmp keepalive
- keepalive
- crypto isakmp keepalive

どの設定もない場合は、DPD の動作を行いませんが、DPD の ACK は返信します。

17.10.2 crypto isakmp keepalive-icmp

【機能】

ICMP による KeepAlive 機能として使用する ICMP Echo メッセージの各種パラメタの設定

【入力形式】

crypto isakmp keepalive-icmp [interval <送信間隔>] [retry <再送間隔>]

[retransmit <再送回数>] [always-send]

no crypto isakmp keepalive-icmp

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
送信間隔	ICMP Echo パケットの送信間隔（単位：秒）を指定します。	10～3600	60
再送間隔	ICMP Echo パケットに応答がなかった場合の再送間隔（単位：秒）を指定します。	2～60	20
再送回数	ICMP Echo パケットの再送回数を指定します。	1～5	1
always-send	通信の状態によらず、定期的に ICMP Echo パケットを送信する場合に指定します。	-	一定期間通信がなかった場合に、ICMP Echo パケットを送信

【動作モード】

基本設定モード（IKEv1/IKEv2 で有効）

【説明】

ICMP による KeepAlive 機能として使用する ICMP Echo メッセージの各種パラメタを設定します。

ISAKMP プロファイル設定モードに keepalive-icmp コマンド設定がある場合はそちらの設定を優先します。

【実行例】

ICMP による KeepAlive 機能として使用する ICMP Echo メッセージの各種パラメタを設定します（送信間隔：10 秒、再送間隔：2 秒、再送回数：3 回）。

```
#configure terminal
(config)#crypto isakmp keepalive-icmp interval 10 retry 2 retransmit 3
```

【未設定時】

ISAKMP プロファイル設定モードに keepalive-icmp コマンド設定もない場合は、ICMP による KeepAlive の動作を行いません。

17.10.3 keepalive

【機能】

KeepAlive 機能として使用する Dead Peer Detection の各種パラメタの設定

【入力形式】

keepalive [interval <送信間隔>] [always-send | no-send]

no keepalive

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
送信間隔	DPD メッセージの送信間隔 (単位：秒) を指定します。	10 ～ 3600	60
always-send no-send	DPD メッセージ送信を制御します。	always-send: 通信の状態によらず、 定期的に DPD メッセージを送信 no-send: 一定期間通信がなかった場 合に DPD メッセージを送信せず、 即時にセッションを解放	一定期間通信がなかった 場合に、DPD メッセージを送信

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

KeepAlive 機能として使用する Dead Peer Detection(DPD)の各種パラメタを設定します。再送パラメタは crypto isakmp negotiation retry コマンドにより、ISAKMP パケット全体の再送パラメタとして設定可能です。

DPD メッセージがタイムアウトした場合、対象となる SA を解放します。

【実行例】

KeepAlive 機能として使用する Dead Peer Detection(DPD)の各種パラメタを設定します (送信間隔：60 秒、一定期間通信がなかった場合に DPD メッセージを送信)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(config-isa-prof)#keepalive
```

【未設定時】

同様の関連コマンドとして 3 つ設定がありますが、以下の順で適用されます。

- username isakmp keepalive
- keepalive
- crypto isakmp keepalive

どの設定もない場合は、DPD の動作を行いませんが、DPD の ACK は返信します。

17.10.4 keepalive-icmp

【機能】

ICMP による KeepAlive 機能として使用する ICMP Echo メッセージの各種パラメタの設定

【入力形式】

keepalive-icmp [interval <送信間隔>] [retry <再送間隔>] [retransmit <再送回数>] [always-send]

no keepalive-icmp

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
送信間隔	ICMP Echo パケットの送信間隔（単位：秒）を指定します。	10～3600	60
再送間隔	ICMP Echo パケットに応答がなかった場合の再送間隔（単位：秒）を指定します。	2～60	20
再送回数	ICMP Echo パケットの再送回数を指定します。	1～5	1
always-send	通信の状態によらず、定期的に ICMP Echo パケットを送信する場合に指定します。	-	一定期間通信がなかった場合に、ICMP Echo パケットを送信

【動作モード】

ISAKMP プロファイル設定モード（IKEv1/IKEv2 で有効）

【説明】

ICMP による KeepAlive 機能として使用する ICMP Echo メッセージの各種パラメタを設定します。

【実行例】

ICMP による KeepAlive 機能として使用する ICMP Echo メッセージの各種パラメタを設定します（送信間隔：10 秒、再送間隔：2 秒、再送回数：3 回）。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(conf-isa-prof)#keepalive-icmp interval 10 retry 2 retransmit 3
```

【未設定時】

crypto isakmp keepalive-icmp コマンドの設定に従います。

17.10.5 local-address-icmp

【機能】

ICMP Echo パケットを送信する際の送信元アドレスの設定

【入力形式】

local-address-icmp <送信元アドレス>

no local-address-icmp

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
送信元アドレス	ICMP Echo パケットを利用した KeepAlive 機能で、ICMP Echo パケットを送信する際の送信元アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

ICMP Echo パケットを利用した KeepAlive 機能で、ICMP Echo パケットを送信する際の送信元アドレスを設定します。

【実行例】

ICMP Echo パケットを送信する際の送信元アドレスを設定します (送信元アドレス: 192.0.2.1)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(config-isa-prof)#local-address-icmp 192.0.2.1
```

【未設定時】

SA を確立した際の送信元 IP アドレスを使用します。

17.10.6 remote-address-icmp

【機能】

ICMP Echo パケットを送信する際の宛先アドレスの設定

【入力形式】

remote-address-icmp <宛先アドレス>

no remote-address-icmp

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
宛先アドレス	ICMP Echo パケットを利用した KeepAlive 機能で、ICMP Echo パケットを送信する際の宛先アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

ICMP Echo パケットを利用した KeepAlive 機能で、ICMP Echo パケットを送信する際の宛先アドレスを設定します。

【実行例】

ICMP Echo パケットを送信する際の宛先アドレスを設定します（宛先アドレス：192.0.2.1）。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(config-isa-prof)#remote-address-icmp 192.0.2.1
```

【未設定時】

SA を確立した VPN ピアの IP アドレスを使用します。

17.10.7 vrf-icmp

【機能】

ICMP Echo パケットを送信する際にマッピングする VRF 名称の設定

【入力形式】

vrf-icmp <VRF 名>

no vrf-icmp

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VRF 名	ICMP Echo パケットを利用した KeepAlive 機能で、ICMP Echo パケットを送信する際にマッピングする VRF の名称を指定します。	63 文字以内の WORD 型	省略不可

【動作モード】

ISAKMP プロファイル設定モード（IKEv1/IKEv2 で有効）

【説明】

ICMP Echo パケットを利用した KeepAlive 機能で、ICMP Echo パケットを送信する際にマッピングする VRF の名称を設定します。VRF 名は ip vrf コマンドで設定します。

【実行例】

ICMP Echo パケットを送信する際にマッピングする VRF の名称を設定します（VRF 名：vrf-A）。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(config-isa-prof)#vrf-icmp vrf-A
```

【未設定時】

VRF のマッピングを行いません。

17.11 ESP の設定

17.11.1 crypto ipsec selector-check

【機能】

すべての SA でセレクトチェック機能を有効にする設定

【入力形式】

crypto ipsec selector-check

no crypto ipsec selector-check

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

すべての SA でセレクトチェック機能を有効にする場合に設定します。セレクトチェック機能とは、復号化後の送信元アドレス、または宛先アドレスが SA のセレクト情報と一致しない場合に、パケットを廃棄する機能です。

crypto ipsec policy 単位に設定がある場合は、そちらの設定を優先します。refresh 後に新たに確立した SA に対して有効となります。既存の SA に対しては次の rekey 後に有効となります。

セレクトチェックは show crypto ipsec sa で表示されるセレクトの上から 4 つ目までしかチェックを行いません。5 つ目以降のセレクトに一致するパケットを受信しても廃棄されます。セレクトが 5 つ以上になる場合は本機能を無効にしてください。

【実行例】

すべての SA でセレクトチェック機能を有効にします。

```
#configure terminal
(config)#crypto ipsec selector-check
```

【未設定時】

装置全体としてのセレクトチェック機能は無効となります。ただし、IPSEC ポリシー設定モードに設定がある場合は、そちらの設定を優先します。

17.11.2 set selector-check

【機能】

SA でセレクトチェック機能を有効にする設定

【入力形式】

set selector-check {enable | disable}

no set selector-check

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
enable disable	セレクトチェック機能の有効／有効を指定します。	-	省略不可

【動作モード】

IPSEC ポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

SA でセレクトチェック機能を有効にする場合に設定します。セレクトチェック機能とは、復号化後の送信元アドレス、または宛先アドレスが SA のセレクト情報と一致しない場合に、パケットを廃棄する機能です。

refresh 後に新たに確立した SA に対して有効となります。既存の SA に対しては次回の rekey 後に有効となります。

セレクトチェックは show crypto ipsec sa で表示されるセレクトの上から 4 つ目までしかチェックを行いません。5 つ目以降のセレクトに一致するパケットを受信しても廃棄されます。セレクトが 5 つ以上になる場合は本機能を無効にしてください。

【実行例】

SA でセレクトチェック機能を有効にします。

```
#configure terminal
(config)#crypto ipsec policy policy-A
(config-ipsec)#set selector-check enable
```

【未設定時】

基本設定モードに crypto ipsec selector-check コマンドの設定がある場合は、その設定に従います。設定がない場合はセレクトチェック機能は無効となります。

17.11.3 crypto ipsec replay-check disable

【機能】

すべての SA でリプレイ攻撃防御機能を無効にする設定

【入力形式】

crypto ipsec replay-check disable

no crypto ipsec replay-check

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

すべての SA でリプレイ攻撃防御機能を無効にする場合に設定します。リプレイ攻撃防御機能とは、受信したパケットのシーケンス番号の最大値を保存し、その値と同一、またはその値より小さなシーケンス番号を受信した場合に、パケットを廃棄する機能です。

crypto ipsec policy 単位に設定がある場合は、そちらの設定を優先します。refresh後に新たに確立したSAに対して有効となります。既存のSAに対しては次回のrekey後に有効となります。

本装置では、ウィンドウサイズは512パケット分であるため、受信済みパケットのシーケンス番号の最大値から511引いたシーケンス番号までは受信可能となります。ただし、ウィンドウサイズ分に関わらず、一度受信したシーケンス番号のパケットについてはリプレイチェックエラーとなります。

【実行例】

すべてのSAでリプレイ攻撃防御機能を無効にします。

```
#configure terminal
(config)#crypto ipsec replay-check disable
```

【未設定時】

装置全体としてリプレイ攻撃防御機能は有効となります。ただし、IPSEC ポリシー設定モードに設定がある場合は、そちらの設定を優先します。また、認証アルゴリズムが設定されていない場合は、リプレイ攻撃防御機能は有効となりません。

17.11.4 set replay-check

【機能】

SAでリプレイ攻撃防御機能を無効にする設定

【入力形式】

set replay-check {enable | disable}

no set replay-check

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
enable disable	リプレイ攻撃防御機能の無効／有効を指定します。	-	省略不可

【動作モード】

IPSEC ポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

SAでリプレイ攻撃防御機能を無効にする場合に設定します。リプレイ攻撃防御機能とは、受信したパケットのシーケンス番号の最大値を保存し、その値と同一、またはその値より小さなシーケンス番号を受信した場合に、パケットを廃棄する機能です。refresh後に新たに確立したSAに対して有効となります。既存のSAに対しては次回のrekey後に有効となります。

本装置では、ウィンドウサイズは512パケット分であるため、受信済みパケットのシーケンス番号の最大値から511引いたシーケンス番号までは受信可能となります。ただし、ウィンドウサイズ分に関わらず、一度受信したシーケンス番号のパケットについてはリプレイチェックエラーとなります。

【実行例】

SA でリプレイ攻撃防御機能を無効にします。

```
#configure terminal
(config)#crypto ipsec policy policy-A
(conf-ipsec)#set replay-check disable
```

【未設定時】

基本設定モードに crypto ipsec replay-check コマンドの設定がある場合は、その設定に従います。設定がない場合は、リプレイ攻撃防御機能は有効となります。認証アルゴリズムが設定されていない場合は、リプレイ攻撃防御機能は有効となりません。

17.11.5 crypto ipsec sequence-overflow disable

【機能】

すべての SA でシーケンス番号監視機能を無効にする設定

【入力形式】

crypto ipsec sequence-overflow disable

no crypto ipsec sequence-overflow

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

すべての SA でシーケンス番号監視機能を無効にする場合に設定します。シーケンス番号監視機能とは、シーケンス番号が 0xffffffff を超えて送信することになった場合に、既存の SA を削除する機能です。本コマンドを設定することで、シーケンス番号が 0xffffffff を超えて送信することになった場合でも、SA を削除せずに 0x0 に戻します。

crypto ipsec policy 単位に設定がある場合は、そちらの設定を優先します。refresh 後に新たに確立した SA に対して有効となります。既存の SA に対しては次の rekey 後に有効となります。

【実行例】

すべての SA でシーケンス番号監視機能を無効にします。

```
#configure terminal
(config)#crypto ipsec sequence-overflow disable
```

【未設定時】

装置全体としてシーケンス番号監視機能は有効となります。ただし、IPSEC ポリシー設定モードに設定がある場合は、そちらの設定を優先します。

17.11.6 set sequence-overflow

【機能】

SA でシーケンス番号監視機能を無効にする設定

【入力形式】

```
set sequence-overflow {enable | disable}
```

```
no set sequence-overflow
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
enable disable	シーケンス番号監視機能の無効／有効を指定します。	-	省略不可

【動作モード】

IPSEC ポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

SA でシーケンス番号監視機能を無効にする場合に設定します。シーケンス番号監視機能とは、シーケンス番号が 0xffffffff を超えて送信することになった場合に、既存の SA を削除する機能です。本コマンドを設定することで、シーケンス番号が 0xffffffff を超えて送信することになった場合でも、SA を削除せずに 0x0 に戻します。

refresh 後に新たに確立した SA に対して有効となります。既存の SA に対しては次回の rekey 後に有効となります。

ESN(Extended Sequence Numbers) 機能を有効にした場合は、本コマンドで "enable" を指定してもシーケンス番号監視機能は無効になります。

【実行例】

SA でシーケンス番号監視機能を無効にします。

```
#configure terminal
(config)#crypto ipsec policy policy-A
(conf-ipsec)#set sequence-overflow disable
```

【未設定時】

基本設定モードに crypto ipsec sequence-overflow コマンドの設定がある場合は、その設定に従います。設定がない場合は、シーケンス番号監視機能は有効 (Overflow 検出時に SA を削除) となります。

17.11.7 set mtu

【機能】

IPSEC-SA/CHILD SA の Outer (ESP パケット) の MTU 長の設定

【入力形式】

```
set mtu <MTU 長>
```

```
no set mtu
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
MTU 長	MTU 長 (単位 : bytes) を指定します。	1280 ~ 9100	省略不可

【動作モード】

IPSEC ポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

IPSEC-SA/CHILD SA の Outer (ESP パケット) の MTU 長 (単位 : bytes) を設定します。

本設定で指定した MTU 長でフラグメントされたあとのサイズが、送信する port-channel インタフェースの MTU 長より大きい場合は、再度フラグメントして送信されます。

MTU に従いパケットを分割する場合、基本的に均等な長さにパケットを分割します。しかし、コントロールプレーンから送信する、またはコントロールプレーンを經由して中継する際に分割するケースでは、MTU 長に合わせたパケットの分割を実施します。

【実行例】

IPSEC-SA/CHILD SA の Outer (ESP パケット) の MTU 長 (単位 : bytes) を設定します (MTU 長 : 1280bytes)。

```
#configure terminal
(config)#crypto ipsec policy policy-A
(conf-ipsec)#set mtu 1280
```

【未設定時】

Outer の MTU 長は 1500bytes で動作します。

17.11.8 set ip tos

【機能】

Outer (ESP パケット) の TOS フィールド値、およびトラフィッククラス値の設定

【入力形式】

```
set ip tos {<TOS フィールド値> | copy}
```

```
no set ip tos
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
TOS フィールド値	IPsec トンネルとして IPv4 トンネルを利用する場合は、Outer (ESP パケット) の IPv4 ヘッダの TOS フィールド値を指定します。 IPsec トンネルとして IPv6 トンネルを利用する場合は、Outer (ESP パケット) の IPv6 ヘッダのトラフィッククラス値を指定します。	1 ~ 255	省略不可
copy	Inner の IPv4 ヘッダの TOS フィールド値、および Inner の IPv6 ヘッダのトラフィッククラス値をそのまま Outer で使用する場合に指定します。	-	

【動作モード】

IPSEC ポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

IPsec トンネルとして IPv4 トンネルを利用する場合は、Outer (ESP パケット) の IPv4 ヘッダの TOS フィールド値を指定します。IPsec トンネルとして IPv6 トンネルを利用する場合は、Outer (ESP パケット) の IPv6 ヘッダのトラフィッククラス値を設定します。Inner の TOS フィールド値、およびトラフィッククラス値をそのまま Outer で使用する場合は、"copy" を設定します。

【実行例】

Outer の TOS フィールド値、およびトラフィッククラス値を設定します (copy)。

```
#configure terminal
(config)#crypto ipsec policy policy-A
(conf-ipsec)#set ip tos copy
```

【未設定時】

Outer の TOS フィールド値、およびトラフィッククラス値は 0 で動作します。

17.11.9 set ip df-bit

【機能】

IPsec トンネルとして IPv4 トンネルを利用する Outer の IPv4 ヘッダの DF ビット値の設定

【入力形式】

set ip df-bit {<DF ビット値> | copy}

no set ip df-bit

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
DF ビット値	IPsec トンネルとして、IPv4 トンネルを利用する場合は、Outer (ESP パケット) の IPv4 ヘッダの DF ビット値 (Don't Fragment ビット) を指定します。	0 1	省略不可
copy	Inner の DF ビット値を使用する場合に指定します。	-	

【動作モード】

IPSEC ポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

IPsec トンネルとして IPv4 トンネルを利用する場合は、Outer (ESP パケット) の IPv4 ヘッダの DF ビット値 (Don't Fragment ビット) を設定します。Inner が IPv4 の場合に、Inner の DF ビット値をそのまま Outer の DF ビット値として使用する場合は、"copy" を指定します。

暗号化対象パケットの DF ビットが ON の場合でも、set ip df-bit 0 コマンドを設定することにより、暗号化後の ESP パケットをフラグメントし中継できます (set ip fragment post コマンドの設定が必要)。この設定を行わない場合、DF ビットが ON のパケットのデータを暗号化した ESP パケットを中継できない可能性があります。このような場合に本装置は、データを送信したホストに対して Need Fragment のエラーを返信します。Need Fragment に付与する MTU 値は、set mtu コマンドで指定した値から暗号化した際のオーバーヘッド分を差し引いた値となります。

【実行例】

IPsec トンネルとして IPv4 トンネルを利用する場合は、Outer (ESP パケット) の IPv4 ヘッダの DF ビット値 (Don't Fragment ビット) を設定します (0)。

```
#configure terminal
(config)#crypto ipsec policy policy-A
(conf-ipsec)#set ip df-bit 0
```

【未設定時】

"copy" で動作します。

17.11.10 set ip fragment

【機能】

Post-Fragment を行う設定

【入力形式】

set ip fragment post

no set ip fragment

【動作モード】

IPSEC ポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

Post-Fragment を行う場合に指定します。

本装置では、フラグメントが必要なパケットの暗号化の際に、2 種類の方式をサポートしています。

1. Pre-Fragment

受信した平文の暗号化をする際にフラグメントが必要と判断した場合、平文をフラグメントしてからそれぞれを暗号化する方式です。

受信側では、個々のフラグメントされたパケットを復号化できるため、すべてのパケットを待つことなく中継できるメリットがあります。ただし、暗号化対象の平文データの DF ビットが ON になっている場合は、中継できない可能性があります。

2. Post-Fragment

受信した平文の暗号化をする際にフラグメントが必要だと判断した場合、平文を暗号化してから、暗号化後の ESP パケットをフラグメントする方式です。

受信側では、フラグメントされたデータすべてが揃うまで復号化できないため、受信データを格納しておく必要があります。ただし、暗号化対象の平文データの DF ビットが ON になっている場合でも、フラグメントするのは ESP パケットなので、中継できます。

本装置は、通常 Pre-Fragment 方式で暗号化パケットのフラグメントを行いますが、本コマンドを設定することにより、設定している IPSEC ポリシーを使用する暗号化の場合は、Post-Fragment 方式を使用します。Post-Fragment の動作は set ip df-bit 0 としている場合のみ有効です。

【実行例】

Post-Fragmentを行います。

```
#configure terminal
(config)#crypto ipsec policy policy-A
(conf-ipsec)#set ip fragment post
```

【未設定時】

Pre-Fragment方式で動作します。

17.11.11 crypto ipsec esn

【機能】

すべてのSAでESN機能を有効にする設定

【入力形式】

crypto ipsec esn enable

no crypto ipsec esn

【動作モード】

基本設定モード (IKEv1/IKEv2で有効)

【説明】

すべてのSAでESN(Extended Sequence Numbers)機能を有効にする場合に設定します。

なお、ESN機能を有効にした場合、sequence-overflow設定に関係なく、シーケンス番号監視機能は無効になります。

【実行例】

すべてのSAでESN機能を有効にします。

```
#configure terminal
(config)#crypto ipsec esn enable
```

【未設定時】

同様の関連コマンドとして2つ設定がありますが以下の順で適用されます。

- set esn
- crypto ipsec esn

どの設定もない場合は、ESN機能を使用しません。

17.11.12 crypto ipsec udp-encapsulation

【機能】

ESPパケットのUDPカプセル化を行う装置全体のデフォルトの方式の設定

【入力形式】

crypto ipsec udp-encapsulation <UDPカプセル化方式> [keepalive interval <送信間隔> [always-send]]


```
no crypto ipsec udp-encapsulation [<UDP カプセル化方式> [keepalive interval <送信間隔> [always-
send]]]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
UDP カプセル化方式	UDP カプセル化を行う方式を指定します。	nat-t : NAT-Traversalを使用します。 spoofed : NAT-Traversalを使用し、常にUDP カプセル化します。	省略不可
送信間隔	NAT-Keepalive メッセージの送信間隔（単位：秒）を指定します。	10～3600	NAT-Keepalive メッセージを送信しない
always-send	通信の状態によらず、定期的に NAT-Keepalive メッセージを送信する場合に指定します。	-	一定期間通信がなかった場合に、NAT-Keepalive メッセージを送信

【動作モード】

基本設定モード（IKEv1/IKEv2 で有効）

【説明】

ESP パケットの UDP カプセル化を行う装置全体のデフォルトの方式を設定します。NAT-Traversal 機能を使用して動的に UDP カプセル化を行う場合は "nat-t" を指定し、NAT-Traversal 機能を使用して NAT の有無に関係なく常に UDP カプセル化を行う場合は "spoofed" を指定します。NAT-Traversal は RFC、および draft に準拠しており、RFC 準拠モードの方を優先させて動作します（RFC3947,3948、および draft-ietf-ipsec-nat-t-ike-00.txt,draft-ietf-ipsec-udp-encaps-00.txt,draft-ietf-ipsec-nat-t-ike-03.txt,draft-ietf-ipsec-udp-encaps-03.txt に対応しています）。

また、自装置が NAT の後ろに存在する場合に NAT-Keepalive パケットを送信する場合は、"keepalive" を指定します。IKEv2 で "spoofed" を NAT が存在しない環境で使用する場合、responder 側には crypto ipsec responder udp-encapsulation spoofed の設定も必要です。

【実行例】

NAT-Traversal 機能を有効にします（UDP カプセル化方式：nat-t）。

```
#configure terminal
(config)#crypto ipsec udp-encapsulation nat-t
```

【未設定時】

同様の関連コマンドとして 2 つ設定がありますが以下の順で適用されます。

- set udp-encapsulation
- crypto ipsec udp-encapsulation

どの設定もない場合は、NAT-Traversal 機能、および UDP カプセル化を行いません。

17.11.13 crypto ipsec responder udp-encapsulation spoofed

【機能】

NAT 装置が存在しない環境で ESP の UDP カプセル化を行う設定

【入力形式】

crypto ipsec responder udp-encapsulation spoofed

no crypto ipsec responder udp-encapsulation spoofed

【動作モード】

基本設定モード (IKEv2 でのみ有効)

【説明】

Initial-Exchange 時に Responder として動作する場合、Initiator が NAT_DETECTION の通知を付与した場合であり、かつ、NAT 装置が存在しない環境においても ESP を UDP カプセル化したい場合に設定します。この設定を行った場合、IKE_SA_INIT のレスポンス送信時に NAT_DETECTION_DESTINATION_IP を書き換えることで Initiator が NAT 装置の後ろに存在するように動作し、自装置も Initiator が NAT 装置の後ろに存在するよう認識して動作します。

【実行例】

NAT 装置が存在しない環境で ESP の UDP カプセル化を行います。

```
#configure terminal
(config)#crypto ipsec responder udp-encapsulation spoofed
```

【未設定時】

Responder は Initiator が NAT-Traversal に対応している場合、NAT 装置の有無を判断し、必要に応じて ESP の UDP カプセル化を行います。

17.12 SA アップルートの設定

IPSEC-SA/CHILD SA の確立時に、セレクトアの宛先に指定された情報や拡張認証時に Radius サーバからの Access-Accept に格納された Attribute 情報を、経路情報として登録できます。この経路情報を SA アップルートとします。SA アップルートを利用することにより、IPSEC-SA/CHILD SA が確立している場合の相手の情報を、ダイナミックルーティングで配布することができるようになります。

なお SA アップルートでは、内部的に "local-prot1"、"local-prot2" という 2 種類のプロトコル名で管理できます。ダイナミックルーティングプロトコルにより、"local-prot1"、"local-prot2" の重み付けを変えて配布できます。

17.12.1 sa-up route

【機能】

生成された SA のセレクトアの宛先情報を経路情報として登録する設定

【入力形式】

sa-up route [local-prot1 | local-prot2] [distance <ディスタンス値>] [metric <メトリック値>]

no sa-up route [local-prot1 | local-prot2] [distance <ディスタンス値>] [metric <メトリック値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
local-prot1 local-prot2	セレクトア情報の SA アップルートを管理するプロトコル名を指定します。	-	local-prot1
ディスタンス値	SA アップルート登録時のディスタンス値を指定します。	1 ～ 255	1
メトリック値	SA アップルート登録時のメトリック値を指定します。	0 ～ 4294967295	0

【動作モード】

IPSEC ポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

生成された SA のセレクトアの宛先情報を、経路情報 (SA アップルート) として登録する場合に設定します。

local-prot1 または local-prot2 のどちらかのプロトコル名で登録し、ダイナミックルーティングで配布する際は、各ルーティングプロトコル設定の redistribute コマンドで、"local-prot1" または "local-prot2" を指定します。配布する際のディスタンス値やメトリック値も設定可能です。

【実行例】

生成された SA のセレクトアの宛先情報を、経路情報 (SA アップルート) として登録します (local-prot2)。

```
#configure terminal
(config)#crypto ipsec policy policy-A
(config-ipsec)#sa-up route local-prot2
```

【未設定時】

SA アップルートを登録しません。

17.12.2 sa-up route-dvpn

【機能】

動的VPNクライアント機能で相手から通知されたネットワークを経路情報として登録する設定

【入力形式】

```
sa-up route-dvpn [{local-prot1 | local-prot2}] [{distance <ディスタンス値> [metric <メトリック値>] |
metric <メトリック値> [distance <ディスタンス値>]]
```

```
no sa-up route-sip-radius [{local-prot1 | local-prot2}] [{distance <ディスタンス値> [metric <メトリック
値>] | metric <メトリック値> [distance <ディスタンス値>]]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
local-prot1 local-prot2	SA アップルートを管理するプロトコル名を指定します。	-	local-prot1
ディスタンス値	SA アップルート登録時のディスタンス値を指定します。	1 ～ 255	1
メトリック値	SA アップルート登録時のメトリック値を指定します。	0 ～ 4294967295	0

【動作モード】

IPSEC ポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

動的VPNクライアント機能で、相手から通知されたネットワークを経路情報として登録する場合に設定します。

local-prot1、local-prot2のどちらかのプロトコル名で登録し、ダイナミックルーティングで配布する際は、各ルーティングプロトコル設定のredistribute コマンドで、"localprot1"または"local-prot2"を指定します。配布する際のディスタンス値やメトリック値も設定可能です。

【実行例】

動的VPNクライアント機能で、相手から通知されたネットワークを経路情報として登録します。

```
(config)# crypto ipsec policy policy-A
(conf-dvpn-client)# sa-up route-dvpn
```

【未設定時】

相手から通知されたネットワークを経路情報として登録しません。

17.12.3 sa-up route-radius

【機能】

Radius サーバからの Access-Accept に格納された Attribute 情報を経路情報として登録する設定

【入力形式】

sa-up route-radius [{local-prot1 | local-prot2}] [distance <ディスタンス値>] [metric <メトリック値>]

no sa-up route-radius [{local-prot1 | local-prot2}] [distance <ディスタンス値>] [metric <メトリック値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
local-prot1 local-prot2	SA アップルートを管理するプロトコル名を指定します。	-	local-prot1
ディスタンス値	SA アップルート登録時のディスタンス値を指定します。	1 ～ 255	1
メトリック値	SA アップルート登録時のメトリック値を指定します。	0 ～ 4294967295	0

【動作モード】

IPSEC ポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

拡張認証時に Radius サーバからの Access-Accept に格納された Attribute 情報を、経路情報 (SA アップルート) として登録する場合に設定します。

local-prot1 または local-prot2 のどちらかのプロトコル名で登録し、ダイナミックルーティングで配布する際は、各ルーティングプロトコル設定の redistribute コマンドで、"local-prot1" または "local-prot2" を指定します。配布する際のディスタンス値やメトリック値も設定可能です。

同一 VPN ピアに対して複数のセレクトを用いて複数 SA を確立する環境では、本設定を使用しないでください。また、Radius サーバ側で払い出しアドレスの指定を変更した場合、それを反映するには既存 ISAKMP-SA/IKE SA、および IPSEC-SA/CHILD SA を削除する必要がありますのでご注意ください。

【実行例】

Radius サーバからの Access-Accept に格納された Attribute 情報を、経路情報 (SA アップルート) として登録します (local-prot1)。

```
#configure terminal
(config)#crypto ipsec policy policy-A
(conf-ipsec)#sa-up route-radius local-prot1
```

【未設定時】

SA アップルートを登録しません。

17.12.4 sa-up route-sip-radius

【機能】

Access-Accept に格納された Attribute 情報を宛先とした経路情報（radius ルート）の登録

【入力形式】

```
sa-up route-sip-radius [{local-prot1 | local-prot2}] [{distance <ディスタンス値>[metric <メトリック値>] |
metric <メトリック値> [distance <ディスタンス値>]]
```

```
no sa-up route-sip-radius [{local-prot1 | local-prot2}] [{distance <ディスタンス値> [metric <メトリック
値>] | metric <メトリック値> [distance <ディスタンス値>]]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
local-prot1 local-prot2	SA アップルートを管理するプロトコル名を指定します。	-	local-prot1
ディスタンス値	SA アップルート登録時のディスタンス値を指定します。	1 ～ 255	1
メトリック値	SA アップルート登録時のメトリック値を指定します。	0 ～ 4294967295	0

【動作モード】

IPSEC ポリシー設定モード（IKEv1/IKEv2 で有効）

【説明】

データコネクトのRADIUS 認証機能で、Radius サーバからの Access-Accept に格納された Attribute 情報を宛先とした経路情報（radius ルート）として登録する場合に設定します。

local-prot1 または local-prot2 のどちらかのプロトコル名で登録し、ダイナミックルーティングで配布する際は、各ルーティングプロトコル設定の redistribute コマンドで、"local-prot1" または "local-prot2" を指定します。配布する際のディスタンス値やメトリック値も設定可能です。

【実行例】

データコネクトのRADIUS 認証機能で、Radius サーバからの Access-Accept に格納された Attribute 情報を宛先とした経路情報（radius ルート）として登録します。

```
#configure terminal
(config)#crypto ipsec policy policy-A
(conf-ipsec)#sa-up route-sip-radius
```

17.13 SA 数制限、および IPsec MIB の設定

IPsec を確立する VPN ピアの数、確立を許可する ISAKMP-SA/IKE SA/IPSEC-SA/CHILD SA 数を規制できます。またそれぞれの規制において、SNMP TRAP で警告を発するしきい値を指定できます。

17.13.1 crypto ipsec-tunnel ike limit

【機能】

許可する最大 ISAKMP-SA/IKE SA 数の設定

【入力形式】

crypto ipsec-tunnel ike limit <最大 ISAKMP-SA/IKE SA 数>

no crypto ipsec-tunnel ike limit

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
最大 ISAKMP-SA/IKE SA 数	許可する最大 ISAKMP-SA/IKE SA 数を指定します。	0 ～ 2147483647	省略不可

【動作モード】

基本設定モード（IKEv1/IKEv2 で有効）

【説明】

許可する最大 ISAKMP-SA/IKE SA 数を設定します。

【実行例】

許可する最大 ISAKMP-SA/IKE SA 数を設定します（最大 ISAKMP-SA/IKE SA 数：1200）。

```
#configure terminal
(config)#crypto ipsec-tunnel ike limit 1200
```

【未設定時】

制限なしで動作します。

17.13.2 crypto ipsec-tunnel ike threshold

【機能】

許容 ISAKMP-SA/IKE SA 数、復旧 ISAKMP-SA/IKE SA 数の設定

【入力形式】

crypto ipsec-tunnel ike threshold <許容 ISAKMP-SA/IKE SA 数> offset <復旧 ISAKMP-SA/IKE SA 数>

no crypto ipsec-tunnel ike threshold

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
許容 ISAKMP-SA/IKE SA 数	SNMP TRAP で通知する ISAKMP-SA/IKE SA 数を指定します。	0 ～ 2147483647	省略不可
復旧 ISAKMP-SA/IKE SA 数	許容 ISAKMP-SA/IKE SA 数からの差を指定します。	0 ～ 2147483647	

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

許容 ISAKMP-SA/IKE SA 数、および復旧 ISAKMP-SA/IKE SA 数を設定します。

ISAKMP-SA/IKE SA 数が許容 ISAKMP-SA/IKE SA 数を超えた場合、または (許容 ISAKMP-SA/IKE SA 数) - (復旧 ISAKMP-SA/IKE SA 数) を下回った場合に、SNMP TRAP を送信します。SNMP TRAP を送信するためには、snmp-server enable traps コマンドや、snmp-server host コマンドで、"ipsec" を指定しておいてください。

【実行例】

許容 ISAKMP-SA/IKE SA 数、および復旧 ISAKMP-SA/IKE SA 数を設定します (許容 ISAKMP-SA/IKE SA 数 : 1100、復旧 ISAKMP-SA/IKE SA 数 : 100)。

```
#configure terminal
(config)#crypto ipsec-tunnel ike threshold 1100 offset 100
```

【未設定時】

ISAKMP-SA/IKE SA 数による SNMP TRAP 送信を行いません。

17.13.3 crypto ipsec-tunnel ipsec-in limit

【機能】

許可する最大 IPSEC-SA/CHILD SA 数の設定

【入力形式】

crypto ipsec-tunnel ipsec-in limit <最大 IPSEC-SA/CHILE SA 数>

no crypto ipsec-tunnel ipsec-in limit

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
最大 IPSEC-SA/CHILD SA 数	許可する最大 IPSEC-SA/CHILD SA 数を指定します。	0 ～ 2147483647	省略不可

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

許可する最大 IPSEC-SA/CHILD SA 数を設定します。

【実行例】

許可する最大 IPSEC-SA/CHILD SA 数を設定します（最大 IPSEC-SA/CHILD SA 数：1200）。

```
#configure terminal
(config)#crypto ipsec-tunnel ipsec-in limit 1200
```

【未設定時】

制限なしで動作します。

17.13.4 crypto ipsec-tunnel ipsec-in threshold

【機能】

許可 IPSEC-SA/CHILD SA 数、復旧 IPSEC-SA/CHILD SA 数の設定

【入力形式】

crypto ipsec-tunnel ipsec-in threshold <許可 IPSEC-SA/CHILD SA 数> offset <復旧 IPSEC-SA/CHILD SA 数>

no crypto ipsec-tunnel ipsec-in threshold

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
許可 IPSEC-SA/CHILD SA 数	SNMP TRAP で通知する IPSEC-SA/CHILD SA 数を指定します。	0 ～ 2147483647	省略不可
復旧 IPSEC-SA/CHILD SA 数	許可 IPSEC-SA/CHILD SA 数からの差を指定します。	0 ～ 2147483647	

【動作モード】

基本設定モード（IKEv1/IKEv2 で有効）

【説明】

許可 IPSEC-SA/CHILD SA 数、および復旧 IPSEC-SA/CHILD SA 数を設定します。

IPSEC-SA/CHILD SA 数が許可 IPSEC-SA/CHILD SA 数を超えた場合、または（許可 IPSEC-SA/CHILD SA 数） - （復旧 IPSEC-SA/CHILD SA 数）を下回った場合に、SNMP TRAP を送信します。SNMP TRAP を送信するためには、snmp-server enable traps コマンドや、snmp-server host コマンドで、"ipsec" を指定しておいてください。

【実行例】

許可 IPSEC-SA/CHILD SA 数、および復旧 IPSEC-SA/CHILD SA 数を設定します（許可 IPSEC-SA/CHILD SA 数：1100、復旧 IPSEC-SA/CHILD SA 数：100）。

```
#configure terminal
(config)#crypto ipsec-tunnel ipsec-in threshold 1100 offset 100
```

【未設定時】

IPSEC-SA/CHILD SA 数による SNMP TRAP 送信を行いません。

17.13.5 crypto ipsec-tunnel session limit

【機能】

許可する最大 VPN ピア数の設定

【入力形式】

crypto ipsec-tunnel session limit <最大 VPN ピア数>

no crypto ipsec-tunnel session limit

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
最大 VPN ピア数	許可する最大 VPN ピア数を指定します。	0 ～ 2147483647	省略不可

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

許可する最大 VPN ピア数を設定します。

【実行例】

許可する最大 VPN ピア数を設定します (最大 VPN ピア数 : 1000)。

```
#configure terminal
(config)#crypto ipsec-tunnel session limit 1000
```

【未設定時】

制限なしで動作します。

17.13.6 crypto ipsec-tunnel session threshold

【機能】

許容 VPN ピア数、復旧 VPN ピア数の設定

【入力形式】

crypto ipsec-tunnel session threshold <許容 VPN ピア数> offset <復旧 VPN ピア数>

no crypto ipsec-tunnel session threshold

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
許容 VPN ピア数	SNMP TRAP で通知する VPN ピア数を指定します。	0 ～ 2147483647	省略不可
復旧 VPN ピア数	許容 VPN ピア数からの差分を指定します。	0 ～ 2147483647	

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

許容 VPN ピア数、および復旧 VPN ピア数を設定します。

VPN ピア数が許容 VPN ピア数を超えた場合、または (許容 VPN ピア数) - (復旧 VPN ピア数) を下回った場合に、SNMP TRAP を送信します。SNMP TRAP を送信するためには、snmp-server enable traps コマンドや、snmp-server host コマンドで、"ipsec" を指定しておいてください。

【実行例】

許容 VPN ピア数、および復旧 VPN ピア数を設定します (許容 VPN ピア数 : 900、復旧 VPN ピア数 : 50)。

```
#configure terminal
(config)#crypto ipsec-tunnel session threshold 900 offset 50
```

【未設定時】

VPN ピア数による SNMP TRAP 送信を行いません。

17.13.7 description

【機能】

説明書きの設定

【入力形式】

description <説明>

no description

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
説明	説明を指定します。	254 文字以内の WORD 型 (*1)	省略不可

*1) 1 文字の空白 (スペース) は使用可能です。複数の空白 (スペース) は 1 文字にまとめられます。

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

説明書きを設定します。わかりやすい名称を割り当ててください。この名称は、データの中継には影響しません。sirgxlmpSecTunIkeDescription として使用します。

【実行例】

説明書きを設定します（説明：This Selector is session to User-A.）。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(conf-isa-prof)#description This Selector is session to User-A.
```

【未設定時】

sirgxlmpSecTunIkeDescription 値を取得できません。

17.13.8 set ipsec-tunnel ike limit

【機能】

許可する最大 ISAKMP-SA/IKE SA 数の設定

【入力形式】

set ipsec-tunnel ike limit <最大 ISAKMP-SA/IKE SA 数>

no set ipsec-tunnel ike limit

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
最大 ISAKMP-SA/IKE SA 数	許可する最大 ISAKMP-SA/IKE SA 数を指定します。	0 ～ 2147483647	省略不可

【動作モード】

ISAKMP プロファイル設定モード（IKEv1/IKEv2 で有効）

【説明】

許可する最大 ISAKMP-SA/IKE SA 数を設定します。

【実行例】

許可する最大 ISAKMP-SA/IKE SA 数を設定します（最大 ISAKMP-SA/IKE SA 数：1200）。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(conf-isa-prof)#set ipsec-tunnel ike limit 1200
```

【未設定時】

制限なしで動作します。

17.13.9 set ipsec-tunnel ike threshold

【機能】

許容 ISAKMP-SA/IKE SA 数、復旧 ISAKMP-SA/IKE SA 数の設定

【入力形式】

set ipsec-tunnel ike threshold <許容 ISAKMP-SA/IKE SA 数> offset <復旧 ISAKMP-SA/IKE SA 数>

no set ipsec-tunnel ike threshold

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
許容 ISAKMP-SA/IKE SA 数	SNMP TRAP で通知する ISAKMP-SA/IKE SA 数を指定します。	0 ～ 2147483647	省略不可
復旧 ISAKMP-SA/IKE SA 数	許容 ISAKMP-SA/IKE SA 数からの差分を指定します。	0 ～ 2147483647	

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

許容 ISAKMP-SA/IKE SA 数、および復旧 ISAKMP-SA/IKE SA 数を設定します。

ISAKMP-SA/IKE SA 数が許容 ISAKMP-SA/IKE SA 数を越えた場合、または (許容 ISAKMP-SA/IKE SA 数) - (復旧 ISAKMP-SA/IKE SA 数) を下回った場合に、SNMP TRAP を送信します。SNMP TRAP を送信するためには、snmp-server enable traps コマンドや、snmp-server host コマンドで、"ipsec" を指定しておいてください。

【実行例】

許容 ISAKMP-SA/IKE SA 数、および復旧 ISAKMP-SA/IKE SA 数を設定します (許容 ISAKMP-SA/IKE SA 数 : 1100、復旧 ISAKMP-SA/IKE SA 数 : 100)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(config-isa-prof)#set ipsec-tunnel ike threshold 1100 offset 100
```

【未設定時】

ISAKMP-SA/IKE SA 数による SNMP TRAP 送信を行いません。

17.13.10 set ipsec-tunnel ipsec-in limit

【機能】

許可する最大 IPSEC-SA/CHILD SA 数の設定

【入力形式】

set ipsec-tunnel ipsec-in limit <最大 IPSEC-SA/CHILE SA 数>

no set ipsec-tunnel ipsec-in limit

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
最大 IPSEC-SA/CHILD SA 数	許可する最大 IPSEC-SA/CHILD SA 数を指定します。	0 ～ 2147483647	省略不可

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

許可する最大 IPSEC-SA/CHILD SA 数を設定します。

【実行例】

許可する最大 IPSEC-SA/CHILD SA 数を設定します (最大 IPSEC-SA/CHILD SA 数：1200)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(config-isa-prof)#set ipsec-tunnel ipsec-in limit 1200
```

【未設定時】

制限なしで動作します。

17.13.11 set ipsec-tunnel ipsec-in threshold

【機能】

許容 IPSEC-SA/CHILD SA 数、復旧 IPSEC-SA/CHILD SA 数の設定

【入力形式】

set ipsec-tunnel ipsec-in threshold < 許容 IPSEC-SA/CHILD SA 数 > offset < 復旧 IPSEC-SA/CHILD SA 数 >

no set ipsec-tunnel ipsec-in threshold

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
許容 IPSEC-SA/CHILD SA 数	SNMP TRAP で通知する IPSEC-SA/CHILD SA 数を指定します。	0 ～ 2147483647	省略不可
復旧 IPSEC-SA/CHILD SA 数	許容 IPSEC-SA/CHILD SA 数からの差分を指定します。	0 ～ 2147483647	

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

許容 IPSEC-SA/CHILD SA 数、および復旧 IPSEC-SA/CHILD SA 数を設定します。

IPSEC-SA/CHILD SA 数が許容 IPSEC-SA/CHILD SA 数を超えた場合、または (許容 IPSEC-SA/CHILD SA 数) - (復旧 IPSEC-SA/CHILD SA 数) を下回った場合に、SNMP TRAP を送信します。SNMP TRAP を送信するためには、snmp-server enable traps コマンドや、snmp-server host コマンドで、"ipsec" を指定しておいてください。

【実行例】

許容 IPSEC-SA/CHILD SA 数、および復旧 IPSEC-SA/CHILD SA 数を設定します（許容 IPSEC-SA/CHILD SA 数：1100、復旧 IPSEC-SA/CHILD SA 数：100）。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(conf-isa-prof)#crypto ipsec-tunnel insec-in threshold 1100 offset 100
```

【未設定時】

IPSEC-SA/CHILD SA 数による SNMP TRAP 送信を行いません。

17.13.12 set ipsec-tunnel index

【機能】

IPSEC-MIB のインデックス番号の設定

【入力形式】

set ipsec-tunnel index <インデックス番号>

no set ipsec-tunnel index

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インデックス番号	インデックス番号を指定します。	1～2147483647	省略不可

【動作モード】

ISAKMP プロファイル設定モード（IKEv1/IKEv2 で有効）

【説明】

IPSEC-MIB のインデックス番号を設定します。

SIRGX-INFMGT-IPSEC-MIB では、本インデックス番号を使用することでセキュリティポリシー単位の MIB 情報を提供します。本インデックス番号が設定されていない場合は、セキュリティポリシーごとの MIB オブジェクト、および TRAP が生成されません。

なお、本インデックス番号は重複しないように設定してください。重複して設定された場合は 1 つのセキュリティポリシーのみ有効となります。

【実行例】

IPSEC-MIB のインデックス番号を設定します（インデックス番号：1）。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(conf-isa-prof)#set ipsec-tunnel index 1
```

【未設定時】

セキュリティポリシーごとの MIB オブジェクト、および TRAP が生成されません。

17.13.13 set ipsec-tunnel name

【機能】

セレクタ識別名の設定

【入力形式】

set ipsec-tunnel name <セレクタ識別名>

no set ipsec-tunnel name

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
セレクタ識別名	セレクタ識別名を指定します。	72文字以内のSTRING型	省略不可

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

セレクタ識別名を設定します。

SIRGX-INFMGT-IPSEC-MIB で、本設定値を参照できます。

【実行例】

セレクタ識別名を設定します (セレクタ識別名: selector-A)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(config-isa-prof)#set ipsec-tunnel name selector-A
```

【未設定時】

セキュリティポリシーに対する識別名を参照できません。

17.13.14 set ipsec-tunnel session limit

【機能】

許可する最大 VPN ピア数の設定

【入力形式】

set ipsec-tunnel session limit <最大 VPN ピア数>

no set ipsec-tunnel session limit

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
最大 VPN ピア数	許可する最大 VPN ピア数を指定します。	0～2147483647	省略不可

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

許可する最大 VPN ピア数を設定します。

【実行例】

許可する最大 VPN ピア数を設定します (最大 VPN ピア数 : 1000)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(config-isa-prof)#set ipsec-tunnel session limit 1000
```

【未設定時】

制限なしで動作します。

17.13.15 set ipsec-tunnel session threshold

【機能】

許容 VPN ピア数、復旧 VPN ピア数の設定

【入力形式】

set ipsec-tunnel session threshold <許容 VPN ピア数> offset <復旧 VPN ピア数>

no set ipsec-tunnel session threshold

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
許容 VPN ピア数	SNMP TRAP で通知する VPN ピア数を指定します。	0 ~ 2147483647	省略不可
復旧 VPN ピア数	許容 VPN ピア数からの差分を指定します。	0 ~ 2147483647	

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

許容 VPN ピア数、および復旧 VPN ピア数を設定します。

VPN ピア数が許容 VPN ピア数を超えた場合、または (許容 VPN ピア数) - (復旧 VPN ピア数) を下回った場合に、SNMP TRAP を送信します。SNMP TRAP を送信するためには、snmp-server enable traps コマンドや、snmp-server host コマンドで、"ipsec" を指定しておいてください。

【実行例】

許容 VPN ピア数、および復旧 VPN ピア数を設定します (許容 VPN ピア数 : 900、復旧 VPN ピア数 : 50)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(config-isa-prof)#set ipsec-tunnel session threshold 900 offset 50
```

【未設定時】

VPN ピア数による SNMP TRAP 送信を行いません。

17.13.16 crypto isakmp negotiation limit

【機能】

新規のネゴシエーションを受け付けなくするネゴシエーションの最大同時処理数の設定

【入力形式】

crypto isakmp negotiation limit <最大値>

no crypto isakmp negotiation limit

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
最大値	IKE SA 確立時のネゴシエーション数の最大同時処理数を指定します。	1 ～ 3000	省略不可

【動作モード】

基本設定モード (IKEv2 のみで有効)

【説明】

Responder として Initial-Exchange、または Phase1 を開始する際に、新規のネゴシエーションを受け付けなくするネゴシエーションの最大同時処理数を設定します。ネゴシエーション数は IKEv1 の Phase1 と IKEv2 の Initial-Exchange、CREATE_CHILD_SA(IKE SA のみ) のネゴシエーションを行っている数の総和となります。

【実行例】

IKE SA 確立時のネゴシエーションの最大同時処理数を設定します (ネゴシエーションの最大同時処理数 : 100)。

```
#configure terminal
(config)#crypto isakmp negotiation limit 100
```

【未設定時】

以下の値で動作します。

- IKE SA 確立時のネゴシエーションの最大同時処理数 : 300

17.13.17 crypto isakmp negotiation cookie-req

【機能】

COOKIE を要求するネゴシエーション数の設定

【入力形式】

crypto isakmp negotiation cookie-req <ネゴシエーション数>

no crypto isakmp negotiation cookie-req

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ネゴシエーション数	ネゴシエーション数を指定します。 IKE SA を確立中のネゴシエーション 数が、指定した値を超えた場合に、 COOKIE を要求します。	0 ～ 3000	省略不可

【動作モード】

基本設定モード (IKEv2 でのみ有効)

【説明】

Responder として Initial-Exchange を開始する際に、COOKIE を要求するネゴシエーション数を設定します。ネゴシエーション数は IKEv1 の Phase1 と IKEv2 の Initial-Exchange、CREATE_CHILD_SA (IKE SA のみ) のネゴシエーションを行っている数の総和となります。

【実行例】

COOKIE を要求するネゴシエーション数を設定します (ネゴシエーション数: 200)。

```
#configure terminal
(config)#crypto isakmp negotiation cookie-req 200
```

【未設定時】

COOKIE を要求しません。

17.14 IPsec の各種設定

17.14.1 crypto ip dns-params

【機能】

DNS の名前解決に関する各種パラメタの設定

【入力形式】

```
crypto ip dns-params [[cache-ttl <生存時間>] [no-auto-refresh]]
```

```
no crypto ip dns-params [[cache-ttl <生存時間>] [no-auto-refresh]]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
生存時間(TTL)	DNS キャッシュの生存時間（単位：秒）を指定します。	120 ～ 86400	DNS サーバが指定した生存時間に従う
no-auto-refresh	DNS キャッシュがエクスパイしても、再度 DNS 問い合わせを行わない場合に指定します。	-	DNS キャッシュの生存時間がエクスパイした際に、再度 DNS 問い合わせを行う

【動作モード】

基本設定モード（IKEv1/IKEv2 で有効）

【説明】

set peer domain コマンドによる、DNS の名前解決に関する各種パラメタを設定します。

DNS キャッシュの生存時間(TTL)にサーバからの生存時間(TTL)を使用せず、一定の値にしたい場合は "cache-ttl" を指定します。サーバからの生存時間(TTL)に従う状態で、範囲外の値を受信した場合、下限（120 秒）または上限（86400 秒）の値を使用します。0 秒で受信した場合は、120 秒で動作します。

DNS キャッシュを定期的に更新しない場合は、"no-auto-refresh" を設定します。

【実行例】

DNS の名前解決に関する各種パラメタを設定します（生存時間(TTL)：600 秒、DNS 問い合わせを行います）。

```
#configure terminal
(config)#crypto ip dns-params cache-ttl 600
```

【未設定時】

以下の値で動作します。

生存時間(TTL)：DNS サーバの生存時間(TTL)に従う

no-auto-refresh: 設定なし

17.14.2 crypto ip dns-query auto-refresh

【機能】

キャッシュを定期更新する際のレート、最大問い合わせ数の設定

【入力形式】

crypto ip dns-query auto-refresh max-initiate <最大クエリ開始数> max-pending <最大同時クエリ数>

no crypto ip dns-query auto-refresh [max-initiate <最大クエリ開始数> max-pending <最大同時クエリ数>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
最大クエリ開始数	1秒間での最大DNS問い合わせ開始数を指定します。	1～20000	省略不可
最大同時クエリ数	同時に問い合わせ可能な数を指定します。	10～20000	

【動作モード】

基本設定モード（IKEv1/IKEv2で有効）

【説明】

set peer domain コマンドによるDNSの名前解決で、キャッシュを定期更新する際のレート、および最大問い合わせ数を設定します。set peer domain によりIPバージョンの指定がない場合は、IPv4/IPv6で問い合わせを同時に行うことがありますが、この場合クエリ数は2ではなく1としてカウントします。

【実行例】

キャッシュを定期更新する際のレート、および最大問い合わせ数を設定します（最大クエリ開始数：600、最大同時クエリ数：2000）。

```
#configure terminal
(config)#crypto ip dns-query auto-refresh max-initiate 600 max-pending 2000
```

【未設定時】

以下の値で動作します。

最大クエリ開始数：300

最大同時クエリ数：1000

17.14.3 crypto ip dns-query negotiation

【機能】

キャッシュをIKEネゴシエーション時に解決する際のレート、最大問い合わせ数の設定

【入力形式】

crypto ip dns-query negotiation max-initiate <最大クエリ開始数> max-pending <最大同時クエリ数>

no crypto ip dns-query negotiation [max-initiate <最大クエリ開始数> max-pending <最大同時クエリ数>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
最大クエリ開始数	1 秒間での最大 DNS 問い合わせ開始数を指定します。	1 ～ 20000	省略不可
最大同時クエリ数	同時に問い合わせ可能な数を指定します。	10 ～ 20000	

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

set peer domain コマンドによる DNS の名前解決で、キャッシュを IKE ネゴシエーション時に解決する際のレート、および最大問い合わせ数を設定します。最大クエリ開始数、および最大同時クエリ数には、キャッシュを定期更新する際の数を含みません。

【実行例】

キャッシュを IKE ネゴシエーション時に解決する際のレート、および最大問い合わせ数を設定します (最大クエリ開始数：200、最大同時クエリ数：2000)。

```
#configure terminal
(config)#crypto ip dns-query negotiation max-initiate 200 max-pending 2000
```

【未設定時】

以下の値で動作します。

最大クエリ開始数： 100

最大同時クエリ数： 1000

17.14.4 crypto ip dns-query timeout

【機能】

応答タイムアウト時間を設定

【入力形式】

crypto ip dns-query timeout <タイムアウト時間>

no crypto ip dns-query timeout <タイムアウト時間>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
タイムアウト時間	DNS サーバからの応答タイムアウト時間 (単位：秒) を指定します。	3 ～ 30	省略不可

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

set peer domain コマンドによる DNS の名前解決時の応答タイムアウト時間（単位：秒）を設定します。
1 つの DNS サーバに対しクエリの再送を行うことはありません。

【実行例】

応答タイムアウト時間を設定します（応答タイムアウト時間：10 秒）。

```
#configure terminal
(config)#crypto ip dns-query timeout 10
```

【未設定時】

応答タイムアウト時間は 5 秒で動作します。

17.14.5 crypto ip domain-name

【機能】

指定した domain を補完して FQDN を生成し DNS 問い合わせを行う設定

【入力形式】

crypto ip domain-name <ドメイン名>

no crypto ip domain-name [<ドメイン名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ドメイン名	ドメイン名を指定します。	253 文字以内の DOMAINWORD 型	省略不可

【動作モード】

基本設定モード（IKEv1/IKEv2 で有効）

【説明】

set peer domain コマンドの設定が FQDN ではなくホスト名のみとなっている場合に、本コマンドで指定した domain を補完して FQDN を生成し DNS 問い合わせを行います。本コマンドで domain が指定されている場合でも、set peer domain コマンドの設定が FQDN となっている場合は、domain 補完はせずにそのまま DNS 問い合わせを行います。

【実行例】

指定した domain を補完します（ドメイン名：example.com）。

```
#configure terminal
(config)#crypto ip domain-name example.com
```

【未設定時】

set peer domain コマンドの内容で DNS 問い合わせを行います。

17.14.6 crypto ip name-server

【機能】

VPN ピアまたは動的VPN サーバのアドレス問い合わせを行う際の DNS サーバの設定

【入力形式】

crypto ip name-server <DNS サーバ> [source-interface <インタフェース名> <インタフェース番号>]

no crypto ip name-server [<DNS サーバ> [source-interface <インタフェース名> <インタフェース番号>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
DNS サーバ	DNS サーバを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
インタフェース名	送信元アドレスとして使用するインタフェース名を指定します。	-	送信インタフェース名
インタフェース番号	送信元アドレスとして使用するインタフェース番号を指定します。	-	送信インタフェース番号

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

set peer domain コマンドによる VPN ピアのアドレス問い合わせを行う、または dvpn-server address コマンドによる動的VPN サーバのアドレス問い合わせを行う際に、DNS サーバを設定します。複数登録した場合には、show current.cfg(show running.cfg) コマンドで表示される上位 3 個までが有効となります。4 個以上は設定上、無効となります。

【実行例】

DNS サーバを設定します (DNS サーバ: 192.0.2.1)。

```
#configure terminal
(config)#crypto ip name-server 192.0.2.1
```

【未設定時】

DNS サーバに問い合わせを行いません。

17.14.7 crypto ipsec ikev2 delay old-sa-delete

【機能】

リキー後に旧 CHILD SA を削除するまでの時間を設定

【入力形式】

crypto ipsec ikev2 delay old-sa-delete <遅延時間>

no crypto ipsec ikev2 delay old-sa-delete [<遅延時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
遅延時間	リキー後に旧 CHILD SA を削除するまでの時間（単位：秒）を指定します。	0 ～ 600	省略不可

【動作モード】

基本設定モード（IKEv2 でのみ有効）

【説明】

IKEv2 の Initiator として CHILD SA のリキーが完了してから、旧 CHILD SA を削除するまでの時間（単位：秒）を指定します。遅延時間に "0" を指定した場合は、ライフタイム満了まで旧 CHILD SA を削除しません。遅延時間が旧 CHILD SA の残りのライフタイムよりも長い場合は、ライフタイム満了で旧 CHILD SA は削除されます。

tunnel インタフェースにおいて QoS によるシェーパ機能を使用している場合、リキー後にキューに溜まっていたパケットが旧 CHILD SA を使用して送信されることがあります。この溜まっていたパケットが旧 CHILD SA の削除通知よりもあとに送信されると、VPN ピア側でパケットロスが発生する可能性があります。この場合、遅延時間を延ばすことでパケットロスを改善できることがあります。

【実行例】

リキー後に旧 CHILD SA を削除するまでの時間を設定します（遅延時間：30 秒）。

```
#configure terminal
(config)#crypto ipsec ikev2 delay old-sa-delete 30
```

【未設定時】

遅延時間は 1 秒で動作します。

17.14.8 crypto ipsec ikev2 delay old-sa-delete-ack

【機能】

CHILD SA 削除通知に対するレスポンス送信を遅延させる時間の設定

【入力形式】

crypto ipsec ikev2 delay old-sa-delete-ack <遅延時間>

no crypto ipsec ikev2 delay old-sa-delete-ack [<遅延時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
遅延時間	CHILD SA 削除通知に対するレスポンス送信を遅延させる時間（単位：秒）を指定します。	0 ～ 600	省略不可

【動作モード】

基本設定モード（IKEv2 でのみ有効）

【説明】

IKEv2 で CHILD SA のリキー完了後、旧 CHILD SA の削除通知を受信し、削除してからレスポンスを送信するまでの時間（単位：秒）を指定します。遅延時間に "0" を指定した場合は、遅延させずレスポンスを送信します。遅延時間を延ばしすぎると、Initiator 側でネゴシエーションタイムアウトが発生する可能性がありますのでご注意ください。

tunnel インタフェースにおいて、QoS によるシェーパ機能を使用している場合、新 CHILD SA に切り替え後、キューに溜まっていたパケットが旧 CHILD SA を使用して送信されることがあります。この溜まっていたパケットが旧 CHILD SA の削除通知に対するレスポンスよりもあとに送信されると、VPN ピア側でパケットロスが発生する可能性があります。この場合、遅延時間を延ばすことでパケットロスを改善することができます。

【実行例】

CHILD SA 削除通知に対するレスポンス送信を遅延させる時間を設定します（遅延時間：30 秒）。

```
#configure terminal
(config)#crypto ipsec ikev2 delay old-sa-delete-ack 30
```

【未設定時】

IPsec ポリシー設定モードに set ikev2 delay old-sa-delete-ack コマンドの設定がある場合は、その設定に従います。設定がない場合は、遅延時間は 0 秒で動作します。

17.14.9 crypto isakmp negotiation always-up-params

【機能】

set security-association always-up コマンドによるネゴシエーション開始タイミングの設定

【入力形式】

crypto isakmp negotiation always-up-params interval <監視間隔> max-initiate <最大ネゴシエーション開始数> max-pending <最大ネゴシエーション数> delay <SA 再チェック遅延時間>

no crypto isakmp negotiation always-up-params

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
監視間隔	always-up 機能の監視間隔（単位：ミリ秒）を指定します。	10 ～ 10000	省略不可
最大ネゴシエーション開始数	一度の監視で行うネゴシエーション開始数の最大値を指定します。	1 ～ 20000	
最大ネゴシエーション数	同時に行うネゴシエーション数の最大値を指定します。	1 ～ 20000	
SA 再チェック遅延時間	SA が確立しているかどうかを再チェックする遅延時間（単位：秒、ジッタあり）を指定します。	1 ～ 120	

【動作モード】

基本設定モード（IKEv1/IKEv2 で有効）

【説明】

set security-association always-up コマンドによるネゴシエーション開始タイミングを設定します。

【実行例】

set security-association always-up コマンドによるネゴシエーション開始タイミングを設定します（監視間隔：100 ミリ秒、最大ネゴシエーション開始数：10、最大ネゴシエーション数：15、SA 再チェック遅延時間 30 秒）。

```
#configure terminal
(config)#crypto isakmp negotiation always-up-params interval 100 max-initiate 10 max-pending 15 delay 30
```

【未設定時】

以下の値で動作します。

監視間隔： 100 ミリ秒

最大ネゴシエーション開始数：
5

最大ネゴシエーション数：
3000

SA 再チェック遅延時間：
60 秒

17.14.10 crypto isakmp negotiation expire-time

【機能】

ISAKMP ネゴシエーションのエキスパイア時間の設定

【入力形式】

crypto isakmp negotiation expire-time <エキスパイア時間>

no crypto isakmp negotiation expire-time

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エキスパイア時間	ISAKMP ネゴシエーションのエキスパイア時間（単位：秒）を指定します。	30 ～ 600	省略不可

【動作モード】

基本設定モード（IKEv1/IKEv2 で有効）

【説明】

ISAKMP ネゴシエーションのエキスパイア時間（単位：秒）を設定します。

IKEv1 では initiator/responder において、各ネゴシエーションモードの開始から指定された時間内に該当モードが完了しなかった場合、ネゴシエーションを終了します。

IKEv2 では responder において、IKE_SA_INIT から IKE_AUTH 完了までのリクエストパケットを受信（再送を除く）してから指定された時間内に、次のリクエストを受信しなかった場合、ネゴシエーションを終了します。

【実行例】

ISAKMP ネゴシエーションのエキスパイア時間（単位：秒）を設定します（エキスパイア時間：120 秒）。

```
#configure terminal
(config)#crypto isakmp negotiation expire-time 120
```

【未設定時】

同様の関連コマンドとして 3 つの設定がありますが以下の順で適用されます。

- username isakmp negotiation expire-time
- set negotiation expire-time
- crypto isakmp negotiation expire-time

どの設定もない場合は、エキスパイア時間は 60 秒で動作します。

17.14.11 crypto isakmp negotiation protected-rekey-interval

【機能】

IKEv2 の CREATE_CHILD_SA によるリキーを許容する間隔の設定

【入力形式】

crypto isakmp negotiation protected-rekey-interval <リキー間隔>

no crypto isakmp negotiation protected-rekey-interval

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
リキー間隔	CREATE_CHILD_SA によるリキーを許容する間隔（単位：秒）を指定します。	1 ～ 36000	省略不可

【動作モード】

基本設定モード（IKEv2 でのみ有効）

【説明】

IKEv2 の CREATE_CHILD_SA によるリキーを許容する間隔（単位：秒）を指定します。IKE SA/CHILD SA それぞれのネゴシエーションにおいて、設定された間隔以内に新規に CREATE_CHILD_SA を受信した場合、そのパケットを破棄します。

【実行例】

IKEv2 の CREATE_CHILD_SA によるリキーを許容する間隔（単位：秒）を設定します（リキー間隔：10 秒）。

```
#configure terminal
(config)#crypto isakmp negotiation protected-rekey-interval 10
```

【未設定時】

negotiation protected-rekey-interval コマンドの設定に従います。

17.14.12 crypto isakmp negotiation retry

【機能】

ISAKMP ネゴシエーションの再送パラメタの設定

【入力形式】

crypto isakmp negotiation retry timer <再送間隔> limit <再送回数> timer-max <最大再送間隔> guard-time <再送ガード時間>

no crypto isakmp negotiation retry

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
再送間隔	ISAKMP ネゴシエーションパケットの再送間隔（単位：秒）を指定します。再送を行うごとに間隔は2倍に増加していきます。	1～60	省略不可
再送回数	ISAKMP ネゴシエーションパケットの再送回数を指定します。	0～5	
最大再送間隔	ISAKMP ネゴシエーションパケットの最大再送間隔（単位：秒）を指定します。再送間隔がこの設定値以上となる場合は、再送間隔をそれ以上増やさず、設定された値の再送間隔で動作します。	1～60	
再送ガード時間	ISAKMP ネゴシエーションパケットを送信してから、再送ガード時間（単位：秒）内に受信したパケット（VPN ピアからの再送パケット）を破棄します。	0～60	

【動作モード】

基本設定モード（IKEv1/IKEv2 で有効）

【説明】

ISAKMP ネゴシエーションの再送パラメタを設定します。

【実行例】

ISAKMP ネゴシエーションの再送パラメタを設定します（再送間隔：5 秒、再送回数：3 回、最大再送間隔：20 秒、再送ガード時間：10 秒）。

```
#configure terminal
(config)#crypto isakmp negotiation retry timer 5 limit 3 timer-max 20 guard-time 10
```

【未設定時】

同様の関連コマンドとして3つ設定がありますが以下の順で適用されます。

- username isakmp negotiation retry
- set negotiation retry
- crypto isakmp negotiation retry

どの設定もない場合は、以下の値で動作します。

再送間隔： 10 秒
再送回数： 2 回
最大再送間隔： 30 秒
再送ガード時間： 0 秒

17.14.13 crypto ipsec qm-addr-zero-any

【機能】

any アドレス (0.0.0.0/0) として取り扱う設定

【入力形式】

crypto ipsec qm-addr-zero-any

no crypto ipsec qm-addr-zero-any

【動作モード】

基本設定モード (IKEv1 でのみ有効)

【説明】

IKEv1 の Quick-mode 時に VPN ピアから ID ペイロードとして ID_IPV4_ADDR=0.0.0.0 を受信した場合、any アドレス (0.0.0.0/0) として取り扱います。

【実行例】

any アドレス (0.0.0.0/0) として取り扱います。

```
#configure terminal
(config)#crypto ipsec qm-addr-zero-any
```

【未設定時】

ID_IPV4_ADDR=0.0.0.0 はホストアドレスとして取り扱います。

17.14.14 crypto session identification address

【機能】

セッションの識別をピア／本装置のアドレス、ポートで識別する設定

【入力形式】

crypto session identification address

no crypto session identification address

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

セッションの識別をピア／本装置のアドレス、ポートで識別します。

セッションの再確立時の旧セッションの削除、および以下のコマンドによるセッション識別時に利用します。

```
crypto isakmp negotiation protected-rekey-interval
```

```
negotiation protected-rekey-interval
```

ISAKMP プロファイル設定モードに set session identification address コマンド設定がある場合は、そちらの設定を優先します。

装置単位での識別となりますので識別子の重複にご注意ください。

【実行例】

セッションの識別をピア／本装置のアドレス、ポートで識別します。

```
#configure terminal
(config)#crypto session identification address
```

【未設定時】

セッションの識別をピア／本装置の IKE の Identity で識別します。

17.14.15 crypto session reject-duplicated-request

【機能】

再確立要求を拒否する設定

【入力形式】

```
crypto session reject-duplicated-request
```

```
no crypto session reject-duplicated-request
```

【動作モード】

基本設定モード（IKEv1/IKEv2 で有効）

【説明】

セッションが確立している状態で、responder として再度 ISAKMP-SA/IKE SA を確立（IKEv1 では Phase1、IKEv2 では Initial-Exchange）しようとする場合に、IPsec の終端アドレスまたは UDP ポートが変更されていた場合は、確立要求を拒否する（応答しない）場合に設定します。セッションの識別をピア／本装置の IKE の Identity で識別する場合（crypto session identification address コマンドや set session identification address コマンドの設定がない）に有効となります。

【実行例】

再確立要求を拒否します（応答しません）。

```
#configure terminal
(config)#crypto session reject-duplicated-request
```

【未設定時】

set session reject-duplicated-request コマンドの設定に従います。set session reject-duplicated-request コマンドの設定がない場合、セッションが確立している状態で IPsec の終端アドレスまたは UDP ポートが変更された Phase1、Initial-Exchange を許容し、再確立します。再確立すると、旧セッションは削除されます。

17.14.16 crypto session release idle-time

【機能】

セッションが一定時間 ESP 通信を行わない場合にセッションを解放する時間の設定

【入力形式】

crypto session release idle-time <セッションアイドル時間> [<監視対象>]

no crypto session release idle-time [<セッションアイドル時間> [<監視対象>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
セッションアイドル時間	セッションのアイドル時間（単位：秒）を指定します。	10 ～ 1000000000	省略不可
監視対象	無通信の監視を受信方向にするか、送信方向にするかを指定します。	send: 送信を監視 receive: 受信を監視	送信と受信を監視する

【動作モード】

基本設定モード（IKEv1/IKEv2 で有効）

【説明】

セッションが一定時間 ESP 通信を行わない場合にセッションを解放する時間（単位：秒）を設定します。

【実行例】

セッションが一定時間 ESP 通信を行わない場合にセッションを解放する時間（単位：秒）を設定します（セッションアイドル時間：10 秒、監視対象：送信を監視）。

```
#configure terminal
(config)#crypto session release idle-time 10 send
```

【未設定時】

セッションを解放しません。

17.14.17 crypto session release ipsec-lost-time

【機能】

IPSEC-SA/CHILD SA がない状態が継続した場合に、ISAKMP-SA/IKE SA を解放するまでの時間の設定

【入力形式】

```
crypto session release ipsec-lost-time {<継続時間 1> [first <継続時間 2>] | first <継続時間 2>}
```

```
no crypto session release ipsec-lost-time [<継続時間 1> [first <継続時間 2>] | first <継続時間 2>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
継続時間 1	IPSEC-SA/CHILD SA がない状態が継続した場合に、ISAKMP-SA/IKE SA を解放するまでの時間（単位：秒）を指定します。	1 ～ 600	省略不可
継続時間 2	初回に ISAKMP-SA を responder として確立した時刻から、IPSEC-SA がない状態が継続した場合に、ISAKMP-SA を解放するまでの時間（単位：秒）を指定します。 IKEv1 でのみ有効です。	1 ～ 600	初回接続時に ISAKMP-SA を解放する動作を行わない

【動作モード】

基本設定モード（IKEv1/IKEv2 で有効）

【説明】

IPSEC-SA/CHILD SA がない状態が継続した場合に、ISAKMP-SA/IKE SA を解放するまでの時間（単位：秒）を設定します。また、IKEv1 で初回接続時に IPSEC-SA の確立が行われない場合、ISAKMP-SA が残ることがあります。この ISAKMP-SA を削除するための時間（単位：秒）を設定します。

設定変更後に確立された IPSEC-SA/CHILD SA から有効になります。

ISAKMP プロファイル設定モードに set session release ipsec-lost-time コマンド設定がある場合は、そちらの設定を優先します。

動的 VPN 機能使用時には、継続時間 1 の設定は無効になり、IPSEC-SA が解放された際に、即 ISAKMP-SA を解放します。

【実行例】

IPSEC-SA/CHILD SA がない状態が継続した場合に、ISAKMP-SA/IKE SA を解放するまでの時間（単位：秒）を設定します（継続時間：100 秒）。

```
#configure terminal
(config)#crypto session release ipsec-lost-time 100
```

【未設定時】

同様の関連コマンドとして以下の設定があれば、それに従います。

- set session release ipsec-lost-time

設定がない場合は、IPSEC-SA の状態に依存した ISAKMP-SA の解放は行いません。

17.14.18 crypto session release isakmp-lost-time

【機能】

IPSEC-SA が存在し、ISAKMP-SA がいない状態が発生した場合に、IPSEC-SA を解放するまでの時間の設定

【入力形式】

crypto session release isakmp-lost-time <継続時間>

no crypto session release isakmp-lost-time [<継続時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
継続時間	ISAKMP-SA がいない状態が継続した場合に、IPSEC-SA を解放するまでの時間（単位：秒）を指定します。	0 ～ 600	省略不可

【動作モード】

基本設定モード（IKEv1 でのみ有効）

【説明】

Dangling SA（IPSEC-SA が存在し、ISAKMP-SA がいない状態）が発生した場合に、IPSEC-SA を解放するまでの時間（単位：秒）を設定します。この間に ISAKMP-SA が新規に確立した場合は IPSEC-SA を削除しません。

ISAKMP-SA の lifetime 満了後、本コマンドで設定した時間よりも前に ISAKMP-SA の再確立を行わないと、セッションが削除されますのでご注意ください（"0" 設定時は、lifetime が満了する前に ISAKMP-SA の再確立を行う必要があります）。

設定変更は確立済み、およびそのあと確立した ISAKMP-SA で有効になります。

ISAKMP プロファイル設定モードに set session release isakmp-lost-time コマンド設定がある場合は、そちらの設定を優先します。

【実行例】

Dangling SA（IPSEC-SA が存在し、ISAKMP-SA がいない状態）が発生した場合に、IPSEC-SA を解放するまでの時間（単位：秒）を設定します（継続時間：0 秒（即時解放））。

```
#configure terminal
(config)#crypto session release isakmp-lost-time 0
```

【未設定時】

同様の関連コマンドとして以下の設定があれば、それに従います。

- set session release isakmp-lost-time

設定がない場合は ISAKMP-SA の状態に依存した IPSEC-SA の解放は行いません。

17.14.19 crypto session release reset acct-stop-send

【機能】

存在する IPsec セッションに関する Accounting-Request を RADIUS サーバに送信する設定

【入力形式】

crypto session release reset acct-stop-send

no crypto session release reset acct-stop-send

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

reset コマンド実行時に、存在する IPsec セッションに関する Accounting-Request(Stop) を RADIUS サーバに送信する場合に設定します。

【実行例】

存在する IPsec セッションに関する Accounting-Request(Stop) を RADIUS サーバに送信します。

```
#configure terminal
(config)#crypto session release reset acct-stop-send
```

【未設定時】

reset コマンド実行時に、Accounting-Request(Stop)を送信しません。

17.14.20 crypto session release reset delete-send

【機能】

存在する IPsec セッションに関する DELETE メッセージを VPN ピアに送信する設定

【入力形式】

crypto session release reset delete-send

no crypto session release reset delete-send

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

reset コマンド実行時に、存在する IPsec セッションに関する DELETE メッセージを VPN ピアに送信する場合に設定します。

【実行例】

存在する IPsec セッションに関する DELETE メッセージを VPN ピアに送信します。

```
#configure terminal
(config)#crypto session release reset delete-send
```

【未設定時】

reset コマンド実行時に、DELETE メッセージを送信しません。

17.14.21 crypto session release reset delay

【機能】

存在する IPsec セッションの削除処理のレートを設定

【入力形式】

crypto session release reset delay <SA 削除数>

no crypto session release reset delay [<SA 削除数>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
SA 削除数	1 秒ごとにセッション削除する数を指定します。	10 ～ 4000	省略不可

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

reset コマンド実行時に、存在する IPsec セッションの削除処理のレートを設定します。

crypto session release reset delete-send、または crypto session release reset acct-stop-send の設定が有効である場合にのみ動作します。

【実行例】

存在する IPsec セッションの削除処理のレートを設定します (SA 削除数 : 2000)。

```
#configure terminal
(config)#crypto session release reset delay 2000
```

【未設定時】

SA 削除数に制限をかけません。

17.14.22 crypto session release session-time

【機能】

セッションを開始してからセッションを解放するまでの時間の設定

【入力形式】

crypto session release session-time <セッション生存時間>

no crypto session release session-time

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
セッション生存時間	セッション生存時間（単位：秒）を指定します。	1 ～ 1000000000	省略不可

【動作モード】

基本設定モード（IKEv1/IKEv2 で有効）

【説明】

セッションを開始してからセッションを解放するまでの時間（単位：秒）を設定します。

【実行例】

セッションを開始してからセッションを解放するまでの時間（単位：秒）を設定します（セッション生存時間：100 秒）。

```
#configure terminal
(config)#crypto session release session-time 100
```

【未設定時】

セッションを解放しません。

17.14.23 link-state

【機能】

インタフェースの状態を SA またはデータコネク트에同期させる設定

【入力形式】

link-state {sync-sa | sync-ngn}

no link-state [{sync-sa | sync-ngn}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
sync-sa sync-ngn	インタフェースの状態を同期させる場合に指定します。	sync-sa: SA 確立に同期 sync-ngn: データコネク トの利用可能状態と同期	省略不可

【動作モード】

tunnel インタフェース設定モード（IKEv1/IKEv2 で有効）

【説明】

インタフェースの状態を SA 確立に同期、またはデータコネクトの状態と同期させる場合に設定します。
survey コマンドによる IPsec tunnel の監視との併用は未サポートとなります。

※Tunnel Down だけでは SA は削除されません。

【sync-sa 設定時】

- SA が確立されていない → tunnel インタフェース DOWN
- SA が確立されている → tunnel インタフェース UP

【sync-ngn 設定時】

- データコネクト発信可能状態でない → tunnel インタフェース Down
- データコネクト発信可能状態である → tunnel インタフェース UP

【実行例】

インタフェースの状態を SA 確立に同期させます。

```
#configure terminal
(config)#interface tunnel 1
(config-if-tun 1)#link-state sync-sa
```

【未設定時】

VPN セレクタ設定モードの link-state 設定に従います。どちらも設定がない場合はスタティックセレクタであれば、SA 確立の状態と同期しません。ダイナミックセレクタであれば、SA 確立に同期します。

17.14.24 set rekey dont-initiate

【機能】

ISAKMP-SA/IKE SA のリキー動作を行わない設定

【入力形式】

set rekey dont-initiate

no set rekey dont-initiate

【動作モード】

ISAKMP ポリシー設定モード (IKEv2 でのみ有効)

【説明】

ISAKMP-SA/IKE SA のリキー動作を行わない場合に設定します。

【実行例】

ISAKMP-SA/IKE SA のリキー動作を行いません。

```
#configure terminal
(config)#crypto isakmp policy policy-A
(config-isakmp)#set rekey dont-initiate
```

【未設定時】

ISAKMP-SA/IKE SA のリキー動作を行います。

17.14.25 negotiation protected-rekey-interval

【機能】

IKEv2 の CREATE_CHILD_SA によるリキーを許容する間隔の設定

【入力形式】

negotiation protected-rekey-interval <リキー間隔>

no negotiation protected-rekey-interval

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
リキー間隔	CREATE_CHILD_SA によるリキーを許容する間隔（単位：秒）を指定します。	1 ～ 36000	省略不可

【動作モード】

ISAKMP プロファイル設定モード（IKEv2 でのみ有効）

【説明】

IKEv2 の CREATE_CHILD_SA によるリキーを許容する間隔（単位：秒）を指定します。IKE SA/CHILD SA それぞれのネゴシエーションにおいて、設定された間隔以内に新規に CREATE_CHILD_SA を受信した場合、そのパケットを破棄します。

【実行例】

IKEv2 の CREATE_CHILD_SA によるリキーを許容する間隔（単位：秒）を設定します（リキー間隔：10 秒）。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(config-isa-prof)#negotiation protected-rekey-interval 10
```

【未設定時】

crypto isakmp negotiation protected-rekey-interval コマンドの設定に従います。設定がない場合は、常に CREATE_CHILD_SA によるリキーを許容します。

17.14.26 set session identification address

【機能】

セッションの識別をピア／本装置のアドレス、ポートで識別する設定

【入力形式】

set session identification address

no set session identification address

【動作モード】

ISAKMP プロファイル設定モード（IKEv1/IKEv2 で有効）

【説明】

セッションの識別をピア／本装置のアドレス、ポートで識別します。

セッションの再確立時の旧セッションの削除、および以下のコマンドによるセッション識別時に利用します。

```
crypto isakmp negotiation protected-rekey-interval
negotiation protected-rekey-interval
```

装置単位での識別となりますので識別子の重複にご注意ください。

【実行例】

セッションの識別をピア／本装置のアドレス、ポートで識別します。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(config-isa-prof)#set session identification address
```

【未設定時】

セッションの識別をピア／本装置の IKE の Identity で識別します。

17.14.27 set session reject-duplicated-request

【機能】

再確立要求を拒否する設定

【入力形式】

```
set session reject-duplicated-request
```

```
no set session reject-duplicated-request
```

【動作モード】

ISAKMP プロファイル設定モード (IKEv1/IKEv2 で有効)

【説明】

セッションが確立している状態で、responder として再度 ISAKMP-SA/IKE SA を確立 (IKEv1 では Phase1、IKEv2 では Initial-Exchange) しようとする場合に、IPsec の終端アドレスまたは UDP ポートが変更されていた場合は、確立要求を拒否する (応答しない) 場合に設定します。セッションの識別をピア／本装置の IKE の Identity で識別する場合 (crypto session identification address コマンドや set session identification address コマンドの設定がない) に有効となります。

【実行例】

再確立要求を拒否します (応答しません)。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(config-isa-prof)#set session reject-duplicated-request
```

【未設定時】

crypto session reject-duplicated-request コマンドの設定に従います。crypto session reject-duplicated-request コマンド設定がない場合、セッションが確立している状態で IPsec の終端アドレスまたは UDP ポートが変更された Phase1、Initial-Exchange を許容し、再確立します。

17.14.28 set session release ipsec-lost-time

【機能】

ISAKMP-SA/IKE SA を解放するまでの時間の設定

【入力形式】

```
set session release ipsec-lost-time {<継続時間 1> [first <継続時間 2>] | first <継続時間 2>}
```

```
no set session release ipsec-lost-time [<継続時間 1> [first <継続時間 2>] | first <継続時間 2>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
継続時間 1	IPSEC-SA/CHILD SA がない状態が継続した場合に、ISAKMP-SA/IKE SA を解放するまでの時間（単位：秒）を指定します。	1 ～ 600	省略不可
継続時間 2	初回に ISAKMP-SA を responder として確立した時刻から、IPSEC-SA がない状態が継続した場合に、ISAKMP-SA を解放するまでの時間（単位：秒）を指定します。IKEv1 でのみ有効です。	1 ～ 600	初回接続時に ISAKMP-SA を解放する動作を行わない

【動作モード】

ISAKMP プロファイル設定モード（IKEv1/IKEv2 で有効）

【説明】

IPSEC-SA/CHILD SA がない状態が継続した場合に、ISAKMP-SA/IKE SA を解放するまでの時間（単位：秒）を設定します。また、IKEv1 で初回接続時に IPSEC-SA の確立が行われない場合、ISAKMP-SA が残ることがあります。この ISAKMP-SA を削除するための時間（単位：秒）を設定します。

設定変更後に確立された IPSEC-SA/CHILD SA から有効になります。

動的 VPN 機能により確立した SA の場合には、継続時間 1 の設定は無効になり、IPSEC-SA が解放された際に、即 ISAKMP-SA を解放します。

【実行例】

ISAKMP-SA/IKE SA を解放するまでの時間（単位：秒）を設定します（継続時間：100 秒）。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(config-isa-prof)#set session release ipsec-lost-time 100
```

【未設定時】

同様の関連コマンドとして以下の設定があれば、それに従います。

- crypto session release ipsec-lost-time

設定がない場合は、IPSEC-SA の状態に依存した ISAKMP-SA の解放は行いません。

17.14.29 set session release idle-time

【機能】

セッションを解放する時間の設定

【入力形式】

set session release idle-time <セッションアイドル時間> [<監視対象>]

no set session release idle-time [<セッションアイドル時間> [<監視対象>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
セッションアイドル時間	セッションのアイドル時間（単位：秒）を指定します。	10～1000000000	省略不可
監視対象	無通信の監視を受信方向にするか、送信方向にするかを指定します。	send: 送信を監視 receive: 受信を監視	送信と受信を監視する

【動作モード】

ISAKMP プロファイル設定モード（IKEv1/IKEv2 で有効）

【説明】

セッションが一定時間 ESP 通信を行わない場合にセッションを解放する時間（単位：秒）を設定します。

【実行例】

セッションが一定時間 ESP 通信を行わない場合にセッションを解放する時間（単位：秒）を設定します（セッションアイドル時間：10 秒、監視対象：送信を監視）。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(conf-isa-prof)#set session release idle-time 10 send
```

【未設定時】

crypto session release idle-time コマンドの設定に従います。

17.14.30 set session release isakmp-lost-time

【機能】

IPSEC-SA を解放するまでの時間の設定

【入力形式】

set session release isakmp-lost-time <継続時間>

no set session release isakmp-lost-time [<継続時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
継続時間	ISAKMP-SA がない状態が継続した場合に、IPSEC-SA を解放するまでの時間（単位：秒）を指定します。	0 ～ 600	省略不可

【動作モード】

ISAKMP プロファイル設定モード（IKEv1 でのみ有効）

【説明】

Dangling SA（IPSEC-SA が存在し、ISAKMP-SA がない状態）が発生した場合に、IPSEC-SA を解放するまでの時間（単位：秒）を設定します。この間に ISAKMP-SA が新規に確立した場合は IPSEC-SA を削除しません。ISAKMP-SA の再確立を lifetime が満了する前に行わないとセッションが削除されますのでご注意ください。

設定変更は確立済み、およびそのあと確立した ISAKMP-SA で有効になります。

【実行例】

Dangling SA（IPSEC-SA が存在し、ISAKMP-SA がない状態）が発生した場合に、IPSEC-SA を解放するまでの時間（単位：秒）を設定します（継続時間：0 秒（即時解放））。

```
#configure terminal
(config)#crypto isakmp profile profile-A
(conf-isa-prof)#set session release isakmp-lost-time 0
```

【未設定時】

同様の関連コマンドとして以下の設定があれば、それに従います。

- crypto session release isakmp-lost-time

設定がない場合は ISAKMP-SA の状態に依存した IPSEC-SA の解放は行いません。

17.14.31 set ikev2 delay old-sa-delete-ack

【機能】

CHILD SA 削除通知に対するレスポンス送信を遅延させる時間の設定

【入力形式】

set ikev2 delay old-sa-delete-ack <遅延時間>

no set ikev2 delay old-sa-delete-ack [<遅延時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
遅延時間	CHILD SA 削除通知に対するレスポンス送信を遅延させる時間（単位：秒）を指定します。	0 ～ 600	省略不可

【動作モード】

IPSEC ポリシー設定モード (IKEv2 でのみ有効)

【説明】

IKEv2 で CHILD SA のリキー完了後、旧 CHILD SA の削除通知を受信し、削除してからレスポンスを送信するまでの時間（単位：秒）を指定します。遅延時間に "0" を指定した場合は、遅延させずレスポンスを送信します。遅延時間を延ばしすぎると、Initiator 側でネゴシエーションタイムアウトが発生する可能性がありますのでご注意ください。

tunnel インタフェースにおいて、QoS によるシェーパ機能を使用している場合、新 CHILD SA に切り替え後、キューに溜まっていたパケットが旧 CHILD SA を使用して送信されることがあります。この溜まっていたパケットが旧 CHILD SA の削除通知に対するレスポンスよりもあとに送信されると、VPN ピア側でパケットロスが発生する可能性があります。この場合、遅延時間を延ばすことでパケットロスを改善することができます。

【実行例】

CHILD SA 削除通知に対するレスポンス送信を遅延させる時間を設定します（遅延時間：30 秒）。

```
#configure terminal
(config)#crypto ipsec policy policy-A
(conf-ipsec)#set ikev2 delay old-sa-delete-ack 30
```

【未設定時】

基本設定モードに `crypto isec ikev2 delay old-sa-delete-ack` コマンドの設定がある場合は、その設定に従います。設定がない場合は、遅延時間は 0 秒で動作します。

17.14.32 set security-association rekey

【機能】

リキー実施有無の設定

【入力形式】

`set security-association rekey {dont-initiate | always}`

`no set security-association rekey`

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
dont-initiate always	リキー実施の有無を指定します。	dont-initiate: Initiator として IPSEC-SA/CHILD SA のリキーを行わない always: Initiator として IPSEC-SA/CHILD SA のリキーを必ず行う	省略不可

【動作モード】

IPSEC ポリシー設定モード (IKEv1/IKEv2 で有効)

【説明】

リキー実施の有無を設定します。

本装置から IPSEC-SA/CHILD SA のリキーを行いたくない場合に "dont-initiate" を設定します。

無通信の状態（接続している IPSEC-SA/CHILD SA を使用した ESP パケットの送受信がない状態）であってもしリキーの鍵交換を開始する場合に "always" を設定します。

【実行例】

リキー実施の有無を設定します (always)。

```
#configure terminal
(config)#crypto ipsec policy policy-A
(config-ipsec)#set security-association rekey always
```

【未設定時】

無通信の状態ではない場合のみリキーを開始します。

17.15 ログの設定

17.15.1 crypto isakmp log

【機能】

SA、セッションの確立／解放、IKE ネゴシエーション失敗のログを出力する設定

【入力形式】

```
crypto isakmp log {sa [detail] | session [detail] | negotiation-fail [detail]}
```

```
no crypto isakmp log {sa [detail] | session [detail] | negotiation-fail [detail]}
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
sa session negotiation-fail	ログを出力する対象を指定します。	sa:SA 確立／解放 session: セッション確立／解放 negotiation-fail:IKE ネゴシエーション失敗	省略不可
detail	詳細ログを出力する場合に指定します。	-	通常出力

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

SA、セッションの確立／解放、IKE ネゴシエーションの失敗のログを出力する場合に設定します。

【実行例】

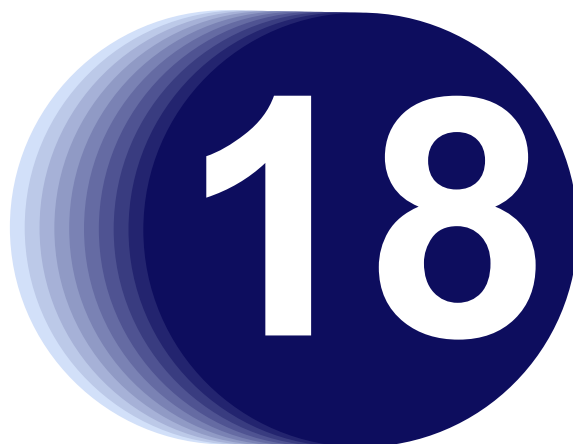
SA やセッションの確立／解放のログを出力します (SA 確立／解放)。

```
#configure terminal
(config)#crypto isakmp log sa
```

【未設定時】

SA、セッションの確立／解放、IKE ネゴシエーションの失敗のログを出力しません。

第18章 動的VPNの設定



この章では、動的VPNの設定に関するコマンドについて説明します。

18.1	INVITEの発信契機の設定	660
18.2	DVPNプロファイル設定	662
18.3	DVPNクライアント情報の設定	670
18.4	DVPNサーバの設定	681

18.1 INVITE の発信契機の設定

18.1.1 dvpn autoignore

【機能】

自動的に ignore 判定する時間の設定

【入力形式】

dvpn autoignore time <time>

no dvpn autoignore time [<time>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
time	ignore 判定する時間（単位：秒）を設定します。	1 ～ 60	省略不可

【動作モード】

基本設定モード

【説明】

接続要求発行済みの送信先に対して、自動的に ignore 判定する時間を設定します。

コネクションの確立が失敗しても、設定された時間、対象の送信先に対しては新規の接続要求を発行しません。

また、autoignore の最大登録数は 1000 件です。登録数が最大数になっている場合は、すべてのパケットが ignore 対象になります。

【実行例】

接続要求発行済みの送信先に対して、ignore 判定する時間を設定します。(time : 10)

```
#configure terminal
(config)# dvpn autoignore time 10
```

【未設定時】

10 秒で動作します。

18.1.2 dvpn ip

【機能】

IPv4 パケットに対する動的 VPN の接続要求の設定

【入力形式】

dvpn ip <シーケンス番号> {invite access-group <アクセスリスト番号> prefix-len <プレフィックス長>
profile <DVPN プロファイル ID> | ignore access-group <アクセスリスト番号>}


```
no dvpn ip <シーケンス番号> [{invite access-group <アクセスリスト番号> prefix-len <プレフィックス長> profile <DVPN プロファイル ID> | ignore access-group <アクセスリスト番号>}]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
シーケンス番号	検索順序を指定します。	1 ～ 8192	省略不可
invite	アクセスリストに match したパケットに対して、動的 VPN の接続要求をします。	-	省略不可
ignore	アクセスリストに match したパケットに対して、動的 VPN の接続要求をしません。	-	省略不可
アクセスリスト番号	アクセスリスト番号 (IPv4) を指定します。	アクセスリスト番号範囲 (IPv4 拡張のみ)	省略不可
プレフィックス長	match したパケットの送信先アドレスに対するプレフィックス長を指定します。	0 ～ 32	省略不可
DVPN プロファイル ID	動的 VPN プロファイルの ID を指定します。	1 ～ 3000	省略不可

【動作モード】

gigaethernet インタフェース設定モード、gigaethernet サブインタフェース設定モード、tunnel インタフェース設定モード (tunnel mode ipsec と tunnel mode pppoe のみ)

【説明】

access-list コマンドで指定したアクセスリストに対して、送信時に動的 VPN の接続要求を発行するか、しないかを設定します。接続要求契機となるパケットの中継は、経路に従います。経路がない場合は、ロスされます。

以下のパケットについては、自動的に ignore の動作になります。

- 自局出し端末監視 ICMP パケット
- 自局出し ICMP (Echo Request を除く)
- 自局出し SIP (UDP 送信元ポート番号：5060、TCP 送信元ポート番号：5060)
- 自局出し ISAKMP (UDP 送信元ポート番号：500 または 4500)

フィルタ／QoS／データコネクト QoS／DVPN ACL／ポリシールーティングのクラシファイエントリはすべて共用です。各機能でエントリを使用していると、データコネクト QoS のエントリが入らないことがあります。

【実行例】

access-list コマンドで指定したアクセスリストに対して、送信時に動的 VPN の接続要求を発行します (シーケンス番号：1、invite、アクセスリスト番号：100、プレフィックス長：32、プロファイル ID：1)。

```
#configure terminal
(config)#interface tunnel 1
(config-if-tun 1)# dvpn ip 1 invite access-group 100 prefix-len 32 profile 1
```

【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。

18.2 DVPN プロファイル設定

18.2.1 dvpn profile

【機能】

動的VPN プロファイル設定モードへの移行

【入力形式】

dvpn profile <DVPN プロファイル ID>

no dvpn profile <DVPN プロファイル ID>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
DVPN プロファイル ID	動的VPN プロファイルの ID を指定します。	1 ～ 3000	省略不可

【動作モード】

基本設定モード

【説明】

動的VPN 接続用の設定を行うために、動的VPN プロファイル設定モードに移行します。no を指定した場合には、該当動的VPN プロファイル設定モードの内容がすべて削除されます。

【実行例】

動的VPN プロファイル設定モードに移行します（DVPN プロファイル ID：1）。

```
#configure terminal
(config)# dvpn profile 1
(dvpn-prof)#
```

18.2.2 description

【機能】

説明書きの設定

【入力形式】

description <説明>

no description

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
説明	説明を指定します。	254 文字以内の WORD 型 (*1)	省略不可

*1) 1 文字の空白（スペース）は使用可能です。複数の空白（スペース）は 1 文字にまとめられます。

【動作モード】

動的VPN プロファイル設定モード

【説明】

動的VPN プロファイルの説明書きを設定します。わかりやすい名称を割り当ててください。この説明書きは動作には影響しません。

【実行例】

説明書きを設定します（説明：TEMPLATE）。

```
#configure terminal
(config)#dvpn profile 1
(dvpn-prof)#description TEMPLATE
```

【未設定時】

説明書きは設定されません。

18.2.3 dvpn-interface

【機能】

VPN ピアと通信するインタフェースの設定

【入力形式】

dvpn-interface 1 <インタフェース名> <インタフェース番号> [tunnel route <IP アドレス>]

no dvpn-interface 1 [<インタフェース名> <インタフェース番号> [tunnel route <IP アドレス>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
1	動的VPN クライアント機能で使用するインタフェースの優先度を指定します。	1: 高優先	省略不可
インタフェース名	動的VPN クライアント機能で使用するインタフェース名を指定します。下記を指定できます。 port-channel tunnel	-	
インタフェース番号	動的VPN クライアント機能で使用するインタフェース番号を指定します。	-	
IP アドレス	VPN ピアのIP アドレスに対する経路を設定する場合にIP アドレスを指定します。tunnel route以降のオプションは、インタフェース名をtunnelに指定した際は設定できません。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

【動作モード】

動的VPN プロファイル設定モード

【説明】

動的VPNクライアント機能において、VPNピアと通信するインタフェースを設定します。

また、本コマンドで指定したインタフェースのIPアドレスがIKEの終端アドレスとしてSIPで相手装置に通知されます。

インタフェース名をtunnelに指定した際は、SIP情報交換によって相手から通知された相手のIKE終端アドレスへのホストルート（tunnelルート）を、指定したtunnel interfaceに向けて登録します。

一方インタフェース名をport-channelに指定した際は、tunnelルートを以下の手順で決定し登録します。

1. dvpn-interface コマンドのtunnel route オプションで指定されたIPアドレス
2. dvpn-interface コマンドで指定されたインタフェースが、DHCP(IPv4)利用の場合、Router Option による決定。

上記の手順でホストルートを決定できなかった場合は、経路情報を検索して使用します。ただし、以下の場合IKEネゴシエーションのタイムアウトによるSIPセッションの解放が発生します。

- 相手のIKE終端アドレスへの経路がない場合
- 検索された経路がdvpn-interface コマンドで設定されたインタフェース経由と異なる場合

【実行例】

動的VPNクライアント機能において、VPNピアと通信するインタフェースを設定します（高優先、インタフェース名：port-channel 1、IPアドレス：192.168.1.1）。

```
#configure terminal
(config)#dvpn profile 1
(dvpn-prof)# dvpn-interface 1 port-channel 1 tunnel route 192.168.1.1
```

【未設定時】

動的VPNクライアント機能を使用できません。

18.2.4 keep connect

【機能】

常時接続機能の設定

【入力形式】

keep connect

no keep connect

【動作モード】

動的VPNプロファイル設定モード

【説明】

動的VPNクライアント機能において常時接続機能を有効にします。常時接続機能による接続を行うためには、remoteid設定またはremotenet設定が必須となります。接続試行は設定開始後15秒後に行われ、接続が成功するまで行われます。セッションが削除された場合も、15秒後から接続試行が開始されます。

【実行例】

動的VPNクライアント機能において常時接続機能を有効にします。

```
#configure terminal
(config)#dvpn profile 1
(dvpn-prof)#keep connect
```

【未設定時】

常時接続機能が無効になります。

18.2.5 remotenet

【機能】

接続相手側ネットワークの設定

【入力形式】

remotenet <ネットワーク定義番号> <ネットワークアドレス> <プレフィックス長>

no remotenet [<ネットワーク定義番号> [<ネットワークアドレス> <プレフィックス長>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ネットワーク定義番号	ネットワーク定義番号を指定します。	1 ～ 100	省略不可
ネットワークアドレス	接続相手側ネットワークを指定します。	IPv4 アドレス形式	
プレフィックス長	プレフィックス長を指定します。	IPv4 の場合：0 ～ 32	

【動作モード】

動的VPNプロファイル設定モード

【説明】

動的VPNクライアント機能での接続相手側ネットワークを設定します。ただし同じネットワークの設定は、同一動的VPNプロファイル設定モードかどうかに関わらず複数設定できません。

接続相手側ユーザIDは、本コマンドで指定した接続相手側ネットワークと domain コマンドで指定されたドメイン名を結合して以下のように生成されます。

例)

ネットワークアドレス:192.168.2.0、プレフィックス長:255.255.255.0、ドメイン名:example.com と指定した場合

IPsecIKE)c0a80200/24@example.com

パケット中継契機の発信では、remoteid が設定されていれば、remoteid から接続相手側ユーザIDを生成して発信します。remoteid が設定されていない場合は、先頭remotenet設定から接続相手側ユーザIDを生成して発信します。remotenet設定もない場合は、中継パケットの宛先アドレスと dvpn ip コマンドで設定したプレフィックス長から接続相手側ユーザIDを生成します。

プロファイル指定でのコマンド発信でも、remoteid 設定、先頭remotenet設定の順に参照し、接続相手側ユーザIDを設定します。このとき、どちらの設定もない場合は発信失敗となります。設定による自動発信を行う場合も同様になります。

また、ユーザ ID 指定でのコマンド発信では、以下のいずれかの条件を満たす動的 VPN プロファイルを用いて発信が行われます。

- (1) 実行コマンドで指定した接続相手側ユーザ ID に対応する remoteid 設定または remotenet 設定がある
- (2) remoteid 設定および remotenet 設定がない

ただし、条件 (1) を満たす動的 VPN プロファイルが優先的に用いられます。

一方着信時には、以下のいずれかの条件を満たす動的 VPN プロファイルを用いて着信が行われます。

- (1) INVITE で通知された接続相手側ユーザ ID に対応する remoteid 設定または remotenet 設定がある
- (2) remoteid 設定および remotenet 設定がない

ただし、条件 (1) を満たす動的 VPN プロファイルが優先的に用いられます。

【実行例】

動的 VPN クライアント機能での接続相手側ネットワークを設定します（ネットワーク定義番号：1、ネットワークアドレス：192.168.3.0、プレフィックス長：24）。

```
#configure terminal
(config)#dvpn profile 1
(dvpn-prof)#remotenet 1 192.168.3.0 24
```

【未設定時】

動的 VPN クライアント機能での接続相手側ネットワークを設定しないものとみなされます。

18.2.6 remoteid

【機能】

接続相手側ユーザ名の設定

【入力形式】

remoteid <ユーザ名>

no remoteid [<ユーザ名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ユーザ名	接続相手側ユーザ ID となるユーザ名を指定します。	50 文字以内の英数字と "-", "_", "."	省略不可

【動作モード】

動的 VPN プロファイル設定モード

【説明】

動的 VPN クライアント機能において接続する相手側ユーザ名を設定します。ただし同じユーザ ID の設定は同一動的 VPN プロファイル設定モードかどうかに関わらず、複数設定できません。

ただし、本設定コマンドでは、domain 名は指定しません。接続相手側ユーザ ID は、本コマンドで指定したユーザ名と、domain コマンドで指定したドメイン名を結合して以下のように生成されます。

例)

ユーザ名：honsya、ドメイン名：example.com と指定した場合

honsya@example.com

パケット中継契機の発信では、remoteid が設定されていれば、remoteid から接続相手側ユーザ ID を生成して発信します。remoteid が設定されていない場合は、先頭 remotenet 設定から接続相手側ユーザ ID を生成して発信します。remotenet 設定もない場合は、中継パケットの宛先アドレスと dvpn ip コマンドで設定したプレフィックス長から接続相手側ユーザ ID を生成します。

プロファイル指定でのコマンド発信でも、remoteid 設定、先頭 remotenet 設定の順に参照し、接続相手側ユーザ ID を設定します。この場合は、どちらの設定もない場合は発信失敗となります。設定による自動発信を行う場合も同様になります。

また、ユーザ ID 指定でのコマンド発信では、以下のいずれかの条件を満たす動的 VPN プロファイルを用いて発信が行われます。

- (1) 実行コマンドで指定した接続相手側ユーザ ID に対応する remoteid 設定または remotenet 設定がある
- (2) remoteid 設定および remotenet 設定がない

ただし、条件 (1) を満たす動的 VPN プロファイルが優先的に用いられます。

一方着信時には、以下のいずれかの条件を満たす動的 VPN プロファイルを用いて着信が行われます。

- (1) INVITE で通知された接続相手側ユーザ ID に対応する remoteid 設定または remotenet 設定がある
- (2) remoteid 設定および remotenet 設定がない

ただし、条件 (1) を満たす動的 VPN プロファイルが優先的に用いられます。

【実行例】

接続相手側ユーザ ID となるユーザ名を設定します（ユーザ名：honsya）。

```
#configure terminal
(config)#dvpn profile 1
(dvpn-prof)#remoteid honsya
```

【未設定時】

動的 VPN クライアント機能での接続相手側ユーザ名を設定しないものとみなされます。

remotenet 設定を参照します。

18.2.7 set dvpn client

【機能】

動的 VPN クライアント定義番号の設定

【入力形式】

set dvpn client <クライアント定義番号>

no set dvpn client [<クライアント定義番号>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
クライアント定義番号	動的 VPN クライアント定義番号を指定します。	1～6	省略不可

【動作モード】

動的VPN プロファイル設定モード

【説明】

この動的VPN プロファイルで使用する動的VPN クライアント定義番号を設定します。

【実行例】

動的VPN クライアント情報を設定します（クライアント定義番号：1）。

```
#configure terminal
(config)#dvpn profile 1
(dvpn-prof)#set dvpn client 1
```

【未設定時】

動的VPN クライアント機能を使用できません。

18.2.8 watch

【機能】

動的端末監視の設定

【入力形式】

watch source <送信元 IP アドレス> [survey-map <survey マップ名> [idleonly]]

no watch [source <送信元 IP アドレス> [survey-map <survey マップ名> [idleonly]]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
送信元 IP アドレス	送信元の IP アドレスを指定します。	IPv4 アドレス形式	省略不可
survey マップ名	survey マップ名を指定します。	254 文字以内の WORD 型	survey 機能のデフォルト値で動作します。
idleonly	IPsec tunnel の受信状態を確認して無受信監視を行います。	-	常時監視を行います。

【動作モード】

動的VPN プロファイル設定モード

【説明】

動的VPN クライアント機能において、動的端末監視を有効にし、端末監視の送信元アドレスを設定します。

動的端末監視では、SIP で相手装置から通知された監視代表アドレスを宛先として、ICMP echo リクエストを送信します。また、本コマンドで指定した送信元アドレスは SIP で相手装置に監視代表アドレスとして通知されます。送信元と宛先アドレスのバージョンが一致しない場合は、ICMP echo リクエストの送信は行われません。

survey-map を指定しない場合は、デフォルト端末監視パラメタで監視を行います。パラメタを変える必要がある場合は、survey-map に変更する内容を登録します。

端末接続監視の結果によって tunnel インタフェースの up/down は同期されます。

ESP パケットの受信がある間に ICMP echo リクエストの送信を行わない場合は、"idleonly" を指定します。

【実行例】

動的 VPN クライアント機能において、端末監視の送信元アドレスを設定します（送信元 IP アドレス：192.168.1.1）。

```
#configure terminal
(config)#dvpn profile 1
(dvpn-prof)#watch source 192.168.1.1
```

【未設定時】

動的 VPN クライアント機能での、動的端末監視機能を使用できません。

18.3 DVPN クライアント情報の設定

18.3.1 dvpn client

【機能】

動的VPNクライアント設定モードへの移行

【入力形式】

dvpn client <クライアント定義番号>

no dvpn client <クライアント定義番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
クライアント定義番号	動的VPNクライアント定義番号を指定します。	1～6	省略不可

【動作モード】

基本設定モード

【説明】

動的VPNクライアント設定モードに移行します。noを指定した場合には、該当動的VPNクライアント設定モードの内容がすべて削除されます。

【実行例】

動的VPNクライアント設定モードに移行します（クライアント定義番号：1）。

```
#configure terminal
(config)# dvpn client 1
(config-dvpn-client)#
```

18.3.2 client-priority

【機能】

優先度の指定

【入力形式】

client-priority <優先度>

no client-priority [<優先度>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
優先度	クライアントの優先度を指定します。	0～10	省略不可

【動作モード】

動的VPNクライアント設定モード

【説明】

複数の動的VPNクライアントが、同じ登録情報（ユーザID）で動的VPNサーバに登録されたときの、優先度を設定します。優先度は数値の小さい方がより高い優先度を示します。同じ優先度で動的VPNサーバに登録された場合、最後に登録されたクライアントが有効となります。

0を指定した際は、優先度をサーバに通知しません。

【実行例】

クライアントの優先度を設定します（優先度：2）。

```
#configure terminal
(config)# dvpn client 1
(conf-dvpn-client)#priority 2
```

【未設定時】

優先度 10 で動作します。

18.3.3 domain

【機能】

動的VPNクライアント機能で使用するドメイン名の設定

【入力形式】

domain <ドメイン名>

no domain [<ドメイン名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ドメイン名	ドメイン名を指定します。	80文字以内の DOMAINWORD型	省略不可

【動作モード】

動的VPNクライアント設定モード

【説明】

動的VPNクライアント機能で使用するドメイン名を設定します。

【実行例】

動的VPNクライアント機能で使用するドメイン名を設定します（ドメイン名：example.com）。

```
#configure terminal
(config)# dvpn client 1
(conf-dvpn-client)# domain example.com
```

【未設定時】

動的VPNクライアント機能を使用できません。

18.3.4 dvpn-server address

【機能】

動的VPNサーバアドレスの設定

【入力形式】

dvpn-server {1 | 2} address {<IP アドレス> | domain <サーバ名> [{v4 | v6}]} [<ポート番号>]

no dvpn-server {1 | 2} address [{<IP アドレス> | domain <サーバ名> [{v4 | v6}]} [<ポート番号>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
1 2	動的VPNサーバの定義番号を指定します。	1: 高優先 2: 低優先	省略不可
IP アドレス	動的VPNサーバアドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
サーバ名	動的VPNサーバ名をFQDNで指定します。	80文字以内の DOMAINWORD型	省略不可
v4 v6	ドメイン名の名前解決をIPv4、IPv6のどちらで行うか指定します。	v4 v6	sip-local address 1で設定したIPアドレスのバージョンに従います。sip-local address 1で指定したインタフェースにIPv4とIPv6両方のアドレスが設定されていた場合は、IPv6で動作します。
ポート番号	動的VPNサーバが使用するポート番号を指定します。	1～65534	5070

【動作モード】

動的VPNクライアント設定モード

【説明】

動的VPNクライアント機能を使用する場合の動的VPNサーバアドレスを設定します。2つ設定した場合は、パラメタ"1"を指定したアドレスをプライマリサーバ、"2"を指定したアドレスをセカンダリサーバのアドレスとして動作します。

動的VPNクライアント機能では、SIPサーバに送信したリクエストメッセージ(REGISTER, INVITE)がタイムアウトした場合、またはサーバエラー(5xx)を受信した場合にSIPサーバを切り替えます。

【実行例】

動的VPNクライアント機能を使用する場合の動的VPNサーバアドレスを設定します（高優先、IPアドレス：192.168.1.1）。

```
#configure terminal
(config)# dvpn client 1
(conf-dvpn-client)# dvpn-server 1 address 192.168.1.1
```

【未設定時】

動的VPNクライアント機能を使用できません。

18.3.5 dvpn-server username

【機能】

認証情報の設定

【入力形式】

```
dvpn-server {1 | 2} username <ユーザ名> password <パスワード> [{secret | private}] [encrypted]]
```

```
no dvpn-server {1 | 2} username [<ユーザ名> password <パスワード> [{secret | private}] [encrypted]]]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
1 2	動的VPNサーバの定義番号を指定します。	1: 高優先 2: 低優先	省略不可
ユーザ名	ユーザ名を指定します。	50文字以内のSTRING型	
パスワード	パスワードを指定します。	50文字以内のSTRING型	
secret private	パスワードとして使用する文字列の暗号化／復号化に、共通の鍵を使用するか、固有の鍵を使用するかを設定します。	secret: 共通の鍵を使用する private: 固有の鍵を使用する	暗号化せずに保存
encrypted	パスワードとして使用する文字列が暗号化されていることを示します。	-	非暗号化文字列として扱う

【動作モード】

動的VPNクライアント設定モード

【説明】

動的VPNクライアント機能において、SIPのREGISTERおよびINVITEに付与する認証情報（ユーザ名とパスワード）を設定します。

"secret"を指定した場合は、すべてのSi-R GX500に共通の鍵を使って暗号化／復号化し、"private"を指定した場合は、装置固有の鍵を使って暗号化／復号化します。encryptedオプションを付けた場合は、入力された文字列を暗号化された文字列と判断しコンフィグに保存します。

"show running.cfg"などで内容を確認すると、暗号化されたパスワードの形式で表示されます。

【実行例】

動的VPNクライアント機能における認証情報を設定します（高優先、ユーザ名：id-b@dvpn、パスワード：pwd-b@dvpn）。

```
#configure terminal
(config)# dvpn client 1
(conf-dvpn-client)# dvpn-server 1 username id-b@dvpn password pwd-b@dvpn
```

【未設定時】

動的VPNクライアント機能において、SIPのREGISTERおよびINVITEに認証情報を付与しません。

18.3.6 dvpn sip encode-off

【機能】

SIP 交換情報をエンコードの設定

【入力形式】

dvpn sip encode-off

no dvpn sip encode-off

【動作モード】

基本設定モード

【説明】

動的 VPN クライアント機能で、SIP 交換情報をエンコードしない場合に設定します。

【実行例】

SIP 交換情報をエンコードしません。

```
#configure terminal
(config)# dvpn sip encode-off
```

【未設定時】

base64 でエンコードされます。

18.3.7 localnet

【機能】

自側ネットワークの設定

【入力形式】

localnet <ネットワーク定義番号> <ネットワークアドレス> <プレフィックス長> [register-off]

no localnet [<ネットワーク定義番号> [<ネットワークアドレス> <プレフィックス長> [register-off]]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ネットワーク定義番号	ネットワーク定義番号を指定します。	1 ~ 100	省略不可
ネットワークアドレス	動的VPNサーバに登録する自側ネットワークアドレスを指定します。	IPv4 アドレス形式	
プレフィックス長	プレフィックス長を指定します。	IPv4 の場合：0 ~ 32	
register-off	本コマンドで生成される自側ユーザIDをサーバに登録しない場合に指定します。	-	サーバに登録を行う

【動作モード】

動的VPNクライアント設定モード

【説明】

動的VPNクライアント機能において、動的VPNサーバに登録する自側ネットワークを設定します。ただし、register-off指定のない同一のネットワーク設定は、同一動的VPNクライアント設定モードかどうかに関わらず複数設定できません。

また、複数設定した場合は、ネットワーク定義番号の小さいネットワークから順に、X-From/X-Toヘッダに付加されます。さらに、本設定で指定したすべての自側ネットワークは、SIP情報交換で経路情報として相手に通知されます。ただし、register-offオプションを指定したネットワークについては、動的VPNサーバへの登録、およびX-From/X-Toヘッダへの付加は行われず、経路情報としての通知にのみ用いられます。

動的VPNサーバに登録される自側ユーザIDは、本コマンドで指定した自側ネットワークと、domainコマンドで指定されたドメイン名を結合して以下のように生成されます。

例)

ネットワークアドレス：192.168.1.0、プレフィックス長：24、ドメイン名：example.comと指定した場合

IPsecIKE)c0a80100/24@example.com

パケット中継契機での発信で、参照元動的VPNプロファイルにremoteid設定またはremotenet設定がある場合は、localid設定、localnet 1設定の順に参照し、自側ユーザIDを生成します。設定による自動発信の際も同様の順に参照し、自側ユーザIDを生成します。

パケット中継契機での発信で、参照元動的VPNプロファイルにremoteid設定またはremotenet設定がない場合は、中継パケットの送信元アドレスを包含するlocalnet設定を用いて発信が行われます。ない場合は発信失敗となります。

プロファイル指定およびユーザID指定でのコマンド発信時には、localid設定から自側ユーザIDを生成して発信を行います。localid設定がない場合はコマンドでの発信は行えません。

着信時には、INVITEで通知された自側ユーザIDと完全一致するlocalid設定またはlocalnet設定がある場合に正常応答を返します。

【実行例】

動的VPNクライアント機能において、動的VPNサーバに登録する自側ネットワークを設定します（ネットワーク定義番号：1、ネットワークアドレス：192.168.2.0、プレフィックス長：24）。

```
#configure terminal
(config)# dvpn client 1
(conf-dvpn-client)# localnet 1 192.168.2.0 24
```

【未設定時】

ネットワーク定義番号に1を指定したlocalnet設定がない場合、動的VPNクライアント機能を使用できません。

18.3.8 localid

【機能】

自ユーザ名の設定

【入力形式】

localid <ユーザ名>

no localid [<ユーザ名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ユーザ名	自側ユーザ ID となるユーザ名を指定します。	50文字以内の英数字と"-","_", "."	省略不可

【動作モード】

動的 VPN クライアント設定モード

【説明】

動的 VPN クライアント機能において、動的 VPN サーバに登録する自ユーザ名を設定します。ただし同じユーザ ID の設定は同一動的 VPN クライアント設定モードかどうかに関わらず複数設定できません。

動的 VPN サーバに登録される自側ユーザ ID は、本コマンドで指定したユーザ名と、domain コマンドで指定したドメイン名を結合して以下のように生成されます。

例)

ユーザ名：shisya、ドメイン名：example.com と指定した場合

shisya@example.com

dvpn connect コマンドで動的 VPN の接続を行いたい場合に必ず指定してください。

パケット中継契機での発信で、参照元動的 VPN プロファイルに remoteid 設定または remotenet 設定がある場合は、localid 設定、localnet 1 設定の順に参照し自側ユーザ ID を生成します。設定による自動発信の際も同様の順に参照し自側ユーザ ID を生成します。

パケット中継契機での発信で、参照元動的 VPN プロファイルに remoteid 設定または remotenet 設定がない場合は、中継パケットの送信元アドレスを包含する localnet 設定を用いて発信が行われます。ない場合は発信失敗となります。

プロファイル指定およびユーザ ID 指定でのコマンド発信時には、localid 設定から自側ユーザ ID を生成して発信を行います。localid 設定がない場合はコマンドでの発信は行えません。

着信時には、INVITE で通知された自側ユーザ ID と完全一致する localid 設定または localnet 設定がある場合に正常応答を返します。

【実行例】

自側ユーザ ID となるユーザ名を設定します（ユーザ ID：shisya）。

```
#configure terminal
(config)# dvpn client 1
(conf-dvpn-client)#localid shisya
```

【未設定時】

動的 VPN サーバに登録する自側ユーザ名を設定しないものとみなされます。

18.3.9 sip expire-register

【機能】

REGISTER 有効期限の設定

【入力形式】

sip expire-register <Expires 値>

no sip expire-register [<Expires 値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
Expires 値	REGISTER 有効期限（単位：秒）を指定します。	90 ～ 86400	省略不可

【動作モード】

動的 VPN クライアント設定モード

【説明】

動的 VPN クライアント機能の REGISTER 有効期限（単位：秒）を設定します。

【実行例】

REGISTER 有効期限（単位：秒）を設定します（タイマ値：1000 秒）。

```
#configure terminal
(config)# dvpn client 1
(conf-dvpn-client)# sip expire-register 1000
```

【未設定時】

REGISTER 有効期限 3600 秒で動作します。

18.3.10 sip expire-session

【機能】

セッション更新間隔の設定

【入力形式】

sip expire-session <タイマ値>

no sip expire-session [<タイマ値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
タイマ値	SIP のセッション更新間隔（単位：秒）を指定します。	90 ～ 3600	省略不可

【動作モード】

動的VPNクライアント設定モード

【説明】

動的VPNクライアント機能で使用するSIPのセッション更新間隔（単位：秒）を設定します。

【実行例】

セッション更新間隔（単位：秒）を設定します（タイム値：1000 秒）。

```
#configure terminal
(config)# dvpn client 1
(conf-dvpn-client)# sip expire-session 1000
```

【未設定時】

セッション更新間隔 300 秒で動作します。

18.3.11 sip expire-session-disable

【機能】

SIPのセッション更新の無効化の設定

【入力形式】

sip expire-session-disable

no sip expire-session-disable

【動作モード】

動的VPNクライアント設定モード

【説明】

動的VPNクライアント機能で、SIPのセッション更新を無効にします。

【実行例】

動的VPNクライアント機能で、SIPのセッション更新を無効にします。

```
#configure terminal
(config)# dvpn client 1
(conf-dvpn-client)# sip expire-session-disable
```

【未設定時】

SIPセッションの更新を行います。

18.3.12 sip encrypt-enable

【機能】

SIP暗号化の設定

【入力形式】

sip encrypt-enable

no sip encrypt-enable

【動作モード】

動的VPNクライアント設定モード

【説明】

動的VPNクライアント機能で、SIP 暗号化を行う場合に設定します。

【実行例】

動的VPNクライアント機能で、SIP 暗号化を行います。

```
#configure terminal
(config)# dvpn client 1
(conf-dvpn-client)# sip encrypt-enable
```

【未設定時】

SIP 暗号化を行いません。

18.3.13 sip local-address

【機能】

SIP の送信元アドレスの設定

【入力形式】

sip local-address 1 {<送信元アドレス> | <インタフェース名> <インタフェース番号>}

no sip local-address [1 {<送信元アドレス> | <インタフェース名> <インタフェース番号> }]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
1	動的VPNクライアント機能で使用するSIPの送信元アドレスの優先度を指定します。	1: 高優先	省略不可
送信元アドレス	動的VPNクライアント機能で使用するSIPの送信元アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	
インタフェース名	インタフェース名を指定します。下記を指定可能です。 port-channel tunnel	-	
インタフェース番号	インタフェース番号を指定します。	-	

【動作モード】

動的VPNクライアント設定モード

【説明】

動的VPNクライアント機能での、SIPの送信元アドレスを設定します。

送信元アドレスのIPバージョンは、SIPサーバのIPバージョンと一致する必要があります。

【実行例】

動的VPNクライアント機能でのSIPの送信元アドレスを設定します（高優先、IPアドレス：192.168.2.1）。

```
#configure terminal
(config)# dvpn client 1
(conf-dvpn-client)# sip local-address 1 192.168.2.1
```

【未設定時】

動的VPNクライアント機能を使用できません。

18.4 DVPN サーバの設定

18.4.1 dvpn server auth aaa

【機能】

参照する AAA の認証グループ名の設定

【入力形式】

dvpn server 1 auth aaa <認証グループ名>

no dvpn server 1 auth aaa [<認証グループ名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
認証グループ名	認証グループ名を指定します。	63 文字以内の CDATA 型	省略不可

【動作モード】

基本設定モード

【説明】

動的 VPN サーバが認証を行う場合に参照する AAA の認証グループ名を設定します。

【実行例】

動的 VPN サーバが認証を行う場合に参照する AAA の認証グループ名を設定します（認証グループ名：AUTH_GROUP1）。

```
#configure terminal
(config)# dvpn server auth aaa AUTH_GROUP1
```

【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。

18.4.2 dvpn server auth use

【機能】

動的 VPN サーバ認証を行う設定

【入力形式】

dvpn server 1 auth use enable

no dvpn server 1 auth use [enable]

【動作モード】

基本設定モード

【説明】

動的VPNサーバで認証を行う場合に設定します。

【実行例】

動的VPNサーバで認証を行う設定をします。

```
#configure terminal
(config)# dvpn server auth use enable
```

【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。

18.4.3 dvpn server domain

【機能】

動的VPNサーバが管理するドメイン名の設定

【入力形式】

dvpn server 1 domain <ドメイン名>

no dvpn server 1 domain [<ドメイン名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ドメイン名	ドメイン名を指定します。	80文字以内の DOMAINWORD型	省略不可

【動作モード】

基本設定モード

【説明】

動的VPNサーバが管理するドメイン名を設定します。

【実行例】

動的VPNサーバが管理するドメイン名を設定します（ドメイン名：netl）。

```
#configure terminal
(config)# dvpn server domain netl
```

【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。

18.4.4 dvpn server sips max-sessions

【機能】

SIPS を利用した際の最大同時接続数の設定

【入力形式】

dvpn server 1 sips max-sessions <セッション数>

no dvpn server 1 sips max-sessions [<セッション数>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
セッション数	sips を使った際の SIP セッション最大同時接続数を指定します。	1 ～ 3000	省略不可

【動作モード】

基本設定モード

【説明】

動的 VPN サーバ機能で、SIPS を利用した際の最大同時接続数を指定します。

【実行例】

動的 VPN サーバ機能で、SIPS を利用した際の最大同時接続数を 3000 に指定します。

```
#configure terminal
(config)# dvpn server 1 sip max-sessions 3000
```

【未設定時】

セッション数 600 として動作します。

18.4.5 dvpn server use enable

【機能】

動的 VPN サーバ利用の設定

【入力形式】

dvpn server use enable

no dvpn server use enable

【動作モード】

基本設定モード

【説明】

動的 VPN サーバを利用するかどうかを設定します。

【実行例】

動的 VPN サーバを利用する設定をします。

```
#configure terminal
(config)# dvpn server use enable
```

【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。

第19章 データコネクトの設定



この章では、データコネクトの設定に関するコマンドについて説明します。

19.1 SIP の設定

19.1.1 incoming-call disable

【機能】

ピアからの着信抑制時の設定

【入力形式】

incoming-call disable

no incoming-call disable

【動作モード】

SIP プロファイル設定モード

【説明】

該当 SIP プロファイルに設定されたピアからの着信を抑制する際に設定します。

【実行例】

着信を抑制します。

```
#configure terminal
(config)#ngn sip profile SIP-PROFILE-A
(sip-prof)#incoming-call disable
```

【未設定時】

他の着信制限に該当していない状況で、着信を許可します。

19.1.2 ipsec-timeout

【機能】

SIP セッションを切断するまでの時間の設定（接続相手単位）

【入力形式】

ipsec-timeout <IPsec タイムアウト時間>

no ipsec-timeout [<IPsec タイムアウト時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
IPsec タイムアウト時間	SIP セッションの確立後、IPsec SA が確立しない場合のタイムアウト時間（単位：秒）を指定します。	0 ～ 600	省略不可

【動作モード】

SIP プロファイル設定モード、SIP RADIUS 認証プロファイル設定モード

【説明】

データコネクト機能で、SIP セッションの確立後、IPsec SA が確立しない場合に、SIP セッションの切断を行うまでの時間を、接続相手単位で設定します。

IPsec タイムアウト時間を "0" に指定した場合は、IPsec SA 非確立時の SIP セッションの切断を行いません。

【実行例】

SIP セッションの確立後、IPsec SA が確立しない場合に、SIP セッションの切断を行うまでの時間を、接続相手単位で設定します (IPsec タイムアウト時間:30 秒)。

```
#configure terminal
(config)#ngn sip profile-radius
(sip-prof-radius)#ipsec-timeout 30
```

【未設定時】

ngn sip agent ipsec-timeout コマンドの設定に従います。

19.1.3 ngn enable

【機能】

SIP 情報の取得

【入力形式】

ngn enable

no ngn enable

【動作モード】

ip dhcp client プロファイル設定モード、ipv6 dhcp client プロファイル設定モード

【説明】

NGN 網を介して通信を行うための SIP 情報を取得します。

【実行例】

NGN 網を介して通信を行うための SIP 情報を取得します。

```
#configure terminal
(config)# ip dhcp client-profile DHCP
(config-dhcp DHCP)#ngn enable
```

【未設定時】

NGN 網を介して通信を行うための SIP 情報を取得しません。

19.1.4 ngn sip agent bind port-channel

【機能】

SIP コントロールパケット、メディアストリームパケットの送受信を行うインタフェースの指定

【入力形式】

ngn sip agent <エントリ番号> bind port-channel <インタフェース番号> [manual]

no ngn sip agent <エントリ番号> bind port-channel [<インタフェース番号> [manual]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エントリ番号	SIP user agentのエントリ番号を指定します。	0: 高優先	省略不可
インタフェース番号	インタフェース番号を指定します。	-	省略不可
manual	データコネクト機能で必要な情報を設定で指定する際に設定します。	-	DHCP(DHCPv6)クライアント機能を使ってデータコネクト機能で必要な情報を取得します。

【動作モード】

基本設定モード

【説明】

データコネクト機能を利用する際の SIP コントロールパケット、メディアストリームパケットの送受信を行うインタフェースを指定します。

データコネクト機能で使用する SIP で必要な情報（SIP サーバアドレス、SIP ドメイン、自局電話番号）を設定で指定する場合、manual オプションを指定します。

フィルタ／QoS／データコネクト QoS／DVPN ACL／ポリシールーティングのクラシファイエントリはすべて共用です。各機能でエントリを使用していると、データコネクト QoS のエントリが入らないことがあります。

【実行例】

port-channel 1 を使ってデータコネクト機能を利用します（DHCP クライアントを利用）。

```
#configure terminal
(config)#ngn sip agent 0 bind port-channel 1
```

【未設定時】

データコネクト機能が利用できません。

19.1.5 ngn sip agent call-timeout

【機能】

SIP 発信キャンセルタイマ値の設定

【入力形式】

ngn sip agent <エントリ番号> call-timeout <SIP 発信キャンセルタイマ値>

no ngn sip agent <エントリ番号> call-timeout [<SIP 発信キャンセルタイマ値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エントリ番号	SIP user agentのエントリ番号を指定します。	0：高優先	省略不可
SIP 発信キャンセルタイマ値	SIP 発信キャンセルタイマ値を指定します。	5～60（秒）	省略不可

【動作モード】

基本設定モード

【説明】

SIP 発信時に指定された時間内で SIP 接続が完了しなかった際に、SIP 発信をキャンセルする場合に指定します。

【実行例】

SIP 発信キャンセルタイマ値を 10 秒に設定します（エントリ番号：0、SIP 発信キャンセルタイマ値：10 秒）。

```
#configure terminal
(config)#ngn sip agent 0 call-timeout 10
```

【未設定時】

SIP パケットの応答待ちタイムアウトまで接続シーケンスを継続します。

19.1.6 ngn sip agent charge-setting

【機能】

課金額計算で用いる値の設定

【入力形式】

ngn sip agent <エントリ番号> charge-setting {64k | 512k | 1m | <帯域値>} <料金> [<時間>]

no ngn sip agent <エントリ番号> charge-setting {64k | 512k | 1m | <帯域値>} [<料金> [<時間>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エントリ番号	SIP user agentのエントリ番号を指定します。	0:高優先	省略不可
64k 512k 1m	SIPセッションの帯域を指定します。	64k:64Kbps 512k:512Kbps 1m:1Mbps	省略不可
帯域値	SIPセッションの帯域（単位：kbps）を指定します。	1～1000000	省略不可
料金	時間（デフォルト 30 秒）あたりの課金額（単位：円）を指定します。	1.0～100.0	省略不可
時間	指定した時間単位（単位：秒）で SIP 接続の課金額を計算します。	1～3600	30 秒

【動作モード】

基本設定モード

【説明】

データコネクト機能において課金額計算で用いる値（金額／時間）を指定します。

帯域に対する課金額計算で用いる値を最大 100 件有効にできます。100 件以上設定した場合、コンフィグで表示される順番で先頭から 100 件が有効となり、以降は無効となります。

【実行例】

データコネクト機能において課金額計算で用いる値（金額／時間）を指定します（帯域値：64kbps、料金：2 円、時間：30 秒）。

```
#configure terminal
(config)#ngn sip agent 0 charge-setting 64k 2 30
```

【未設定時】

以下のように課金額計算を行います。

1～64kbps：	1 円／ 30 秒
65～512kbps：	1.5 円／ 30 秒
513kbps～：	2 円／ 30 秒

19.1.7 ngn sip agent control session

【機能】

セッションの同時接続数の最大値指定

【入力形式】

ngn sip agent <エントリ番号> control session <同時接続数>

no ngn sip agent <エントリ番号> control session [<同時接続数>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エントリ番号	SIP user agentのエントリ番号を指定します。	0: 高優先	省略不可
同時接続数	SIP 同時接続数を指定します。	1 ～ 300	省略不可

【動作モード】

基本設定モード

【説明】

SIP の発信／着信による確立するセッションの同時接続数の最大値を指定します。

同時接続数に達したあとの発信は行われず、着信はすべて拒否します。

【実行例】

最大同時接続数を指定します（最大同時接続数：100 セッション）。

```
#configure terminal
(config)#ngn sip agent 0 control session 100
```

【未設定時】

最大同時接続数は 300 セッションで動作します。

19.1.8 ngn sip agent ipsec-timeout

【機能】

SIP セッションを切断するまでの時間の設定（回線単位）

【入力形式】

ngn sip agent <エントリ番号> ipsec-timeout <IPsec タイムアウト時間>

no ngn sip agent <エントリ番号> ipsec-timeout [<IPsec タイムアウト時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エントリ番号	SIP user agentのエントリ番号を指定します。	0: 高優先	省略不可
IPsec タイムアウト時間	SIP セッションの確立後、IPsec SA が確立しない場合のタイムアウト時間（単位：秒）を指定します。	0 ～ 600	省略不可

【動作モード】

基本設定モード

【説明】

データコネクト機能で、SIP セッションの確立後、IPsec SA が確立しない場合に、SIP セッションの切断を行うまでの時間を、回線単位で設定します。

IPsec タイムアウト時間を "0" に指定した場合は、IPsec SA 非確立時の SIP セッションの切断を行いません。

【実行例】

SIP セッションの確立後、IPsec SA が確立しない場合に、SIP セッションの切断を行うまでの時間を、回線単位で設定します (IPsec タイムアウト時間:30 秒)。

```
#configure terminal
(config)#ngn sip agent 0 ipsec-timeout 30
```

【未設定時】

IPsec タイムアウト時間 20 秒で動作します。

19.1.9 ngn sip agent limit

【機能】

SIP による発信抑制

【入力形式】

ngn sip agent < エントリ番号 > limit {second < 時間 > | charge < 金額 >} [disconnect]

no ngn sip agent < エントリ番号 > limit {second [< 時間 >] | charge [< 金額 >]} [disconnect]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エントリ番号	SIP user agent のエントリ番号を指定します。	0: 高優先	省略不可
時間	累計通信時間による発信抑制を行うための時間 (単位: 秒) を指定します。	1 ~ 31536000	省略不可
金額	累計課金額による発信抑制を行うための金額 (単位: 円) を指定します。	1 ~ 999999	省略不可
disconnect	設定した上限時間、金額に達した際、現在接続している SIP の切断を行う場合に指定します。	-	現在接続している SIP の切断を行わない

【動作モード】

基本設定モード

【説明】

回線単位で SIP による発信を累計通信時間、累計課金額により、発信抑制を行います。

累計通信時間、累計課金額、はそれぞれ 1 つずつ指定できます。

条件を満たしたあとに発信を行いたい場合は、設定をクリアするか、clear ngn account コマンドを使用する必要があります。

disconnect オプションを指定すると、接続中の SIP について一定時間ごとに発信による累計通信時間、累計課金額の監視を行い、指定した時間、金額に到達した際に SIP 切断を行います。disconnect オプションを指定しない場合は、指定した時間、金額に到達しても SIP 切断を行わないのでご注意ください。

【実行例】

累計通信時間、累計課金額により発信抑制します（累計時間：30 分、累計課金額：1000 円）。

```
#configure terminal
(config)#ngn sip agent 0 limit second 1800
(config)#ngn sip agent 0 limit charge 1000
```

【未設定時】

課金額、発信時の接続時間による発信抑制を行いません。

19.1.10 ngn sip agent proxy server address

【機能】

SIP プロキシサーバアドレスの指定

【入力形式】

ngn sip agent <エントリ番号> proxy server {ipv4 | ipv6} address <IP アドレス>

no ngn sip agent <エントリ番号> proxy server {ipv4 | ipv6} address [<IP アドレス>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エントリ番号	SIP user agentのエントリ番号を指定します。	0: 高優先	省略不可
ipv4 ipv6	SIP機能でプロキシサーバのIPアドレスについて用いるプロトコルを指定します。	ipv4 ipv6	省略不可
IP アドレス	SIP プロキシサーバアドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

【動作モード】

基本設定モード

【説明】

DHCP(DHCPv6)クライアント機能を使用せず、SIP 機能を利用する際の SIP プロキシサーバアドレスを指定します。

ngn sip agent bind port-channel コマンドで manual オプションの指定がなかった場合、本設定は無効となります。

【実行例】

SIP プロキシサーバの IP アドレスを指定します（SIP プロキシサーバ：192.0.3.1）。

```
#configure terminal
(config)#ngn sip agent 0 proxy server ipv4 address 192.0.3.1
```

【未設定時】

設定による SIP プロキシサーバを用いたデータコネクト動作を行いません。

19.1.11 ngn sip agent proxy server domain

【機能】

装置 SIP ドメインの指定

【入力形式】

ngn sip agent <エントリ番号> proxy server {ipv4 | ipv6} domain <ドメイン名>

no ngn sip agent <エントリ番号> proxy server {ipv4 | ipv6} domain [<ドメイン名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エントリ番号	SIP user agentのエントリ番号を指定します。	0: 高優先	省略不可
ipv4 ipv6	SIP 機能で自装置 SIP ドメインについて用いる IP プロトコルを指定します。	ipv4 ipv6	省略不可
ドメイン名	SIP 機能で用いる自装置のドメインを指定します。	253 文字以内の DOMAINWORD 型	省略不可

【動作モード】

基本設定モード

【説明】

DHCP(DHCPv6)クライアント機能を使用せず、SIP 機能を利用する際の自装置 SIP ドメインを指定します。

ngn sip agent bind port-channel コマンドで manual オプションの指定がなかった場合、本設定は無効となります。

【実行例】

SIP ドメインを指定します (プロトコル: IPv4、SIP ドメイン: ntt-east.ne.jp)。

```
#configure terminal
(config)#ngn sip agent 0 proxy server ipv4 domain ntt-east.ne.jp
```

【未設定時】

設定によるドメインを用いたデータコネクツ動作を行いません。

19.1.12 ngn sip agent registrar expire

【機能】

SIP レジストラの有効期限指定

【入力形式】

ngn sip agent <エントリ番号> registrar expire <タイマ値>

no ngn sip agent <エントリ番号> registrar expire [<タイマ値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エントリ番号	SIP user agentのエントリ番号を指定します。	0: 高優先	省略不可
タイマ値	SIPレジストラの有効期限（単位：秒）を指定します。	10～864000	省略不可

【動作モード】

基本設定モード

【説明】

SIP レジストラの有効期限を指定します。

【実行例】

SIP レジストラの有効期限を指定します（有効期限：3600 秒）。

```
#configure terminal
(config)#ngn sip agent 0 registrar expire 3600
```

【未設定時】

有効期限は 3600 秒で動作します。

19.1.13 ngn sip agent registrar retry

【機能】

SIP レジストラの再登録時間指定

【入力形式】

ngn sip agent <エントリ番号> registrar retry <タイマ値>

no ngn sip agent <エントリ番号> registrar retry[<タイマ値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エントリ番号	SIP user agentのエントリ番号を指定します。	0: 高優先	省略不可
タイマ値	SIPレジストラの再登録時間（単位：秒）を指定します。	10～864000	省略不可

【動作モード】

基本設定モード

【説明】

SIP レジストラの再登録時間を指定します。

【実行例】

SIP レジストラの再登録時間を指定します（再登録時間：300 秒）。

```
#configure terminal
(config)#ngn sip agent 0 registrar retry 300
```

【未設定時】

再登録時間は 300 秒で動作します。

19.1.14 ngn sip agent registrar server address

【機能】

SIP レジストラサーバアドレスの指定

【入力形式】

ngn sip agent <エントリ番号> registrar server address <IP アドレス>

no ngn sip agent <エントリ番号> registrar server [address <IP アドレス>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エントリ番号	SIP user agent のエントリ番号を指定します。	0: 高優先	省略不可
IP アドレス	SIP レジストラサーバアドレスを指定します。	IPv4 アドレス形式	省略不可

【動作モード】

基本設定モード

【説明】

DHCP(DHCPv6)クライアント機能を使用せず、SIP 機能を利用する際の SIP レジストラサーバアドレスを指定します。

ngn sip agent bind port-channel コマンドで manual オプションの指定がなかった場合、本設定は無効となります。

【実行例】

SIP レジストラサーバの IP アドレスを指定します（SIP レジストラサーバ：192.168.0.1）。

```
#configure terminal
(config)#ngn sip agent 0 registrar server address 192.168.0.1
```

【未設定時】

設定による SIP レジストラサーバを用いたデータコネクト動作を行いません。

19.1.15 ngn sip agent sessiontimer default

【機能】

SIP session timer の有効期限指定

【入力形式】

ngn sip agent <エントリ番号> sessiontimer default <タイマ値>

no ngn sip agent <エントリ番号> sessiontimer default [<タイマ値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エントリ番号	SIP user agent のエントリ番号を指定します。	0: 高優先	省略不可
タイマ値	SIP Session timer の有効期限（単位：秒）を指定します。	10 ～ 86400	省略不可

【動作モード】

基本設定モード

【説明】

SIP session timer の有効期限を指定します。指定した時間の半分か経過すると SIP セッションの更新が行われます。

SIP セッションの更新動作は発信側か着信側かで異なります。

発信側：SIP セッション確立からタイマ値の半分経過で SIP セッションの更新を行います。

着信側：発信側から SIP セッションの更新を依頼されていた場合、SIP セッション確立からタイマ値の半分経過で SIP セッションの更新を行います。発信側から SIP セッションの更新を依頼されていない場合、自装置から SIP セッションの更新は行いません。

SIP セッションの更新が行われず、指定された時間に到達した場合、SIP セッションを切断します。

【実行例】

SIP session timer の有効期限を指定します（有効期限：600 秒、更新時間：300 秒）。

```
#configure terminal
(config)#ngn sip agent 0 sessiontimer default 600
```

【未設定時】

有効期限は 300 秒で動作します。

19.1.16 ngn sip agent sessiontimer use disable

【機能】

SIP session timer 動作の無効化

【入力形式】

ngn sip agent <エントリ番号> sessiontimer use disable

no ngn sip agent <エントリ番号> sessiontimer use disable

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エントリ番号	SIP user agentのエントリ番号を指定します。	0: 高優先	省略不可

【動作モード】

基本設定モード

【説明】

SIP session timer の動作を無効化します。

【実行例】

SIP session timer の動作を無効化します。

```
#configure terminal
(config)#ngn sip agent 0 sessiontimer use disable
```

【未設定時】

SIP session timer の動作は有効になります。

19.1.17 ngn sip agent survey sip-server invite

【機能】

REGISTRAR のやり直し

【入力形式】

ngn sip agent <エントリ番号> survey sip-server invite

no ngn sip agent <エントリ番号> survey sip-server invite

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エントリ番号	SIP user agentのエントリ番号を指定します。	0: 高優先	省略不可

【動作モード】

基本設定モード

【説明】

INVITE 送信時、SIP サーバから 100Trying 応答がない状態で 32 秒が経過した際、SIP 接続をすべて切断し、REGISTRAR のやり直しを行います。

【実行例】

SIP 発信時、SIP サーバから 100Trying 応答がない状態で 32 秒が経過した際、SIP 接続をすべて切断し、REGISTRAR のやり直しを行います。

```
#configure terminal
(config)#ngn sip agent 0 survey sip-server invite
```

【未設定時】

INVITE に対する 100Trying 応答がない状態で 32 秒が経過した際、SIP 接続の切断、並びに REGISTRAR のやり直しを行いません。

19.1.18 ngn sip agent user

【機能】

自装置電話番号の指定

【入力形式】

ngn sip agent <エントリ番号> {ipv4 | ipv6} user <電話番号>

no ngn sip agent <エントリ番号> {ipv4 | ipv6} [user <電話番号>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エントリ番号	SIP user agent のエントリ番号を指定します。	0: 高優先	省略不可
ipv4 ipv6	SIP 機能で自装置 IP アドレスについて用いる IP プロトコルを指定します。	ipv4 ipv6	省略不可
電話番号	SIP 機能で用いる自装置の電話番号を指定します。	1 ～ 32 桁の数字、*、#	省略不可

【動作モード】

基本設定モード

【説明】

DHCP(DHCPv6) クライアント機能を使用せず、SIP 機能を利用する際の自装置電話番号を指定します。

ngn sip agent bind port-channel コマンドで manual オプションの指定がなかった場合、本設定は無効となります。

【実行例】

自装置電話番号を指定します（プロトコル：IPv4、電話番号：0120111222）。

```
#configure terminal
(config)#ngn sip agent 0 ipv4 user 0120111222
```

【未設定時】

設定による電話番号を用いたデータコネクト機能がご利用になれません。

19.1.19 ngn sip profile

【機能】

SIP プロファイル設定モードへの移行

【入力形式】

ngn sip profile <プロファイル名>

no ngn sip profile <プロファイル名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プロファイル名	SIP 接続用のプロファイル名を指定します。	63 文字以内の CDATA 型	省略不可

【動作モード】

基本設定モード

【説明】

SIP 接続用の設定を行うために、SIP プロファイル設定モードに移行します。

コマンドの先頭に "no" を指定することで、該当 SIP プロファイル設定モードの内容がすべて削除されます。

【実行例】

SIP プロファイル設定モードに移行します（プロファイル名：SIP-PROFILE-A）。

```
#configure terminal
(config)#ngn sip profile SIP-PROFILE-A
(sip-prof)#
```

19.1.20 ngn sip use enable

【機能】

NGN 網への接続とデータコネクト機能の利用

【入力形式】

ngn sip use enable

no ngn sip use enable

【動作モード】

基本設定モード

【説明】

NGN 網に接続し、データコネクト機能を利用する際に設定します。

【実行例】

NGN 網に接続し、データコネクト機能を利用します。

```
#configure terminal
(config)#ngn sip use enable
```

【未設定時】

データコネクト機能をご利用になれません。

19.1.21 outgoing-call disable

【機能】

ピアに対する発信抑制

【入力形式】

outgoing-call disable

no outgoing-call disable

【動作モード】

SIP プロファイル設定モード

【説明】

該当 SIP プロファイルに設定されたピアに対する発信を抑制する際に設定します。

本設定で発信抑制可能なのはトラフィック契機による発信のみとなります。ngn connect、ipsec connect による接続は発信抑制の対象外となります。

【実行例】

発信を抑制します。

```
#configure terminal
(config)#ngn sip profile SIP-PROFILE-A
(sip-prof)#outgoing-call disable
```

【未設定時】

他の発信制限に該当していない状況で、発信を許可します。

19.1.22 remote dial number

【機能】

接続相手の指定

【入力形式】

remote dial <発信順> number <電話番号> [connect priority <優先動作>]

no remote dial <発信順> number [<電話番号> [connect priority <優先動作>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
発信順	マルチダイヤル発信順番を指定します。 発信は番号の小さい順から行います。	0～2	省略不可
電話番号	SIP 接続相手の電話番号を指定します。	1～32 桁の数字、*、#	省略不可
優先動作	発信と着信が競合した際にどちらを優先するかを指定します。	initiator: 発信を優先します responder: 着信を優先します	発信を優先

【動作モード】

SIP プロファイル設定モード

【説明】

データコネクト機能の接続相手を指定します。

自装置から発信を行う場合、電話番号で指定された相手以外への発信は行いません。connect priority オプションを指定することで発信と着信が競合した際に、どちらを優先するか指定できます。connect priority オプションが指定されていない場合、発信が優先されます。

マルチダイヤル機能に対応しており、電話番号の前に指定された番号順に発信を行い、接続に失敗した場合、次の番号の電話番号に発信します。着信時は電話番号認証で使します。

【実行例】

SIP 接続相手の番号を指定します（電話番号：0987654321）。

```
#configure terminal
(config)#ngn sip profile SIP-PROFILE-A
(sip-prof)#remote dial 0 number 0987654321
```

【未設定時】

データコネクト機能での発信は行いません。

19.1.23 remote dial speed

【機能】

通信帯域の指定

【入力形式】

remote dial <発信順> speed {64k | 512k | 1m | <帯域値>}

no remote dial <発信順> speed {64k | 512k | 1m | <帯域値>}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
発信順	マルチダイヤル発信順番を指定します。	0 ～ 2	省略不可
64k 512k 1m	SIP セッションの帯域を指定します。	64k:64Kbps 512k:512Kbps 1m:1Mbps	省略不可
帯域値	SIP セッションの帯域 (単位 : kbps) を指定します。	1 ～ 1000000	省略不可

【動作モード】

SIP プロファイル設定モード

【説明】

データコネクト機能の通信帯域を指定します。

発信時は設定された帯域で、着信時は発信側が指定した帯域で接続を行います。

【実行例】

発信時の帯域を指定します (帯域 : 512Kbps)。

```
#configure terminal
(config)#ngn sip profile SIP-PROFILE-A
(sip-prof)# remote dial 0 speed 512k
```

【未設定時】

通信帯域は 1Mbps で動作します。

19.1.24 sip limit

【機能】

SIP による発信抑制

【入力形式】

sip limit {second < 時間> | charge < 金額>} [disconnect]

no sip limit {second [< 時間>] | charge [< 金額>]} [disconnect]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
時間	累計通信時間による発信抑制を行うための時間 (単位 : 秒) を指定します。	1 ～ 31536000	省略不可
金額	累計課金額による発信抑制を行うための金額 (単位 : 円) を指定します。	1 ～ 999999	省略不可
disconnect	設定した上限時間、金額に達した際、現在接続している SIP の切断を行う場合に指定します。	-	現在接続している SIP の切断を行わない

【動作モード】

SIP プロファイル設定モード

【説明】

接続相手単位で SIP による発信を累計通信時間、累計課金額により、発信抑制を行います。

累計時間、累計課金額、はそれぞれ1つずつ指定できます。

条件を満たしたあとに発信を行いたい場合は、設定をクリアする必要があります。

disconnect オプションを指定すると、接続中の SIP について一定時間ごとに発信による累計接続時間、累計課金額の監視を行い、指定した時間、金額に到達した際に SIP 切断を行います。disconnect オプションを指定しない場合は、指定した時間、金額に到達しても SIP 切断を行わないのでご注意ください。

【実行例】

累計通信時間、累計課金額により発信抑制します（プロファイル名：SIP-PROFILE-A、累計時間：30 分、累計課金額：1000 円）。

```
#configure terminal
(config)#ngn sip profile SIP-PROFILE-A
(sip-prof)#sip limit second 1800
(sip-prof)#sip limit charge 1000
```

【未設定時】

課金額、発信時の接続時間による発信抑制を行いません。

第20章

データコネクトおよび IPsecで用いる RADIUSサーバの設定



この章では、データコネクトおよびIPsecで用いるRADIUSサーバの設定に関するコマンドについて説明します。

20.1	IPsecで用いるRADIUSサーバの設定	706
20.2	データコネクトで用いるRADIUSサーバの設定	715
20.3	共通で用いるRADIUSサーバの設定	721

20.1 IPsec で用いる RADIUS サーバの設定

RADIUS サーバで拡張認証を行った際に、受信した Access-Accept 内の attribute については以下をサポートしています。

Framed-IP-Address(8)	Mode-cfg/CP によるアドレス通知および IPsec tunnel 向け経路として利用可能です。経路として利用する場合は sa-up route-radius を設定してください。
Framed-IP-Netmask(9)	Mode-cfg/CP によるアドレス通知および IPsec tunnel 向け経路として利用可能です。経路として利用する場合は sa-up route-radius を設定してください。
Framed-Route(22)	IPsec tunnel 向け経路として利用可能です。経路として利用する場合は sa-up route-radius を設定してください。
Vendor-Specific(26) Vendor-ID(9)	
Vendor-Type(1)	Attribute-Specific で指定された ipsec:tunnel-password の値を IKE の Pre-shared Key として利用可能です。
Session-Timeout(27)	crypto session release session-time と同等の機能として利用可能です。
Idle-Timeout(28)	crypto session release idle-time と同等の機能として利用可能です。
Tunnel-Password(69)	IKE の Pre-shared Key として利用可能です。
Delegated-IPv6-Prefix(123)	IPsec tunnel 向け経路として利用可能です。経路として利用する場合は sa-up route-radius を設定してください。

各 Attribute は初回接続時にのみ反映されます。

IKEv1 の場合の Phase1 再確立時にはこれらの Attribute 値は反映されません。反映するには crypto session release ipsec-lost-time 設定や clear コマンドを使用して一度セッションを解放する必要があります。

IKEv2 では初回接続以外で RADIUS サーバによる認証を行うことがないため、上記動作の考慮は不要です。

拡張認証を RADIUS で行うために、RADIUS サーバの登録を行います。

IPsec セッションの開始／終了について、アカウントティングサーバへの通知を行うことができます。

20.1.1 aaa accounting network

【機能】

NETWORK アカウンティングを有効にする設定

【入力形式】

aaa accounting network <アカウント方式名> start-stop group <認証グループ名>

no aaa accounting network <アカウント方式名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アカウント方式名	アカウント方式名を指定します。	63 文字以内の CDATA 型	省略不可
認証グループ名	認証グループ名を指定します。	63 文字以内の CDATA 型	

【動作モード】

基本設定モード (IKEv1/IKEv2 で有効)

【説明】

NETWORK アカウンティングを有効にします。NETWORK アカウンティングとは、IPsec セッションの開始／終了の事象が発生した場合に、RADIUS アカウンティングサーバへ通知を行う機能です。本設定内容は ISAKMP プロファイル設定モードで参照されます。

【実行例】

NETWORK アカウンティングを有効にします (アカウント方式名: ACCT-A、認証グループ名: RADIUS-A)。

```
#configure terminal
(config)#aaa accounting network ACCT-A start-stop group RADIUS-A
```

【未設定時】

NETWORK アカウンティングを行いません。

20.1.2 ip vrf forwarding

【機能】

RADIUS サーバが存在する VRF の VRF 名の設定

【入力形式】

ip vrf forwarding <VRF 名>

no ip vrf forwarding

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VRF 名	RADIUS サーバが VRF インタフェースに存在する場合、存在する VRF の VRF 名を指定します。	63 文字以内の WORD 型	省略不可

【動作モード】

CLIENT-RADIUS サーバ設定モード (IKEv1/IKEv2 で有効)

【説明】

RADIUS サーバが VRF インタフェースに存在する場合、存在する VRF の VRF 名を設定します。

【実行例】

RADIUS サーバが存在する VRF の VRF 名を設定します (VRF 名: vrf-A)。

```
#configure terminal
(config)#aaa group server radius radius-A
(config-sg-radius)#ip vrf forwarding vrf-A
```

【未設定時】

VRF には存在しません。

20.1.3 attribute ignore

【機能】

RADIUS サーバへの Access-Request で、Calling-Station-ID アトリビュートを通知する設定

【入力形式】

attribute ignore <attribute 番号>

no attribute ignore

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
attribute 番号	RADIUS サーバから受信した attribute の type 値を指定します。 複数指定が可能です。	1 ～ 255	省略不可

【動作モード】

CLIENT-RADIUS サーバ設定モード (IKEv1/IKEv2 で有効)

【説明】

RADIUS サーバから受信した attribute を無効にしたい type 値を指定します。最大 3 つまで設定可能です。

【実行例】

RADIUS サーバから受信した attribute を無効にしたい type 値を指定します (type 値 : 10,30)。

```
#configure terminal
(config)#aaa group server radius radius-A
(config-sg-radius)#attribute ignore 10 30
```

【未設定時】

RADIUS サーバから受信した attribute を無効にしません。

20.1.4 attribute 31 include-in-access-req

【機能】

Access-Request 送信時に Calling-Station-ID アトリビュートを通知する設定

【入力形式】

attribute 31 include-in-access-req

no attribute 31 include-in-access-req

【動作モード】

CLIENT-RADIUS サーバ設定モード (IKEv1/IKEv2 で有効)

【説明】

RADIUS サーバへの Access-Request で、Calling-Station-ID アトリビュートを通知する場合に指定します。

Calling-Station-ID アトリビュートでは、VPN ピアの IP/IPv6 アドレスを通知します。

通知する IP アドレス / IPv6 アドレスの書式は以下のとおりです。

IPv4 アドレス： 1 バイトずつ "." で区切った表記。各数値は 10 進数。

例) 192.0.2.1

IPv6 アドレス： 2 バイトずつ ":" で区切った表記。各数値は 16 進数。IPv6 アドレス特有の表記方法である 0 が連続しても省略書式はしない。

例) 2001:0db8:0000:0000:0000:0000:0001

【実行例】

Access-Request 送信時に Calling-Station-ID アトリビュートを通知します。

```
#configure terminal
(config)#aaa group server radius radius-A
(config-sg-radius)#attribute 31 include-in-access-req
```

【未設定時】

Access-request 送信時に Calling-Station-ID アトリビュートを通知しません。

20.1.5 attribute 31 include-in-acct-req

【機能】

Accounting-Request(start/stop) で、Calling-Station-ID アトリビュートを通知する設定

【入力形式】

attribute 31 include-in-acct-req

no attribute 31 include-in-acct-req

【動作モード】

CLIENT-RADIUS サーバ設定モード (IKEv1/IKEv2 で有効)

【説明】

RADIUS アカウンティングサーバへの Accounting-Request(start/stop) で、Calling-Station-ID アトリビュートを通知する場合に指定します。

Calling-Station-ID アトリビュートでは、VPN ピアの IP/IPv6 アドレスを通知します。

【実行例】

Accounting-Request(start/stop) 送信時に Calling-Station-ID アトリビュートを通知します。

```
#configure terminal
(config)#aaa group server radius radius-A
(config-sg-radius)#attribute 31 include-in-acct-req
```

【未設定時】

Accounting-Request(start/stop)送信時に Calling-Station-ID アトリビュートを通知しません。

20.1.6 attribute 31 extend-with-prefixlen

【機能】

通知する IP/IPv6 アドレスの有効プレフィックス長の設定

【入力形式】

attribute 31 extend-with-prefixlen <有効プレフィックス長>

no attribute 31 extend-with-prefixlen [<有効プレフィックス長>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
有効プレフィックス長	プレフィックス長を指定します。	1 ～ 128	省略不可

【動作モード】

CLIENT-RADIUS サーバ設定モード (IKEv1/IKEv2 で有効)

【説明】

RADIUS サーバ／RADIUS アカウンティングサーバに、Calling-Station-ID アトリビュートを通知する設定になっている際、通知する IP/IPv6 アドレスの有効プレフィックス長を設定します。たとえば、通知する IPv6 アドレスが "2001:0db8:0000:0000:0000:0000:0001" で、本設定により有効プレフィックス長を "16" とした場合、実際に通知する値は "2001:0000:0000:0000:0000:0000:0000" となります。

本設定で "33" 以上を設定した場合で、通知するアドレスが IPv4 だった場合は、有効プレフィックス長は 32 とします。

【実行例】

有効プレフィックス長を設定します (有効プレフィックス長：64)。

```
#configure terminal
(config)#aaa group server radius radius-A
(config-sg-radius)#attribute 31 extend-with-prefixlen 64
```

【未設定時】

以下の値で動作します。

IPv4 の場合： 32

IPv6 の場合： 128

20.1.7 attribute 81 include-in-access-req

【機能】

Access-request 送信時に Radius Attribute の Tunnel-Private-Group-ID(81) を通知

【入力形式】

attribute 81 include-in-access-req

no attribute 81 include-in-access-req

【動作モード】

CLIENT-RADIUS サーバ設定モード (IKEv1/IKEv2 で有効)

【説明】

Access-request 送信時に Radius Attribute の Tunnel-Private-Group-ID(81) を通知します。

Attribute の値には set ipsec-tunnel index コマンドによる index 値を入れます。

【実行例】

Access-request 送信時に Tunnel-Private-Group-ID(81) を通知します。

```
#configure terminal
(config)#aaa group server radius radius-A
(config-sg-radius)#attribute 81 include-in-access-req
```

【未設定時】

Access-request 送信時に Tunnel-Private-Group-ID(81) を通知しません。

20.1.8 attribute 81 include-in-acct-req

【機能】

Accounting-request 送信時に Radius Attribute の Tunnel-Private-Group-ID(81) を通知

【入力形式】

attribute 81 include-in-acct-req

no attribute 81 include-in-acct-req

【動作モード】

CLIENT-RADIUS サーバ設定モード (IKEv1/IKEv2 で有効)

【説明】

Accounting-request 送信時に Radius Attribute の Tunnel-Private-Group-ID(81) を通知します。

Attribute の値には set ipsec-tunnel index コマンドによる index 値を入れます。

【実行例】

Accounting-request 送信時に、Tunnel-Private-Group-ID(81) を通知します。

```
#configure terminal
(config)#aaa group server radius radius-A
(config-sg-radius)#attribute 81 include-in-acct-req
```

【未設定時】

Accounting-request 送信時に Tunnel-Private-Group-ID(81) を通知しません。

20.1.9 nas-port-type

【機能】

RADIUS サーバに通知する NAS-Port-Type 値の設定

【入力形式】

nas-port-type <NAS-Port-Type 値>

no nas-port-type <NAS-Port-Type 値>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
NAS-Port-Type 値	NAS-Port-Type 値を指定します。	0 ～ 19	省略不可

【動作モード】

CLIENT-RADIUS サーバ設定モード (IKEv1 / IKEv2 / Accounting 機能 / Radius サーバからの情報取得機能で有効)

【説明】

RADIUS サーバに通知する NAS-Port-Type の値を設定します。

【実行例】

RADIUS サーバに通知する NAS-Port-Type の値を設定する (NAS-Port-Type 値 : 5)。

```
#configure terminal
(config)#aaa group server radius radius-A
(config-sg-radius)#nas-port-type 5
```

【未設定時】

Virtual(5) で通知します。

20.1.10 service-type

【機能】

RADIUS サーバに通知する Service-Type 値の設定

【入力形式】

service-type <Service-Type 値>

no service-type <Service-Type 値>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
Service-Type 値	Service-Type 値を指定します。	1 ～ 11	省略不可

【動作モード】

CLIENT-RADIUS サーバ設定モード (IKEv1/IKEv2/Accounting 機能 /Radius サーバからの情報取得機能で有効)

【説明】

RADIUS サーバに通知する Service-Type の値を設定します。

【実行例】

RADIUS サーバに通知する Service-Type の値を設定します (Service-Type 値 : 5)。

```
#configure terminal
(config)#aaa group server radius radius-A
(config-sg-radius)#service-type 5
```

【未設定時】

Service-Type を通知しません。

20.1.11 user-password

【機能】

User-Password(2)のためのパスワードの設定

【入力形式】

user-password <パスワード> [{secret|private} [encrypted]]

no user-password <パスワード> [{secret|private} [encrypted]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
パスワード	Radius サーバからの情報取得機能で使用するパスワードを指定します。	128 文字以内の STRING 型	省略不可
secret/private	パスワードとして使用する文字列の暗号化／復号化に、共通の鍵を使用するか、固有の鍵を使用するかを指定します。	secret: 共通の鍵を使用する private: 固有の鍵を使用する	暗号化せずに保存
encrypted	パスワードとして使用する文字列が暗号化されていることを示します。	-	非暗号化文字列として扱う

【動作モード】

CLIENT-RADIUS サーバ設定モード (Radius サーバからの情報取得機能でのみ有効)

【説明】

Radius サーバからの情報取得機能による Access-request 送信時に、User-Password(2)のためのパスワードを設定します。パスワードは RFC 2865 により暗号化されます。

【実行例】

Radius サーバからの情報取得機能による Access-request 送信時に、User-Password(2) のためのパスワードを設定します (パスワード: secret1)。

```
#configure terminal
(config)#aaa group server radius radius-A
(config-sg-radius)#user-password secret1
```

【未設定時】

User-Name の値をパスワードとします。パスワードは RFC2865 により暗号化されます。

20.2 データコネクトで用いる RADIUS サーバの設定

20.2.1 aaa accounting ngn-sip start-stop group

【機能】

RADIUS アカウンティング機能を使用する際の指定

【入力形式】

aaa accounting ngn-sip <アカウント方式名> start-stop group <認証グループ名>

no aaa accounting ngn-sip [<アカウント方式名> start-stop group <認証グループ名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アカウント方式名	アカウント方式名を指定します	63 文字以内の CDATA 型	省略不可
認証グループ名	認証グループ名を指定します。	63 文字以内の CDATA 型	省略不可

【動作モード】

基本設定モード

【説明】

データコネクト機能で RADIUS アカウンティング機能を使用する際に指定します。

RADIUS アカウンティング機能は、RADIUS 認証機能によって認証を行った相手に対してのみ有効となります。

【実行例】

データコネクト機能で RADIUS アカウンティングを有効にします（アカウント方式名：RADIUS-ACCT、認証グループ名：radius-A）。

```
#configure terminal
(config)#aaa accounting ngn-sip RADIUS-ACCT start-stop group radius-A
```

【未設定時】

データコネクト機能で、RADIUS アカウンティング機能が使用できません。

20.2.2 aaa authentication ngn-sip group

【機能】

相手電話番号の認証を RADIUS サーバで行う場合の指定

【入力形式】

aaa authentication ngn-sip <認証方式名> group <認証グループ名>

no aaa authentication ngn-sip [<認証方式名> group <認証グループ名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
認証方式名	認証方式名を指定します。	63 文字以内の CDATA 型	省略不可
認証グループ名	認証グループ名を指定します。	63 文字以内の CDATA 型	省略不可

【動作モード】

基本設定モード

【説明】

データコネクト機能で相手電話番号の認証を RADIUS サーバで行う場合に指定します。

【実行例】

データコネクト機能で相手電話番号の認証を RADIUS サーバで行います（認証方式名：RADIUS-AUTH、認証グループ名：radius-A）。

```
#configure terminal
(config)#aaa authentication ngn-sip RADIUS-AUTH group radius-A
```

【未設定時】

データコネクト機能で、RADIUS 認証機能が使用できません。

20.2.3 accounting

【機能】

RADIUS アカウンティング機能を使用する場合の指定

【入力形式】

accounting

no accounting

【動作モード】

SIP プロファイル設定モード、SIP RADIUS 認証プロファイル設定モード

【説明】

データコネクト機能で、RADIUS アカウンティング機能を使用する場合に指定します。

【実行例】

データコネクト機能で、RADIUS アカウンティング機能を使用します。

```
#configure terminal
(config)#ngn sip profile-radius
(sip-prof-radius)#accounting
```

【未設定時】

該当 SIP プロファイル設定モード、または RADIUS 認証によって接続した相手について、RADIUS アカウンティング機能を使用しません。

20.2.4 client authentication type

【機能】

RADIUS 認証を行う際の認証タイプの指定

【入力形式】

client authentication type <認証タイプ>

no client authentication type [<認証タイプ>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
認証タイプ	RADIUS 認証を行う際の認証タイプを指定します。	chap : CHAP 認証 pap : PAP 認証	省略不可

【動作モード】

SIP RADIUS 認証プロファイル設定モード

【説明】

データコネクト機能で、RADIUS 認証を行う際の認証タイプを指定します。

【実行例】

データコネクト機能で、RADIUS 認証を行う際の認証タイプを指定します（認証タイプ：PAP 認証）。

```
#configure terminal
(config)#ngn sip profile-radius
(sip-prof-radius)#client authentication type pap
```

【未設定時】

PAP 認証を行います。

20.2.5 password

【機能】

サーバに通知するユーザパスワードの指定

【入力形式】

password <パスワード> [{secret | private} [encrypted]]

no password <パスワード> [{secret | private} [encrypted]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
パスワード	パスワードを指定します。	128 文字以内の STRING 型	省略不可

パラメタ	設定内容	設定範囲	省略時
secret/private	パスワードとして使用する文字列の暗号化／復号化に、共通の鍵を使用するか、固有の鍵を使用するかを指定します。	secret: 共通の鍵 private: 固有の鍵	暗号化せずに保存
encrypted	パスワードとして使用する文字列が暗号化されていることを示します。	-	非暗号化文字列として扱う

【動作モード】

SIP RADIUS 認証プロファイル設定モード

【説明】

データコネクト機能で RADIUS による相手電話番号認証を行う際、サーバに通知するユーザパスワードを指定します。

"secret" を指定した場合は、すべての GX500 に共通の鍵を使って暗号化／復号化し、"private" を指定した場合は、装置固有の鍵を使って暗号化／復号化します。encrypted オプションを付けた場合は、入力された文字列を暗号化された文字列と判断しコンフィグに保存します。

show running.cfg コマンドなどで内容を確認すると、暗号化されたパスワードの形式で表示されます。

【実行例】

データコネクト機能で RADIUS 認証時、サーバに通知するユーザパスワードを指定します（パスワード：secretpass、暗号化：しない）。

```
#configure terminal
(config)#ngn sip profile-radius
(sip-prof-radius)#password secretpass
```

【未設定時】

データコネクト機能で、RADIUS 認証機能を用いた相手番号認証が利用できません。

20.2.6 ngn sip profile-radius

【機能】

SIP RADIUS 認証プロファイル設定モードへの移行

【入力形式】

ngn sip profile-radius

no ngn sip profile-radius

【動作モード】

基本設定モード

【説明】

SIP RADIUS 認証プロファイル設定モードに移行します。

RADIUS 認証を用いた相手番号認証を行う場合に設定します。

【実行例】

SIP RADIUS 認証プロファイル設定モードに移行します。

```
#configure terminal
(config)#ngn sip profile-radius
(sip-prof-radius)#
```

20.2.7 ngn sip radius acct

【機能】

RADIUS アカウンティング機能の有効化

【入力形式】

ngn sip radius auth <アカウント方式名>

no ngn sip radius [auth <アカウント方式名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アカウント方式名	アカウント方式名を指定します。	63 文字以内の CDATA 型	省略不可

【動作モード】

基本設定モード

【説明】

SIP の RADIUS アカウンティング機能を有効化します。

【実行例】

SIP の RADIUS アカウンティング機能を有効化します。

```
#configure terminal
(config)#ngn sip radius acct RADIUS-ACCT
```

【未設定時】

データコネクト機能で、RADIUS アカウンティング機能が使用できません。

20.2.8 ngn sip radius auth

【機能】

RADIUS サーバでの相手電話番号認証の有効化

【入力形式】

ngn sip radius auth <認証方式名>

no ngn sip radius [auth <認証方式名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
認証方式名	認証方式名を指定します。	63文字以内のCDATA型	省略不可

【動作モード】

基本設定モード

【説明】

SIP 着信時、相手電話番号を RADIUS サーバでの認証を有効化します。

【実行例】

SIP 着信時、相手電話番号を RADIUS サーバでの認証を有効化します。

```
#configure terminal
(config)#ngn sip radius auth RADIUS-AUTH
```

【未設定時】

データコネクト機能で、RADIUS 認証機能を用いた相手番号認証が使用できません。

20.3 共通で用いる RADIUS サーバの設定

20.3.1 aaa group server radius

【機能】

CLIENT-RADIUS サーバ設定モードへの移行

【入力形式】

aaa group server radius <認証グループ名>

no aaa group server radius <認証グループ名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
認証グループ名	認証グループ名を指定します。	63 文字以内の CDATA 型	省略不可

【動作モード】

基本設定モード (IKEv1/IKEv2/データコネクトで有効)

【説明】

拡張認証 (Xauth/EAP) を行う RADIUS サーバを登録するために、CLIENT-RADIUS サーバ設定モードに移行します。コマンドの先頭に "no" を指定することで、該当 CLIENT-RADIUS サーバ設定モードの内容がすべて消去されます。

【実行例】

CLIENT-RADIUS サーバ設定モードに移行します (認証グループ名: radius-A)。

```
#configure terminal
(config)#aaa group server radius radius-A
(config-sg-radius)#
```

20.3.2 changeback-time

【機能】

問い合わせ順序を再度プライマリサーバへ切り戻すまでの時間の設定

【入力形式】

changeback-time <切り戻し時間>

no changeback-time

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
切り戻し時間	問い合わせ順序をプライマリサーバ (1 番目に書いた server-private) へ切り戻す時間 (単位: 分) を指定します。	0 ~ 1440	省略不可

【動作モード】

CLIENT-RADIUS サーバ設定モード (IKEv1/IKEv2/ データコネクトで有効)

【説明】

プライマリサーバへの問い合わせがタイムアウトしてから、問い合わせ順序を再度プライマリサーバへ切り戻すまでの時間 (単位: 分) を設定します。

【実行例】

再度プライマリサーバへ切り戻すまでの時間 (単位: 分) を設定します (切り戻し時間: 3分)。

```
#configure terminal
(config)#aaa group server radius radius-A
(config-sg-radius)#changeback-time 3
```

【未設定時】

プライマリサーバへの切り戻しを行いません。

20.3.3 nas-ip-address

【機能】

RADIUS サーバに通知する Network Access Server の IP アドレスの設定

【入力形式】

nas-ip-address <NAS アドレス>

no nas-ip-address

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
NAS アドレス	RADIUS サーバに通知する NAS の IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

【動作モード】

CLIENT-RADIUS サーバ設定モード (IKEv1/IKEv2/ データコネクトで有効)

【説明】

RADIUS サーバに通知する Network Access Server(NAS) の IP アドレスを設定します。

【実行例】

RADIUS サーバに通知する Network Access Server(NAS) の IP アドレスを設定します (NAS アドレス: 192.0.2.16)。

```
#configure terminal
(config)#aaa group server radius radius-A
(config-sg-radius)#nas-ip-address 192.0.2.16
```

【未設定時】

NAS の IP アドレスを通知しません。

20.3.4 retransmit

【機能】

RADIUS サーバへのリクエストパケットの再送回数の設定

【入力形式】

retransmit <リクエスト再送回数>

no retransmit [<リクエスト再送回数>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
リクエスト再送回数	RADIUS サーバへのリクエストパケットの再送回数を指定します。	0 ～ 100	省略不可

【動作モード】

CLIENT-RADIUS サーバ設定モード (IKEv1/IKEv2/ データコネクトで有効)

【説明】

拡張認証 (Xauth/EAP) で RADIUS サーバを使用する場合に、RADIUS サーバへのリクエストパケットの再送回数を設定します。

【実行例】

RADIUS サーバへのリクエストパケットの再送回数を設定します (リクエスト再送回数：16 回)。

```
#configure terminal
(config)#aaa group server radius radius-A
(config-sg-radius)#retransmit 16
```

【未設定時】

リクエスト再送回数は 3 回で動作します。

20.3.5 server-private

【機能】

拡張認証 (Xauth/EAP) を行う RADIUS サーバの設定

【入力形式】

server-private <RADIUS サーバ> [auth-port <UDP ポート番号 1>] [acct-port <UDP ポート番号 2>] key
<共有暗号キー>

no server-private <RADIUS サーバ> [auth-port <UDP ポート番号 1>] [acct-port <UDP ポート番号 2>]
[key <共有暗号キー>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
RADIUS サーバ	RADIUS サーバの IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
UDP ポート番号 1	RADIUS サーバが使用する UDP ポート番号を指定します。	1 ～ 65535	1812
UDP ポート番号 2	RADIUS アカウンティングサーバが使用する UDP ポート番号を指定します。	1 ～ 65535	1813
共有暗号キー	RADIUS サーバとの共有暗号キーを指定します。	128 文字以内の STRING 型	省略不可

【動作モード】

CLIENT-RADIUS サーバ設定モード (IKEv1/IKEv2/ データコネクトで有効)

【説明】

拡張認証 (Xauth/EAP) を行う RADIUS サーバを設定します。本設定は、設定順にソートされます。

【実行例】

拡張認証 (Xauth/EAP) を行う RADIUS サーバを設定します (RADIUS サーバ：192.0.2.1、共有暗号キー：secret)。

```
#configure terminal
(config)#aaa group server radius radius-A
(config-sg-radius)#server-private 192.0.2.1 key secret
```

【未設定時】

RADIUS による IPsec/ データコネクトの拡張認証を行いません。

20.3.6 source-address

【機能】

RADIUS サーバへの送信元アドレスの設定

【入力形式】

source-address <送信元アドレス>

no source-address

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
送信元アドレス	RADIUS サーバへの送信元アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

【動作モード】

CLIENT-RADIUS サーバ設定モード (IKEv1/IKEv2/ データコネクトで有効)

【説明】

RADIUS サーバへの送信元アドレスを設定します。

【実行例】

RADIUS サーバへの送信元アドレスを設定します（送信元アドレス：192.0.2.1）。

```
#configure terminal
(config)#aaa group server radius radius-A
(config-sg-radius)#source-address 192.0.2.1
```

【未設定時】

送信元アドレスは実際に送信するインタフェースのアドレスで動作します。

20.3.7 timeout

【機能】

RADIUS サーバからの応答タイムアウト時間の設定

【入力形式】

timeout <タイムアウト時間>

no timeout

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
タイムアウト時間	RADIUS サーバからの応答タイムアウト時間（単位：秒）を指定します。	1～600	省略不可

【動作モード】

CLIENT-RADIUS サーバ設定モード（IKEv1/IKEv2/ データコネクトで有効）

【説明】

拡張認証(Xauth/EAP)でRADIUS サーバを使用する場合に、RADIUS サーバからの応答タイムアウト時間（単位：秒）を設定します。

【実行例】

RADIUS サーバからの応答タイムアウト時間（単位：秒）を設定します（タイムアウト時間：30 秒）。

```
#configure terminal
(config)#aaa group server radius radius-A
(config-sg-radius)#timeout 30
```

【未設定時】

タイムアウト時間は5秒で動作します。

第21章 モデム通信機能の設定



この章では、モデム通信機能の設定に関するコマンドについて説明します。

21.1 モデム通信機能の設定

21.1.1 modem profile

【機能】

モデムプロファイル設定モードへの移行

【入力形式】

modem profile <モデムプロファイル名>

no modem profile <モデムプロファイル名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
モデムプロファイル名	モデム設定情報を識別する文字列を指定します。	63文字以内のWORD型	省略不可

【動作モード】

基本設定モード

【説明】

モデム情報を設定するモデムプロファイル設定モードに移行します。

モデムタイプとルータタイプを切り替えられるUSB通信ドングルに対しては、以下のルールでタイプ切り替えを行います。

- 有効なモデムプロファイル設定がある場合はモデムタイプに切り替える。
- 有効なモデムプロファイル設定がない場合はルータタイプに切り替える。

タイプ切り替え後に設定変更した場合、変更後のタイプに切り替えるにはusb resetまたは抜き差しが必要です。

【実行例】

モデムプロファイル設定モードに移行します（モデムプロファイル名：modem-profile-A）。

```
#configure terminal
(config)#modem profile modem-profile-A
(config-modem-profile)#
```

21.1.2 tunnel mode modem profile

【機能】

tunnelインタフェースで有効にするモデムプロファイルの設定

【入力形式】

tunnel mode modem profile <モデムプロファイル名>

no tunnel mode [modem profile <モデムプロファイル名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
モデムプロファイル名	モデム設定情報を識別する文字列を指定します。	63文字以内のWORD型	省略不可

【動作モード】

tunnel インタフェース設定モード

【説明】

tunnel インタフェースで有効にするモデムプロファイルを設定します。

モデムプロファイル名には modem profile コマンドで設定した名称を指定します。

複数の tunnel インタフェースに本設定を行った場合は、モデムプロファイル設定が有効かつインタフェース番号が最も小さい tunnel インタフェースを使用します。

ただし、すでに使用中の tunnel インタフェースが存在する場合はそちらを優先します。

本設定を行った tunnel インタフェースに ip address が設定されている場合は PPP 通信の機能が動作しません。

本設定を行った tunnel インタフェースをルーティングのインタフェースとして設定することはサポートしていません。

【実行例】

tunnel インタフェースで有効にするモデムプロファイルを設定します（モデムプロファイル名：modem-profile-A）。

```
#configure terminal
(config)#interface tunnel 1
(config-if-tun 1)#tunnel mode modem profile modem-profile-A
```

【未設定時】

tunnel インタフェースで PPP 通信の機能が動作しません。

21.1.3 remote dial number

【機能】

接続先アクセスポイントの電話番号の設定

【入力形式】

remote dial number <AP 電話番号>

no remote dial number [<AP 電話番号>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
AP 電話番号	接続するアクセスポイントの電話番号を指定します。	32桁以内の数字、*、#	省略不可

【動作モード】

モデムプロファイル設定モード

【説明】

接続先アクセスポイントの電話番号を設定します。

【実行例】

接続するアクセスポイントの電話番号を設定します (AP 電話番号：*99***1#)。

```
#configure terminal
(config)#modem profile modem-profile-A
(config-modem-profile)#remote dial number *99***1#
```

【未設定時】

発信によるワイヤレス回線の接続ができません。

21.1.4 account

【機能】

PPP の認証に使用するユーザ ID とパスワードの設定

【入力形式】

account <ユーザ ID> <パスワード> [{secret | private} [encrypted]]

no account [<ユーザ ID> <パスワード> [{secret | private} [encrypted]]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ユーザ ID	PPP 接続する際のユーザ ID を設定します。	127 文字以内の STRING 型	省略不可
パスワード	PPP 接続する際のパスワードを設定します。	128 文字以内の STRING 型 (暗号化されていない場合) 254 文字以内の STRING 型 (暗号化されている場合)	省略不可
secret private	パスワードとして使用する文字列の暗号化/複合化に 共通の鍵を使用するか、固有の鍵を使用するかを指定します。	secret : 共通の鍵を使用する private : 固有の鍵を使用する	暗号化せずに保存する。
encrypted	パスワードとして使用する文字列が暗号化されている場合に指定します。	-	非暗号化文字列

【動作モード】

モデムプロファイル設定モード

【説明】

PPP の認証に使用するユーザ ID とパスワードを設定します。

【実行例】

PPP の認証に使用するユーザ ID とパスワードを設定します（ユーザ ID：user@example.ne.jp、パスワード：pass）。

```
#configure terminal
(config)#modem profile modem-profile-A
(config-modem-profile)#account user@example.ne.jp pass
```

【未設定時】

tunnel インタフェースで PPP 通信の機能が動作しません。

21.1.5 auto connect

【機能】

常時接続モードの設定

【入力形式】

auto connect {disable | continuous [delay <再接続間隔>]}

no auto connect [disable | continuous [delay <再接続間隔>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
disable continuous	常時接続モードを有効にするかどうかを指定します。	disable : 無効 continuous : 有効	省略不可
再接続間隔	常時接続モードを有効とした場合に、回線切断後から再接続するまでの間隔（単位：秒）を指定します。	1 ～ 255	回線切断後即再接続

【動作モード】

モデムプロファイル設定モード

【説明】

常時接続モードの設定をします。

常時接続モードが有効な状態で、modem disconnect コマンドを実行した場合は、常時接続モードが無効になります。

この状態で下記のどれかの操作を行うと再び常時接続モードが有効になります。

- modem connect コマンドを実行する。
- データ通信端末を抜き挿しする。
- usb reset コマンドを実行する。
- usb detach コマンド実行後に usb attach コマンドを実行する。

PPP セッションが未確立のときに電波状態が圏外となるデータ通信端末で、電波信号品質の監視の設定がされている場合は、常時接続モードによる発信が行われません。

【実行例】

常時接続モードの設定をします（常時接続モード：有効、再接続間隔：5 秒）。

```
#configure terminal
(config)#modem profile modem-profile-A
(config-modem-profile)#auto connect continuous delay 5
```

【未設定時】

常時接続モードを有効にし、回線切断後は即再接続します。

21.1.6 authentication accept

【機能】

PPP で認証を許可する認証プロトコルの設定

【入力形式】

authentication accept < 認証プロトコル >

no authentication accept [< 認証プロトコル >]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
認証プロトコル	認証を許可する認証プロトコル（CHAP または PAP）を指定します。	any :CHAP、PAP chap :CHAP pap :PAP	省略不可

【動作モード】

モデムプロファイル設定モード

【説明】

PPP で認証を許可する認証プロトコルを設定します。

【実行例】

PPP で認証を許可する認証プロトコルを設定します（認証プロトコル：chap）。

```
#configure terminal
(config)#modem profile modem-profile-A
(config-modem-profile)#authentication accept chap
```

【未設定時】

CHAP、PAP での認証を許可します。

21.1.7 max-call

【機能】

ワイヤレス接続の接続回数のリミッタ設定

【入力形式】

max-call <リミッタが動作する回数>

no max-call [<リミッタが動作する回数>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
リミッタが動作する回数	リミッタが動作する、1時間あたりの発呼回数を指定します。 disable を指定すると発呼回数の監視を行いません。	1 ～ 1000 disable	省略不可

【動作モード】

モデムプロファイル設定モード

【説明】

データ通信端末によるワイヤレス接続で、リミッタが動作する1時間あたりの接続回数を設定します。

設定を変更してrefreshした場合、リミッタが動作していれば解除し、カウンタをクリアします。

modem connect コマンドによる接続の場合、リミッタは動作しません。

【実行例】

リミッタが動作する1時間あたりの接続回数を設定します（発呼回数の監視を行わない）。

```
#configure terminal
(config)#modem profile modem-profile-A
(config-modem-profile)#max-call disable
```

【未設定時】

リミッタが動作する1時間あたりの接続回数を40回にします。

21.1.8 modem out-strings init

【機能】

データ通信端末を初期化するための文字列の設定

【入力形式】

modem out-strings init <シーケンス番号> <初期化文字列>

no modem out-strings init <シーケンス番号> [<初期化文字列>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
シーケンス番号	シーケンス番号を選択します。	1 ～ 3	省略不可
初期化文字列	データ通信端末を初期化するための文字列を設定する。	254文字以内のSTRING型	省略不可

【動作モード】

モデムプロファイル設定モード

【説明】

データ通信端末を初期化するための文字列を任意に設定します。

初期化する文字列が異なる場合は、使用するデータ通信端末に合わせて適切な文字列を設定する必要があります。

【実行例】

データ通信端末に対して初期化文字列を設定します（シーケンス番号：1、初期化文字列：ATE0V1Q0&C1&D2）。

```
#configure terminal
(config)#modem profile modem-profile-A
(config-modem-profile)#modem out-strings init 1 ATE0V1Q0&C1&D2
```

【未設定時】

ファームウェアが個別に保持している適切な文字列 (ATE0V1Q0&D2&C1) が送信されます。

21.1.9 set mtu

【機能】

PPP 通信で使用する tunnel インタフェースの MTU 長の設定

【入力形式】

set mtu <MTU 長>

no set mtu [<MTU 長>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
MTU 長	MTU 長（単位：bytes）を指定します。	1280 ～ 1500	省略不可

【動作モード】

モデムプロファイル設定モード

【説明】

PPP で使用する tunnel インタフェースの MTU 長（単位：bytes）を設定します。

受信した MRU 長が MTU の設定長よりも小さかった場合は、MRU 長を MTU 長として使用します。

ただし、MRU 長が 1280bytes 未満の場合は、MTU 長は 1280bytes となります。

MTU に従いパケットを分割する場合、基本的に均等な長さにパケットを分割します。しかし、コントロールプレーンから送信する、またはコントロールプレーンを経由して中継する際に分割するケースでは、MTU 長に合わせたパケットの分割を実施します。

【実行例】

PPP で使用する tunnel インタフェースの MTU 長を設定します (MTU 長：1420bytes)。

```
#configure terminal
(config)#modem profile modem-profile-A
(config-modem-profile)#set mtu 1420
```

【未設定時】

PPP で使用する tunnel インタフェースの MTU 長は 1500bytes になります。

21.1.10 set mss

【機能】

PPP で使用する tunnel インタフェースの MSS 値の設定

【入力形式】

set mss {<MSS 値> | auto | off}

no set mss [<MSS 値> | auto | off]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
<MSS 値> auto off	MSS 値 (単位：bytes) を指定します。 "auto" を指定した場合は MSS 値を MTU 長 -40 とします。"off" を指定した 場合は MSS 値を変更しません。	1240～1460 auto off	省略不可

【動作モード】

モデムプロファイル設定モード

【説明】

PPP で使用する tunnel インタフェースで MSS 書き換えを行う場合の書き換え値 (単位：bytes) を設定します。

MSS 書き換えはパケットの送信、受信時に行います。

パケットの MSS オプションが設定値より大きい場合に書き換えを行います。

【実行例】

PPP で使用する tunnel インタフェースの MSS 値を設定します (MSS 値：1240)。

```
#configure terminal
(config)#modem profile modem-profile-A
(config-modem-profile)#set mss 1240
```

【未設定時】

auto で動作します。

21.1.11 set session release idle-time

【機能】

無通信監視時間の設定

【入力形式】

set session release idle-time <無通信監視時間> [send | receive]

no set session release idle-time [<無通信監視時間> [send | receive]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
無通信監視時間	送受信データに関する無通信監視時間を指定します（単位：秒）。	1 ～ 3600	省略不可
send receive	無通信監視を行う方向を指定します。	send : 送信 receive : 受信	送信および受信データの無通信監視を行う

【動作モード】

モデムプロファイル設定モード

【説明】

送受信データに関する無通信監視時間（単位：秒）を設定します。

ここで指定した時間内に、送受信データがない場合は、データ通信端末によるワイヤレス接続を切断します。

ただし常時接続モードが有効な場合は切断しません。

【実行例】

送信データに関する無通信監視時間を設定します（無通信監視時間：60 秒、方向：送信）。

```
#configure terminal
(config)#modem profile modem-profile-A
(config-modem-profile)#set session release idle-time 60 send
```

【未設定時】

無通信監視を行いません。

21.1.12 monitor signal-quality enable level

【機能】

電波信号品質の監視の設定

【入力形式】

monitor signal-quality enable level <電波信号品質判定レベル> [logging]

no monitor signal-quality enable [level <電波信号品質判定レベル>] [logging]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
電波信号品質判定レベル	電波信号品質判定レベル（単位：dBm）を指定します。	-113 ～ -50	省略不可
logging	電波信号品質を syslog に記録する場合に指定します。	-	データ通信端末の電波信号品質を syslog に記録しない

【動作モード】

モデムプロファイル設定モード

【説明】

データ通信端末が +CSQ コマンドに対応している場合に、端末の電波信号品質を定期的に監視します。

電波信号品質が設定レベルを下回っている場合は電波信号品質が不良と判断され、新規接続を禁止します。

レベルを -113 に設定した場合は、電波信号品質に関わらず常に接続可能と判断されます。

【実行例】

端末の電波信号品質を定期的に監視します（電波信号品質判定レベル：-100dBm、syslog：記録する）。

```
#configure terminal
(config)#modem profile modem-profile-A
(config-modem-profile)#monitor signal-quality enable level -100 logging
```

【未設定時】

信号品質の監視を行いません。

21.1.13 monitor signal-quality interval

【機能】

電波信号品質を監視する間隔の設定

【入力形式】

monitor signal-quality interval <監視間隔>

no monitor signal-quality interval [<監視間隔>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
監視間隔	電波信号品質を監視する間隔（単位：秒）を設定します。	10 ～ 86400	省略不可

【動作モード】

モデムプロファイル設定モード

【説明】

電波信号品質を監視する間隔（単位：秒）を設定します。

【実行例】

電波信号品質を監視する間隔を設定します（監視間隔：120 秒）。

```
#configure terminal
(config)#modem profile modem-profile-A
(config-modem-profile)#monitor signal-quality interval 120
```

【未設定時】

監視間隔は 60 秒となります。

第22章 VRFの設定



この章では、VRFの設定に関するコマンドについて説明します。

22.1 VRF の設定

22.1.1 ip vrf

【機能】

VRF 設定モードへの移行

【入力形式】

ip vrf <VRF 名>

no ip vrf <VRF 名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VRF 名	VRF 名を指定します。	63 文字以内の WORD 型	省略不可

【動作モード】

基本設定モード

【説明】

vrf 設定モードに移行します。no を指定した場合には、該当 vrf 設定モードの内容がすべて消去されます。

【動作モード】

基本設定モード

【実行例】

vrf 設定モードに移行します。(VRF 名 : vrf-A)

```
#configure terminal
(config)#ip vrf vrf-A
(config-vrf vrf-A)#
```

22.1.2 arp vrf

【機能】

VRF ネットワークの ARP エントリ (スタティック) の登録

【入力形式】

arp vrf <VRF 名> <IPv4 アドレス> <MAC アドレス> <インタフェース名> <インタフェース番号>

no arp vrf <VRF 名> <IPv4 アドレス>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VRF 名	VRF 名を指定します。	63 文字以内の WORD 型	省略不可
IPv4 アドレス	IPv4 アドレスを指定します。	IPv4 アドレス形式	
MAC アドレス	MAC アドレスを指定します。	HHHH.HHHH.HHHH 型式	
インタフェース名	インタフェース名を指定します。	-	
インタフェース番号	インタフェース番号を指定します。	-	

【動作モード】

基本設定モード

【説明】

VRF ネットワークの ARP エントリ（スタティック）を登録します。

【実行例】

VRF ネットワークの ARP エントリを登録します（VRF 名：vrf-A、IPv4 アドレス：192.0.2.1、MAC アドレス：2ed4:4401:2345、インタフェース名：gigaethernet、インタフェース番号：1/1）。

```
#configure terminal
(config)#arp vrf vrf-A 192.0.2.1 2ed4.4401.2345 gigaethernet 1/1
```

【未設定時】

VRF ネットワークの ARP エントリを登録しません。

22.1.3 ip route vrf

【機能】

VRF 側のスタティック経路の設定

【入力形式】

```
ip route vrf <VRF 名> <ネットワークアドレス> <ネットマスク> <インタフェース名> <インタフェース番号> [tag <タグ値>] [<ディスタンス値>]
```

```
no ip route vrf <VRF 名> <ネットワークアドレス> <ネットマスク> <インタフェース名> <インタフェース番号> [tag <タグ値>] [<ディスタンス値>]
```

```
ip route vrf <VRF 名> <ネットワークアドレス> <ネットマスク> <Next-hop> [tag <タグ値>] [<ディスタンス値>]
```

```
no ip route vrf <VRF 名> <ネットワークアドレス> <ネットマスク> <Next-hop> [tag <タグ値>] [<ディスタンス値>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VRF 名	VRF 名を指定します。	63 文字以内の WORD 型	省略不可
ネットワークアドレス	ネットワークアドレスを指定します。	IPv4 アドレス形式	
ネットマスク	ネットマスクを指定します。	IPv4 アドレス形式	
インタフェース名	インタフェース名を指定します。	-	
インタフェース番号	インタフェース番号を指定します。	-	
Next-hop	Next-hop のアドレスを指定します。	IPv4 アドレス形式	タグ値を使用しない
タグ値 (*1)	タグ値を指定します。	1 ～ 2147483647	
ディスタンス値	ディスタンス値を指定します。	2 ～ 255	

*1) インタフェース名に "null" を指定した場合、"tag" は指定できません。

【動作モード】

基本設定モード

【説明】

VRF 側のスタティック経路を設定します。

宛先プレフィックスの同じ経路情報が複数存在した場合の優先度（小さい方が優先）をディスタンス値で設定します。

 参照 survey 連携機能を使用する場合は、[\[29.1.3 ip route vrf survey\]](#) (P.872) を参照してください。

【実行例】

VRF 側のスタティック経路を設定します（VRF 名：vrf-A、ネットワークアドレス：192.0.2.128、ネットマスク：255.255.255.128、Next-hop:192.0.2.1）。

```
#configure terminal
(config)#ip route vrf vrf-A 192.0.2.128 255.255.255.128 192.168.1.1
```

【未設定時】

VRF 側のスタティック経路を登録しません。

22.1.4 ipv6 neighbor vrf

【機能】

スタティックで Neighbor Discovery の登録

【入力形式】

ipv6 neighbor vrf <VRF 名> <IPv6 アドレス> <インタフェース名> <インタフェース番号> <MAC アドレス>

no ipv6 neighbor vrf <VRF 名> <IPv6 アドレス>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VRF 名	VRF 名を指定します。	63 文字以内の WORD 型	省略不可
IPv6 アドレス	スタティックで ND を登録する IPv6 アドレスを指定します。	IPv6 アドレス型式	
インタフェース名	インタフェース名を指定します。	-	
インタフェース番号	インタフェース番号を指定します。	-	
MAC アドレス	指定する IPv6 アドレスを持つノードの MAC アドレスを指定します。	XXXX.XXXX.XXXX 形式	

【動作モード】

基本設定モード

【説明】

スタティックで Neighbor Discovery (ND) を登録します。

【実行例】

スタティックで ND を登録します (VRF 名: vrf-A、IPv6 アドレス: 2001:db8::1、インタフェース名: gig Ethernet、インタフェース番号: 1/1、MAC アドレス: 2ed4:4401:2345)。

```
#configure terminal
(config)#ipv6 neighbor vrf vrf-A 2001:db8::1 gig Ethernet 1/1 2ed4.4401.2345
```

【未設定時】

NDP を使用して、学習します。

22.1.5 ipv6 route vrf

【機能】

VRF 側のスタティック経路の設定

【入力形式】

```
ipv6 route vrf <VRF 名> <ネットワークアドレス>/<プレフィックス長> <インタフェース名> <インタフェース番号> [tag <タグ値>] [<ディスタンス値>]
```

```
no ipv6 route vrf <VRF 名> <ネットワークアドレス>/<プレフィックス長> <インタフェース名> <インタフェース番号> [tag <タグ値>] [<ディスタンス値>]
```

```
ipv6 route vrf <VRF 名> <ネットワークアドレス>/<プレフィックス長> <Next-hop> [tag <タグ値>] [<ディスタンス値>]
```

```
no ipv6 route vrf <VRF 名> <ネットワークアドレス>/<プレフィックス長> <Next-hop> [tag <タグ値>] [<ディスタンス値>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VRF 名	VRF 名を指定します。	63 文字以内の WORD 型	省略不可
ネットワークアドレス	ネットワークアドレスを指定します。	IPv6 アドレス形式	
プレフィックス長	プレフィックス長を指定します。	0 ～ 128	
インタフェース名	インタフェース名を指定します。	-	
インタフェース番号	インタフェース番号を指定します。	-	
Next-hop	Next-hop アドレスを指定します。	IPv6 アドレス形式	タグ値を使用しない
タグ値 (*1)	タグ値を指定します。	1 ～ 2147483647	
ディスタンス値	ディスタンス値を指定します。	2 ～ 255	

*1) インタフェース名に "null" を指定した場合、"tag" は指定できません。

【動作モード】

基本設定モード

【説明】

VRF 側のスタティック経路を設定します。

 参照 survey 連携機能を使用する場合は、[\[29.1.5 ipv6 route vrf survey\]](#) (P.875) を参照してください。

【実行例】

VRF 側のスタティック経路を設定します (VRF 名: vrf-A、ネットワークアドレス: 2001:db8:2::、プレフィックス長: 48、Next-hop: 2001:db8:1::1)。

```
#configure terminal
(config)#ipv6 route vrf vrf-A 2001:db8:2::/48 2001:db8:1::1
```

【未設定時】

VRF 側のスタティック経路を登録しません。

22.1.6 ip vrf forwarding

【機能】

VRF インタフェースの設定

【入力形式】

ip vrf forwarding <VRF 名>

no ip vrf forwarding <VRF 名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VRF 名	VRF 名を指定します。	63 文字以内の WORD 型	省略不可

【動作モード】

loopback インタフェース設定モード、port-channel インタフェース設定モード、tunnel インタフェース設定モード

【説明】

VRF インタフェースとして使用する場合に設定します。

【実行例】

VRF インタフェースとして使用します。(VRF 名：vrf-A)

```
【port-channel インタフェース設定モードの場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ip vrf forwarding vrf-A
```

【未設定時】

VRF インタフェースとして使用しません。

22.1.7 bgp local-as

【機能】

local AS 番号の設定

【入力形式】

bgp local-as <AS 番号>

no bgp local-as [<AS 番号>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
AS 番号	AS 番号を指定します。	1 ～ 4294967295	省略不可

【動作モード】

vrf 設定モード

【説明】

BGP セッションを確立するときの local AS 番号を設定します。

既に BGP セッションが確立されていて local AS が変更になった場合、Notification を送信して BGP セッションを一度切断し、変更後の AS 番号を用いて BGP セッションの再確立が行われます。

【実行例】

BGP セッションを確立するときの local AS 番号を設定します。(AS 番号：100)

```
#configure terminal
(config)#ip vrf vrf-A
(config-vrf vrf-A)#bgp local-as 100
```

【未設定時】

router bgp コマンドで指定された AS 番号を使用します。

22.1.8 description

【機能】

説明書きの設定

【入力形式】

description <説明>

no description

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
説明	説明を指定します。	254 文字以内の WORD 型 (*1)	省略不可

*1) 1 文字の空白（スペース）は使用可能です。複数の空白（スペース）は 1 文字にまとめられます。

【動作モード】

vrf 設定モード、各インタフェース設定モード

【説明】

説明書きを設定します。わかりやすい名称を割り当ててください。この名称は、データの中継には影響しません。

【実行例】

説明書きを設定します。(説明：GigaEther-A)

```
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#description GigaEther-A
```

【未設定時】

説明書きは設定されません。

22.1.9 rd

【機能】

RD 値の設定

【入力形式】

rd <RD 値>

no rd <RD 値>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
RD 値	Route Distinguisher (RD) 値を指定します。書式の種類は 2 種類あり、<AS 番号>:0-4294967295 または <IP アドレス>:0-65535 で指定します。	1 ～ 65535 : 0 ～ 4294967295 または IPv4 アドレス形式 : 0 ～ 65535	

【動作モード】

vrf 設定モード

【説明】

該当 VRF の RD 値を設定します。

【実行例】

RD 値を設定を設定します。(RD 値 : 1:1000)

```
#configure terminal
(config)#ip vrf vrf-A
(config-vrf vrf-A)#rd 1:1000
```

【未設定時】

VRF を使用することができません。

第23章 L2TPv3 の設定



この章では、L2TPv3 の設定に関するコマンドについて説明します。

23.1 L2TPv3 の設定

23.1.1 l2-encapsulation map cos-dscp

【機能】

Precedence フィールド、Traffic-Class フィールドへマッピングする値の設定

【入力形式】

```
l2-encapsulation map cos-dscp {<TOS 値> | <Traffic-Class 値>} {<TOS 値> | <Traffic-Class 値>} {<TOS 値> | <Traffic-Class 値>} {<TOS 値> | <Traffic-Class 値>} {<TOS 値> | <Traffic-Class 値>} {<TOS 値> | <Traffic-Class 値>} {<TOS 値> | <Traffic-Class 値>} {<TOS 値> | <Traffic-Class 値>} {<TOS 値> | <Traffic-Class 値>} {<TOS 値> | <Traffic-Class 値>}
```

```
no l2-encapsulation map cos-dscp
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
TOS 値 Traffic-Class 値	TOS 値、または Traffic-Class 値を指定します。	0 ～ 255	省略不可

【動作モード】

基本設定モード

【説明】

EtherIP にてカプセル化を行う際に、ctag（二段目のタグ）の CoS 値（0 ～ 7）を元にカプセル化するヘッダの Precedence フィールド、または Traffic-Class フィールドへマッピングする値を設定します。
ctag がない場合、設定は無視されます。

【実行例】

Precedence フィールド、または Traffic-Class フィールドへマッピングする値を設定します。

```
#configure terminal
(config)#l2-encapsulation map cos-dscp 2 2 2 2 2 2 2 2
```

【未設定時】

TOS 値、または Traffic-Class 値は 0 で動作します。

23.1.2 l2tpv3 tunnel-profile

【機能】

L2TPv3 プロファイル設定モードへの移行

【入力形式】

```
l2tpv3 tunnel-profile <トンネルプロファイル名>
```

```
no l2tpv3 tunnel-profile <トンネルプロファイル名>
```


【パラメタ】

パラメタ	設定内容	設定範囲	省略時
トンネルプロファイル名	トンネルプロファイル名を指定します。	63 文字以内の CDATA 型	省略不可

【動作モード】

基本設定モード

【説明】

L2TPv3 プロファイル設定モードに移行します。"no" を指定した場合は、該当 L2TPv3 プロファイル設定モードの内容がすべて消去されます。

【実行例】

L2TPv3 プロファイル設定モードに移行します（トンネルプロファイル名：l2tpv3-A）。

```
#configure terminal
(config)#l2tpv3 tunnel-profile l2tpv3-A
```

23.1.3 l2tpv3 pseudowire

【機能】

L2TPv3 Pseudowire 設定モードへの移行

【入力形式】

l2tpv3 pseudowire <pseudowire 名>

no l2tpv3 pseudowire <pseudowire 名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
pseudowire 名	pseudowire 名を指定します。	63 文字以内の CDATA 型	省略不可

【動作モード】

基本設定モード

【説明】

L2TPv3 Pseudowire 設定モードに移行します。"no" を指定した場合は、該当 L2TPv3 Pseudowire 設定モードの内容がすべて消去されます。

【実行例】

L2TPv3 Pseudowire 設定モードに移行します（pseudowire 名：session-A）。

```
#configure terminal
(config)#l2tpv3 pseudowire session-A
(config-l2tpv3-pseudowire)#
```

23.1.4 l2tpv3 always-up

【機能】

常に L2TPv3 セッションを確立しておく設定

【入力形式】

l2tpv3 always-up

no l2tpv3 always-up

【動作モード】

基本設定モード

【説明】

常に L2TPv3 セッションを確立しておく場合に設定します。なんらかの原因でセッションが解放されてしまった場合には、セッション確立動作を行います。

L2TPv3 ピアのアドレスが不定の場合は、セッション確立動作ができませんので、そのようなケースではご使用になれません。

【実行例】

常にセッションを確立する設定をします。

```
#configure terminal
(config)#l2tpv3 always-up
```

【未設定時】

同様の関連コマンドとして 2 つの設定がありますが以下の順で適用されます。

- always-up (L2TPv3 Pseudowire 設定モード)
- l2tpv3 always-up (基本設定モード)

どの設定もない場合、セッションが解放されても自動で接続開始しません。

23.1.5 l2tpv3 always-up-params

【機能】

always-up コマンドによるネゴシエーション開始タイミングの設定

【入力形式】

l2tpv3 always-up-params interval <監視間隔> max-initiate <最大ネゴシエーション開始数>

no l2tpv3 always-up-params [interval <監視間隔> max-initiate <最大ネゴシエーション開始数>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
監視間隔	l2tpv3 の always-up 機能の監視間隔 (単位：ミリ秒) を指定します。	100 ～ 100000	省略不可
最大ネゴシエーション開始数	一度の監視で行うネゴシエーション開始数の最大値を指定します。	1 ～ 20000	省略不可

【未設定時】

同様の関連コマンドとして2つの設定がありますが以下の順で適用されます。

- hello interval (L2TPv3 プロファイル設定モード)
- l2tpv3 hello interval (基本設定モード)

どの設定もない場合、Hello メッセージの送信を行いません。

23.1.7 l2tpv3 log

【機能】

L2TPv3 のログを出力する設定

【入力形式】

l2tpv3 log {ccn | session | negotiation-fail}

no l2tpv3 log [{ccn | session | negotiation-fail}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ccn session negotiation-fail	ログを出力する対象を指定します。	ccn: Control connection の確立／解放 session: セッション確立／解放 negotiation-fail: ネゴシエーション失敗	省略不可

【動作モード】

基本設定モード

【説明】

Control connection やセッションの確立／解放、L2TPv3 ネゴシエーションの失敗ログを出力する場合に設定します。

【実行例】

セッションの確立／解放のログを出力するように設定します。

```
#configure terminal
(config)#l2tpv3 log session
```

【未設定時】

Control connection やセッションの確立／解放、L2TPv3 ネゴシエーションの失敗ログを出力しません。

23.1.8 l2tpv3 retransmit retries

【機能】

L2TPv3 メッセージを再送するときの再送回数の設定

【入力形式】

l2tpv3 retransmit retries <再送回数>

no l2tpv3 retransmit retries [<再送回数>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
再送回数	L2TPv3 メッセージを再送するときの再送回数を指定します。	1 ～ 255	省略不可

【動作モード】

基本設定モード

【説明】

L2TPv3 メッセージを再送するときの再送回数を設定します。

【実行例】

L2TPv3 メッセージを再送するときの再送回数を設定します（再送回数：5）。

```
#configure terminal
(config)#l2tpv3 retransmit retries 5
```

【未設定時】

同様の関連コマンドとして2つの設定がありますが、以下の順で適用されます。

- retransmit retries (L2TPv3 プロファイル設定モード)
- l2tpv3 retransmit retries (基本設定モード)

どちらの設定もない場合、再送回数は 10 回で動作します。

23.1.9 l2tpv3 retransmit timer

【機能】

L2TPv3 メッセージを再送するときの再送間隔の設定

【入力形式】

l2tpv3 retransmit timer <再送間隔> timer-max <最大再送間隔>

no l2tpv3 retransmit timer [<再送間隔> timer-max <最大再送間隔>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
再送間隔	L2TPv3 メッセージの再送間隔（単位：秒）を指定します。再送を行うごとに間隔は 2 倍に増加していきます。	1 ～ 60	省略不可
最大再送間隔	L2TPv3 メッセージの最大再送間隔（単位：秒）を指定します。再送間隔がこの設定値以上となる場合は、再送間隔をそれ以上増やさず、設定された値の再送間隔で動作します。	1 ～ 60	省略不可

【動作モード】

基本設定モード

【説明】

L2TPv3 メッセージを再送するときの再送間隔を設定します。最大再送間隔は最初の送信から 1 回目の再送までの間隔には適用されません。

【実行例】

L2TPv3 メッセージを再送するときの再送間隔を設定します（再送間隔：3 秒、最大再送間隔：10 秒）。

```
#configure terminal
(config)#l2tpv3 retransmit timer 3 timer-max 10
```

【未設定時】

同様の関連コマンドとして 2 つの設定がありますが、以下の順で適用されます。

- retransmit timer（L2TPv3 プロファイル設定モード）
- l2tpv3 retransmit timer（基本設定モード）

どちらの設定もない場合、再送間隔は 1 秒、最大再送間隔は 8 秒で動作します。

23.1.10 digest type

【機能】

L2TPv3 の制御メッセージの認証で使用する Digest アルゴリズム、および、パスワードの設定

【入力形式】

digest type {md5 | sha1} <パスワード> [{secret | private} [encrypted]]

no digest type [{md5 | sha1} <パスワード> [{secret | private} [encrypted]]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
md5 sha1	Digest アルゴリズムを指定します。	md5:MD5 sha1:SHA1	省略不可
パスワード	パスワードを指定します。	128 文字以内の STRING 型 (暗号化されていない場合) 254 文字以内の STRING 型 (暗号化されている場合)	省略不可
secret private	パスワードを暗号化する際に共有暗号鍵を使用するか、装置固有暗号鍵を使用するかを指定します。	secret : 暗号化する際に共有暗号鍵を使用する private : 暗号化する際に装置固有暗号鍵を使用する	パスワードを暗号化しない
encrypted	パスワードを暗号化処理するかどうかを指定します。本オプションを付加することにより、パスワードは暗号化済みと判定されます。	-	パスワードを暗号化データとして扱わない

【動作モード】

L2TPv3 プロファイル設定モード

【説明】

L2TPv3 の制御メッセージの認証で使用する Digest アルゴリズム、および、パスワードを設定します。

【実行例】

Digest アルゴリズム、および、パスワードを設定する（Digest アルゴリズム：sha1、パスワード：secret）。

```
#configure terminal
(config)#l2tpv3 tunnel-profile l2tpv3-A
(config-l2tpv3)#digest type sha1 secret
```

【未設定時】

L2TPv3 認証を使用しません。

23.1.11 hello interval

【機能】

Hello メッセージの送信間隔の設定

【入力形式】

hello interval <送信間隔>

no hello interval [<送信間隔>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
送信間隔	Hello メッセージの送信間隔（単位：秒）を指定します。	1 ～ 3600	省略不可

【動作モード】

L2TPv3 プロファイル設定モード

【説明】

L2TPv3 の keepalive で使用する Hello メッセージの送信間隔（単位：秒）を設定します。

【実行例】

L2TPv3 の keepalive で使用する Hello メッセージの送信間隔を設定します（送信間隔：10 秒）。

```
#configure terminal
(config)#l2tpv3 tunnel-profile l2tpv3-A
(config-l2tpv3)#hello interval 10
```

【未設定時】

同様の関連コマンドとして2つの設定がありますが以下の順で適用されます。

- hello interval（L2TPv3 プロファイル設定モード）
- l2tpv3 hello interval（基本設定モード）

どの設定もない場合、Hello メッセージの送信を行いません。

23.1.12 hidden

【機能】

AVP hiding 機能を使用する設定

【入力形式】

hidden

no hidden

【動作モード】

L2TPv3 プロファイル設定モード

【説明】

L2TPv3 の AVP hiding 機能を使用する場合に設定します。digest 設定が設定されている場合に有効となります。

【実行例】

L2TPv3 の AVP hiding 機能を使用します。

```
#configure terminal
(config)#l2tpv3 tunnel-profile l2tpv3-A
(config-l2tpv3)#hidden
```

【未設定時】

L2TPv3 の AVP hiding を使用しません。

23.1.13 hostname local

【機能】

自装置から送信される Host Name AVP に含まれるホスト名の設定

【入力形式】

hostname local <ホスト名>

no hostname local [<ホスト名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ホスト名	L2TPv3 で使用する自装置のホスト名を指定します。	128 文字以内の STRING 型	省略不可

【動作モード】

L2TPv3 プロファイル設定モード

【説明】

L2TPv3のコントロールコネクションを識別するための値で、自装置から送信される Host Name AVP に含まれるホスト名を設定します。

【実行例】

自装置から送信される Host Name AVP に含まれるホスト名を設定します。

```
#configure terminal
(config)#l2tpv3 tunnel-profile l2tpv3-A
(config-l2tpv3)#hostname local host-A
```

【未設定時】

L2TPv3が使用できません。

23.1.14 hostname remote

【機能】

対向装置から受信した Host Name AVP の値をチェックする設定

【入力形式】

hostname remote < ホスト名 >

no hostname remote [< ホスト名 >]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ホスト名	L2TPv3 で使用する対向装置のホスト名を指定します。	128 文字以内の STRING 型	省略不可

【動作モード】

L2TPv3 プロファイル設定モード

【説明】

L2TPv3のコントロールコネクションを識別するための値で、対向装置から受信した Host Name AVP の値と一致するかチェックする場合に設定します。

【実行例】

対向装置から受信した Host Name AVP の値と一致するかチェックします（ホスト名：host-B）。

```
#configure terminal
(config)#l2tpv3 tunnel-profile l2tpv3-A
(config-l2tpv3)#hostname remote host-B
```

【未設定時】

受信した Host Name AVP のチェックを行いません。

23.1.15 mode

【機能】

L2TPv3 のモードの設定

【入力形式】

mode {l2tpv3 | l2tpv3ext}[udp]

no mode [{l2tpv3 | l2tpv3ext} [udp]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
l2tpv3 l2tpv3ext	L2TPv3 のモードを指定します。	l2tpv3 : RFC3931 準拠 l2tpv3ext : cisco 独自モード	省略不可
udp	L2TPv3 を UDP モードで動作させる際に指定します。	-	IP モードで動作

【動作モード】

L2TPv3 プロファイル設定モード

【説明】

L2TPv3 のモードを設定します。

【実行例】

L2TPv3 のモードを設定します (cisco 独自モードを IP モードで動作させる)。

```
#configure terminal
(config)#l2tpv3 tunnel-profile l2tpv3-A
(config-l2tpv3)#mode l2tpv3ext
```

【未設定時】

RFC3931 準拠の L2TPv3 モードが IP モードで動作します。

23.1.16 retransmit retries

【機能】

L2TPv3 メッセージを再送するときの再送回数の設定

【入力形式】

retransmit retries <再送回数>

no retransmit retries [<再送回数>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
再送回数	L2TPv3 メッセージを再送するときの再送回数を指定します。	1 ~ 255	省略不可

【動作モード】

L2TPv3 プロファイル設定モード

【説明】

L2TPv3 メッセージを再送するときの再送回数を設定します。

【実行例】

L2TPv3 メッセージを再送するの再送回数を設定します（再送回数：5）。

```
#configure terminal
(config)#l2tpv3 tunnel-profile l2tpv3-A
(config-l2tpv3)#retransmit retries 5
```

【未設定時】

同様の関連コマンドとして 2 つの設定がありますが、以下の順で適用されます。

- retransmit retries（L2TPv3 プロファイル設定モード）
- l2tpv3 retransmit retries（基本設定モード）

どちらの設定もない場合、再送回数は 10 回で動作します。

23.1.17 retransmit timer

【機能】

L2TPv3 メッセージを再送するときの再送間隔の設定

【入力形式】

retransmit timer <再送間隔> timer-max <最大再送間隔>

no retransmit timer [<再送間隔> timer-max <最大再送間隔>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
再送間隔	L2TPv3 メッセージの再送間隔（単位：秒）を指定します。再送を行うごとに間隔は 2 倍に増加していきます。	1 ～ 60	省略不可
最大再送間隔	L2TPv3 メッセージの最大再送間隔（単位：秒）を指定します。再送間隔がこの設定値以上となる場合は、再送間隔をそれ以上増やさず、設定された値の再送間隔で動作します。	1 ～ 60	省略不可

【動作モード】

L2TPv3 プロファイル設定モード

【説明】

L2TPv3 メッセージを再送するときの再送間隔を設定します。最大再送間隔は最初の送信から 1 回目の再送までの間隔には適用されません。

【実行例】

L2TPv3 メッセージを再送するときの再送間隔を設定します（再送間隔：3 秒、最大再送間隔：10 秒）。

```
#configure terminal
(config)#l2tpv3 tunnel-profile l2tpv3-A
(config-l2tpv3)#retransmit timer 3 timer-max 10
```

【未設定時】

同様の関連コマンドとして 2 つの設定がありますが以下の順で適用されます。

- retransmit timer（L2TPv3 プロファイル設定モード）
- l2tpv3 retransmit timer（基本設定モード）

どちらの設定もない場合、再送間隔は 1 秒、最大再送間隔は 8 秒で動作します。

23.1.18 router-id local

【機能】

自装置から送信される Router ID AVP に含まれる ID の設定

【入力形式】

router-id local <ルータ ID>

no router-id local [<ルータ ID>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ルータ ID	L2TPv3 で使用する自装置のルータ ID を指定します。	IPv4 アドレス形式	省略不可

【動作モード】

L2TPv3 プロファイル設定モード

【説明】

L2TPv3 のコントロールコネクションを識別するための値で、自装置から送信される Router ID AVP に含まれる ID を設定します。

【実行例】

自装置から送信される Router ID AVP に含まれる ID を設定します。

```
#configure terminal
(config)#l2tpv3 tunnel-profile l2tpv3-A
(config-l2tpv3)#router-id local 192.0.2.1
```

【未設定時】

トランスポートが IPv4 の場合は、tunnel source コマンドのアドレスを使用します。IPv6 の場合は、L2TPv3 が使用できません。

23.1.19 router-id remote

【機能】

対向装置から受信した Router ID AVP の値をチェックする設定

【入力形式】

router-id remote <ルータ ID>

no router-id remote [<ルータ ID>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ルータ ID	L2TPv3 で使用する対向装置のルータ ID を指定します。	IPv4 アドレス形式	省略不可

【動作モード】

L2TPv3 プロファイル設定モード

【説明】

L2TPv3 のコントロールコネクションを識別するための値で、対向装置から受信した Router ID AVP の値と一致するかチェックする場合に設定します。

【実行例】

対向装置から受信した Router ID AVP の値と一致するかチェックする場合に設定します（ルータ ID : 192.0.2.2）。

```
#configure terminal
(config)#l2tpv3 tunnel-profile l2tpv3-A
(config-l2tpv3)#router-id remote 192.0.2.2
```

【未設定時】

受信した Router-ID AVP のチェックを行いません。

23.1.20 tunnel destination

【機能】

L2TPv3 を確立する対向装置の IP アドレスの設定

【入力形式】

tunnel destination <IP アドレス>

no tunnel destination [<IP アドレス>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
IP アドレス	L2TPv3 トンネルを確立する対向装置の IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

【動作モード】

L2TPv3 プロファイル設定モード

【説明】

L2TPv3 トンネルを確立する対向装置の IP アドレスを設定します。

【実行例】

L2TPv3 トンネルを確立する対向装置の IP アドレスを設定します（IP アドレス：192.0.2.2）。

```
#configure terminal
(config)#l2tpv3 tunnel-profile l2tpv3-A
(config-l2tpv3)#tunnel destination 192.0.2.2
```

【未設定時】

自装置側からの L2TPv3 ネゴシエーション始動ができません。

23.1.21 tunnel protection

【機能】

L2TPv3 over IPsec 環境下で、L2TPv3 tunnel インタフェースと紐付ける IPsec tunnel インタフェースの設定

【入力形式】

tunnel protection ipsec {map <VPN セレクタ名> | tunnel <tunnel 番号>}

no tunnel protection [ipsec {map <VPN セレクタ名> | tunnel <tunnel 番号>}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VPN セレクタ名	L2TPv3 パケットをカプセル化する VPN セレクタを指定します。	63 文字以内の CDATA 型	省略不可
tunnel 番号	tunnel インタフェースの番号を指定します。	1 ～ 16777215	省略不可

【動作モード】

L2TPv3 プロファイル設定モード

【説明】

L2TPv3 のパケットを IPsec により保護したい場合に、IPsec で使用している VPN セレクタ名、または tunnel インタフェースを設定します。

この設定を行った場合、L2TPv3 でカプセル化したあとのパケットを、経路情報に従わず、指定した tunnel または VPN セレクタと紐付く tunnel に転送します。また、指定した tunnel または VPN セレクタと紐付く tunnel 以外から受信した L2TPv3 のパケットを破棄します。

【実行例】

IPsec で使用している tunnel インタフェースを設定します (tunnel 番号 : 1)。

```
#configure terminal
(config)#l2tpv3 tunnel-profile l2tpv3-A
(config-l2tpv3)#tunnel protection ipsec tunnel 1
```

【未設定時】

経路情報に従って L2TPv3 のパケットを送信します。

23.1.22 tunnel source

【機能】

L2TPv3 トンネルを確立する自装置の IP アドレスの設定

【入力形式】

tunnel source <IP アドレス>

no tunnel source [<IP アドレス>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
IP アドレス	L2TPv3 トンネルを確立する自装置の IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

【動作モード】

L2TPv3 プロファイル設定モード

【説明】

L2TPv3 トンネルを確立する自装置の IP アドレスを設定します。

【実行例】

L2TPv3 トンネルを確立する自装置の IP アドレスを設定します (IP アドレス : 192.0.2.1)。

```
#configure terminal
(config)#l2tpv3 tunnel-profile l2tpv3-A
(config-l2tpv3)#tunnel source 192.0.2.1
```

【未設定時】

L2TPv3 トンネルを確立する対向装置と通信するインタフェースの IP アドレスを送信元アドレスとします。

23.1.23 always-up

【機能】

常に L2TPv3 セッションを確立しておく設定

【入力形式】

always-up

no always-up

【動作モード】

L2TPv3 Pseudowire 設定モード

【説明】

常に L2TPv3 セッションを確立しておく場合に設定します。なんらかの原因でセッションが解放されてしまった場合には、セッション確立動作を行います。

L2TPv3 ピアのアドレスが不定の場合は、セッション確立動作ができませんので、そのようなケースではご使用になれません。

【実行例】

常にセッションを確立する設定をします。

```
#configure terminal
(config)#l2tpv3 pseudowire session-A
(config-l2tpv3-pseudowire)#always-up
```

【未設定時】

同様の関連コマンドとして 2 つの設定がありますが以下の順で適用されます。

- always-up (L2TPv3 Pseudowire 設定モード)
- l2tpv3 always-up (基本設定モード)

どの設定もない場合、セッションが解放されても自動で接続開始しません。

23.1.24 cookie size

【機能】

L2TPv3 ヘッダにつける Cookie のサイズの設定

【入力形式】

cookie size {4 | 8}

no cookie size [4 | 8]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
4 8	L2TPv3 ヘッダにつける Cookie のサイズを指定します。	-	省略不可

【動作モード】

L2TPv3 Pseudowire 設定モード

【説明】

データプレーンの自局でカプセル化する L2TPv3 ヘッドにつける Cookie のサイズを設定します。

【実行例】

L2TPv3 ヘッドにつける Cookie のサイズを設定します (8)。

```
#configure terminal
(config)#l2tpv3 pseudowire session-A
(config-l2tpv3-pseudowire)#cookie size 8
```

【未設定時】

L2TPv3 Cookie を使用しません。

23.1.25 pw-type

【機能】

Pseudowire Type の設定

【入力形式】

pw-type {etherport | ethervlan}

no pw-type [{etherport | ethervlan}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
etherport ethervlan	Pseudowire Type を指定します。	etherport: Ethernet Pseudowire Type(5) ethervlan: Ethernet VLAN Pseudowire Type(4)	省略不可

【動作モード】

L2TPv3 Pseudowire 設定モード

【説明】

L2TPv3 ネゴシエーションで使用する Pseudowire Type を設定します。

【実行例】

L2TPv3 ネゴシエーションで使用する Pseudowire Type を設定します (pw-type: ethervlan)。

```
#configure terminal
(config)#l2tpv3 pseudowire session-A
(config-l2tpv3-pseudowire)#pw-type ethervlan
```

【未設定時】

etherport で動作します。

23.1.26 remote-end-id ascii

【機能】

セッションを識別するための ID の設定

【入力形式】

remote-end-id ascii <ID 名>

no remote-end-id ascii <ID 名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ID 名	L2TPv3 でセッションを識別するための ID を指定します。	128 文字以内の STRING 型	省略不可

【動作モード】

L2TPv3 Pseudowire 設定モード

【説明】

L2TPv3 でセッションを識別するための ID を設定します。

対向装置から受信する Remote End ID AVP に含まれる値と一致させる必要があります。

【実行例】

L2TPv3 でセッションを識別するための ID を設定します (ID 名: id-A)。

```
#configure terminal
(config)#l2tpv3 pseudowire session-A
(config-l2tpv3-pseudowire)#remote-end-id id-A
```

【未設定時】

L2TPv3 が使用できません。

23.1.27 sequencing both

【機能】

sequencing の設定

【入力形式】

sequencing both

no sequencing [both]

【動作モード】

L2TPv3 Pseudowire 設定モード

【説明】

sequencing を使用し、順序が入れ替わったパケットを破棄する場合に設定します。

【実行例】

順序が入れ替わったパケットを破棄します。

```
#configure terminal
(config)#l2tpv3 pseudowire session-A
(config-l2tpv3-pseudowire)#sequencing both
```

【未設定時】

sequencing を使用しません。

23.1.28 set mtu

【機能】

MTU 長の設定

【入力形式】

set mtu <MTU 長>

no set mtu [<MTU 長>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
MTU 長	MTU 長（単位：bytes）を指定します。	1280～9100	省略不可

【動作モード】

L2TPv3 Pseudowire 設定モード

【説明】

L2TPv3 トンネルインタフェースの MTU 長（単位：bytes）を設定します。送信時の MTU 値はカプセル化後のパケットに対して適用されます。

カプセル化後のパケットが IPv6 である場合、実際に送信する port-channel インタフェース設定モードで設定されている MTU 長よりも、L2TPv3 トンネルインタフェースの MTU 長の方が小さくなるように設定してください。

MTU に従いパケットを分割する場合、基本的に均等な長さにパケットを分割します。しかし、コントロールプレーンから送信する、またはコントロールプレーンを経由して中継する際に分割するケースでは、MTU 長に合わせたパケットの分割を実施します。

【実行例】

L2TPv3 トンネルインタフェースの MTU 長を設定します（MTU 長：1280bytes）。

```
#configure terminal
(config)#l2tpv3 pseudowire session-A
(config-l2tpv3-pseudowire)#set mtu 1280
```

【未設定時】

MTU 長は 1500bytes で動作します。

23.1.29 set profile

【機能】

L2TPv3 プロファイルの設定

【入力形式】

set profile <プロファイル名>

no set profile [<プロファイル名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プロファイル名	L2TPv3 プロファイルを指定します。	63文字以内のCDATA型	省略不可

【動作モード】

L2TPv3 Pseudowire 設定モード

【説明】

L2TPv3 プロファイルを設定します。

【実行例】

L2TPv3 プロファイルを設定します (プロファイル名: profile-A)。

```
#configure terminal
(config)#l2tpv3 pseudowire session-A
(config-l2tpv3-pseudowire)#set profile profile-A
```

【未設定時】

L2TPv3が使用できません。

第24章 bridge の設定



この章では、bridge の設定に関するコマンドについて説明します。

24.1 bridge の設定

24.1.1 bridge-group

【機能】

bridge 設定モードへの移行

【入力形式】

bridge-group <ブリッジグループ番号>

no bridge-group <ブリッジグループ番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ブリッジグループ番号	ブリッジグループ番号を指定します。	1 ～ 16777215	省略不可

【動作モード】

基本設定モード

【説明】

bridge 設定モードに移行します。コマンドの先頭に "no" を指定することで、該当 bridge 設定モードの内容がすべて消去されます。

【実行例】

bridge 設定モードに移行します（ブリッジグループ番号：100）。

```
#configure terminal
(config)#bridge-group 100
(config-bridge 100)#
```

24.1.2 bridge loop-detect-disable

【機能】

MAC アドレス切り替えりによるループ検知機能を無効にする設定

【入力形式】

bridge loop-detect-disable

no bridge loop-detect-disable

【動作モード】

bridge 設定モード

【説明】

MAC アドレス切り替わりによるループ検知機能を無効にする場合に設定します。本設定を行うとループ発生を検知する状態になっても、警告ログ出力、および検知した MAC アドレスの記録、インタフェースの loop-detected 状態への移行を行いません。

【実行例】

MAC アドレス切り替わりによるループ検知機能を無効にします。

```
#configure terminal
(config)#bridge-group 100
(config-bridge 100)#bridge loop-detect-disable
```

【未設定時】

MAC アドレス切り替わりによるループ検知機能は有効で動作します。

24.1.3 bridge loop-detect-time

【機能】

ループが発生したと判断するまでの時間の設定

【入力形式】

bridge loop-detect-time [<時間>]

no bridge loop-detect-time [<時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
時間	ループが発生したと判断するまでの時間（単位：秒）を指定します。	2～60	省略不可

【動作モード】

bridge 設定モード

【説明】

ループが発生したと判断するまでの時間（単位：秒）を設定します。MAC アドレス移動回数が 1 秒間に 1 回以上発生する状態が指定した時間継続した場合にループが発生したと判断します。

loop-detect-disable コマンドが設定されている場合は無効になります。

【実行例】

ループが発生したと判断するまでの時間（単位：秒）を設定します（時間：10 秒）。

```
#configure terminal
(config)#bridge-group 100
(config-bridge 100)#bridge loop-detect-time 10
```

【未設定時】

5 秒で動作します。

24.1.4 bridge transparent eap

【機能】

設定したインタフェース／ブリッジで受信した EAPOL フレームを L2 中継する設定

【入力形式】

bridge transparent eap

no bridge transparent eap

【動作モード】

bridge 設定モード

【説明】

設定したインタフェース／ブリッジで受信した EAPOL フレームを通常のマルチキャストと同様に L2 中継する場合に設定します（EAP 透過機能）。

【実行例】

設定したインタフェース／ブリッジで受信した EAPOL フレームを通常のマルチキャストと同様に L2 中継します。

```
#configure terminal
(config)#bridge-group 100
(config-bridge 100)#bridge transparent eap
```

【未設定時】

受信した EAPOL フレームは廃棄されます。

24.1.5 bridge transparent bpdu

【機能】

設定したインタフェース／ブリッジで受信した BPDU フレームを L2 中継する設定

【入力形式】

bridge transparent bpdu

no bridge transparent bpdu

【動作モード】

bridge 設定モード

【説明】

設定したインタフェース／ブリッジで受信した BPDU フレームを通常のマルチキャストと同様に L2 中継する場合に設定します（BPDU 透過機能）。

【実行例】

設定したインタフェース／ブリッジで受信した BPDU フレームを通常のマルチキャストと同様に L2 中継します。

```
#configure terminal
(config)#bridge-group 100
(config-bridge 100)#bridge transparent bpdu
```

【未設定時】

受信した BPDU フレームは廃棄されます。

24.1.6 bridge transparent lacp

【機能】

設定したインタフェース／ブリッジで受信した LACP フレームを L2 中継する設定

【入力形式】

bridge transparent lacp

no bridge transparent lacp

【動作モード】

bridge 設定モード

【説明】

設定したインタフェース／ブリッジで受信した LACP フレーム (01:80:C2:00:00:02) を通常のマルチキャストと同様に L2 中継します (LACP 透過機能)。

【実行例】

設定したインタフェース／ブリッジで受信した LACP フレーム (01:80:C2:00:00:02) を通常のマルチキャストと同様に L2 中継します。

```
#configure terminal
(config)#bridge-group 100
(config-bridge 100)#bridge transparent lacp
```

【未設定時】

受信した LACP フレームは廃棄されます。

24.1.7 bridge transparent other

【機能】

設定したインタフェース／ブリッジで受信した 01:80:C2:00:00:04～01:80:C2:00:00:10 および 01:80:C2:00:00:20～01:80:C2:00:00:2F のフレームを L2 中継する設定

【入力形式】

bridge transparent other

no bridge transparent other

【動作モード】

bridge 設定モード

【説明】

設定したインタフェース／ブリッジで受信した 01:80:C2:00:00:04～01:80:C2:00:00:10 および 01:80:C2:00:00:20～01:80:C2:00:00:2F のフレームを通常のマルチキャストと同様に L2 中継します (other フレーム透過機能)。

【実行例】

設定したインタフェース／ブリッジで受信した 01:80:C2:00:00:04～01:80:C2:00:00:10 および 01:80:C2:00:00:20～01:80:C2:00:00:2F のフレームを通常のマルチキャストと同様に L2 中継します。

```
#configure terminal
(config)#bridge-group 100
(config-bridge 100)#bridge transparent bridge transparent other
```

【未設定時】

受信した 01:80:C2:00:00:04～01:80:C2:00:00:10 および 01:80:C2:00:00:20～01:80:C2:00:00:2F のフレームは廃棄されます。

24.1.8 mac-address-table max-entry

【機能】

ブリッジ学習の最大エントリ数をブリッジグループ単位で制限する設定

【入力形式】

mac-address-table max-entry <最大学習エントリ数> [threshold <警告エントリ数>]

no mac-address-table max-entry [<最大学習エントリ数> [threshold [<警告エントリ数>]]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
最大学習エントリ数	ブリッジ最大学習エントリ数を指定します。	0～64535	省略不可
警告エントリ数	ログを出力する警告エントリ数を指定します。	1～64535	ログを出力しない

【動作モード】

bridge 設定モード

【説明】

ブリッジ学習の最大エントリ数をブリッジグループ単位で制限する場合に設定します。最大学習エントリ数に到達した場合、学習できないことを通知するログを出力します。また、警告エントリ数を指定することで最大学習エントリ数に到達する前にログを出力できます。警告ログは警告エントリ数に到達したときに出力されます。なお、いったん警告ログを出力すると、clear mac-address-table max-entry warning コマンドを実行されるまでの間、学習数の変化によらず警告ログは出力されなくなります。



- 最大学習エントリ数 ≤ 警告学習エントリ数となるように設定を行った場合、警告学習エントリ数の設定は無視されます。
- 本コマンドを使用して最大学習エントリ数、警告エントリ数を変更した場合、現在のエントリ数の状態に応じて以下の処理が行われます。
 - 最大学習エントリ数 > 現在の学習エントリ数：変化なし
 - 最大学習エントリ数 = 現在の学習エントリ数：最大学習エントリ数到達ログ出力
 - 最大学習エントリ数 < 現在の学習エントリ数：エラーログを出力
 - 警告学習エントリ数 > 現在の学習エントリ数：変化なし
 - 警告学習エントリ数 ≤ 現在の学習エントリ数：警告ログ出力
- 最大学習エントリ数は、静的 MAC テーブル数を含みません。

【実行例】

ブリッジグループの最大学習エントリ数を制限します（最大学習エントリ数：100、警告エントリ数：なし）。

```
#configure terminal
(config)#bridge-group 100
(config-bridge 100)#mac-address-table max-entry 100
```

【未設定時】

以下の値で動作します。

最大学習エントリ数：64535

警告エントリ数：なし

24.1.9 mac-address-table cvid-enable

【機能】

mac-address-table への学習の有効／無効の切り替え

【入力形式】

mac-address-table cvid-enable

no mac-address-table cvid-enable

【動作モード】

bridge 設定モード

【説明】

mac-address-table への学習を cvid（カスタム VLAN ID）込みで学習します。本設定の有効／無効設定を切り替えると、学習した mac-address が使えなくなるので、clear mac-address-table コマンドを実行して設定を変更した bridge の mac-address-table の内容を消去する必要があります。

【実行例】

bridge-group 100 に対して cvid 込みの学習機能を有効にします。

```
#configure terminal
(config)#bridge-group 100
(config-bridge 100)#mac-address-table cvid-enable
```

【未設定時】

cvid は学習テーブルの情報に含めません。

第25章 QoS/CoS の設定



この章では、QoS/CoS の設定に関するコマンドについて説明します。

25.1	classifier の登録	779
25.2	service-policy の登録	789
25.3	Traffic Manager の設定	803
25.4	データコネクットの QoS/CoS の設定	821

QoS/CoS 機能について

- IPsec 機能と QoS 機能を併用する場合の注意事項

IPsec 中継に QoS 機能を適用した場合、暗号化パケットがシーケンス番号順ではなく QoS の送信優先度順で中継されるため、対向装置側でシーケンス番号によるリプレイ攻撃防御機能（アンチリプレイ機能）が有効化されていると、優先度の低いパケットがリプレイ攻撃と認識されて廃棄される場合があります。

IPsec 機能と QoS 機能を併用する場合には、対向装置側でシーケンス番号によるアンチリプレイ機能を無効にしてください。

25.1 classifier の登録

25.1.1 class-map

【機能】

class-map 設定モードへの移行

【入力形式】

class-map <class-map 名>

no class-map <class-map 名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
class-map 名	class-map 名を指定します。	63 文字以内の TMNAME 型	省略不可

【動作モード】

基本設定モード

【説明】

class-map 設定モードに移行します。コマンドの先頭に "no" を指定することで、該当 class-map 設定モードの内容がすべて消去されます。

【実行例】

class-map 設定モードに移行します (class-map 名: class-map-A)。

```
#configure terminal
(config)#class-map class-map-A
(config-cmap)#
```

25.1.2 match-all

【機能】

すべての match コマンドに一致した場合に QoS/CoS 機能の対象とする設定

【入力形式】

match-all

no match-all

【動作モード】

class-map 設定モード

【説明】

class-map 内の複数の match コマンドについて、すべての match コマンドに一致した場合に QoS/CoS 機能の対象とします。

【実行例】

すべての match コマンドに一致した場合に QoS/CoS 機能の対象とします。

```
#configure terminal
(config)#class-map class-map-A
(config-cmap)#match-all
```

【未設定時】

match-any の設定があれば match-any で動作します。match-all/match-any どちらの設定もない場合は、match-all で動作します。

25.1.3 match-any

【機能】

1 つ以上の match コマンドに一致した場合に QoS/CoS 機能の対象とする設定

【入力形式】

match-any

no match-any

【動作モード】

class-map 設定モード

【説明】

class-map 内の複数の match コマンドについて、1 つ以上の match コマンドに一致した場合に QoS/CoS 機能の対象とします。match-all コマンドと同時に設定した場合は match-all コマンドが優先となります。match-all から match-any に設定を変更する場合は、一度 match-all を削除してから、match-any を入力してください。

【実行例】

1 つ以上の match コマンドに一致した場合に QoS/CoS 機能の対象とします。

```
#configure terminal
(config)#class-map class-map-A
(config-cmap)#match-any
```

【未設定時】

match-all で動作します。

25.1.4 match 802.1p priority

【機能】

指定した VLAN タグプライオリティを持つパケットにマッチする条件の設定

【入力形式】

match 802.1p priority <802.1p priority 値>

no match 802.1p priority <802.1p priority 値>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
802.1p priority 値	VLAN ヘッダ内の priority フィールドの値を指定します。	0～7	省略不可

【動作モード】

class-map 設定モード

【説明】

指定した VLAN タグプライオリティを持つパケットにマッチする条件を設定します。

ポリシールーティング機能で適用されるパケットの条件には使えません。

【実行例】

指定した VLAN タグプライオリティを持つパケットにマッチする条件を設定します（802.1p priority 値：0）。

```
#configure terminal
(config)#class-map class-map-A
(config-cmap)#match 802.1p priority 0
```

【未設定時】

条件を設定しません。

25.1.5 match any

【機能】

すべてのパケットに QoS/CoS 機能を適用させることを登録する設定

【入力形式】

match any

no match any

【動作モード】

class-map 設定モード

【説明】

すべてのパケットに QoS/CoS 機能を適用させることを登録します。

ポリシールーティング機能で適用されるパケットの条件には使えません。

【実行例】

すべてのパケットに QoS/CoS 機能を適用させることを登録します。

```
#configure terminal
(config)#class-map class-map-A
(config-cmap)#match any
```

【未設定時】

すべてのパケットに QoS/CoS 機能を適用させることを登録しません。

25.1.6 match ip access-group

【機能】

QoS/CoS 機能を適用させる IPv4 パケットの条件を指定したアクセスリストを登録する設定

【入力形式】

match ip access-group <アクセスリスト番号>

no match ip access-group <アクセスリスト番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アクセスリスト番号	アクセスリスト番号を指定します。	アクセスリスト番号	省略不可

【動作モード】

class-map 設定モード

【説明】

QoS/CoS 機能を適用させる IPv4 パケットの条件を指定したアクセスリストを登録します。

action が permit のアクセスリストのみ指定可能です。

action が deny のアクセスリストを指定した場合は、そのアクセスリストは無効になります。

【実行例】

QoS/CoS 機能を適用させる IPv4 パケットの条件を指定したアクセスリストを登録します（アクセスリスト番号：100）。

```
#configure terminal
(config)#class-map class-map-A
(config-cmap)#match ip access-group 100
```

【未設定時】

アクセスリストを登録しません。

25.1.7 match ip dscp

【機能】

IP パケットで、かつ、IP ヘッダ内の DSCP 値が指定した値のパケットにマッチする条件の設定

【入力形式】

match ip dscp {<DSCP 値>|<DSCP 名>}

no match ip dscp {<DSCP 値>|<DSCP 名>}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
DSCP 値 DSCP 名	DSCP 値を指定します。	DSCP 値：0～63 DSCP 名： af11,af12,af13,af21,af22,af23,af31,af32,af33,af41,af42,af43,bf,ef	省略不可

【動作モード】

class-map 設定モード

【説明】

IP パケットで、かつ、IP ヘッダ内の DSCP 値が指定した値のパケットにマッチする条件を設定します。
ポリシールーティング機能で適用されるパケットの条件には使えません。

【実行例】

IP パケットで、かつ、IP ヘッダ内の DSCP 値が指定した値のパケットにマッチする条件を設定します (DSCP 値：0)。

```
#configure terminal
(config)#class-map class-map-A
(config-cmap)#match ip dscp 0
```

【未設定時】

マッチ条件を設定しません。

25.1.8 match ip precedence

【機能】

IP パケットで、かつ、IP ヘッダ内の ToS バイトの上位 3bits が指定した値のパケットにマッチする条件の設定

【入力形式】

match ip precedence {<precedence 値>|<precedence 名>}

no match ip precedence {<precedence 値>|<precedence 名>}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
precedence 値 precedence 名	IP ヘッダの ToS バイトの上位 3bits の値を指定します。	precedence 値：0～7 precedence 名： critical,flash,flash-override,immediate,internet,network,priority,routine	省略不可

【動作モード】

class-map 設定モード

【説明】

IP パケットで、かつ、IP ヘッダ内の ToS バイトの上位 3bits が指定した値のパケットにマッチする条件を設定します。

ポリシールーティング機能で適用されるパケットの条件には使えません。

【実行例】

IP パケットで、かつ、IP ヘッダ内の ToS バイトの上位 3bits が指定した値のパケットにマッチする条件を設定します（precedence 値：1）。

```
#configure terminal
(config)#class-map class-map-A
(config-cmap)#match ip precedence 1
```

【未設定時】

マッチ条件を設定しません。

25.1.9 match ip tos

【機能】

IP パケットで、かつ、IP ヘッダ内の ToS バイトの 1bit から 8bit が指定した値のパケットにマッチする条件の設定

【入力形式】

match ip tos <ToS 値>

no match ip tos <ToS 値>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ToS 値	IP ヘッダの ToS バイトの値を指定します。	0 ～ 255	省略不可

【動作モード】

class-map 設定モード

【説明】

IP パケットで、かつ、IP ヘッダ内の ToS バイトが指定した値のパケットにマッチする条件を設定します。

ポリシールーティング機能で適用されるパケットの条件には使えません。

【実行例】

IP パケットで、かつ、IP ヘッダ内の ToS バイトが指定した値のパケットにマッチする条件を設定します（ToS 値：1）。

```
#configure terminal
(config)#class-map class-map-A
(config-cmap)#match ip tos 1
```

【未設定時】

マッチ条件を設定しません。

25.1.10 match local-source

【機能】

自局が送信したパケットにマッチする条件の設定

【入力形式】

match local-source

no match local-source

【動作モード】

class-map 設定モード

【説明】

自局が送信したパケットにマッチする条件を設定します。

ポリシールーティング機能で適用されるパケットの条件には使えません。

【実行例】

自局が送信したパケットにマッチする条件を設定します。

```
#configure terminal
(config)#class-map class-map-A
(config-cmap)#match local-source
```

【未設定時】

条件を設定しません。

25.1.11 match ipv6 access-group

【機能】

QoS/CoS 機能を適用させる IPv6 パケットの条件を指定したアクセスリストを登録する設定

【入力形式】

match ipv6 access-group <アクセスリスト番号>

no match ipv6 access-group <アクセスリスト番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アクセスリスト番号	アクセスリスト番号を指定します。	アクセスリスト番号	省略不可

【動作モード】

class-map 設定モード

【説明】

QoS/CoS 機能を適用させる IPv6 パケットの条件を指定したアクセスリストを登録します。

【実行例】

QoS/CoS 機能を適用させる IPv6 パケットの条件を指定したアクセスリストを登録します（アクセスリスト番号：4000）。

```
#configure terminal
(config)#class-map class-map-A
(config-cmap)#match ipv6 access-group 4000
```

【未設定時】

アクセスリストを登録しません。

25.1.12 match mac access-group

【機能】

L2 中継パケットに対して、指定したアクセスリストによってマッチする条件の登録の設定

【入力形式】

match mac access-group <アクセスリスト番号>

no match mac access-group <アクセスリスト番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アクセスリスト番号	アクセスリスト番号を指定します。	500～599、 5000～5999、 50000～59999、 500000～599999	省略不可

【動作モード】

class-map 設定モード

【説明】

L2 中継パケットに対して、指定したアクセスリストによってマッチする条件を登録します。

【実行例】

L2 中継パケットに対して、指定したアクセスリストによってマッチする条件を登録します（アクセスリスト番号：500）。

```
#configure terminal
(config)#class-map class-map-A
(config-cmap)#match mac access-group 500
```

【未設定時】

マッチ条件を設定しません。

25.1.13 match mac unknown-unicast

【機能】

L2 中継パケットのうち、unknown unicast パケットにマッチする条件の設定

【入力形式】

match mac unknown-unicast

no match mac unknown-unicast

【動作モード】

class-map 設定モード

【説明】

L2 中継パケットのうち、unknown unicast パケットにマッチする条件を設定します。

【実行例】

L2 中継パケットのうち、unknown unicast パケットにマッチする条件を設定します。

```
#configure terminal
(config)#class-map class-map-A
(config-cmap)#match mac unknown-unicast
```

【未設定時】

マッチ条件を設定しません。

25.1.14 match mac stag-priority

【機能】

L2 中継パケットのうち、サービスタグのプライオリティフィールドが指定した値を持つパケットにマッチする条件の設定

【入力形式】

match mac stag-priority <プライオリティ値>

no match mac ctag-priority <プライオリティ値>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プライオリティ値	プライオリティ値を指定します。	0～7	省略不可

【動作モード】

class-map 設定モード

【説明】

L2 中継パケットのうち、サービスタグのプライオリティフィールドが指定した値を持つパケットにマッチする条件を設定します。

【実行例】

L2 中継パケットのうち、サービスタグのプライオリティフィールドが指定した値を持つパケットにマッチする条件を設定します（プライオリティ値：1）。

```
#configure terminal
(config)#class-map class-map-A
(config-cmap)#match mac stag-priority 1
```

【未設定時】

マッチ条件を設定しません。

25.1.15 match mac ctag-priority

【機能】

L2 中継パケットのうち、カスタマタグのプライオリティフィールドが指定した値を持つパケットにマッチするマッチ条件の設定

【入力形式】

match mac ctag-priority <プライオリティ値>

no match mac ctag-priority <プライオリティ値>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プライオリティ値	プライオリティ値を指定します。	0～7	省略不可

【動作モード】

class-map 設定モード

【説明】

L2 中継パケットのうち、カスタマタグのプライオリティフィールドが指定した値を持つパケットにマッチするマッチ条件を設定します。

【実行例】

L2 中継パケットのうち、カスタマタグのプライオリティフィールドが指定した値を持つパケットにマッチするマッチ条件を設定します（プライオリティ値：1）。

```
#configure terminal
(config)#class-map class-map-A
(config-cmap)#match mac ctag-priority 1
```

【未設定時】

マッチ条件を設定しません。

25.2 service-policy の登録

25.2.1 policy-map

【機能】

policy-map 設定モードへの移行

【入力形式】

policy-map <policy-map 名>

no policy-map <policy-map 名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
policy-map 名	policy-map 名を指定します。	63 文字以内の TMNAME 型	省略不可

【動作モード】

基本設定モード

【説明】

policy-map 設定モードに移行します。コマンドの先頭に "no" を指定することで、該当 policy-map 設定モードの内容がすべて消去されます。

【実行例】

policy-map 設定モードに移行します (policy-map 名 : policy-map-A)。

```
#configure terminal
(config)#policy-map policy-map-A
(config-pmap)#
```

25.2.2 class

【機能】

policy-map-class 設定モードへの移行

【入力形式】

class {<class-map 名> | class-default}

no class {<class-map 名> | class-default}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
class-map 名	class-map 名を指定します。	63 文字以内の TMNAME 型	省略不可
class-default	どのクラスにも属さないフローに対するポリシーを設定する場合に指定します。	-	

【動作モード】

policy-map 設定モード

【説明】

policy-map-class 設定モードに移行します。コマンドの先頭に "no" を指定することで、該当 policy-map-class 設定モードの内容がすべて消去されます。

【実行例】

policy-map-class 設定モードに移行します (class-map 名 : policy-map-class-A)。

```
#configure terminal
(config)#policy-map policy-map-A
(config-pmap)#class policy-map-class-A
(config-pmap-c)#
```

25.2.3 bandwidth

【機能】

ユーザレベルスケジューラの割り当て

【入力形式】

bandwidth profile <bandwidth プロファイル名>

no bandwidth [profile <bandwidth プロファイル名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
bandwidth プロファイル名	bandwidth プロファイル名を指定します。	63 文字以内の TMNAME 型	省略不可

【動作モード】

policy-map-class 設定モード

【説明】

クラスにマッチしたトラフィックに対して、ユーザレベルスケジューラを割り当てます。

Output のみで動作します (Input に設定した場合、無効となります)。

指定したプロファイルが設定されていない場合は、ログを出してコマンドは無視されます。

本コマンドは ipinip tunnel インタフェースに設定した場合、無効になります。

bandwidth コマンドの追加と削除の設定変更を同時に行った場合に、変更前の bandwidth コマンド設定数と追加した bandwidth コマンド数の合計がポートスケジューラの bandwidth scale 設定数を超えていた場合は、たとえ設定変更後の bandwidth コマンド設定数が bandwidth scale 設定数を超えていなくても、追加した bandwidth コマンドの一部または全部が設定できない場合があります。

無効となった設定は show policy-map interface コマンドの出力結果で (failed) と表示されます。

再度 refresh を実行した際に、現在の bandwidth コマンド設定数が bandwidth scale 設定数を超えていなければ復旧します。

【実行例】

ユーザレベルスケジューラを割り当てます。

```
#configure terminal
(config)#policy-map policy-map-A
(config-pmap)#class policy-map-class-A
(config-pmap-c)#bandwidth profile policy-map-bandwidth-A
```

【未設定時】

ユーザレベルスケジューラを割り当てません。

25.2.4 count

【機能】

クラスにマッチしたパケット数をカウントする設定

【入力形式】

count

no count

【動作モード】

policy-map-class 設定モード

【説明】

クラスにマッチしたパケット数をカウントする場合に設定します。

【実行例】

クラスにマッチしたパケット数をカウントします。

```
#configure terminal
(config)#policy-map policy-map-A
(config-pmap)#class policy-map-class-A
(config-pmap-c)#count
```

【未設定時】

パケット数をカウントしません。

25.2.5 drop

【機能】

クラスにマッチするパケットの廃棄

【入力形式】

drop

no drop

【動作モード】

policy-map-class 設定モード

【説明】

クラスにマッチするパケットを廃棄します。

【実行例】

クラスにマッチするパケットを廃棄します。

```
#configure terminal
(config)#policy-map policy-map-A
(config-pmap)#class policy-map-class-A
(config-pmap-c)#drop
```

【未設定時】

パケットを廃棄しません。

25.2.6 extended-queue

【機能】

クラスにマッチしたトラフィックが入力される拡張キューの設定

【入力形式】

extended-queue <プライオリティ値> <キュー ID>

no extended-queue [<プライオリティ値> <キュー ID>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プライオリティ値	送信優先度を指定します。	0～4	省略不可
キュー ID	キュー ID を指定します。	0～3	

【動作モード】

policy-map-class 設定モード

【説明】

クラスにマッチしたトラフィックが入力される拡張キューを指定します。

Outputのみで動作します（Inputに設定しても無効です）。

ソフトキューイングの設定がされたクラスに extended-queue コマンドを設定しても、extended-queue コマンドの設定は反映されず、パケットはソフトキューイングのデフォルトのキューに入力されます。

【実行例】

クラスにマッチしたトラフィックが入力される拡張キューを指定します（プライオリティ値：1、キュー ID：2）。

```
#configure terminal
(config)#policy-map policy-map-A
(config-pmap)#class policy-map-class-A
(config-pmap-c)#extended-queue 1 2
```

【未設定時】

デフォルトの拡張キューにキューイングされます。

25.2.7 police

【機能】

ポリシングの設定

【入力形式】

police single cir <CIR 値> cbs <CBS 値> conform-action <conform アクション> exceed-action <exceed アクション>

no police [single cir <CIR 値> cbs <CBS 値> conform-action <conform アクション> exceed-action <exceed アクション>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
single	シングルタイプのポリシングを行います。	-	省略不可
CIR 値	committed information rate(CIR) 値 (単位: bps) を指定します。	8192 ~ 10000000000	省略不可
CBS 値	committed burst size(CBS) 値 (単位: bytes) を指定します。	1 ~ 536870912	省略不可
conform アクション	トラフィックフローのレートが CIR 値 / CBS 値以内と判定されたパケットに適用する QoS 処理を指定します。	transmit	省略不可
exceed アクション	トラフィックフローのレートが CIR 値 / CBS 値を超えたと判定されたパケットに適用する QoS 処理を指定します。	drop	省略不可

【動作モード】

policy-map-class 設定モード

【説明】

クラスにマッチしたトラフィックに対してのポリシングの設定をします。

ポリシングの各アクションに該当したパケットのバイト数は自動でカウントされ、show policy-map interface コマンドで表示することができます。

【実行例】

クラスにマッチしたトラフィックに対してのポリシングの設定をします (CIR 値: 1000000、CBS 値: 1024、conform アクション: transmit、exceed アクション: drop)。

```
#configure terminal
(config)#policy-map policy-map-A
(config-pmap)#class policy-map-class-A
(config-pmap-c)# police single cir 1000000 cbs 1024 conform-action transmit exceed-action drop
```

【未設定時】

ポリシングを行いません。

25.2.8 policing-header

【機能】

ポリシングを行う際の packetsize の補正値の設定

【入力形式】

policing-header <補正値>

no policing-header [<補正値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
補正値	ポリシング時の補正値を指定します。	-128 ~ 128	省略不可

【動作モード】

policy-map-class 設定モード

【説明】

police コマンドでポリシングを行う際の、ethernet packetsize に対する補正値を設定します。

補正の結果、packetsize がマイナスになる場合は、packetsize を 0 とします。

【実行例】

ethernet packetsize に対する補正値を設定します（補正値：20）。

```
#configure terminal
(config)#policy-map policy-map-A
(config-pmap)#class policy-map-class-A
(config-pmap-c)#policing-header 20
```

【未設定時】

補正値は 0 で動作します。

25.2.9 queue

【機能】

クラスにマッチしたトラフィックが入力されるキューの設定

【入力形式】

queue { besteffort | express | normal <キュー ID> }

no queue [{ besteffort | express | normal <キュー ID> }]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
besteffort	低優先キューを指定します。	-	省略不可
express	高優先キューを指定します。	-	省略不可
normal	中優先のキューを指定します。	-	省略不可
キュー ID	キュー ID を指定します。	0 ～ 5	省略不可

【動作モード】

policy-map-class 設定モード

【説明】

クラスにマッチしたトラフィックが入力されるキューを設定します。

同一クラス、または、上位クラスに、bandwidth コマンドの設定がない場合は、無効となります。

Output のみで動作します（Input に設定した場合、無効となります）。

本コマンドは ipinip tunnel インタフェースに設定した場合、無効になります。

【実行例】

QoS パラメタを設定します（中優先：normal、キュー ID：0）。

```
#configure terminal
(config)#policy-map policy-map-A
(config-pmap)#class policy-map-class-A
(config-pmap-c)#queue normal 0
```

【未設定時】

besteffort キューに入力されます。

25.2.10 search-sequence

【機能】

policy-map 内の検索優先度の設定

【入力形式】

search-sequence <検索優先度>

no search-sequence [<検索優先度>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
検索優先度	検索優先度を指定します。	1 ～ 65534	省略不可

【動作モード】

policy-map-class 設定モード

【説明】

policy-map 内の検索優先度を設定します。検索優先度の小さい方が優先的にマッチします。

【実行例】

検索優先度を設定します（検索優先度：100）。

```
#configure terminal
(config)#policy-map policy-map-A
(config-pmap)#class policy-map-class-A
(config-pmap-c)#search-sequence 100
```

【未設定時】

検索優先度は 65535 で動作します。

25.2.11 service-policy

【機能】

policy-map 名で指定したサービスポリシーの適用

【入力形式】

service-policy <policy-map 名>

no service-policy [<policy-map 名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
policy-map 名	policy-map 名を指定します。	63 文字以内の TMNAME 型	省略不可

【動作モード】

policy-map-class 設定モード

【説明】

policy-map 名で指定したサービスポリシーを適用します。

【実行例】

policy-map 名で指定したサービスポリシーを適用します（policy-map 名：policy-map-A）。

```
#configure terminal
(config)#policy-map policy-map-A
(config-pmap)#class policy-map-class-A
(config-pmap-c)#service-policy policy-map-A
```

【未設定時】

サービスポリシーは適用されません。

25.2.12 set 802.1p priority

【機能】

IP パケットの VLAN タグのプライオリティフィールドを書き換える設定

【入力形式】

set 802.1p priority <プライオリティ値>

no set 802.1p priority [<プライオリティ値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プライオリティ値	VLAN タグプライオリティの値を指定します。	0～7	省略不可

【動作モード】

policy-map-class 設定モード

【説明】

IP パケットの VLAN タグのプライオリティフィールドの書き換えを行う場合に設定します。

【実行例】

IP パケットの VLAN タグのプライオリティフィールドの書き換えを行います（プライオリティ値：0）。

```
#configure terminal
(config)#policy-map policy-map-A
(config-pmap)#class policy-map-class-A
(config-pmap-c)#set 802.1p priority 0
```

【未設定時】

書き換えを行いません。

25.2.13 set ip dscp

【機能】

IP パケットヘッダの ToS バイトの上位 6bit を書き換える設定

【入力形式】

set ip dscp <DSCP 値>

no set ip dscp [<DSCP 値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
DSCP 値	DSCP の値を指定します。	0～63	省略不可

【動作モード】

policy-map-class 設定モード

【説明】

IP パケットヘッダの ToS バイトの上位 6bit (DSCP フィールド) の書き換えを行う場合に設定します。

【実行例】

IP パケットヘッダの ToS バイトの上位 6bit (DSCP フィールド) の書き換えを行います (DSCP 値 : 0)。

```
#configure terminal
(config)#policy-map policy-map-A
(config-pmap)#class policy-map-class-A
(config-pmap-c)#set ip dscp 0
```

【未設定時】

書き換えを行いません。

25.2.14 set ip prec

【機能】

IP パケットの ToS バイトの上位 3bit(precedence)の書き換えを行う設定

【入力形式】

set ip prec <precedence 値>

no set ip prec [<precedence 値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
precedence 値	IP ヘッダの ToS バイトの上位 3bits の値を指定します。	0 ~ 7	省略不可

【動作モード】

policy-map-class 設定モード

【説明】

IP パケットの ToS バイトの上位 3bit(precedence)の書き換えを行う場合に設定します。

【実行例】

IP パケットの ToS バイトの上位 3bit(precedence)の書き換えを行います (precedence 値 : 1)。

```
#configure terminal
(config)#policy-map policy-map-A
(config-pmap)#class policy-map-class-A
(config-pmap-c)#set ip prec 1
```

【未設定時】

書き換えを行いません。

25.2.15 set ip tos

【機能】

IP パケットヘッダの ToS 値の書き換える設定

【入力形式】

set ip tos <tos 値>

no set ip tos [<tos 値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
tos 値	IP ヘッダの tos の値を指定します。	0 ～ 255	省略不可

【動作モード】

policy-map-class 設定モード

【説明】

IP パケットヘッダの ToS 値の書き換えを行う場合に設定します。

【実行例】

IP パケットヘッダの ToS 値の書き換えを行います (ToS 値 : 7)。

```
#configure terminal
(config)#policy-map policy-map-A
(config-pmap)#class policy-map-class-A
(config-pmap-c)#set ip tos 7
```

【未設定時】

書き換えを行いません。

25.2.16 set ipv6 dscp

【機能】

IPv6 パケットヘッダのトラフィッククラスフィールドの上位 6bit を書き換える設定

【入力形式】

set ipv6 dscp <DSCP 値>

no set ipv6 dscp [<DSCP 値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
DSCP 値	DSCP の値を指定します。	0 ～ 63	省略不可

【動作モード】

policy-map-class 設定モード

【説明】

IPv6 パケットヘッダのトラフィッククラスフィールドの上位 6bit (DSCP フィールド) の書き換えを行う場合に設定します。

【実行例】

IPv6 パケットヘッダのトラフィッククラスフィールドの上位 6bit (DSCP フィールド) の書き換えを行います (DSCP 値: 0)。

```
#configure terminal
(config)#policy-map policy-map-A
(config-pmap)#class policy-map-class-A
(config-pmap-c)#set ipv6 dscp 0
```

【未設定時】

書き換えを行いません。

25.2.17 set ipv6 traffic-class

【機能】

IPv6 パケットヘッダのトラフィッククラスフィールドを書き換える設定

【入力形式】

set ipv6 traffic-class <トラフィッククラス値>

no set ipv6 traffic-class [<トラフィッククラス値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
トラフィッククラス値	トラフィッククラスの値を指定します。	0～255	省略不可

【動作モード】

policy-map-class 設定モード

【説明】

IPv6 パケットヘッダのトラフィッククラスフィールドの書き換えを行う場合に設定します。

【実行例】

IPv6 パケットヘッダのトラフィッククラスフィールドの書き換えを行います (トラフィッククラス値: 0)。

```
#configure terminal
(config)#policy-map policy-map-A
(config-pmap)#class policy-map-class-A
(config-pmap-c)#set ipv6 traffic-class 0
```

【未設定時】

書き換えを行いません。

25.2.18 set mac stag-priority

【機能】

L2 中継パケットのサービスタグのプライオリティフィールドに指定された値を書き込む設定

【入力形式】

set mac stag-priority <プライオリティ値>

no set mac stag-priority [<プライオリティ値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プライオリティ値	プライオリティ値を指定します。	0～7	省略不可

【動作モード】

policy-map-class 設定モード

【説明】

L2 中継パケットのサービスタグのプライオリティフィールドに指定された値の書き込みを行う場合に設定します。

【実行例】

L2 中継パケットのサービスタグのプライオリティフィールドに指定された値の書き込みを行う設定をします（プライオリティ値：1）。

```
#configure terminal
(config)#policy-map policy-map-A
(config-pmap)#class policy-map-class-A
(config-pmap-c)#set mac stag-priority 1
```

【未設定時】

書き込みを行いません。

25.2.19 transmit

【機能】

クラスにマッチするパケットの送信

【入力形式】

transmit

no transmit

【動作モード】

policy-map-class 設定モード

【説明】

クラスにマッチするパケットを送信します。

【実行例】

クラスにマッチするパケットを送信します。

```
#configure terminal
(config)#policy-map policy-map-A
(config-pmap)#class policy-map-class-A
(config-pmap-c)#transmit
```

【未設定時】

パケットを送信します。送信されることを明示的に示したい場合に設定します。

25.3 Traffic Manager の設定

25.3.1 traffic-manager network

【機能】

traffic-manager-network 設定モードへの移行

【入力形式】

traffic-manager network

no traffic-manager network

【動作モード】

基本設定モード

【説明】

traffic-manager-network 設定モードに移行します。コマンドの先頭に "no" を指定することで、traffic-manager-network 設定モードの内容がすべて消去されます。

【実行例】

traffic-manager-network 設定モードに移行します。

```
#configure terminal
(config)#traffic-manager network
(config-tm-n)
```

25.3.2 traffic-manager extended

【機能】

traffic-manager-extended 設定モードへの移行

【入力形式】

traffic-manager extended

no traffic-manager extended

【動作モード】

基本設定モード

【説明】

traffic-manager-extended 設定モードに移行します。コマンドの先頭に "no" を指定することで、traffic-manager-extended 設定モードの内容がすべて消去されます。

【実行例】

traffic-manager-extended 設定モードに移行します。

```
#configure terminal
(config)#traffic-manager extended
(config-tm-e)
```

25.3.3 bandwidth profile

【機能】

traffic-manager-network-bandwidth プロファイル設定モードへの移行

【入力形式】

bandwidth profile <bandwidth プロファイル名>

no bandwidth profile <bandwidth プロファイル名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
bandwidth プロファイル名	bandwidth プロファイル名を指定します。	63 文字以内の TMNAME 型	省略不可

【動作モード】

traffic-manager-network 設定モード

【説明】

traffic-manager-network-bandwidth プロファイル設定モードに移行します。コマンドの先頭に "no" を指定することで、該当 traffic-manager-network-bandwidth プロファイル設定モードの内容がすべて消去されます。

【実行例】

traffic-manager-network-bandwidth プロファイル設定モードに移行します (bandwidth プロファイル名 : bw-A)。

```
#configure terminal
(config)#traffic-manager network
(config-tm-n)#bandwidth profile bw-A
(config-tm-n-bw-t bw-A)
```

25.3.4 port profile

【機能】

traffic-manager-network-port プロファイル設定モードへの移行

【入力形式】

port profile <port プロファイル名>

no port profile <port プロファイル名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
port プロファイル名	port プロファイル名を指定します。	63 文字以内の TMNAME 型	省略不可

【動作モード】

traffic-manager-network 設定モード

【説明】

traffic-manager-network-port プロファイル設定モードに移行します。コマンドの先頭に "no" を指定することで、該当 traffic-manager-network-port プロファイル設定モードの内容がすべて消去されます。

【実行例】

traffic-manager-network-port プロファイル設定モードに移行します (port プロファイル名: port-A)。

```
#configure terminal
(config)#traffic-manager network
(config-tm-n)#port profile port-A
(config-tm-n-port port-A)
```

25.3.5 port scheduler

【機能】

ポートレベルスケジューラを有効にする設定

【入力形式】

port scheduler <インタフェース名> <インタフェース番号> <ポートプロファイル名>

no port scheduler <インタフェース名> <インタフェース番号> [<ポートプロファイル名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース名	インタフェース名を指定します。	-	省略不可
インタフェース番号	インタフェース番号を指定します。	-	
ポートプロファイル名	ポートプロファイル名を指定します。	63 文字以内の TMNAME 型	

【動作モード】

traffic-manager-network 設定モード

【説明】

指定したポートプロファイル名に基づき、ポートレベルスケジューラを有効にします。

指定するポートプロファイル名を変更したり、削除した場合に既存のスケジューラにパケットが残留していると、それらのパケットは廃棄されます。

【実行例】

ポートレベルスケジューラを有効にします（インタフェース名：gigaethernet、インタフェース番号：1/1、ポートプロファイル名：port-A）。

```
#configure terminal
(config)#traffic-manager network
(config-tm-n)#port profile port-A
(config-tm-n-port port-A)#exit
(config-tm-n)#port scheduler gigaethernet 1/1 port-A
```

【未設定時】

ソフトキューイングを使用しません。

25.3.6 port scheduler

【機能】

拡張キューイングのポートレベルスケジューラのパラメタ設定

【入力形式】

port scheduler <インタフェース名> <インタフェース番号> <ポートプロファイル名>

no port scheduler <インタフェース名> <インタフェース番号> [<ポートプロファイル名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース名	インタフェース名を指定します。	-	省略不可
インタフェース番号	インタフェース番号を指定します。	-	
ポートプロファイル名	ポートプロファイル名を指定します。	63文字以内のTMNAME型	

【動作モード】

traffic-manager-extended 設定モード

【説明】

指定したポートプロファイル名に基づき、拡張キューイングのポートレベルスケジューラのパラメタを設定します。

【実行例】

拡張キューイングのポートレベルスケジューラのパラメタを設定します（インタフェース名：gigaethernet、インタフェース番号：1/1、ポートプロファイル名：rate-10M）。

```
#configure terminal
(config)#traffic-manager extended
(config-tm-e)#port profile rate-10M
(config-tm-e-port port-A)#shape pir 10000 pbs 1250
(config-tm-e-port port-A)#exit
(config-tm-e)#port scheduler gigaethernet 1/1 rate-10M
```

【未設定時】

シェーピングしません。

25.3.7 to-host protocol

【機能】

自局宛トラフィックが入力されるポリサーの設定

【入力形式】

to-host protocol {ipv4 | ipv6} <プロトコル名> policer <id>

no to-host protocol {ipv4 | ipv6} <プロトコル名> [policer <id>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ipv4 ipv6	プロトコルを指定します。	ipv4 ipv6	省略不可
プロトコル名	プロトコル名を指定します。	【IPv4 の場合】 bfd,bgp,dhcp,domain,ftp, icmp,ipsec-ha,isakmp, l2tp,l2tpv3,ntp, ospf, radius,snmp,ssh, survey, tacacs,telnet,vrrp,sip,rip 【IPv6 の場合】 bfd,bgp,dhcp,domain,ftp, icmp,ipsec-ha,isakmp, l2tp,l2tpv3,nd,ntp,ospf, snmp,ssh,survey,telnet, vrrp,sip	省略不可
id	ポリシングの ID を指定します	0 ～ 15	省略不可

【動作モード】

traffic-manager-network 設定モード

【説明】

デフォルトで自局宛優先制御対象となっているプロトコルについて、その自局宛トラフィックが入力されるポリサーを設定します。

【実行例】

自局宛トラフィックが入力されるポリサーを設定します (ipv4、プロトコル名：bgp、ポリサー ID：1)。

```
#configure terminal
(config)#traffic-manager network
(config-tm-n)#to-host protocol ipv4 bgp policer 1
```

【未設定時】

設定されていないプロトコルは、以下のポリサーを使用します。

IP バージョン	プロトコル名	policer ID
IPv4	bfd	4
	bgp	0
	dhcp	0
	domain	1
	ftp	1
	icmp	3
	ipsec-ha	2
	isakmp	2
	l2tp	2
	l2tpv3	2
	ntp	1
	ospf	0
	radius	1
	snmp	1
	ssh	1
	survey	4
	tacacs	1
	telnet	1
	vrrp	2
	sip	2
	rip	0

IP バージョン	プロトコル名	policer ID
IPv6	bfd	4
	bgp	0
	dhcp	0
	domain	1
	ftp	1
	icmp	3
	ipsec-ha	2
	isakmp	2
	l2tp	2
	l2tpv3	2
	nd	5
	ntp	1
	ospf	0
	snmp	1
	ssh	1
	survey	4
	telnet	1
	vrrp	2
	sip	2

25.3.8 to-host police

【機能】

ポリサーごとの QoS パラメタの設定

【入力形式】

to-host police <id> single cir <cir> cbs <cbs> conform-action {transmit | drop} exceed-action {transmit | drop}

no to-host police <id> [single cir <cir> cbs <cbs> conform-action {transmit | drop} exceed-action {transmit | drop}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
id	ポリシングの id を指定します。	0 ～ 15	省略不可
cir	ポリシングの committed information rate(pps) を指定します。	1 ～ 65535	省略不可
cbs	ポリシングの committed burst size(packets) を指定します。	1 ～ 65535	省略不可

パラメタ	設定内容	設定範囲	省略時
conform-action	トラフィックフローのレートが cir/cbs 以内と判定されたパケットに適用する QoS 処理を指定します。	transmit: パケットを送信します。 drop: パケットを廃棄します。	省略不可
exceed-action	トラフィックフローのレートが cir/cbs を超えたと判定されたパケットに適用する QoS 処理を指定します。	transmit: パケットを送信します。 drop: パケットを廃棄します。	省略不可

【動作モード】

traffic-manager-network 設定モード

【説明】

ポリサーごとの QoS パラメタを設定します。

【実行例】

ポリサーごとの QoS パラメタを設定します（ポリシング ID：1、cir：300、cbs：1024、cir/cbs 以内のパケット：送信、cir/cbs を超えるパケット：破棄する）。

```
#configure terminal
(config)#traffic-manager network
(config-tm-n)#to-host police 1 single cir 300 cbs 1024 conform-act transmit exceed-action drop
```

【未設定時】

以下の値で動作します。

id	cir(pps)	cbs(packets)	conform-action	exceed-action
0	3598	2048	transmit	drop
1	300	212	transmit	drop
2	6058	2000	transmit	drop
3	1024	1024	transmit	drop
4	512	1024	transmit	drop
5	512	1024	transmit	drop
6	512	512	transmit	drop
7	256	256	transmit	drop
それ以外	8192	8192	transmit	drop

25.3.9 to-host reason

【機能】

自局宛トラフィックが入力されるポリサーの指定

【入力形式】

to-host reason {<要因 ID> | {ipv4 | ipv6} <要因名> | arp | lacp | marker-protocol | micro-bfd | pppoe-discovery | pppoe-session} policer <id>

no to-host reason {<要因 ID> | {ipv4 | ipv6} <要因名> | arp | lacp | marker-protocol | micro-bfd | pppoe-discovery | pppoe-session} policer <id>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
要因 ID	自局転送要因の ID を指定します。	0 ～ 255	省略不可
要因名	自局転送要因名を指定します。	【IPv4 の場合】 arp-miss, arp-miss-link, broadcast, ip-option, localhost, reserved-multicast, route-error, route-unknown, too-big, ttl-expire, tunnel-error, tunnel-localhost, 【IPv6 の場合】 hop-by-hop, hop-limit, localhost, nb-miss, nb-miss-link, reserved-multicast, route-error, route-unknown, too-big, tunnel-error, tunnel-localhost,	省略不可
arp	ARP パケットを指定します。	-	省略不可
lACP	LACP(Link aggregation Control Protocol) パケットを指定します。	-	省略不可
marker-protocol	リンクアグリゲーションで用いる marker protocol パケットを指定します。	-	省略不可
pppoe-discovery	PPPoE の discovery ステージで使用するパケットを指定します。	-	省略不可
pppoe-session	PPPoE の session ステージで使用するパケットを指定します。	-	省略不可
id	ポリサーの id を指定します。	0 ～ 15	省略不可

【動作モード】

traffic-manager-network 設定モード

【説明】

自局宛トラフィックが入力されるポリサーを指定します。

【実行例】

自局宛トラフィックが入力されるポリサーを指定します (reason:localhost、ポリサー : 0)。

```
#configure terminal
(config)#traffic-manager network
(config-tm-n)#to-host reason ipv4 localhost policer 0
```

【未設定時】

すべての自局転送要因について、以下の値で動作します。

要因名	ポリサー ID
localhost	6
broadcast	6

要因名	ポリシー ID
reserved-multicast	7
ip-option	6
ttl-expire	7
arp-miss	7
arp-miss-link	7
route-unknown	7
tunnel-error	7
route-error	7
too-big	7
localhost	6
hop-by-hop	6
hop-limit	7
nb-miss	7
nb-miss-link	7
arp	5
tunnel-localhost	6
lACP	0
marker-protocol	1
pppoe-discovery	0
pppoe-session	0
Micro BFD	4

25.3.10 frame-overhead

【機能】

イーサネットフレーム長（FCS を除く）に追加するオーバーヘッド長（プリアンブルなど）の設定

【入力形式】

frame-overhead <フレームオーバーヘッド長>

no frame-overhead [<フレームオーバーヘッド長>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
フレームオーバーヘッド長	フレームオーバーヘッド長(bytes)を指定します。	0～256	省略不可

【動作モード】

traffic-manager-network-port プロファイル設定モード

【説明】

シェーピングの際にイーサネットフレーム長（FCS を除く）に追加するオーバーヘッド長（プリアンブルなど）を指定します。本コマンドの追加、削除、変更を行うとポートスケジューラが再設定されます。

【実行例】

イーサネットフレーム長に追加するオーバーヘッド長を指定します（オーバーヘッド長：4byte）。

```
#configure terminal
(config)#traffic-manager network
(config-tm-n)#port profile port-A
(config-tm-n-port port-A)# frame-overhead 4
```

【未設定時】

イーサネットフレーム長に追加されるオーバーヘッド長は 24byte となります。

25.3.11 shape

【機能】

シェーピングレートとバーストサイズの設定

【入力形式】

shape pir <シェーピングレート> [pbs <バーストサイズ>]

no shape [pir <シェーピングレート> pbs <バーストサイズ>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
シェーピングレート	シェーピングレート（単位：kbps）を指定します。	32 ～ 5000000	省略不可
バーストサイズ	バーストサイズ（単位：bytes）を指定します。	1 ～ 262144	1

【動作モード】

traffic-manager-network-port プロファイル設定モード

【説明】

シェーピングレートとバーストサイズを指定します。本コマンドの追加、削除、変更を行った結果、シェーピング動作に変更があった場合、ポートスケジューラが再設定されます。

【実行例】

シェーピングレートとバーストサイズを指定します（シェーピングレート：1000kbps、バーストサイズ：1024byte）。

```
#configure terminal
(config)#traffic-manager network
(config-tm-n)#port profile port-A
(config-tm-n-port port-A)# shape pir 1000 pbs 1024
```

【未設定時】

シェーピングレートは 2000000kbps、バーストサイズは 262144byte で動作します。

25.3.12 shape

【機能】

シェーピングレートとバーストサイズの設定

【入力形式】

shape pir <シェーピングレート> [pbs <バーストサイズ>]

no shape [pir <シェーピングレート> pbs <バーストサイズ>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
シェーピングレート	シェーピングレート（単位：kbps）を指定します。	1～2000000	省略不可
バーストサイズ	バーストサイズ（単位：bytes）を指定します。	1～262144	1

【動作モード】

traffic-manager-network-bandwidth プロファイル設定モード

【説明】

シェーピングレートとバーストサイズを指定します。

【実行例】

シェーピングレートとバーストサイズを指定します（シェーピングレート：1000kbps、バーストサイズ：1024byte）。

```
#configure terminal
(config)#traffic-manager network
(config-tm-n)#bandwidth profile bandwidth-A
(config-tm-n-bw bandwidth-A)# shape pir 1000 pbs 1024
```

【未設定時】

シェーピングレートは 2000000kbps、バーストサイズは 262144byte で動作します。

25.3.13 shape

【機能】

シェーピングレートとバーストサイズの設定

【入力形式】

shape pir <シェーピングレート> pbs <バーストサイズ>

no shape [pir <シェーピングレート> pbs <バーストサイズ>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
シェーピングレート	シェーピングレート（単位：kbps）を指定します。	33 ～ 2000000	省略不可
バーストサイズ	バーストサイズ（単位：bytes）を指定します。	2 ～ 130816	省略不可

【動作モード】

traffic-manager-extended-port プロファイル設定モード

【説明】

ポートごとのシェーピングレートとバーストサイズを指定します。

【実行例】

シェーピングレートとバーストサイズを指定します（シェーピングレート：1000kbps、バーストサイズ：1024byte）。

```
#configure terminal
(config)#traffic-manager extended
(config-tm-e)#port profile port-A
(config-tm-e-port port-A)# shape pir 1000 pbs 1024
```

【未設定時】

シェーピングしません。

25.3.14 bandwidth scale

【機能】

ユーザレベルスケジューラ数の設定

【入力形式】

bandwidth scale <スケジューラ>

no bandwidth scale [<スケジューラ>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
スケジューラ	設定可能なユーザレベルスケジューラ数を指定します。	1 ～ 4096	省略不可

【動作モード】

traffic-manager-network-port プロファイル設定モード

【説明】

ユーザレベルスケジューラ数を指定します。本コマンドの追加、削除、変更を行った結果、ユーザレベルスケジューラ数に変更があった場合、ポートスケジューラが再設定されます。

【実行例】

ユーザレベルスケジューラ数を指定します（ユーザレベルスケジューラ数：2）。

```
#configure terminal
(config)#traffic-manager network
(config-tm-n)#port profile port-A
(config-tm-n-port port-A)# bandwidth scale 2
```

【未設定時】

ユーザレベルスケジューラ数は、1 で動作します。

25.3.15 queue normal rate

【機能】

ユーザレベルスケジューラの中優先度のキューの WFQ 重みの設定

【入力形式】

queue normal <キュー ID> rate {<レート> | weight <WFQ 重み>}

no queue normal <キュー ID> rate [{<レート> | weight <WFQ 重み>}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
normalID	中優先度を指定します。	-	省略不可
キュー ID	キュー ID を指定します。	0 ～ 5	省略不可
レート	レート（単位：kbps）を指定します。	1 ～ 2000000	省略不可
WFQ 重み	WFQ 重みを指定します。	1 ～ 100	省略不可

【動作モード】

traffic-manager-network-bandwidth プロファイル設定モード

【説明】

ユーザレベルスケジューラの中優先度のキューの WFQ 重みを指定します。レートを指定した場合はシェーピングレートに対する指定レートの割合を WFQ 重みとして動作します。

輻輳時には指定した重みの割合で各キューから送信が行われます。

【実行例】

中優先度のキューの WFQ 重みを指定します（キュー ID：0、weight:1）。

```
#configure terminal
(config)#traffic-manager network
(config-tm-n)#bandwidth profile bandwidth-A
(config-tm-n-bw bandwidth-A)# queue normal 0 rate weight 1
```

【未設定時】

すべてのキューが WFQ 重み 1 で動作します。

25.3.16 queue limit

【機能】

最大キュー長をパケット数の設定

【入力形式】

queue {besteffort | express | normal <キュー ID>} limit <最大キュー長>

no queue {besteffort | express | normal <キュー ID>} limit [<最大キュー長>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
besteffort	低優先キューを指定します。	-	省略不可
express	高優先キューを指定します。	-	省略不可
normal	中優先キューを指定します。	-	省略不可
キュー ID	中優先度のキュー ID を指定します。	0 ～ 5	省略不可
最大キュー長	キュー長制限を指定します。	0 ～ 65536	省略不可

【動作モード】

traffic-manager-network-bandwidth プロファイル設定モード

【説明】

各キューの最大キュー長をパケット数で指定します。

【実行例】

最大キュー長のパケット数を指定します（優先度：normal、キュー ID：0、パケット数：1024）。

```
#configure terminal
(config)#traffic-manager network
(config-tm-n)#bandwidth profile bandwidth-A
(config-tm-n-bw bandwidth-A)#queue normal 0 limit 1024
```

【未設定時】

すべてのキューの最大キュー長にパケット数 256 が指定されたものとして動作します。

25.3.17 port profile

【機能】

traffic-manager-extended-port プロファイル設定モードへの移行

【入力形式】

port profile <port プロファイル名>

no port profile <port プロファイル名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
port プロファイル名	port プロファイル名を指定します。	63 文字以内の TMNAME 型	省略不可

【動作モード】

traffic-manager-extended 設定モード

【説明】

traffic-manager-extended-port プロファイル設定モードに移行します。コマンドの先頭に "no" を指定することで、該当 traffic-manager-extended-port プロファイル設定モードの内容がすべて消去されます。

【実行例】

traffic-manager-extended-port プロファイル設定モードに移行します (port プロファイル名: port-A)。

```
#configure terminal
(config)#traffic-manager extended
(config-tm-e)#port profile port-A
(config-tm-e-port port-A)
```

25.3.18 frame-overhead

【機能】

シェーピングの際にイーサネットフレーム長 (FCS を除く) に追加するオーバーヘッド長 (プリアンブルなど) の設定

【入力形式】

frame-overhead <フレームオーバーヘッド長>

no frame-overhead [<フレームオーバーヘッド長>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
フレームオーバーヘッド長	フレームオーバーヘッド長 (単位: bytes) を指定します。	0 ~ 255	省略不可

【動作モード】

traffic-manager-extended-port プロファイル設定モード

【説明】

シェーピングの際にイーサネットフレーム長 (FCS を除く) に追加するオーバーヘッド長 (プリアンブルなど) を指定します。

同じモードの shape コマンド、queue shape コマンドに対して同じ frame-overhead の値が適用されます。

【実行例】

イーサネットフレーム長に追加するオーバーヘッド長を指定します（オーバーヘッド長：4byte）。

```
#configure terminal
(config)#traffic-manager extended
(config-tm-e)#port profile port-A
(config-tm-e-port port-A)# frame-overhead 4
```

【未設定時】

イーサネットフレーム長に追加されるオーバーヘッド長は 24byte となります。

25.3.19 queue limit

【機能】

キューに溜められる最大パケット数の設定

【入力形式】

queue <プライオリティ値> <キュー ID> limit <最大パケット数>

no queue <プライオリティ値> <キュー ID> limit [< 最大パケット数>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プライオリティ値	送信優先度を指定します。	0～4	省略不可
キュー ID	キュー ID を指定します。	0～3	省略不可
最大パケット数	キューに溜められる最大パケット数を指定します。	8～256000	省略不可

【動作モード】

traffic-manager-extended-port プロファイル設定モード

【説明】

キューに溜められる最大パケット数を指定します。

【実行例】

キューに溜められる最大パケット数を指定します（プライオリティ値：0、キュー ID：0、最大パケット数：512）。

```
#configure terminal
(config)#traffic-manager extended
(config-tm-e)#port profile port-A
(config-tm-e-port port-A)# queue 0 0 limit 512
```

【未設定時】

プライオリティ値：4、キュー ID：0 のキューは、最大パケット数は 4096 となり、それ以外のキューでは最大パケット数は 256 となります。

25.3.20 queue shape

【機能】

拡張キューイングのキューごとのシェーピングレートとバーストサイズの設定

【入力形式】

queue <プライオリティ値> <キュー ID> shape pir <シェーピングレート> pbs <バーストサイズ>

no queue <プライオリティ値> <キュー ID> shape [pir <シェーピングレート> pbs <バーストサイズ>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プライオリティ値	送信優先度を指定します。	0～4	省略不可
キュー ID	キュー ID を指定します。	0～3	
シェーピングレート	シェーピングレート（単位：kbps）を指定します。	3～2000000	
バーストサイズ	バーストサイズ（単位：bytes）を指定します。	2～130816	

【動作モード】

traffic-manager-extended-port プロファイル設定モード

【説明】

拡張キューイングのキューごとのシェーピングレートとバーストサイズを設定します。

【実行例】

拡張キューイングのキューごとのシェーピングレートとバーストサイズを設定します（プライオリティ値：1、キュー ID：2、シェーピングレート：5000kbps、バーストサイズ：5120bytes）。

```
#configure terminal
(config)#traffic-manager extended
(config-tm-e)#port profile port-A
(config-tm-e-port port-A)#queue 1 2 shape pir 5000 pbs 5120
```

【未設定時】

シェーピングしません。

25.4 データコネク트의 QoS/CoS の設定

25.4.1 set service-policy

【機能】

SIP セッションごとのデータコネクート用ポリシーマップの設定

【入力形式】

set service-policy <データコネクート用ポリシーマップ ID>

no set service-policy [<データコネクート用ポリシーマップ ID>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
データコネクート用ポリシーマップ ID	データコネクート用ポリシーマップの ID を指定します。	1 ～ 65535	省略不可

【動作モード】

SIP プロファイル設定モード

【説明】

SIP セッションごとのデータコネクート用ポリシーマップを指定します。

存在しない ID が指定されていた場合は、そのセッションの確立処理は失敗します。

【実行例】

SIP セッションごとのデータコネクート用ポリシーマップを指定します（データコネクート用ポリシーマップ ID：1）。

```
#configure terminal
(config)#ngn sip profile SIP-PROFILE-A
(sip-prof)# (sip-prof)# set service-policy 1
```

【未設定時】

以下のデフォルトのデータコネクート用ポリシーマップで動作します。

```
burst 1
queue express limit 10
queue normal 0 limit 0
queue normal 1 limit 0
queue normal 2 limit 0
queue normal 3 limit 0
queue normal 4 limit 0
queue normal 5 limit 0
queue besteffort limit base 1
match-list 1 local-source queue express
set dscp 32
```

25.4.2 ngn sip agent service-policy

【機能】

SIP セッション全体のデータコネクト用ポリシーマップの指定

【入力形式】

ngn sip agent <エントリ番号> service-policy <データコネクト用ポリシーマップ ID>

no ngn sip agent <エントリ番号> service-policy [<データコネクト用ポリシーマップ ID>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
エントリ番号	SIP user agent のエントリ番号を指定します。	0: 高優先	省略不可
データコネクト用ポリシーマップ ID	データコネクト用ポリシーマップの ID を指定します。	1 ～ 65535	省略不可

【動作モード】

基本設定モード

【説明】

SIP セッション全体のデータコネクト用ポリシーマップを指定します。セッションに個別のデータコネクト用ポリシーマップが指定されている場合、個別の設定が優先されます。存在しない ID が指定されていた場合、このコマンドの指定が有効になっているセッションの確立処理は失敗します。

【実行例】

SIP セッション全体のデータコネクト用ポリシーマップを指定します（データコネクト用ポリシーマップ ID : 10）。

```
#configure terminal
(config)# ngn sip agent 0 service-policy 10
```

【未設定時】

個別のポリシーマップも未指定であれば、以下のデフォルトのデータコネクト用ポリシーマップで動作します。

```
burst 1
queue express limit 10
queue normal 0 limit 0
queue normal 1 limit 0
queue normal 2 limit 0
queue normal 3 limit 0
queue normal 4 limit 0
queue normal 5 limit 0
queue besteffort limit base 1
match-list 1 local-source queue express
set dscp 32
```

25.4.3 dataconnect-policy-map

【機能】

データコネクト用 policy-map 設定モードへの移行

【入力形式】

dataconnect-policy-map <データコネクト用ポリシーマップ ID>

no dataconnect-policy-map <データコネクト用ポリシーマップ ID>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
データコネクト用ポリシーマップ ID	データコネクト用ポリシーマップの ID を指定します。	1～65535	省略不可

【動作モード】

基本設定モード

【説明】

データコネクト用 policy-map 設定モードに移行します。コマンドの先頭に "no" を指定することで、該当データコネクト用 policy-map 設定モードの内容がすべて消去されます。

【実行例】

データコネクト用 policy-map 設定モードに移行します（データコネクト用ポリシーマップ ID：100）。

```
#configure terminal
(config)# dataconnect-policy-map 100
(config-dcpmap 100)
```

25.4.4 burst

【機能】

通信帯域に対するミリ秒単位でのバーストサイズの設定

【入力形式】

burst <バーストサイズ>

no burst [<バーストサイズ>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
バーストサイズ	バーストサイズ（単位：ミリ秒）を指定します。	1～100	省略不可

【動作モード】

データコネクト用 policy-map 設定モード

【説明】

SIP セッションの指定した通信帯域に対してのバーストサイズを、通信帯域に対するミリ秒で設定します。
通信帯域を、1 ミリ秒単位で送信できる byte 数に変換し、バーストサイズを計算します。
1 ミリ秒単位で送信できる byte 数 = (通信帯域 (単位: bps) / 8) / 1000
計算の結果、バーストサイズが 262144bytes を超える場合、262144bytes が設定されます。

【実行例】

SIP セッションの指定した通信帯域に対してのバーストサイズを設定します (バーストサイズ: 10 ミリ秒、通信帯域が 64kbps の場合はバーストサイズは 80bytes となります)。

```
#configure terminal
(config)# dataconnect-policy-map 100
(config-dcpmap 100)# burst 10
```

【未設定時】

各通信帯域の 1 ミリ秒分のバーストサイズで動作します。

25.4.5 queue limit

【機能】

SIP セッションの指定した帯域で使用する各キューの最大キュー長の設定

【入力形式】

queue {besteffort | express | normal <キュー ID>} limit {base <倍数> | <packets>}

no queue {besteffort | express | normal <キュー ID>} limit [{base [<倍数>] | <packets>}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
besteffort	低優先キューを指定します。	-	省略不可
express	高優先キューを指定します。	-	省略不可
normal	中優先キューを指定します。	-	省略不可
キュー ID	中優先キューのキュー ID を指定します。	0 ～ 5	省略不可
倍数	キュー長制限を帯域別の基本キュー長の倍数で指定します。	1 ～ 10	省略不可
packets	キュー長制限をパケット数で指定します。	0 ～ 65536	省略不可

【動作モード】

データコネクト用 policy-map 設定モード

【説明】

SIP セッションの指定した帯域で使用する各キューの最大キュー長を帯域別の基本キュー長の倍数、またはパケット数で設定します。
倍数指定した場合の queue limit が 65536 を超える場合、65536 が設定されます。

帯域別の基本キュー長は、データコネクト通信の最小のイーサネットフレーム長(122bytes)から 18bytes (イーサネットヘッダと FCS の合計) を引いた値換算で約 50msec 分を切り上げた値とします。

64kbps の場合： $(64 \times 1000 / 8) / (122 - 18) / 20 = 3.84 \dots$ 切り上げて 4packets

データコネクトの最小パケット長は、以下の条件で算出しています。

- ・ ショートパケット (IP データグラム長 46bytes)
- ・ 暗号化アルゴリズム 3DES
- ・ NAT-Traversal あり

【実行例】

最大キュー長を設定します (対象キュー：高優先キュー、倍数：2)。

```
#configure terminal
(config)# dataconnect-policy-map 100
(config-dcpmap 100)# queue express limit base 2
```

【未設定時】

match-list コマンドで指定されているキューおよび低優先キューは各帯域の基本キュー長の等倍、match-list コマンドで指定されていない高優先キュー、中優先キューは 0 で動作します。

25.4.6 queue normal rate

【機能】

中優先度キューの WFQ 重みの設定

【入力形式】

queue normal <キュー ID> rate {<レート> | weight <WFQ 重み>}

no queue normal <キュー ID> rate [<レート> | weight <WFQ 重み>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
キュー ID	中優先キューのキュー ID を指定します。	0 ～ 5	省略不可
レート	レート (単位：kbps) を指定します。	1 ～ 1000000	省略不可
WFQ 重み	WFQ 重みを指定します。	1 ～ 100	省略不可

【動作モード】

データコネクト用 policy-map 設定モード

【説明】

中優先度キューの WFQ 重みを設定します。

レートを指定した場合は、SIP セッションの指定した帯域に対する指定レートの割合を WFQ 重みとして動作します。

SIP セッションの指定した帯域より大きいレートが指定されていた場合、セッション確立は失敗します。

輻輳時には指定した重みの割合で各キューから送信が行われます。

【実行例】

中優先度キューの WFQ 重みを設定します（キュー ID：0、レート：100）。

```
#configure terminal
(config)# dataconnect-policy-map 100
(config-dcpmap 100)# queue normal 0 rate 100
```

【未設定時】

すべての中優先度キューが WFQ 重みは 1 で動作します。

25.4.7 match-list

【機能】

データコネクト通信のデータパケットを入力するキューの設定

【入力形式】

match-list <マッチリスト番号> {local-source | dscp <dscp 値>} queue {besteffort | express | normal
<キュー ID>}

no match-list <マッチリスト番号> [{local-source | dscp <dscp 値>} queue {besteffort | express | normal
<キュー ID>}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
マッチリスト番号	マッチリスト番号を指定します。	1～10	省略不可
local-source	自局送信パケットを指定します。	-	省略不可
dscp 値	キューを設定する dscp 値を指定します。	0～63	省略不可
besteffort	低優先キューを指定します。	-	省略不可
express	高優先キューを指定します。	-	省略不可
normal	中優先キューを指定します。	-	省略不可
キュー ID	中優先キューのキュー ID を指定します。	0～5	省略不可

【動作モード】

データコネクト用 policy-map 設定モード

【説明】

データコネクト通信のデータパケットを入力するキューを設定します。

マッチリスト番号の小さいエントリが優先して動作します。

【実行例】

データコネクト通信のデータパケットを入力するキューを設定します（マッチリスト番号：2、dscp 値：32、対象キュー：中優先キュー、キュー ID：0）。

```
#configure terminal
(config)# dataconnect-policy-map 100
(config-dcpmap 100)# match-list 2 dscp 32 queue normal 0
```

【未設定時】

すべてのパケットが低優先キューに入力されます。

25.4.8 set dscp

【機能】

データコネクト対象パケットのアウトターにマーキングする dscp 値の設定

【入力形式】

set dscp <dscp 値>

no set dscp [<dscp 値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
dscp 値	データコネクト対象パケットのアウトターにマーキングする dscp 値を指定します。	0～63	省略不可

【動作モード】

データコネクト用 policy-map 設定モード

【説明】

データコネクト対象パケットのアウトターにマーキングする dscp 値を設定します。

【実行例】

アウトターにマーキングする dscp 値の設定します (dscp 値：32)。

```
#configure terminal
(config)# dataconnect-policy-map 100
(config-dcpmap 100)#set dscp 32
```

【未設定時】

32 をマーキングします。

第26章 ポリシールー ティングの設定



この章では、ポリシールーティングの設定に関するコマンドについて説明します。

26.1	classifierの登録	829
26.2	ポリシーマップの定義	831

26.1 classifier の登録

26.1.1 policy-route input

【機能】

ポリシールーティングの設定

【入力形式】

policy-route input <ポリシールートマップ名>

no policy-route input <ポリシールートマップ名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ポリシールートマップ名	ポリシールートマップ名を指定します。	63 文字以内の TMNAME 型	省略不可

【動作モード】

gigaethernet インタフェース設定モード、gigaethernet サブインタフェース設定モード、tunnel インタフェース設定モード、trunk-channel インタフェース設定モード、trunk-channel サブインタフェース設定モード、USB Ethernet インタフェース設定モード

【説明】

当該インタフェースに対して、指定したポリシールートマップを適用します。

1 つのインタフェースに設定できるポリシールートマップは 1 つだけです。

フィルタ／QoS／データコネクト QoS／DVPN ACL／ポリシールーティングのクラシファイエントリはすべて共用です。各機能でエントリを使用していると、データコネクト QoS のエントリが入らないことがあります。

【実行例】

ポリシールーティングを設定します（ポリシールートマップ名：test）。

```
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)# policy-route input test
```

【未設定時】

ポリシールーティングを設定しません。

26.1.2 local policy-route

【機能】

ポリシールーティングの設定

【入力形式】

local [vrf <VRF 名>] policy-route <ポリシールートマップ名>

no local [vrf <VRF 名>] policy-route <ポリシールートマップ名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VRF 名	VRF 名を指定します。	63 文字以内の WORD 型	省略不可
ポリシールートマップ名	ポリシールートマップ名を指定します。	63 文字以内の TMNAME 型	省略不可

【動作モード】

基本設定モード

【説明】

自発のパケットで、ポリシールートマップ名で指定したポリシールートマップを適用します。
適用できる設定は 1 つだけです。

【実行例】

ポリシールーティングを設定します（ポリシールートマップ名：test）。

```
#configure terminal
(config)# local policy-route test
```

【未設定時】

ポリシールーティングは適用されません。

26.2 ポリシーマップの定義

26.2.1 policy-route-map

【機能】

policy-route-map 設定モードへの移行

【入力形式】

policy-route-map <ポリシールートマップ名>

no policy-route-map <ポリシールートマップ名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ポリシールートマップ名	ポリシールートマップ名を指定します。	63 文字以内の TMNAME 型	省略不可

【動作モード】

基本設定モード

【説明】

policy-route-map 設定モードに移行します。

【実行例】

policy-route-map 設定モードに移行します（ポリシールートマップ名：test）。

```
#configure terminal
(config)# policy-route-map test
(config-prmap)#
```

26.2.2 class

【機能】

policy-route-map-class 設定モードへの移行

【入力形式】

class <class-map 名>

no class <class-map 名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
class-map 名	class-map 名を指定します。	63 文字以内の TMNAME 型	省略不可

【動作モード】

policy-route-map 設定モード

【説明】

policy-route-map-class 設定モードに移行します。コマンドの先頭に "no" を指定することで、該当 policy-map-class 設定モードの内容がすべて消去されます。

【実行例】

policy-route-map-class 設定モードに移行します (class-map 名: policy-route-map-class)。

```
#configure terminal
(config)#policy-route-map policy-route-map
(config-prmap)#class policy-route-map-class
(config-prmap-c)#
```

26.2.3 search-sequence

【機能】

policy-route-map 内の検索優先度の設定

【入力形式】

search-sequence <検索優先度>

no search-sequence [<検索優先度>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
検索優先度	検索優先度を指定します。	1 ～ 65534	省略不可

【動作モード】

policy-route-map-class 設定モード

【説明】

policy-route-map 内の検索優先度を設定します。検索優先度の小さい方が優先的にマッチします。

【実行例】

検索優先度を設定します (検索優先度: 100)。

```
#configure terminal
(config)#policy-route-map policy-route-map
(config-prmap)#class policy-route-map-class
(config-prmap-c)#search-sequence 100
```

【未設定時】

検索優先度は 65535 で動作します。

26.2.4 count

【機能】

クラスにマッチしたパケット数をカウントする設定

【入力形式】

count

no count

【動作モード】

policy-route-map-class 設定モード

【説明】

クラスにマッチしたパケット数をカウントする場合に設定します。

【実行例】

クラスにマッチしたパケット数をカウントします。

```
#configure terminal
(config)#policy-route-map policy-route-map
(config-prmap)#class policy-route-map-class
(config-prmap-c)#count
```

【未設定時】

パケット数をカウントしません。

26.2.5 action

【機能】

送信方法の設定

【入力形式】

action {nexthop [vrf <VRF 名>] [<IPv4 アドレス> | <IPv6 アドレス> [port-channel <port-channel-num>] | tunnel <tunnel-num>] | transmit | drop}

no action {nexthop [vrf <VRF 名>] [<IPv4 アドレス> | <IPv6 アドレス> [port-channel <port-channel-num>] | tunnel <tunnel-num>] | transmit | drop}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
nexthop	設定した送信先に送信する場合に指定します。	-	省略不可
VRF 名	VRF 名を指定します。	63 文字以内の word 形式	省略不可
IPv4 アドレス	IPv4 アドレスを指定します。	IPv4 アドレス形式	省略不可
IPv6 アドレス	IPv6 アドレスを指定します。	IPv6 アドレス形式	省略不可
port-channel-num	送信先の port-channel 番号を指定します。	0 ～ 16777215	省略不可

パラメタ	設定内容	設定範囲	省略時
tunnel-num	送信先のトンネル番号を指定します。	1 ～ 16777215	省略不可
transmit	経路表に従って送信する場合に指定します。	-	省略不可
drop	パケットを破棄する場合に指定します。	-	省略不可

【動作モード】

policy-route-map-class 設定モード

【説明】

指定されたクラスに対して、送信方法を設定します。

【実行例】

送信先の IPv4 アドレスとして、10.10.10.1 を設定します。

```
#configure terminal
(config)#policy-route-map policy-route-map-A
(config-prmap)#class policy-map-class-A
(config-prmap-c)#action nexthop 10.10.10.1
```

【未設定時】

ポリシールーティングを行いません。

26.2.6 watch

【機能】

監視アドレスの設定

【入力形式】

watch [vrf <VRF 名>] <監視先 IP アドレス> [source {<送信元インタフェース> <送信元インタフェース番号> | <送信元 IP アドレス>}] [survey-map <survey マップ名>]

no watch [vrf <VRF 名>] <監視先 IP アドレス> [source {<送信元インタフェース> <送信元インタフェース番号> | <送信元 IP アドレス>}] [survey-map <survey マップ名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VRF 名	VRF 名を指定します。	63 文字以内の WORD 形式	省略不可
監視先 IP アドレス	監視先の IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
送信元インタフェース	送信元インタフェースを指定します。	-	実際に送信するインタフェースとなります。
送信元インタフェース番号	送信元インタフェース番号を指定します。	-	実際に送信するインタフェースとなります。
送信元 IP アドレス	送信元の IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	実際に送信するインタフェースのアドレスとなります。
survey マップ名	survey マップ名を指定します。	254 文字以内の WORD 型	survey 機能のデフォルト値で動作します。

【動作モード】

policy-route-map-class 設定モード

【説明】

監視アドレスを設定します。

survey 機能で、同じ宛先に対する設定がされている場合には、監視は開始されず、エラーとなります。

survey-map が設定されていないものを指定した場合、設定が入るまで監視は開始されません。

別の policy-route-map で、同じ宛先の監視設定が行われており、送信元インタフェースや survey map が違う場合、監視は開始されず、エラーとなります。

【実行例】

監視先の IPv4 アドレスとして、10.10.10.1 を設定します。

```
#configure terminal
(config)#policy-route-map policy-route-map-A
(config-prmap)#class policy-map-class-A
(config-prmap-c)# watch 10.10.10.1
```

【未設定時】

監視を行いません。

第27章 IDSの設定



この章では、IDSの設定に関するコマンドについて説明します。

27.1 IDS の設定

27.1.1 ids profile

【機能】

traffic-manager-network-ids プロファイル設定モードへの移行

【入力形式】

ids profile <IDS プロファイル名>

no ids profile <IDS プロファイル名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
IDS プロファイル名	IDS プロファイル名を指定します。	63 文字以内の TMNAME 型	省略不可

【動作モード】

traffic-manager network 設定モード

【説明】

traffic-manager-network-ids プロファイル設定モードに移行します。

【実行例】

traffic-manager-network-ids プロファイル設定モードに移行します (IDS プロファイル名: sample)。

```
#configure terminal
(config)#traffic-manager network
(config-tm-n)#ids profile sample
(config-tm-n-ids sample)#
```

27.1.2 ip ids

【機能】

IPv4 パケットに対して IDS を動作させる設定

【入力形式】

ip ids { in | out } profile <IDS プロファイル名>

no ip ids { in | out } [profile <IDS プロファイル名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
in out	IDS を動作させるパケットの方向を指定します。	in: 受信方向 out: 送信方向	省略不可
IDS プロファイル名	IDS プロファイル名を指定します。	63 文字以内の TMNAME 型	省略不可

【動作モード】

gigaethernet インタフェース設定モード、gigaethernet サブインタフェース設定モード、trunk-channel インタフェース設定モード、trunk-channel サブインタフェース設定モード

【説明】

IPv4 パケットに対して IDS を動作させる場合に設定します。

設定されたインタフェースで動作します。

【実行例】

IPv4 パケットに対して IDS を動作させる設定をします（IDS を動作させるパケットの方向：受信方向、IDS プロファイル名：sample）。

```
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#ip ids in profile sample
```

【未設定時】

IPv4 パケットに対して IDS は動作しません。

27.1.3 ipv6 ids

【機能】

IPv6 パケットに対して IDS を動作させる設定

【入力形式】

ipv6 ids { in | out } profile <IDS プロファイル名>

no ipv6 ids { in | out } [profile <IDS プロファイル名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
in out	IDS を動作させるパケットの方向を指定します。	in: 受信方向 out: 送信方向	省略不可
IDS プロファイル名	IDS プロファイル名を指定します。	63 文字以内の TMNAME 型	省略不可

【動作モード】

gigaethernet インタフェース設定モード、gigaethernet サブインタフェース設定モード、trunk-channel インタフェース設定モード、trunk-channel サブインタフェース設定モード

【説明】

IPv6 パケットに対して IDS を動作させる場合に設定します。

設定されたインタフェースで動作します。

【実行例】

IPv6 パケットに対して IDS を動作させる設定をします (IDS を動作させるパケットの方向：受信方向、IDS プロファイル名：sample)。

```
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#ipv6 ids in profile sample
```

【未設定時】

IPv6 パケットに対して IDS は動作しません。

27.1.4 type

【機能】

IDS タイプでのパケットの取り扱いの設定

【入力形式】

type <IDS タイプ> <動作モード>

no type <IDS タイプ> [<動作モード>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
IDS タイプ	IDS 対象となるタイプを指定します。	header header-option fragment icmp udp tcp ftp default	省略不可
動作モード	IDS タイプごとの動作を指定します。	on: 検知有効 off: 検知無効 drop: 廃棄	省略不可

【動作モード】

traffic-manager-network-ids プロファイル設定モード

【説明】

IDS タイプでのパケットの取り扱いを設定します。

IDS タイプに "default" を指定した場合は、明示的に設定していないすべての IDS タイプに対して指定した動作モードが適用されます。

【実行例】

IDS タイプでのパケットの取り扱いを設定します (IDS タイプ：icmp、動作モード：on)。

```
#configure terminal
(config)#traffic-manager network
(config-tm-n)#ids profile sample
(config-tm-n-ids sample)# type icmp on
```

【未設定時】

すべてのパケットに対して検知無効となります。

第28章 VRRPの設定



この章では、VRRPの設定に関するコマンドについて説明します。

28.1	VRRPの設定.....	842
28.2	IPv4 VRRPの設定.....	849
28.3	IPv6 VRRPの設定.....	859

28.1 VRRP の設定

28.1.1 ip vrrp enable

【機能】

VRRP ルータとして動作する、track 機能を有効にする設定

【入力形式】

ip vrrp enable

no ip vrrp enable

【動作モード】

基本設定モード

【説明】

VRRP ルータとして動作する場合、または、track 機能を利用する場合に設定します。

【実行例】

VRRP ルータとして動作させ、track 機能を有効にします。

```
#configure terminal
(config)#ip vrrp enable
```

【未設定時】

VRRP ルータとして動作しません。track 機能が利用できません。

28.1.2 track down-action

【機能】

トラック状態が DOWN となった際にインタフェースを shutdown 状態とする設定

【入力形式】

track <トラック番号> down-action shutdown [expire <expire 時間>]

no track <トラック番号> down-action shutdown [expire <expire 時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
トラック番号	トラックオブジェクトの番号を指定します。	IPv4 の場合：1 ～ 500 IPv6 の場合：1001 ～ 1500	省略不可
expire 時間 (*1)	shutdown ～ no shutdown までの時間 (単位：秒) を指定します。	0 ～ 60	5

*1) gigabitEthernet サブインタフェース設定モード、trunk-channel サブインタフェース設定モードでは指定できません。

【動作モード】

gigaethernet インタフェース設定モード、gigaethernet サブインタフェース設定モード、trunk-channel インタフェース設定モード、trunk-channel サブインタフェース設定モード

【説明】

track vhost コマンドで設定されたトラックの状態を監視し、状態が DOWN となった際にインタフェースを shutdown 状態とすること、また、その後 no shutdown 状態にするまでの expire 時間（単位：秒）を設定します。

expire 時間による no shutdown は、物理インタフェースは UP しますが、論理インタフェースは DOWN を継続するため、本コマンドを設定しているインタフェースの通信はできません（サブインタフェースに本コマンドの設定がなければ、そのサブインタフェースでの通信は可能になります）。

論理インタフェースが UP するのは監視しているトラックの状態が UP となったタイミングになります。

サブインタフェース設定モードでは、時間経過による no shutdown 処理はありません。expire 時間に 0 を設定した場合は shutdown 状態を継続し、トラック状態が UP 後、または、トラック設定が削除された場合に no shutdown 状態とします。

【実行例】

トラック状態が DOWN となった際にインタフェースを shutdown 状態とする（トラック番号：1、expire 時間：10 秒）。

```
【gigaethernet インタフェース設定モードの場合】
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#track 1 down-action shutdown expire 10
```

【未設定時】

track shutdown 機能が動作しません。

28.1.3 track management

【機能】

トラックの状態を management インタフェースの状態と連動させる設定

【入力形式】

track <トラック番号> management 1 line-protocol [delay-up <遅延時間>] [delay-down <遅延時間>]

no track <トラック番号> [management 1 line-protocol [delay-up <遅延時間>] [delay-down <遅延時間>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
トラック番号	トラックオブジェクトの番号を指定します。	IPv4 の場合：1～500 IPv6 の場合：1001～1500	省略不可
遅延時間	UP/DOWN した際に、状態を変化させるまでの時間（単位：秒）を指定します。	1～180	0

【動作モード】

基本設定モード

【説明】

トラックの状態を management インタフェースの状態と連動させる場合に設定します。

management インタフェースの状態が UP である場合はトラックの状態を UP に、management インタフェースの状態が DOWN である場合はトラックの状態を DOWN にします。

【実行例】

トラックの状態を management インタフェースの状態と連動させます（トラック番号：100）。

```
#configure terminal
(config)#track 100 management 1 line-protocol
```

【未設定時】

management インタフェースの状態と VRRP は連携しません。

28.1.4 track port-channel

【機能】

トラックの状態を port-channel インタフェースの状態と連動させる設定

【入力形式】

track <トラック番号> port-channel <インタフェース番号> line-protocol [delay-up <遅延時間>] [delay-down <遅延時間>]

no track <トラック番号> [port-channel <インタフェース番号> line-protocol [delay-up <遅延時間>] [delay-down <遅延時間>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
トラック番号	トラックオブジェクトの番号を指定します。	IPv4 の場合：1～500 IPv6 の場合：1001～1500	省略不可
インタフェース番号	インタフェース番号を指定します。	-	
遅延時間	UP/DOWN した際に、状態を変化させるまでの時間（単位：秒）を指定します。	1～180	0

【動作モード】

基本設定モード

【説明】

トラックの状態を port-channel インタフェースの状態と連動させる場合に設定します。

port-channel インタフェースの状態が UP である場合はトラックの状態を UP に、port-channel インタフェースの状態が DOWN である場合はトラックの状態を DOWN にします。

【実行例】

トラックの状態を port-channel インタフェースの状態と連動させます（トラック番号：100、インタフェース番号：1）。

```
#configure terminal
(config)#track 100 port-channel 1 line-protocol
```

【未設定時】

port-channel インタフェースの状態と VRRP は連携しません。

28.1.5 track survey

【機能】

トラックの状態を survey 機能による端末接続監視状態と連動させる設定

【入力形式】

track <トラック番号> survey {<IP アドレス> [vrf <VRF 名>] | name <survey 名>} [delay-up <遅延時間>] [delay-down <遅延時間>]

no track <トラック番号> [survey {<IP アドレス> [vrf <VRF 名>] | name <survey 名>} [delay-up <遅延時間>] [delaydown <遅延時間>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
トラック番号	トラックオブジェクトの番号を指定します。	IPv4 の場合：1～500 IPv6 の場合：1001～1500	省略不可
IP アドレス	survey 機能により接続監視を行っている端末の IP アドレス	トラック番号 1～500：IPv4 アドレス形式 トラック番号 1001～1500：IPv6 アドレス形式	
VRF 名	VRF 名を指定します。	63 文字以内の WORD 型	VRF を使用しない
survey 名	survey 機能により接続監視を行っている端末の名前	63 文字以内の WORD 型	省略不可
遅延時間	UP/DOWN した際に、状態を変化させるまでの時間（単位：秒）を指定します。	1～180	0

【動作モード】

基本設定モード

【説明】

トラックの状態を survey 機能による端末接続監視状態と連動させる場合に設定します。

監視状態が UP の場合はトラックの状態を UP に、監視状態が DOWN の場合はトラックの状態を DOWN にします。

【実行例】

トラックの状態を survey 機能による端末接続監視状態と連動させます（トラック番号：100、接続監視先：192.0.2.1）。

```
#configure terminal
(config)#track 100 survey 192.0.2.1
```

【未設定時】

survey 機能による端末接続監視と VRRP は連携しません。

28.1.6 track vhost

【機能】

トラックの状態を VRRP の状態と連動させる設定

【入力形式】

track <トラック番号> vhost <仮想アドレス> [<インタフェース名> <インタフェース番号>] [vrf <VRF 名>] vrrp-status [delay-up <up 遅延時間>] [delay-down <down 遅延時間>] | [delay-down-init <init 遅延時間>] [delay-down-backup <backup 遅延時間>]]

no track <トラック番号> [vhost <仮想アドレス> [<インタフェース名> <インタフェース番号>] [vrf <VRF 名>] vrrp-status [delay-up <up 遅延時間>] [delay-down <down 遅延時間>] | [delay-down-init <init 遅延時間>] [delay-down-backup <backup 遅延時間>]]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
トラック番号	トラックオブジェクトの番号を指定します。	IPv4 の場合：1～500 IPv6 の場合：1001～1500	省略不可
仮想アドレス	VRRP の仮想アドレスを指定し、仮想アドレスの状態の変化により、トラックの状態変化を行います。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
インタフェース名(*1)	連動させる VRRP のインタフェース名を指定します（複数のインタフェースで同じリンクローカルアドレスの仮想アドレスを使用する場合に指定します）。	-	仮想アドレスの状態と VRRP は連携しない
インタフェース番号(*1)	インタフェース番号を指定します。	-	省略不可
VRF 名	VRF 名を指定します。	63 文字以内の WORD 型	VRF を使用しない
up 遅延時間	トラックの状態が UP になる場合の状態遷移の遅延時間（単位：秒）を指定します。	1～180	0
down 遅延時間	トラックの状態が DOWN になる場合の状態遷移の遅延時間（単位：秒）を指定します。「init 遅延時間」、「backup 遅延時間」を共通の値に設定します。	1～180	0
init 遅延時間	トラックの状態が DOWN(Initialize) になる場合の状態遷移の遅延時間（単位：秒）を指定します。	1～180	0

パラメタ	設定内容	設定範囲	省略時
backup 遅延時間	トラックの状態が DOWN(Backup) になる場合の状態遷移の遅延時間(単位: 秒)を指定します。	1 ~ 180	0

*1) ipv6 の場合 (トラック番号 1001 ~ 1500) のみ指定できます。

【動作モード】

基本設定モード

【説明】

トラックの状態を VRRP の状態と連動させる場合に設定します。

指定した仮想アドレスの VRRP の状態が Master の場合はトラックの状態を UP に、VRRP の状態が Initialize または Backup の場合はトラックの状態を DOWN にします。

【実行例】

トラックの状態を VRRP の状態と連動させる (トラック番号: 100、仮想アドレス: 192.0.2.1、up 遅延時間: 10 秒、init 遅延時間: 20 秒、backup 遅延時間: 10 秒)。

```
#configure terminal
(config)#track 100 vhost 192.0.2.1 vrrp-status delay-up 10 delay-down-init 20 delay-down-backup 10
```

【未設定時】

トラックの状態を VRRP の状態と連動させません。

28.1.7 vrrp version

【機能】

VRRP ルータのバージョンの設定

【入力形式】

vrrp version <バージョン>

no vrrp version [<バージョン>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
バージョン	VRRP ルータのバージョンを指定します。	2 : Version 2 3 : Version 3	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

VRRP ルータのバージョンを設定します。

【実行例】

VRRP ルータのバージョンを設定します（バージョン：2）。

```
【port-channel の場合】  
#configure terminal  
(config)#interface port-channel 1  
(config-if-ch 1)#vrrp version 2
```

【未設定時】

バージョンは 3 で動作します。

28.2 IPv4 VRRP の設定

28.2.1 ip vrrp advertise_delay_timer

【機能】

GARP の送信、advertise の送信を開始するまでの遅延時間の設定

【入力形式】

```
ip vrrp advertise_delay_timer <遅延時間>
```

```
no ip vrrp advertise_delay_timer [<遅延時間>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
遅延時間	Masterへ遷移した場合に、GARP の送信、advertise の送信を開始するまでの遅延時間（単位：秒）を指定します。	1 ～ 60	省略不可

【動作モード】

基本設定モード

【説明】

priority=0 の advertise パケット受信により Masterへ遷移した場合に、GARP の送信、advertise の送信を開始するまでの遅延時間（単位：秒）を設定します。

priority=0 の advertise パケット受信以外で Masterへ遷移した場合は、本タイマは動作しません。

旧 Master の手動切り替えで Backup から Master に遷移した際、CP が Master に遷移していてもネットワークプロセッサへの Master 登録が完了するまでは仮想 MAC 宛のフレームを中継することができないため、GARP と advertise の送信を遅らせることで、ネットワークプロセッサへの Master 登録が完了するまでは旧 Master で中継を継続させます。

【実行例】

Masterへ遷移した場合に、GARP の送信、advertise の送信を開始するまでの遅延時間（単位：秒）を設定します（遅延時間：3 秒）。

```
#configure terminal
(config)#ip vrrp advertise_delay_timer 3
```

【未設定時】

遅延時間は 6 秒で動作します。

28.2.2 ip vrrp initialize_delay_time

【機能】

インタフェースが UP してから Backup に遷移するまでの遅延時間の設定

【入力形式】

ip vrrp initialize_delay_time <遅延時間>

no ip vrrp initialize_delay_time [<遅延時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
遅延時間	VRRP の状態が Initialize から Backup に変化する場合において、インタフェースが UP してから遅延させる時間（単位：秒）を指定します。	3 ～ 60	省略不可

【動作モード】

基本設定モード

【説明】

VRRP の状態が Initialize から Backup に変化する場合において、インタフェースが UP してから Backup に遷移するまでの遅延時間（単位：秒）を設定します。

Master で手動切り替えを実施した際、priority=0 の advertise を送信し自装置は一度 Initialize に遷移した後 Backup に遷移しますが、新 Master が GARP と advertise の送信を "ip vrrp advertise_delay_timer" 設定で遅らせているため、Backup（対向からの advertise を監視する状態）になるタイミングがそれより早いと切り戻りが発生します。

【実行例】

インタフェースが UP してから Backup に遷移するまでの遅延時間（単位：秒）を設定します（遅延時間：30 秒）。

```
#configure terminal
(config)#ip vrrp initialize_delay_time 30
```

【未設定時】

遅延時間は 3 秒で動作します。

28.2.3 ip vrrp np_delay_timer

【機能】

ネットワークプロセッサへの Master 以外の状態の登録を遅延する時間の設定

【入力形式】

ip vrrp np_delay_timer <遅延時間>

no ip vrrp np_delay_timer [<遅延時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
遅延時間	Master->Master以外へ遷移した場合に、ネットワークプロセッサへのMaster以外の状態の登録を遅延する時間（単位：秒）を指定します。	1 ～ 60	省略不可

【動作モード】

基本設定モード

【説明】

Master->Master以外へ遷移した場合に、ネットワークプロセッサへのMaster以外の状態の登録を遅延する時間（単位：秒）を設定します。

Masterで手動切り替えを実施した際、L2SWのMAC学習が切り替わるまでは旧Masterで中継フレームを受信することになるため、非Master状態でも一時的に中継可能な状態にして断時間を低減させます。

【実行例】

ネットワークプロセッサへのMaster以外の状態の登録を遅延する時間（単位：秒）を設定します（遅延時間：3秒）。

```
#configure terminal
(config)#ip vrrp np_delay_timer 3
```

【未設定時】

遅延時間は10秒で動作します。

28.2.4 ip vrrp mode interface-delegation

【機能】

interface-delegation モードを動作させる設定

【入力形式】

ip vrrp mode interface-delegation

no ip vrrp mode interface-delegation

【動作モード】

基本設定モード

【説明】

interface-delegation モードで動作させる場合に設定します。

interface-delegation モードでは、同一物理インタフェース、同一VRIDを束ね、代表のPort-ChannelのVRRP設定に従って、その単位で状態遷移を行います。

また、vrrp advertisement packet 送信に関しては、同一物理インタフェース、同一VRIDに所属するVLANを巡回して送信します。

【実行例】

```
#configure terminal
(config)#ip vrrp mode interface-delegation
```

【未設定時】

同一物理インタフェース、同一VRIDであっても、各 port-channel の設定に従って動作します。

28.2.5 ip vrrp mode trap-enable-all

【機能】

interface-delegation モードにおいて、vrrp の Master 遷移 trap を出力する設定

【入力形式】

```
ip vrrp mode trap-enable-all
```

```
no ip vrrp mode trap-enable-all
```

【動作モード】

基本設定モード

【説明】

interface-delegation モードにおいて、非代表インタフェースを含めたすべてのインタフェースで vrrp の Master 遷移 trap を出力する場合に設定します。

【実行例】

```
#configure terminal
(config)#ip vrrp mode trap-enable-all
```

【未設定時】

代表インタフェースのみ Master 遷移 trap を出力します。

28.2.6 track ip

【機能】

トラックの状態を宛先ネットワーク／宛先ホストに対する到達性と連動させる設定

【入力形式】

```
track <トラック番号> ip {route <宛先ネットワーク／プレフィックス> | host <宛先ホスト>} [vrf <VRF 名>] reachability [delay-up <遅延時間>] [delay-down <遅延時間>]
```

```
no track <トラック番号> [ip {route <宛先ネットワーク／プレフィックス> | host <宛先ホスト>} [vrf <VRF 名>] reachability [delay-up <遅延時間>] [delay-down <遅延時間>]]
```


【パラメタ】

パラメタ	設定内容	設定範囲	省略時
トラック番号	トラックオブジェクトの番号を指定します。	1 ～ 500	省略不可
宛先ネットワーク プレフィックス	宛先ネットワークへの到達性により、 トラックの状態変化を行います。	IPv4 アドレス形式	
		0 ～ 32	
宛先ホスト	宛先ホストへの到達性により、トラックの状態変化を行います。	IPv4 アドレス形式	VRF を使用しない
VRF 名	VRF 名を指定します。	63 文字以内の WORD 型	
遅延時間	UP/DOWN した際に、状態を変化させるまでの時間（単位：秒）を指定します。	1 ～ 180	0

【動作モード】

基本設定モード

【説明】

トラックの状態を、宛先ネットワーク／宛先ホストに対する到達性と連動させる場合に設定します。宛先への到達性がある場合はトラックの状態を UP に、宛先への到達性がない場合はトラックの状態を DOWN にします。宛先への到達性は、track 設定のアドレス／プレフィックス長に完全一致する経路情報があるかどうかにより判断します。

【実行例】

トラックの状態を、宛先ネットワークに対する到達性と連動させます（トラック番号：100、宛先ネットワーク：192.0.2.0/24）。

```
#configure terminal
(config)#track 100 ip route 192.0.2.0/24 reachability
```

【未設定時】

宛先への到達性と VRRP は連携しません。

28.2.7 vrrp address

【機能】

ルータグループの仮想 IPv4 アドレスの設定

【入力形式】

vrrp <vr-id 値> address <VRRP ルータアドレス>

no vrrp <vr-id 値> address [<VRRP ルータアドレス>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
vr-id 値	VRRP ルータの VRID を指定します。	1 ～ 255	省略不可
VRRP ルータアドレス	VRRP ルータアドレスを指定します。	IPv4 アドレス形式	

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

ルータグループの仮想 IPv4 アドレスを設定します。

通常は、自分が Master ルータの場合であっても、実 IPv4 アドレスとは違うアドレスをグループの仮想 IPv4 アドレスとして指定します。

VRRP ルータアドレスがインタフェースの実 IPv4 アドレスと同じ場合、owner として動作します。

【実行例】

ルータグループの仮想 IPv4 アドレスを設定します (vr-id 値 : 1、VRRP ルータアドレス : 192.0.2.1)。

```
【port-channel の場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#vrrp 1 address 192.0.2.1
```

【未設定時】

VRRP ルータアドレスの設定を行いません。

28.2.8 vrrp adver-interval

【機能】

ADVERTISEMENT パケットの送信間隔の設定

【入力形式】

vrrp <vr-id 値> adver-interval {<送信間隔 sec 指定> | dsec <送信間隔 dsec 指定>}

no vrrp <vr-id 値> adver-interval [{<送信間隔 sec 指定> | dsec <送信間隔 dsec 指定>}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
vr-id 値	VRRP ルータの VRID を指定します。	1 ～ 255	省略不可
送信間隔 sec 指定	ADVERTISEMENT パケットの送信間隔 (単位 : 秒) を指定します。	1 ～ 30	
送信間隔 dsec 指定	ADVERTISEMENT パケットの送信間隔 (単位 : 1/10 秒) を指定します。	1 ～ 300	

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

ADVERTISEMENT パケットの送信間隔を設定します。

【実行例】

ADVERTISEMENT パケットの送信間隔を設定します (vr-id 値：1、送信間隔：10 秒)。

```
【port-channel の場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#vrrp 1 adver-interval 10
```

【未設定時】

送信間隔は 1 秒で動作します。

28.2.9 vrrp delegated-interface

【機能】

interface-delegation モードにおいて、代表インタフェースとして動作させる設定

【入力形式】

vrrp <vr-id 値> delegated-interface

no vrrp <vr-id 値> delegated-interface

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
vr-id 値	VRRP ルータの VRID を指定します。	1 ～ 255	省略不可

【動作モード】

port-channel インタフェース設定モード

【説明】

interface-delegation モードにおいて、代表インタフェースとして動作させる場合に設定します。

同一物理インタフェース、同一 VRID のどの port-channel インタフェースにも本設定がない場合は、port-channel 番号の小さいインタフェースが代表インタフェースとして動作します。

【実行例】

interface-delegation モードにおいて、代表インタフェースとして動作させる設定をします。(vr-id 値：1)

```
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#vrrp 1 delegated-interface
```

【未設定時】

代表インタフェースとして動作しません。

28.2.10 vrrp preempt

【機能】

Preempt mode を有効とする設定

【入力形式】

```
vrrp <vr-id 値> preempt
```

```
no vrrp <vr-id 値> preempt
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
vr-id 値	VRRP ルータの VRID を指定します。	1 ～ 255	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

Preempt mode を有効とする場合に設定します。

Master ルータに障害が発生し Backup ルータに切り替わる場合や、Master ルータが復旧し Backup ルータから切り戻る場合の動作を指定します。

Preempt mode が有効な場合	vrrp priority コマンドで設定した優先度で判断し、常に優先度の高いルータが Master ルータとなります。
Preempt mode が無効の場合	Master ルータに障害が発生し Backup ルータが Master ルータになったあとに、最初の Master ルータが復旧したとしても、vrrp priority コマンドで設定した優先度に関係なく、現在の Master ルータ（元 Backup ルータ）が動作し続けます。

【実行例】

Preempt mode を有効とします（vr-id 値：1）。

```
【port-channel の場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#vrrp 1 preempt
```

【未設定時】

Preempt mode は無効となります。

28.2.11 vrrp priority

【機能】

VRRP ルータの優先度の設定

【入力形式】

```
vrrp <vr-id 値> priority <優先度>
```

```
no vrrp <vr-id 値> priority [<優先度>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
vr-id 値	VRRP ルータの VRID を指定します。	1 ～ 255	省略不可
優先度	Master ルータに遷移するための優先度を指定します。	1 ～ 254	

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

VRRP ルータの優先度を設定します。大きい数字ほど優先度は高くなります。現在の Master ルータに障害が発生した場合、他のルータ群の中で優先度の一番高いルータが次の Master ルータとして動作します。

【実行例】

VRRP ルータの優先度を設定します（vr-id 値：1、優先度：50）。

```

【port-channel の場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#vrrp 1 priority 50

```

【未設定時】

優先度は 100 で動作します。

28.2.12 vrrp track

【機能】

優先度の減算

【入力形式】

vrrp <vr-id 値> track <トラック番号> [decrement <減算値>]

no vrrp <vr-id 値> track <トラック番号> [decrement <減算値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
vr-id 値	VRRP ルータの VRID を指定します。	1 ～ 255	省略不可
トラック番号	トラックオブジェクトの番号を指定します。	1 ～ 500	
減算値	指定したトラック状態になった場合、減算する値を指定します。	1 ～ 255	10

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

インタフェース状態、経路状態のトラッキングを有効にし、優先度から減算します。ただし、インタフェースの実アドレスと VRRP ルータアドレスが同じアドレスになっている場合 (owner : priority=255) には減算を行いません。

同一の vrid に対して、track 番号を変えて複数の decrement を設定した場合、track down に応じて、decrement する優先度が加算されますが、decrement の合計が 255 を超えない優先度を設定してください。

減算後の priority が 0 以下になる場合は、priority=0 として動作します。

priority=0 になると、その契機で priority=0 の advertise を送信せずに Initialize 状態に遷移し、他の状態に遷移せずに待機し続けます。

【実行例】

優先度から減算します (vr-id 値 : 1、トラック番号 : 100、減算値 : 20)。

```
【port-channel の場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#vrrp 1 track 100 decrement 20
```

【未設定時】

インタフェース状態、経路状態のトラッキングを無効にします。

28.3 IPv6 VRRP の設定

28.3.1 ipv6 vrrp advertise_delay_timer

【機能】

NA の送信、advertise の送信を開始するまでの遅延時間の設定

【入力形式】

```
ipv6 vrrp advertise_delay_timer <遅延時間>
```

```
no ipv6 vrrp advertise_delay_timer [<遅延時間>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
遅延時間	Master へ遷移した場合に、NA の送信、advertise の送信を開始するまでの遅延時間（単位：秒）を指定します。	1 ～ 60	省略不可

【動作モード】

基本設定モード

【説明】

priority=0 の advertise パケット受信により Master へ遷移した場合に、NA の送信、advertise の送信を開始するまでの遅延時間（単位：秒）を設定します。

priority=0 の advertise パケット受信以外で Master へ遷移した場合は、本タイマは動作しません。

旧 Master の手動切り替えで Backup から Master に遷移した際、CP が Master に遷移していてもネットワークプロセッサへの Master 登録が完了するまでは仮想 MAC 宛のフレームを中継することができないため、NA と advertise の送信を遅らせることで、ネットワークプロセッサへの Master 登録が完了するまでは旧 Master で中継を継続させます。

【実行例】

Master へ遷移した場合に、NA の送信、advertise の送信を開始するまでの遅延時間を設定します（遅延時間：3 秒）。

```
#configure terminal
(config)#ipv6 vrrp advertise_delay_timer 3
```

【未設定時】

遅延時間は 6 秒で動作します。

28.3.2 ipv6 vrrp initialize_delay_time

【機能】

インタフェースがUPしてからBackupに遷移するまでの遅延時間の設定

【入力形式】

ipv6 vrrp initialize_delay_time <遅延時間>

no ipv6 vrrp initialize_delay_time [<遅延時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
遅延時間	VRRPの状態がInitializeからBackupに変化する場合において、インタフェースがUPしてから遅延させる時間（単位：秒）を指定します。	3～60	省略不可

【動作モード】

基本設定モード

【説明】

VRRPの状態がInitializeからBackupに変化する場合において、インタフェースがUPしてからBackupに遷移するまでの遅延時間（単位：秒）を設定します。

Masterで手動切り替えを実施した際、priority=0のadvertiseを送信し自装置は一度Initializeに遷移したあとBackupに遷移しますが、新MasterがNAとadvertiseの送信をipv6 vrrp advertise_delay_timer設定で遅らせているため、Backup（対向からのadvertiseを監視する状態）になるタイミングがそれより早いと切り戻りが発生します。

【実行例】

インタフェースがUPしてからBackupに遷移するまでの遅延時間を設定します（遅延時間：30秒）。

```
#configure terminal
(config)#ipv6 vrrp initialize_delay_time 30
```

【未設定時】

遅延時間は3秒で動作する。

28.3.3 ipv6 vrrp np_delay_timer

【機能】

ネットワークプロセッサへのMaster以外の状態の登録を遅延する時間の設定

【入力形式】

ipv6 vrrp np_delay_timer <遅延時間>

no ipv6 vrrp np_delay_timer [<遅延時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
遅延時間	Master->Master以外へ遷移した場合に、ネットワークプロセッサへのMaster以外の状態の登録を遅延する時間(単位: 秒)を指定します。	1 ~ 60	省略不可

【動作モード】

基本設定モード

【説明】

Master->Master以外へ遷移した場合に、ネットワークプロセッサへのMaster以外の状態の登録を遅延する時間(単位: 秒)を設定します。

Masterで手動切り替えを実施した際、L2SWのMAC学習が切り替わるまでは旧Masterで中継フレームを受信することになるため、非Master状態でも一時的に中継可能な状態にして断時間を低減させます。

【実行例】

ネットワークプロセッサへのMaster以外の状態の登録を遅延する時間を設定します(遅延時間: 3秒)。

```
#configure terminal
(config)#ipv6 vrrp np_delay_timer 3
```

【未設定時】

遅延時間は10秒で動作します。

28.3.4 ipv6 vrrp address

【機能】

ルータグループの仮想IPv6アドレスの設定

【入力形式】

ipv6 vrrp <vr-id 値> address <VRRP ルータアドレス>

no ipv6 vrrp <vr-id 値> address [<VRRP ルータアドレス>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
vr-id 値	VRRP ルータの VRID を指定します。	1 ~ 255	省略不可
VRRP ルータアドレス	VRRP ルータアドレスを指定します。	IPv6 アドレス形式	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

ルータグループの仮想IPv6アドレスを設定します。

通常は、自分が Master ルータの場合であっても、実 IPv6 アドレスとは違うアドレスをグループの仮想 IPv6 アドレスとして指定します。

VRRP ルータアドレスがインタフェースの実 IPv6 アドレスと同じ場合、owner として動作します。

【実行例】

ルータグループの仮想 IPv6 アドレスを設定します (vr-id 値：1、VRRP ルータアドレス：2001:db8::1/32)。

```
【port-channel の場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 vrrp 1 address 2001::db8:1/32
```

【未設定時】

VRRP ルータアドレスの設定を行いません。

28.3.5 ipv6 vrrp adver-interval

【機能】

ADVERTISEMENT パケットの送信間隔の設定

【入力形式】

ipv6 vrrp <vr-id 値> adver-interval {<送信間隔 sec 指定> | dsec <送信間隔 dsec 指定>}

no ipv6 vrrp <vr-id 値> adver-interval [{<送信間隔 sec 指定> | dsec <送信間隔 dsec 指定>}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
vr-id 値	VRRP ルータの VRID を指定します。	1 ～ 255	省略不可
送信間隔 sec 指定	ADVERTISEMENT パケットの送信間隔 (単位：秒) を指定します。	1 ～ 30	省略不可
送信間隔 dsec 指定	ADVERTISEMENT パケットの送信間隔 (単位：1/10 秒) を指定します。	1 ～ 300	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

ADVERTISEMENT パケットの送信間隔を設定します。

【実行例】

ADVERTISEMENT パケットの送信間隔を設定します (vr-id 値：1、送信間隔：10 秒)。

```
【port-channel の場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 vrrp 1 adver-interval 10
```

【未設定時】

送信間隔は 1 秒で動作します。

28.3.6 ipv6 vrrp delegated-interface

【機能】

interface-delegation モードにおいて、代表インタフェースとして動作させる設定

【入力形式】

```
ipv6 vrrp <vr-id 値> delegated-interface
```

```
no ipv6 vrrp <vr-id 値> delegated-interface
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
vr-id 値	VRRP ルータの VRID を指定します。	1 ～ 255	省略不可

【動作モード】

port-channel インタフェース設定モード

【説明】

interface-delegation モードにおいて、代表インタフェースとして動作させる場合に設定します。

同一物理インタフェース、同一 VRID のどの port-channel インタフェースにも本設定がない場合は、port-channel 番号の小さいインタフェースが代表インタフェースとして動作します。

【実行例】

interface-delegation モードにおいて、代表インタフェースとして動作させる設定をします。(vr-id 値：1)

```
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 vrrp 1 delegated-interface
```

【未設定時】

代表インタフェースとして動作しません。

28.3.7 ipv6 vrrp mode interface-delegation

【機能】

interface-delegation モードを動作させる設定

【入力形式】

```
ipv6 vrrp mode interface-delegation
```

```
no ipv6 vrrp mode interface-delegation
```

【動作モード】

基本設定モード

【説明】

interface-delegation モードで動作させる場合に設定します。

interface-delegation モードでは、同一物理インタフェース、同一 VRID を束ね、代表の Port-Channel の VRRP 設定に従って、その単位で状態遷移を行います。

【実行例】

```
#configure terminal
(config)#ipv6 vrrp mode interface-delegation
```

【未設定時】

同一物理インタフェース、同一 VRID であっても、各 port-channel の設定に従って動作します。

28.3.8 ipv6 vrrp mode trap-enable-all

【機能】

interface-delegation モードにおいて、vrrp の Master 遷移 trap を出力する設定

【入力形式】

ipv6 vrrp mode trap-enable-all

no ipv6 vrrp mode trap-enable-all

【動作モード】

基本設定モード

【説明】

interface-delegation モードにおいて、非代表インタフェースを含めた全てのインタフェースで vrrp の Master 遷移 trap を出力する場合に設定します。

【実行例】

```
#configure terminal
(config)#ipv6 vrrp mode trap-enable-all
```

【未設定時】

代表インタフェースのみ Master 遷移 trap を出力します。

28.3.9 ipv6 vrrp preempt

【機能】

Preempt mode を有効とする設定

【入力形式】

```
ipv6 vrrp <vr-id 値> preempt
```

```
no ipv6 vrrp <vr-id 値> preempt
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
vr-id 値	VRRP ルータの VRID を指定します。	1 ～ 255	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

Preempt mode を有効とする場合に設定します。

Master ルータに障害が発生し Backup ルータに切り替わる場合や、Master ルータが復旧し Backup ルータから切り戻す場合の動作を指定します。

Preempt mode が有効な場合	ipv6 vrrp priority コマンドで設定した優先度で判断し、常に優先度の高いルータが Master ルータとなります。
Preempt mode が無効の場合	Master ルータに障害が発生し Backup ルータが Master ルータになったあとに、最初の Master ルータが復旧したとしても、ipv6 vrrp priority コマンドで設定した優先度に関係なく、現在の Master ルータ（元 Backup ルータ）が動作し続けます。

【実行例】

Preempt mode を有効とする（vr-id 値：1）。

```
【port-channel の場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 vrrp 1 preempt
```

【未設定時】

Preempt mode は無効となります。

28.3.10 ipv6 vrrp priority

【機能】

VRRP ルータの優先度の設定

【入力形式】

```
ipv6 vrrp <vr-id 値> priority <優先度>
```

```
no ipv6 vrrp <vr-id 値> priority [<優先度>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
vr-id 値	VRRP ルータの VRID を指定します。	1 ～ 255	省略不可

パラメタ	設定内容	設定範囲	省略時
優先度	Master ルータに遷移するための優先度を指定します。	1 ～ 254	省略不可

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

VRRP ルータの優先度を設定します。大きい数字ほど優先度は高くなります。現在の Master ルータに障害が発生した場合、ほかのルータ群の中で優先度の一番高いルータが次の Master ルータとして動作します。

【実行例】

VRRP ルータの優先度を設定します（vr-id 値：1、優先度：50）。

```

【port-channel の場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 vrrp 1 priority 50

```

【未設定時】

優先度は 100 で動作します。

28.3.11 ipv6 vrrp track

【機能】

優先度の減算

【入力形式】

ipv6 vrrp <vr-id 値> track <トラック番号> [decrement <減算値>]

no ipv6 vrrp <vr-id 値> track <トラック番号> [decrement <減算値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
vr-id 値	VRRP ルータの VRID を指定します。	1 ～ 255	省略不可
トラック番号	トラックオブジェクトの番号を指定します。	1001 ～ 1500	省略不可
減算値	指定したトラック状態になった場合、減算する値を指定します。	1 ～ 255	10

【動作モード】

management インタフェース設定モード、port-channel インタフェース設定モード

【説明】

インタフェース状態、経路状態のトラッキングを有効にし、優先度から減算します。ただし、インタフェースの実アドレスと VRRP ルータアドレスが同じアドレスになっている場合（owner：priority=255）には減算を行いません。

同一の vrid に対して、track 番号を変えて複数の decrement を設定した場合、track down に応じて、decrement する優先度が加算されますが、decrement の合計が 255 を超えない優先度を設定してください。

減算後の priority が 0 以下になる場合は、priority=0 として動作します。priority=0 になると、その契機で priority=0 の advertise を送信せずに Initialize 状態に遷移し、ほかの状態に遷移せずに待機し続けます。

【実行例】

インタフェース状態、経路状態のトラッキングを有効にし、優先度から減算します（vr-id 値：1、トラック番号：1100、優先度：20）。

```
【port-channel の場合】
#configure terminal
(config)#interface port-channel 1
(config-if-ch 1)#ipv6 vrrp 1 track 1100 decrement 20
```

【未設定時】

インタフェース状態、経路状態のトラッキングを無効にします。

28.3.12 track ipv6

【機能】

トラックの状態を宛先ネットワーク／宛先ホストに対する到達性と連動させる設定

【入力形式】

track <トラック番号> ipv6 {route <宛先ネットワーク／プレフィックス> | host <宛先ホスト>} [vrf <VRF 名>] reachability [delay-up <遅延時間>] [delay-down <遅延時間>]

no track <トラック番号> [ipv6 {route <宛先ネットワーク／プレフィックス> | host <宛先ホスト>} [vrf <VRF 名>] reachability [delay-up <遅延時間>] [delay-down <遅延時間>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
トラック番号	トラックオブジェクトの番号を指定します。	1001～1500	省略不可
宛先ネットワーク	宛先ネットワークへの到達性により、トラックの状態変化を行います。	IPv6 アドレス形式	省略不可
プレフィックス	宛先ネットワークへの到達性により、トラックの状態変化を行います。	IPv6 アドレス形式	省略不可
宛先ホスト	宛先ホストへの到達性により、トラックの状態変化を行います。	IPv6 アドレス形式	省略不可
VRF 名	VRF 名を指定します。	63 文字以内の WORD 型	VRF を使用しない
遅延時間	UP/DOWN した際に、状態を変化させるまでの時間（単位：秒）を指定します。	1～180	0

【動作モード】

基本設定モード

【説明】

トラックの状態を、宛先ネットワーク／宛先ホストに対する到達性と連動させる場合に設定します。

宛先への到達性がある場合はトラックの状態を UP に、宛先への到達性がない場合はトラックの状態を DOWN にします。

宛先への到達性は、track 設定のアドレス／プレフィックス長に完全一致する経路情報があるかどうかにより判断します。

【実行例】

トラックの状態を、宛先ネットワークに対する到達性と連動させる（トラック番号：1100、宛先ネットワーク：2001:db8::/48）。

```
#configure terminal
(config)#track 1100 ipv6 route 2001:db8::/48 reachability
```

【未設定時】

宛先への到達性と VRRP は連携しません。

第29章 surveyの設定



この章では、surveyの設定に関するコマンドについて説明します。

29.1 survey の設定

29.1.1 survey-map

【機能】

survey-map 設定モードへの移行

【入力形式】

survey-map <survey-map 名>

no survey-map <survey-map 名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
survey-map 名	survey-map 名を指定します。	254 文字以内の WORD 型	省略不可

【動作モード】

基本設定モード

【説明】

survey-map 設定モードに移行します。コマンドの先頭に "no" を指定することで、該当 survey-map 設定モードの内容がすべて消去されます。

【注意】

survey 設定（survey コマンド、および survey-map コマンド）とスタティック経路連携設定（ip route survey コマンド、ipv6 route survey コマンド、ip route vrf survey コマンド、ipv6 route vrf survey コマンド）は同時設定（1 度の refresh コマンド）しないでください。

該当スタティック経路宛のパケットが廃棄される可能性があります。

必ず、以下のように分割設定（2 度の refresh コマンドに分割）としてください。

1. survey 設定（survey コマンド、および survey-map コマンド）
2. refresh コマンド実行
3. スタティック経路連携設定（ip route survey コマンド、ipv6 route survey コマンド、ip route vrf survey コマンド、ipv6 route vrf survey コマンド）
4. refresh コマンド実行

【実行例】

survey-map 設定モードに移行します（survey-map 名：survey-map-A）。

```
#configure terminal
(config)#survey-map survey-map-A
(config-svmap survey-map-A)#
```

29.1.2 ip route survey

【機能】

端末接続監視による経路制御機能を有効にする設定

【入力形式】

ip route <ネットワークアドレス> <ネットマスク> {<Next-hop> | <インタフェース名> <インタフェース番号>} survey {[vrf <VRF 名>] <宛先アドレス> | name <survey 名>} [<ディスタンス値>]

no ip route <ネットワークアドレス> <ネットマスク> {<Next-hop> | <インタフェース名> <インタフェース番号>} survey {[vrf <VRF 名>] <宛先アドレス> | name <survey 名>} [<ディスタンス値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ネットワークアドレス	ネットワークアドレスを指定します。	IPv4 アドレス形式	省略不可
ネットマスク	ネットマスクを指定します。	IPv4 アドレス形式	
Next-hop	Next-hop アドレスを指定します。	IPv4 アドレス形式	
インタフェース名	インタフェース名を指定します。	-	
インタフェース番号	インタフェース番号を指定します。	-	
VRF 名	VRF 名を指定します。	63 文字以内の WORD 型	
宛先アドレス	端末接続監視を行う相手端末の IP アドレスを指定します。	IPv4 アドレス形式	
survey 名	端末接続監視を行う相手端末を名前指定します。	63 文字以内の WORD 型	1
ディスタンス値	ディスタンス値を指定します。	2 ～ 255	

【動作モード】

基本設定モード

【説明】

端末接続監視による経路制御機能を有効にする場合に設定します。

端末接続状態が UP の場合、設定したスタティック経路を有効とします。

端末接続状態が DOWN の場合、設定したスタティック経路を無効とします。

【注意】

survey 設定 (survey コマンド、および survey-map コマンド) とスタティック経路連携設定 (ip route survey コマンド、ipv6 route survey コマンド、ip route vrf survey コマンド、ipv6 route vrf survey コマンド) は同時設定 (1 度の refresh コマンド) しないでください。

該当スタティック経路宛のパケットがロスする可能性があります。

必ず、以下のように分割設定 (2 度の refresh コマンドに分割) としてください。

1. survey 設定 (survey コマンド、および survey-map コマンド)
2. refresh コマンド実行
3. スタティック経路連携設定 (ip route survey コマンド、ipv6 route survey コマンド、ip route vrf survey コマンド、ipv6 route vrf survey コマンド)
4. refresh コマンド実行

【実行例】

端末接続監視による経路制御機能を有効にします（ネットワークアドレス：192.0.2.128、ネットマスク：255.255.255.128、インタフェース名：tunnel、インタフェース番号：1、宛先アドレス：192.0.2.1）。

```
#configure terminal
(config)#ip route 192.0.2.128 255.255.255.128 tunnel 1 survey 192.0.2.1
```

【未設定時】

端末接続監視による経路制御機能は動作しません。

29.1.3 ip route vrf survey

【機能】

端末接続監視による経路制御機能を有効にする設定

【入力形式】

ip route vrf <VRF 名 1> <ネットワークアドレス> <ネットマスク> {<Next-hop> | <インタフェース名> <インタフェース番号>} survey {[vrf <VRF 名 2>] <宛先アドレス> | name <survey 名>} [<ディスタンス値>]

no ip route vrf <VRF 名 1> <ネットワークアドレス> <ネットマスク> {<Next-hop> | <インタフェース名> <インタフェース番号>} survey {[vrf <VRF 名 2>] <宛先アドレス> | name <survey 名>} [<ディスタンス値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VRF 名 1	VRF 名 1 を指定します。	63 文字以内の WORD 型	省略不可
ネットワークアドレス	ネットワークアドレスを指定します。	IPv4 アドレス形式	
ネットマスク	ネットマスクを指定します。	IPv4 アドレス形式	
Next-hop	Next-hop アドレスを指定します。	IPv4 アドレス形式	
インタフェース名	インタフェース名を指定します。	-	
インタフェース番号	インタフェース番号を指定します。	-	
VRF 名 2	VRF 名 2 を指定します。	63 文字以内の WORD 型	
宛先アドレス	端末接続監視を行う相手端末の IP アドレスを指定します。	IPv4 アドレス形式	
survey 名	端末接続監視を行う相手端末を名前指定します。	63 文字以内の WORD 型	1
ディスタンス値	ディスタンス値を指定します。	2 ～ 255	

【動作モード】

基本設定モード

【説明】

端末接続監視による経路制御機能を有効にする場合に設定します。

端末接続状態が UP の場合、設定したスタティック経路を有効とします。

端末接続状態が DOWN の場合、設定したスタティック経路を無効とします。

【注意】

survey 設定 (survey コマンド、および survey-map コマンド) とスタティック経路連携設定 (ip route survey コマンド、ipv6 route survey コマンド、ip route vrf survey コマンド、ipv6 route vrf survey コマンド) は同時設定 (1 度の refresh コマンド) しないでください。

該当スタティック経路宛のパケットがロスする可能性があります。

必ず、以下のように分割設定 (2 度の refresh コマンドに分割) としてください。

1. survey 設定 (survey コマンド、および survey-map コマンド)
2. refresh コマンド実行
3. スタティック経路連携設定 (ip route survey コマンド、ipv6 route survey コマンド、ip route vrf survey コマンド、ipv6 route vrf survey コマンド)
4. refresh コマンド実行

【実行例】

端末接続監視による経路制御機能を有効にします (VRF 名 1: vrf-A、ネットワークアドレス: 192.0.2.128、ネットマスク: 255.255.255.128、インタフェース名: tunnel、インタフェース番号: 1、宛先アドレス: 192.0.2.1)。

```
#configure terminal
(config)#ip route vrf vrf-A 192.0.2.128 255.255.255.128 tunnel 1 survey 192.0.2.1
```

【未設定時】

端末接続監視による経路制御機能は動作しません。

29.1.4 ipv6 route survey

【機能】

端末接続監視による経路制御機能を有効にする設定

【入力形式】

ipv6 route <ネットワークアドレス><プレフィックス長> {<Next-hop> | <インタフェース名> <インタフェース番号> [<リンクローカルアドレス>]} survey {[vrf <VRF 名>] <宛先アドレス> | name <survey 名>} [<ディスタンス値>]

no ipv6 route <ネットワークアドレス><プレフィックス長> {<Next-hop> | <インタフェース名> <インタフェース番号> [<リンクローカルアドレス>]} surve

y {[vrf <VRF 名>] <宛先アドレス> | name <survey 名>} [<ディスタンス値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ネットワークアドレス	ネットワークアドレスを指定します。	IPv6 アドレス形式	省略不可
プレフィックス長	プレフィックス長を指定します。	0 ~ 128	
Next-hop	Next-hop アドレスを指定します。	IPv6 アドレス形式	
インタフェース名	インタフェース名を指定します。	-	
インタフェース番号	インタフェース番号を指定します。	-	

パラメタ	設定内容	設定範囲	省略時
リンクローカルアドレス (*1)	リンクローカルアドレスを指定します。	IPv6 アドレス形式	リンクローカルアドレスを指定しない
VRF 名	VRF 名を指定します。	63 文字以内の WORD 型	省略不可
宛先アドレス	端末接続監視を行う相手端末の IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	
survey 名	端末接続監視を行う相手端末を名前指定します。	63 文字以内の WORD 型	
ディスタンス値	ディスタンス値を指定します。	2 ～ 255	1

*1) インタフェース名に "port-channel" を指定した場合のみ、"リンクローカルアドレス" を指定できます。

【動作モード】

基本設定モード

【説明】

端末接続監視による経路制御機能を有効にする場合に設定します。

端末接続状態が UP の場合、設定したスタティック経路を有効とします。

端末接続状態が DOWN の場合、設定したスタティック経路を無効とします。

【注意】

survey 設定 (survey コマンド、および survey-map コマンド) とスタティック経路連携設定 (ip route survey コマンド、ipv6 route survey コマンド、ip route vrf survey コマンド、ipv6 route vrf survey コマンド) は同時設定 (1 度の refresh コマンド) しないでください。

該当スタティック経路宛のパケットがロスする可能性があります。

必ず、以下のように分割設定 (2 度の refresh コマンドに分割) としてください。

1. survey 設定 (survey コマンド、および survey-map コマンド)
2. refresh コマンド実行
3. スタティック経路連携設定 (ip route survey コマンド、ipv6 route survey コマンド、ip route vrf survey コマンド、ipv6 route vrf survey コマンド)
4. refresh コマンド実行

【実行例】

端末接続監視による経路制御機能を有効にします (ネットワークアドレス: 2001:db8:2::、プレフィックス長: 48、インタフェース名: tunnel、インタフェース番号: 1、宛先アドレス: 2001:db8:1::1)。

```
#configure terminal
(config)#ipv6 route 2001:db8:2::/48 tunnel 1 survey 2001:db8:1::1
```

【未設定時】

端末接続監視による経路制御機能は動作しません。

29.1.5 ipv6 route vrf survey

【機能】

端末接続監視による経路制御機能を有効にする設定

【入力形式】

```
ipv6 route vrf <VRF 名 1> <ネットワークアドレス>/<プレフィックス長> {<Next-hop> | <インタフェース名> <インタフェース番号> [<リンクローカルアドレス>]} survey {[vrf <VRF 名 2>] <宛先アドレス> | name <survey 名>} [<ディスタンス値>]
```

```
no ipv6 route vrf <VRF 名 1> <ネットワークアドレス>/<プレフィックス長> {<Next-hop> | <インタフェース名> <インタフェース番号> [<リンクローカルアドレス>]} survey {[vrf <VRF 名 2>] <宛先アドレス> | name <survey 名>} [<ディスタンス値>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VRF 名 1	VRF 名 1 を指定します。	63 文字以内の WORD 型	省略不可
ネットワークアドレス	ネットワークアドレスを指定します。	IPv6 アドレス形式	
プレフィックス長	プレフィックス長を指定します。	0 ～ 128	
Next-hop	Next-hop アドレスを指定します。	IPv6 アドレス形式	
インタフェース名	インタフェース名を指定します。	-	
インタフェース番号	インタフェース番号を指定します。	-	
リンクローカルアドレス(*1)	リンクローカルアドレスを指定します。	IPv6 アドレス形式	リンクローカルアドレスを指定しない
VRF 名 2	VRF 名 2 を指定します。	63 文字以内の WORD 型	省略不可
宛先アドレス	端末接続監視を行う相手端末の IP アドレスを指定します。	IPv4 アドレス形式： IPv6 アドレス形式：	
survey 名	端末監視を行う相手端末を名前指定します。	63 文字以内の WORD 型	
ディスタンス値	ディスタンス値を指定します。	2 ～ 255	1

*1) インタフェース名に "port-channel" を指定した場合のみ、"リンクローカルアドレス" を指定できます。

【動作モード】

基本設定モード

【説明】

端末接続監視による経路制御機能を有効にする場合に設定します。

端末接続状態が UP の場合、設定したスタティック経路を有効とします。

端末接続状態が DOWN の場合、設定したスタティック経路を無効とします。

【注意】

survey 設定 (survey コマンド、および survey-map コマンド) とスタティック経路連携設定 (ip route survey コマンド、ipv6 route survey コマンド、ip route vrf survey コマンド、ipv6 route vrf survey コマンド) は同時設定 (1 度の refresh コマンド) しないでください。

該当スタティック経路宛のパケットがロスする可能性があります。

必ず、以下のように分割設定（2度の refresh コマンドに分割）としてください。

1. survey 設定（survey コマンド、および survey-map コマンド）
2. refresh コマンド実行
3. スタティック経路連携設定（ip route survey コマンド、ipv6 route survey コマンド、ip route vrf survey コマンド、ipv6 route vrf survey コマンド）
4. refresh コマンド実行

【実行例】

端末接続監視による経路制御機能を有効にします（VRF 名 1：vrf-A、ネットワークアドレス：2001:db8:2::、プレフィックス長：48、インタフェース名：tunnel、インタフェース番号：1、宛先アドレス：2001:db8:1::1）。

```
#configure terminal
(config)#ipv6 route vrf vrf-A 2001:db8:2::/48 tunnel 1 survey 2001:db8:1::1
```

【未設定時】

端末接続監視による経路制御機能は動作しません。

29.1.6 survey

【機能】

端末接続監視を行う相手端末の IP アドレスの設定

【入力形式】

survey [vrf <VRF 名>] <宛先アドレス> [name <survey 名>] [survey-map <survey-map 名>] [source <送信元インタフェース名> <送信元インタフェース番号>] [nexthop tunnel <tunnel インタフェース番号>] [{interworking | idleonly}]

no survey [vrf <VRF 名>] <宛先アドレス> [name <survey 名>] [survey-map <survey-map 名>] [source <送信元インタフェース名> <送信元インタフェース番号>] [nexthop tunnel <tunnel インタフェース番号>] [{interworking | idleonly}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
VRF 名	VRF 名を指定します。	63 文字以内の WORD 型	VRF を使用しない
宛先アドレス	端末接続監視を行う相手端末の IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
survey 名	端末接続監視対象に名前を付けます。	63 文字以内の WORD 型	名前を指定しての連携機能が使用不可
survey-map 名	survey-map 名を指定します。	254 文字以内の WORD 型	デフォルトで動作
送信元インタフェース名	ICMP echo request の送信元インタフェース名を指定します。	-	実際に送信するインタフェースの IPv4/IPv6 アドレス
送信元インタフェース番号	ICMP echo request の送信元インタフェース番号を指定します。	-	
tunnel インタフェース番号	tunnel 固定送受信とする tunnel インタフェース番号を指定します。	1 ～ 16777215	省略不可

パラメタ	設定内容	設定範囲	省略時
interworking	IPsec tunnel, IPinIP tunnel の up/down 状態を同期させます。	-	状態を同期させません。
idleonly	IPsec tunnel の受信状態を確認して無受信監視を行います。	-	常時監視を行います。

【動作モード】

基本設定モード

【説明】

端末接続監視を行う相手端末の IP アドレスを設定します。survey-map を指定しない場合は、デフォルト端末監視パラメタで監視を行います。パラメタを変える必要がある場合は、survey-map に変更する内容を登録します。

監視対象に survey 名をつける場合は、それぞれ重複しない名前を設定してください。survey 名が重複した場合、あとから設定された survey 設定は監視停止状態となり監視を行いません。

端末接続監視の結果によって tunnel インタフェースの up/down を同期させたい場合は、nexthop に tunnel インタフェースを指定して "interworking" とします。

このとき、複数の相手端末の同期対象に同一の tunnel インタフェースを指定することもできますが、その場合の動作はサポートしていません。

また、同期対象とした tunnel インタフェースを送信元インタフェースに指定すると、接続が切断状態となった場合、そのあと接続状態が復旧しなくなります。

そのような設定はしないでください。

tunnel インタフェースの受信がある間に ICMP echo リクエストの送信を行わない場合は、nexthop に tunnel インタフェースを指定して "idleonly" とします。

【デフォルト端末監視パラメタ】

ICMP echo のデータグラムサイズ	IPv4 アドレス監視：32bytes IPv6 アドレス監視：52bytes
ICMP echo の送信元アドレス	実際に送信するインタフェースの IPv4/IPv6 アドレス
DSCP 値	0
TTL 値	1
応答待ち時間	1 秒
定期送信間隔	60 秒
連続して応答がなかった場合に、DOWN とみなす回数	6 回
連続して応答があった場合に、UP とみなす回数	3 回
DOWN 状態で、応答があった場合の送信間隔	1 秒
開始時間	refresh コマンド実行後
終了時刻	終了しない

【注意】

survey 設定 (survey コマンド、および survey-map コマンド) とスタティック経路連携設定 (ip route survey コマンド、ipv6 route survey コマンド、ip route vrf survey コマンド、ipv6 route vrf survey コマンド) は同時設定 (1 度の refresh コマンド) しないでください。

該当スタティック経路宛のパケットがロスする可能性があります。

必ず、以下のように分割設定 (2 度の refresh コマンドに分割) としてください。

1. survey 設定 (survey コマンド、および survey-map コマンド)

2. refresh コマンド実行
3. スタティック経路連携設定 (ip route survey コマンド、ipv6 route survey コマンド、ip route vrf survey コマンド、ipv6 route vrf survey コマンド)
4. refresh コマンド実行

【実行例】

相手端末の IP アドレスを設定します (宛先アドレス：192.0.2.1、送信元インタフェース名：port-channel、送信元インタフェース番号：100)。

```
#configure terminal
(config)#survey 192.0.2.1 source port-channel 100
```

【未設定時】

端末接続監視を行いません。

29.1.7 neighbor surveillance nexthop-validation-check

【機能】

BGP で通知する経路情報を変更する設定

【入力形式】

neighbor <BGP ピア> surveillance nexthop-validation-check

no neighbor <BGP ピア> surveillance nexthop-validation-check

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可

【動作モード】

BGP サービス設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

BGP ピアへの端末接続監視機能を行い、その結果により、BGP で通知する経路情報の変更を行う場合に指定します。本コマンドを指定すると、BGP ピアへの端末接続監視結果が UP の場合は、その BGP ピアから受信した経路情報は Active、BGP ピアへの端末接続監視結果が DOWN になった場合は、その BGP ピアから受信した経路情報を Inactive とします。端末接続監視機能で、BGP ピアへの設定を行っている必要があります。

【実行例】

BGP で通知する経路情報の変更を行います (BGP ピア：192.0.2.1)。

```
【BGP サービス設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor 192.0.2.1 surveillance nexthop-validation-check
```

【未設定時】

BGP で通知する経路情報の変更を行いません。

29.1.8 neighbor surveillance peer-address

【機能】

UPDATE メッセージを送信しなおす設定

【入力形式】

neighbor <BGP ピア> surveillance peer-address <宛先アドレス>

no neighbor <BGP ピア> surveillance peer-address <宛先アドレス>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名 : 255 文字以内の CDATA 型	省略不可
宛先アドレス	端末接続監視を行う相手端末の IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	

【動作モード】

BGP サービス設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

端末接続監視先の状態により、BGP ピアへの経路情報の内容を変更し、UPDATE メッセージを送信しなおす場合に設定します。たとえば、冗長構成を形成している状態でメイン側に端末接続監視を行い、DOWN 状態になった場合にバックアップ側の経路情報の優先度を上げて通知するようなことが可能になります。DOWN 状態になった場合にどのような変更を行うかは、neighbor surveillance down-action コマンドで指定します。UPDATE メッセージは、指定している BGP ピアに対してはすべての経路情報を、他の BGP ピアに対しては指定している BGP ピアから受信した経路情報を送信しなおします。

【実行例】

UPDATE メッセージを送信しなおします (BGP ピア : 192.0.2.1、宛先アドレス : 192.0.2.2)。

```
【BGP サービス設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#neighbor 192.0.2.1 surveillance peer-address 192.0.2.2
```

【未設定時】

UPDATE メッセージを送信しなおしません。

29.1.9 neighbor surveillance down-action

【機能】

BGP ピアへ送信する経路情報の設定

【入力形式】

neighbor <BGP ピア> surveillance down-action <route-map 名>

no neighbor <BGP ピア> surveillance down-action <route-map 名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
BGP ピア	BGP ピアを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 peer-group 名：255 文字以内の CDATA 型	省略不可
route-map 名	route-map 名を指定します。	254 文字以内の WORD 型	

【動作モード】

address-family ipv4 設定モード、address-family ipv6 設定モード、address-family ipv4 VRF 設定モード、address-family ipv6 VRF 設定モード

【説明】

端末接続監視が DOWN した場合に、BGP ピアへ送信する経路情報の内容をどのようにするかを route-map を利用して指定します。端末接続監視が UP した場合は、元の経路情報を送信します。たとえば冗長構成を形成している状態で、メイン側に端末接続監視を行い、DOWN 状態になった場合は、LOCAL-PREF 属性を 100 増加して通知するといった運用が可能となります。どの接続端末が DOWN 状態になった場合に、通知する経路情報の内容を変更するかは、neighbor surveillance peer-address コマンドで指定します。

【実行例】

BGP ピアへ送信する経路情報の内容をどのようにするかを設定します（BGP ピア：192.0.2.1、route-map 名：route-map-A）。

```

【address-family ipv4 設定モードの場合】
#configure terminal
(config)#router bgp 64496
(config-bgp)#address-family ipv4 unicast
(config-af ipv4 unicast)#neighbor 192.0.2.1 surveillance down-action route-map-A

```

【未設定時】

端末接続監視機能と連携しません。

29.1.10 dont-route

【機能】

経路表を検索せずに監視先アドレスと同一ネットワークのインタフェースに監視パケットを送信する設定

【入力形式】

dont-route

no dont-route

【動作モード】

survey-map 設定モード

【説明】

survey 監視時、経路表を検索せずに監視先アドレスと同一ネットワークのインタフェースに監視パケットを送信する場合に設定します。

同一ネットワークのインタフェースが存在しない場合には、監視パケットを送信しません。

tunnel インタフェース固定拡張機能を行う場合、本設定は無効となります。

【実行例】

経路表を検索せずに監視先アドレスと同一ネットワークのインタフェースに監視パケットを送信します。

```
#configure terminal
(config)#survey-map survey-map-A
(config-svmap survey-map-A)#dont-route
```

【未設定時】

survey 監視時、経路表を検索した結果得られたインタフェースに監視パケットを送信します。

29.1.11 dscp

【機能】

ICMP echo パケットの DSCP 値の設定

【入力形式】

dscp <DSCP 値>

no dscp [<DSCP 値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
DSCP 値	設定している survey-map で使用する ICMP エコーパケットの IP ヘッダの TOS フィールド値を設定します。	0 ～ 255	省略不可

【動作モード】

survey-map 設定モード

【説明】

設定している survey-map で使用する ICMP エコーパケットの IP ヘッダの TOS フィールド値を設定します。

【実行例】

設定している survey-map で使用する ICMP エコーパケットの IP ヘッダの TOS フィールド値を設定します。(DSCP 値：100)。

```
#configure terminal
(config)#survey-map survey-map-A
(config-svmap survey-map-A)#dscp 100
```

【未設定時】

DSCP 値は 0 で動作します。

29.1.12 frequency

【機能】

定期監視間隔の設定

【入力形式】

frequency every <定期送信間隔>

no frequency [every <定期送信間隔>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
定期送信間隔	送信する間隔をミリ秒単位で指定します。	1000～86400000	省略不可

【動作モード】

survey-map 設定モード

【説明】

定期送信間隔をミリ秒単位で設定します。実際の動作時間は秒単位（百の位以下は切り上げ）となります。

【実行例】

定期監視間隔を設定します（定期監視間隔：1 秒）。

```
#configure terminal
(config)#survey-map survey-map-A
(config-svmap survey-map-A)#frequency every 1000
```

【未設定時】

定期監視間隔は 60 秒で動作します。

29.1.13 hop-limit

【機能】

ICMPv6 echo パケットの hop-limit 値の設定

【入力形式】

hop-limit <hop-limit 値>

no hop-limit [<hop-limit 値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
hop-limit 値	ICMPv6 echo パケットの hop-limit 値を指定します。	1 ～ 255	省略不可

【動作モード】

survey-map 設定モード

【説明】

ICMPv6 echo パケットの hop-limit 値を設定します。

【実行例】

ICMPv6 echo パケットの hop-limit 値を設定します (hop-limit 値：255)。

```
#configure terminal
(config)#survey-map survey-map-A
(config-svmap survey-map-A)#hop-limit 255
```

【未設定時】

hop-limit 値は 1 で動作します。

29.1.14 retry

【機能】

再送回数の設定

【入力形式】

retry <再送信回数> [interval <再送信間隔>]

no retry [<再送信回数> [interval <再送信間隔>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
再送信回数	ICMP echo パケットの再送信回数を指定します。	0 ～ 60	省略不可
再送信間隔	再送信間隔（単位：秒）をミリ秒単位で指定します。	1000 ～ 86400000	0 秒（即時）

【動作モード】

survey-map 設定モード

【説明】

再送信回数と再送信間隔（単位：秒）をミリ秒単位で設定します。実際の動作時間は秒単位（百の位以下は切り上げ）となります。

timeout コマンドで設定した時間内に応答がなかった場合、timeout 後に再送信間隔だけ待ってから再送信を行います。再送信回数分の応答がなかった場合は、切断状態（DOWN 状態）となります。

再送信間隔が設定されていない場合、timeout 後に即時に再送信を行います。

【実行例】

再送信回数を設定します（再送信回数：10 回）。

```
#configure terminal
(config)#survey-map survey-map-A
(config-svmap survey-map-A)#retry 10
```

【未設定時】

以下の値で動作します。

再送信回数： 5 回

再送信間隔： 0 秒（即時）

29.1.15 size

【機能】

ICMP echo パケットのデータグラムサイズの設定

【入力形式】

size <データサイズ>

no size [<データサイズ>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
データサイズ	ICMP echo パケットのデータグラムサイズ（単位：bytes）を指定します。	32 ～ 2048	省略不可

【動作モード】

survey-map 設定モード

【説明】

ICMP echo パケットのデータグラムサイズ（単位：bytes）を設定します。

【実行例】

ICMP echo パケットのデータグラムサイズを設定します（データサイズ：100bytes）。

```
#configure terminal
(config)#survey-map survey-map-A
(config-svmap survey-map-A)#size 100
```

【未設定時】

IPv4 アドレス監視ならば 32byte、IPv6 アドレス監視は 52byte で動作します。

29.1.16 stability

【機能】

相手の復旧を確認するための再送回数と送信間隔の設定

【入力形式】

stability <連続受信回数> [interval <送信間隔>]

no stability [<連続受信回数> [interval <送信間隔>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
連続受信回数	監視切断状態（DOWN 状態）から復旧するために、応答を何回連続して受信するか回数を指定します。	1～60	省略不可
送信間隔	監視切断状態（DOWN 状態）から復旧する際の送信間隔（単位：秒）をミリ秒単位で指定します。	1000～60000	1 秒間隔

【動作モード】

survey-map 設定モード

【説明】

監視切断状態（DOWN 状態）から復旧を確認するための連続受信回数とその際の送信間隔（単位：ミリ秒）を設定します。送信間隔については秒単位（百の位以下は切り上げ）となります。

【実行例】

切断状態から復旧を確認するための連続受信回数と送信間隔を設定します（受信回数：5 回、送信間隔：1 秒）。

```
#configure terminal
(config)#survey-map survey-map-A
(config-svmap survey-map-A)#stability 5 interval 1000
```

【未設定時】

以下の値で動作します。

連続受信回数：3 回

送信間隔：1 秒

29.1.17 timeout

【機能】

応答待ち時間の設定

【入力形式】

timeout < 応答待ち時間 >

no timeout [< 応答待ち時間 >]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
応答待ち時間	応答待ち時間（単位：秒）をミリ秒単位で指定します。	1000 ～ 60000	省略不可

【動作モード】

survey-map 設定モード

【説明】

応答待ち時間（単位：秒）をミリ秒単位で設定します。実際の動作時間は秒単位（百の位以下は切り上げ）となります。

設定した時間内に応答がなかった場合、retry コマンドで設定した回数の再送を行います。

【実行例】

応答待ち時間を設定します（応答待ち時間：2 秒）。

```
#configure terminal
(config)#survey-map survey-map-A
(config-svmap survey-map-A)#timeout 2000
```

【未設定時】

応答待ち時間は 1 秒で動作します。

29.1.18 traffic-class

【機能】

ICMPv6 echo パケットのトラフィッククラス値の設定

【入力形式】

traffic-class < トラフィッククラス値 >

no traffic-class [< トラフィッククラス値 >]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
トラフィッククラス値	ICMPv6 echo パケットのトラフィッククラス値を指定します。	0 ～ 255	省略不可

【動作モード】

survey-map 設定モード

【説明】

ICMPv6 echo パケットのトラフィッククラス値を設定します。

【実行例】

ICMPv6 echo パケットのトラフィッククラス値を設定します（トラフィッククラス値：16）。

```
#configure terminal
(config)#survey-map survey-map-A
(config-svmap survey-map-A)#traffic-class 16
```

【未設定時】

トラフィッククラス値は 0 で動作します。

29.1.19 ttl

【機能】

ICMP echo パケットの TTL 値の設定

【入力形式】

ttl <TTL 値>

no ttl [<TTL 値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
TTL 値	ICMP echo パケットの TTL 値を指定します。	1～255	省略不可

【動作モード】

survey-map 設定モード

【説明】

ICMP echo パケットの TTL 値を設定します。

【実行例】

ICMP echo パケットの TTL 値を設定します（TTL 値：200）。

```
#configure terminal
(config)#survey-map survey-map-A
(config-svmap survey-map-A)#ttl 200
```

【未設定時】

TTL 値は 1 で動作します。

29.1.20 tunnel-unused

【機能】

ICMP パケットの送信

【入力形式】

tunnel-unused

no tunnel-unused

【動作モード】

survey-map 設定モード

【説明】

端末接続監視時、tunnel インタフェースを除いたインタフェースに監視パケットを送信する場合に設定します。

tunnel インタフェース固定拡張機能を行う場合、本設定は無効となります。

【実行例】

端末接続監視時、tunnel インタフェースを除いたインタフェースに監視パケットを送信します。

```
#configure terminal
(config)#survey-map survey-map-A
(config-svmap survey-map-A)#tunnel-unused
```

【未設定時】

survey 監視時、経路表を検索した結果得られたインタフェースに監視パケットを送信します。

第30章 SNMPの設定



この章では、SNMPの設定に関するコマンドについて説明します。

30.1	SNMPv1、v2の設定.....	890
30.2	SNMPv3の設定.....	900

30.1 SNMPv1、v2 の設定

30.1.1 snmp-server community

【機能】

SNMP マネージャのコミュニティ名の設定

【入力形式】

snmp-server community <コミュニティ名> [ro | rw] [<アクセスリスト番号>]

no snmp-server community <コミュニティ名> [ro | rw] [<アクセスリスト番号>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
コミュニティ名	SNMP のコミュニティ名を指定します。	32 文字以内の WORD 型	省略不可
ro rw	read only か read/write かを指定します。	ro:read only rw:read/write	ro
アクセスリスト番号	アクセスリスト番号を指定します。	-	すべて許可

【動作モード】

基本設定モード

【説明】

SNMP マネージャのコミュニティ名を設定します。本設定は、設定順にソートされます。

【実行例】

SNMP マネージャのコミュニティ名を設定します（コミュニティ名：public、アクセス権：rw、アクセスリスト番号：20）。

```
#configure terminal
(config)#snmp-server community public rw 20
```

【未設定時】

SNMP 機能を使用できません。

30.1.2 snmp-server contact

【機能】

管理者名の設定

【入力形式】

snmp-server contact <管理者名>

no snmp-server contact

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
管理者名	管理者名を指定します。	254文字以内のWORD型(*1)	省略不可

*1) 1文字の空白（スペース）は使用可能です。複数の空白（スペース）は1文字にまとめられます。

【動作モード】

基本設定モード

【説明】

管理者名を設定します。

【実行例】

管理者名を設定します（管理者名：superuser-A）。

```
#configure terminal
(config)#snmp-server contact superuser-A
```

【未設定時】

管理者名を設定しません。

30.1.3 snmp-server enable traps

【機能】

トラップ送信機能の設定

【入力形式】

snmp-server enable traps [トラップ種別]

no snmp-server enable traps

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
トラップ種別	SNMP マネージャに送信するトラップの種別を指定します。 複数指定が可能です。	snmp event syslog entity bgp auth ospf ipsec vrrp ipsec-session event-action	すべてのトラップ種別

【動作モード】

基本設定モード

【説明】

トラップ送信機能を有効にします。

snmp	標準 MIB のトラップを送信
event	アラームなどの Event に関するトラップを送信
syslog	ログのトラップを送信
entity	Entity トラップを送信
bgp	BGP 関連のトラップを送信
auth	login/ftp 認証失敗時のトラップを送信
ospf	OSPF に関するトラップを送信
ipsec	IPsec に関するトラップを送信
vrrp	VRRP に関するトラップを送信
ipsec-session	IPsec session に関するトラップを送信
event-action	event-action に関するトラップを送信
指定しない	すべてのトラップ種別

【実行例】

トラップ送信機能を有効にします（トラップ種別：bgp ospf）。

```
#configure terminal
(config)#snmp-server enable traps bgp ospf
```

【未設定時】

トラップを送信しません。

30.1.4 snmp-server host

【機能】

トラップを送信する際の SNMP マネージャの各種パラメタの設定

【入力形式】

snmp-server host <SNMP マネージャ> <コミュニティ名> [v1 | v2c] [トラップ種別]

no snmp-server host <SNMP マネージャ>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
SNMP マネージャ	SNMP マネージャを指定します。	IPv4 アドレス形式 ホスト名 254 文字以内の WORD 型	省略不可
コミュニティ名	コミュニティ名を指定します。	32 文字以内の WORD 型	
v1 v2c	SNMP の動作バージョンを指定します。	v1 v2c	v1

パラメタ	設定内容	設定範囲	省略時
トラップ種別	SNMP マネージャに送信するトラップの種別を指定します。 複数指定が可能です。	snmp event syslog entity bgp auth ospf ipsec vrrp ipsec-session event-action	すべてのトラップ種別

【動作モード】

基本設定モード

【説明】

トラップを送信する際の SNMP マネージャの各種パラメタを設定します。

複数登録した場合には、show current.cfg(show running.cfg) コマンドで表示される上位 20 個までが有効となります。21 個以上は設定上、無効となります。

【実行例】

トラップを送信する際の SNMP マネージャの各種パラメタを設定します (SNMP マネージャ：192.0.2.1、コミュニティ名：public、SNMP 動作バージョン：v1、トラップ種別：bgp)。

```
#configure terminal
(config)#snmp-server host 192.0.2.1 public v1 bgp
```

【未設定時】

SNMP のトラップを送信しません。

30.1.5 snmp-server host-queue timeout

【機能】

TRAP メッセージをキューに保存しておく時間の設定

【入力形式】

snmp-server host-queue timeout <タイムアウト値>

no snmp-server host-queue timeout

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
タイムアウト値	トラップメッセージをキューに保存しておく時間（単位：秒）を指定します。	1～1000	省略不可

【動作モード】

基本設定モード

【説明】

TRAP メッセージをキューに保存しておく時間（単位：秒）を設定します。

【実行例】

TRAP メッセージをキューに保存しておく時間を設定します（タイムアウト値：1000 秒）。

```
#configure terminal
(config)#snmp-server host-queue timeout 1000
```

【未設定時】

タイムアウト値は 600 秒で動作します。

30.1.6 snmp-server location

【機能】

設置場所の設定

【入力形式】

snmp-server location <設置場所>

no snmp-server location

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
設置場所	設置場所を指定します。	254 文字以内の WORD 型(*1)	省略不可

*1) 1 文字の空白（スペース）は使用可能です。複数の空白（スペース）は 1 文字にまとめられます。

【動作モード】

基本設定モード

【説明】

設置場所を設定します。

【実行例】

設置場所を設定します（設置場所：Honsha）。

```
#configure terminal
(config)#snmp-server location Honsha
```

【未設定時】

設置場所を設定しません。

30.1.7 snmp-server name

【機能】

system グループの sysName に表示するシステム名称の設定

【入力形式】

snmp-server name <システム名称>

no snmp-server name

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
システム名称	システム名称を指定します。	254 文字以内の WORD 型 (*1)	省略不可

*1) 1 文字の空白（スペース）は使用可能です。複数の空白（スペース）は 1 文字にまとめられます。

【動作モード】

基本設定モード

【説明】

system グループの sysName に表示するシステム名称を設定します。

【実行例】

system グループの sysName に表示するシステム名称を設定します（システム名称：GX500）。

```
#configure terminal
(config)#snmp-server name GX500
```

【未設定時】

システム名称は設定されません。ただし、hostname コマンドでホスト名が設定されている場合は、ホスト名をシステム名称として使用します。

30.1.8 snmp-server queue-length

【機能】

TRAP ホストごとに保存可能なメッセージ数の設定

【入力形式】

snmp-server queue-length <メッセージ数>

no snmp-server queue-length

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
メッセージ数	保存可能なメッセージ数を指定します。	1 ～ 5000	省略不可

【動作モード】

基本設定モード

【説明】

TRAP ホストごとに保存可能なメッセージ数を設定します。

【実行例】

TRAP ホストごとに保存可能なメッセージ数を設定します（メッセージ数：2000）。

```
#configure terminal
(config)#snmp-server queue-length 2000
```

【未設定時】

メッセージ数は 1500 で動作します。

30.1.9 snmp-server source-interface

【機能】

SNMP TRAP の送信元 IP アドレスとして使用するインタフェースの設定

【入力形式】

snmp-server source-interface <インタフェース名> <インタフェース番号>

no snmp-server source-interface

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース名	送信元アドレスとして使用するインタフェース名を指定します。	-	省略不可
インタフェース番号	送信元アドレスとして使用するインタフェース番号を指定します。	-	

【動作モード】

基本設定モード

【説明】

SNMP TRAP の送信元 IP アドレスとして使用するインタフェースを設定します。

本コマンドで指定したインタフェースの IPv4 アドレスは、SNMPv1-Trap-PDU 内の agent-addr フィールドの値にも設定されます。

IPv6 ネットワーク上の SNMP マネージャに対して SNMPv1 TRAP を送信する場合の agent-addr は常に "0.0.0.0" の値となります。

【実行例】

SNMP TRAP の送信元 IP アドレスとして使用するインタフェースを設定します（インタフェース名：loopback、インタフェース番号：1）。

```
#configure terminal
(config)#snmp-server source-interface loopback 1
```

【未設定時】

SNMP TRAP の送信元 IP アドレスとして使用するインタフェースは、設定上のインタフェースを検索し最初に見つけたアドレスを使用します。設定は以下の順に検索します。

1. loopback
2. port-channel
3. management

30.1.10 snmp-server trap-timeout

【機能】

キューに保存された TRAP メッセージの再送を試みる時間の設定

【入力形式】

snmp-server trap-timeout <タイムアウト値>

no snmp-server trap-timeout

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
タイムアウト値	キューに保存されたトラップメッセージの再送を試みる時間（単位：秒）を指定します。	1～1000	省略不可

【動作モード】

基本設定モード

【説明】

キューに保存された TRAP メッセージの再送を試みる時間（単位：秒）を設定します。

【実行例】

キューに保存された TRAP メッセージの再送を試みる時間を設定します（タイムアウト値：1000）。

```
#configure terminal
(config)#snmp-server trap-timeout 1000
```

【未設定時】

タイムアウト値は1秒で動作します。

30.1.11 no snmp trap link-status

【機能】

リンクアップ／リンクダウンの TRAP 送信を抑制するインタフェースの設定

【入力形式】

no snmp trap link-status <インタフェース名>

snmp trap link-status <インタフェース名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース名	インタフェース名を指定します。	-	省略不可

【動作モード】

基本設定モード

【説明】

リンクアップ／リンクダウンの TRAP 送信を抑制するインタフェースを設定します。

【実行例】

リンクアップ／リンクダウンの TRAP 送信を抑制します（インタフェース名：gigaethernet）。

```
#configure terminal
(config)#no snmp trap link-status gigaethernet
```

【未設定時】

各インタフェース設定モードに設定がある場合は、その設定に従います。設定がない場合は、リンクアップ／リンクダウンの TRAP 送信を行います。

30.1.12 no snmp trap link-status

【機能】

リンクアップ／リンクダウンの TRAP 送信の抑制

【入力形式】

no snmp trap link-status

snmp trap link-status

【動作モード】

各インタフェース設定モード

【説明】

リンクアップ／リンクダウンの TRAP 送信を抑制する場合に設定します。

【実行例】

リンクアップ／リンクダウンの TRAP 送信を抑制します。

```
【gigaethernet インタフェース設定モードの場合】
#configure terminal
(config)#interface gigaethernet 1/1
(config-if-ge 1/1)#no snmp trap link-status
```

【未設定時】

基本設定モードに設定がある場合は、その設定に従います。設定がない場合は、リンクアップ／リンクダウンの TRAP 送信を行います。

30.2 SNMPv3 の設定

30.2.1 snmp-server engine-id

【機能】

SNMPv3 の EngineID の設定

【入力形式】

snmp-server engine-id <EngineID>

no snmp-server engine-id [<EngineID>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
EngineID	EngineID を指定します。	24 文字以内の WORD 型	省略不可

【動作モード】

基本設定モード

【説明】

SNMPv3 の EngineID を設定します。

【実行例】

SNMPv3 の EngineID を設定します (EngineID : engine-id-A)。

```
#configure terminal
(config)#snmp-server engine-id engine-id-A
```

【未設定時】

management ポートの MAC アドレスで動作します。

30.2.2 snmp-server group

【機能】

SNMPv3 の VACM のグループ設定、アクセス可能な view の設定

【入力形式】

snmp-server group <グループ名> v3 {noauth | auth | priv} read {none | <view 名>} write {none | <view 名>} [access <アクセスリスト番号>]

no snmp-server group <グループ名> [v3 {noauth | auth | priv} read {none | <view 名>} write {none | view 名} [access <アクセスリスト番号>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
グループ名	グループ名を指定します。	31文字以内のWORD型 先頭に "#" は使用不可	省略不可
noauth auth priv	グループのセキュリティレベルを指定します。	noauth: 認証、および暗号化なし auth: 認証あり、暗号化なし priv: 認証、および暗号化あり	
read {none <view 名>}	読み込み可能な view 名を指定します。	31文字以内のWORD型 先頭に "#" は使用不可	
write {none view 名}	書き込み可能な view 名を指定します。	31文字以内のWORD型 先頭に "#" は使用不可	
アクセスリスト番号	アクセスリスト番号を指定します。	-	

【動作モード】

基本設定モード

【説明】

SNMPv3 の VACM のグループ設定、およびアクセス可能な view を設定します。

【実行例】

SNMPv3 の VACM のグループ設定、およびアクセス可能な view を設定します（グループ名：group-A、セキュリティレベル：noauth、view 名：view-A）。

```
#configure terminal
(config)#snmp-server group group-A v3 noauth read view-A write view-A
```

【未設定時】

SNMPv3 で MIB の Get/Set ができません。

30.2.3 snmp-server host

【機能】

トラップを送信する際の SNMP マネージャの各種パラメタの設定

【入力形式】

```
snmp-server host <SNMP マネージャ> <ユーザ名> v3 {noauth | auth | priv} [トラップ種別]
```

```
no snmp-server host <SNMP マネージャ> [<ユーザ名> v3 [{noauth | auth | priv} [トラップ種別]]]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
SNMP マネージャ	SNMP マネージャを指定します。	IPv4 アドレス形式 ホスト名： 254 文字以内の WORD 型	省略不可
ユーザ名	ユーザ名を指定します。	32 文字以内の WORD 型 先頭に "#" は使用不可	
noauth auth priv	セキュリティレベルを指定します。	noauth: 認証、および暗号化なし auth: 認証あり、暗号化なし priv: 認証、および暗号化あり	省略不可
トラップ種別	SNMP マネージャに送信するトラップの種別を指定します。 複数指定が可能です。	snmp event syslog entity bgp auth ospf ipsec vrrp ipsec-session event-action	すべてのトラップ種別

【動作モード】

基本設定モード

【説明】

トラップを送信する際の SNMP マネージャの各種パラメタを設定します。

複数登録した場合には、show current.cfg(show running.cfg) コマンドで表示される上位 20 個までが有効となります。21 個以上は設定上、無効となります。

【実行例】

トラップを送信する際の SNMP マネージャの各種パラメタを設定します (SNMP マネージャ: 192.0.2.1、ユーザ名: public、セキュリティレベル: noauth、トラップ種別: config)。

```
#configure terminal
(config)#snmp-server host 192.0.2.1 public v3 noauth config
```

【未設定時】

SNMP のトラップを送信しません。

30.2.4 snmp-server user

【機能】

SNMPv3 の USM のユーザ認証設定、グループの設定

【入力形式】

```
snmp-server user <ユーザ名> <グループ名> v3 [auth {md5 | sha} <認証パスワード> [priv des <暗号化パスワード>]] [access <アクセスリスト番号>]
```

```
no snmp-server user <ユーザ名> [<グループ名> v3 [auth {md5 | sha} <認証パスワード> [priv des <暗号化パスワード>]] [access <アクセスリスト番号>]
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ユーザ名	ユーザ名を指定します。	32 文字以内の WORD 型 先頭に "#" は使用不可	省略不可
グループ名	グループ名を指定します。	31 文字以内の WORD 型 先頭に "#" は使用不可	
md5 sha	認証アルゴリズムを指定します。	md5:MD5 sha:SHA-1	
認証パスワード	認証パスワードを指定します。	63 文字以内の WORD 型	
暗号化パスワード	暗号化パスワードを指定します。	63 文字以内の WORD 型	
アクセスリスト番号	アクセスリスト番号を指定します。	-	アクセスリストを指定しない

【動作モード】

基本設定モード

【説明】

SNMPv3 の USM のユーザ認証設定、およびグループを設定します。

【実行例】

SNMPv3 の USM のユーザ認証設定、およびグループを設定します（ユーザ名：user-A、グループ名：group-A）。

```
#configure terminal
(config)#snmp-server user user-A group group-A v3
```

【未設定時】

SNMPv3 を使用できません。

30.2.5 snmp-server view

【機能】

SNMPv3 の VACM でアクセス対象とする view 名、MIB の設定

【入力形式】

snmp-server view <view 名> <OID> {included | excluded}

no snmp-server view <view 名> [<OID> {included | excluded}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
view 名	view 名を指定します。	31 文字以内の WORD 型 先頭に "#" は使用不可	省略不可
OID	view に指定する OID を指定します。	OID 形式 (最大 128 文字)	
included excluded	対象とする MIB の view 範囲を指定します。	include: 設定 OID を有効 excluded: 設定 OID を無効	

【動作モード】

基本設定モード

【説明】

SNMPv3 の VACM でアクセス対象とする view 名、および MIB を設定します。

【実行例】

SNMPv3 でアクセス対象とする view 名、および MIB を設定します (view 名: view-A、OID: すべての MIB, included)。

```
#configure terminal
(config)#snmp-server view view-A .1 included
```

【未設定時】

SNMPv3 で各 MIB へアクセスできません。

第31章 SYSLOGの設定



この章では、SYSLOGの設定に関するコマンドについて説明します。

31.1 SYSLOG の設定

31.1.1 syslog filter

【機能】

syslog filter 設定モードへの移行

【入力形式】

syslog filter <ログフィルタ名>

no syslog filter <ログフィルタ名>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ログフィルタ名	ログフィルタ名を指定します。	32文字以内のWORD 型	省略不可

【動作モード】

基本設定モード

【説明】

syslog filter 設定モードに移行します。コマンドの先頭に "no" を指定することで、該当 syslog filter 設定モードの内容がすべて消去されます。

モード内の以下の設定コマンドは AND 条件で評価され、すべてにマッチしたログがフィルタ対象となります。

- process
- message
- level
- facility

level コマンド、および facility コマンドについては、OR 条件（どれかにマッチ）の複数エントリが設定可能です。

【実行例】

syslog filter 設定モードに移行します（ログフィルタ名：filter-A）。

```
#configure terminal
(config)#syslog filter filter-A
(config-syslog-filter)#
```

31.1.2 no logging buffer

【機能】

内部バッファへログ情報を出力しない設定

【入力形式】

no logging buffer

logging buffer

【動作モード】

基本設定モード

【説明】

内部バッファへのログ情報出力を行わない場合に設定します。

【実行例】

内部バッファへのログ情報出力を行いません。

```
#configure terminal
(config)#no logging buffer
```

【未設定時】

内部バッファへのログ情報出力を行います。

31.1.3 logging buffer facility

【機能】

ファシリティ名称の設定

【入力形式】

logging buffer facility {[no] <ファシリティ名称> | all}

no logging buffer facility [[no] <ファシリティ名称>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ファシリティ名称 all	フィルタするファシリティ名称を指定します。	ファシリティ名称または all	省略不可

ファシリティ名称	ファシリティ値	ファシリティ名称	ファシリティ値
user	1	ftp	11
mail	2	local0	16
daemon	3	local1	17
auth	4	local2	18
syslog	5	local3	19

ファシリティ名称	ファシリティ値	ファシリティ名称	ファシリティ値
lpr	6	local4	20
news	7	local5	21
uucp	8	local6	22
cron	9	local7	23
authpriv	10	all	すべてのファシリティのログ情報を出力

【動作モード】

基本設定モード

【説明】

内部バッファに出力するログ情報をフィルタする際に、ファシリティ名称を設定します。設定されたファシリティ名称のログ情報のみ出力します。ファシリティ名称の前に "no" を指定した場合には、そのファシリティのログ情報を出力しません。logging facility コマンドの設定よりも優先されます。

【実行例】

ファシリティ名称を設定します (all)。

```
#configure terminal
(config)#logging buffer facility all
```

【未設定時】

logging facility コマンドの設定に従います。

31.1.4 logging buffer level

【機能】

レベル名称の設定

【入力形式】

logging buffer level {<レベル名称> | <レベル番号>}

no logging buffer level

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
レベル名称 レベル番号	フィルタするレベル名称、または、レベル番号を指定します。	レベル名称、または、0～7	省略不可

SYSLOG のレベルとは、ログメッセージの緊急度を表します。RFC3164 では、以下のように規定されています。

レベル名称	レベル番号
emergencies	0
alert	1
critical	2
errors	3
warnings	4
notifications	5
informational	6
debugging	7

【動作モード】

基本設定モード

【説明】

内部バッファに出力するログ情報をフィルタする際に、レベル名称またはレベル番号を設定します。設定したレベル名称以上（番号の場合はより小さい）のログ情報のみ、出力します。logging level コマンドの設定よりも優先されます。

【実行例】

レベル名称を設定します（レベル名称：errors）。

```
#configure terminal
(config)#logging buffer level errors
```

【未設定時】

logging level コマンドの設定に従います。

31.1.5 logging buffer timestamps msec

【機能】

内部バッファに出力するログ情報のタイムスタンプの設定

【入力形式】

logging buffer timestamps msec

no logging buffer timestamps [msec]

【動作モード】

基本設定モード

【説明】

内部バッファに出力するログ情報のタイムスタンプを、ミリ秒単位で出力する場合に設定します。

【実行例】

ミリ秒単位で出力します。

```
#configure terminal
(config)#logging buffer timestamps msec
```

【未設定時】

秒単位で出力します。

31.1.6 no logging console

【機能】

コンソールへログ情報を出力しない設定

【入力形式】

no logging console

logging console

【動作モード】

基本設定モード

【説明】

コンソールへのログ情報出力を行わない場合に設定します。

【実行例】

コンソールへのログ情報出力を行いません。

```
#configure terminal
(config)#no logging console
```

【未設定時】

コンソールへのログ情報出力を行います。

31.1.7 logging console facility

【機能】

ファシリティ名称の設定

【入力形式】

logging console facility {[no] <ファシリティ名称> | all}

no logging console facility [[no] <ファシリティ名称>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ファシリティ名称 all	フィルタするファシリティ名称を指定します。	ファシリティ名称または all	省略不可

ファシリティ名称	ファシリティ値	ファシリティ名称	ファシリティ値
user	1	ftp	11
mail	2	local0	16
daemon	3	local1	17
auth	4	local2	18
syslog	5	local3	19
lpr	6	local4	20
news	7	local5	21
uucp	8	local6	22
cron	9	local7	23
authpriv	10	all	すべてのファシリティのログ情報を出力

【動作モード】

基本設定モード

【説明】

コンソールに出力するログ情報をフィルタする際に、ファシリティ名称を設定します。設定されたファシリティ名称のログ情報のみ出力します。ファシリティ名称の前に "no" を指定した場合には、そのファシリティのログ情報を出力しません。logging facility コマンドの設定よりも優先されます。

【実行例】

ファシリティ名称を設定します (all)。

```
#configure terminal
(config)#logging console facility all
```

【未設定時】

logging facility コマンドの設定に従います。

31.1.8 logging console level

【機能】

レベル名称の設定

【入力形式】

logging console level {<レベル名称> | <レベル番号>}

no logging console level

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
レベル名称 レベル番号	フィルタするレベル名称またはレベル番号を指定します。	レベル名称または0～7	省略不可

SYSLOGのレベルとは、ログメッセージの緊急度を表します。RFC3164 では、以下のように規定されています。

レベル名称	レベル番号
emergencies	0
alert	1
critical	2
errors	3
warnings	4
notifications	5
informational	6
debugging	7

【動作モード】

基本設定モード

【説明】

コンソールに出力するログ情報をフィルタする際に、レベル名称またはレベル番号を設定します。設定したレベル名称以上（番号の場合はより小さい）のログ情報のみ、出力します。logging level コマンドの設定よりも優先されます。

【実行例】

レベル名称を設定します（レベル名称：errors）。

```
#configure terminal
(config)#logging console level errors
```

【未設定時】

logging level コマンドの設定に従います。

31.1.9 logging console timestamps msec

【機能】

内部バッファに出力するログ情報のタイムスタンプの設定

【入力形式】

logging console timestamps msec

no logging console timestamps [msec]

【動作モード】

基本設定モード

【説明】

コンソールに出力するログ情報のタイムスタンプを、ミリ秒単位で出力する場合に設定します。

【実行例】

ミリ秒単位で出力します。

```
#configure terminal
(config)#logging console timestamps msec
```

【未設定時】

秒単位で出力します。

31.1.10 logging facility

【機能】

ファシリティ名称の設定

【入力形式】

logging facility {[no] <ファシリティ名称> | all}

no logging facility [[no] <ファシリティ名称>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ファシリティ名称 all	フィルタするファシリティ名称を指定します。	ファシリティ名称または all	省略不可

ファシリティ名称	ファシリティ値	ファシリティ名称	ファシリティ値
user	1	ftp	11
mail	2	local0	16
daemon	3	local1	17
auth	4	local2	18
syslog	5	local3	19
lpr	6	local4	20
news	7	local5	21
uucp	8	local6	22
cron	9	local7	23
authpriv	10	all	すべてのファシリティのログ情報を出力

【動作モード】

基本設定モード

【説明】

ログ情報をフィルタする際に、ファシリティ名称を設定します。設定されたファシリティ名称のログ情報のみ出力します。ファシリティ名称の前に "no" を指定した場合には、そのファシリティのログ情報を出力しません。

【実行例】

ファシリティ名称を設定します（ファシリティ名称：all）。

```
#configure terminal
(config)#logging facility all
```

【未設定時】

すべてのログ情報を出力します。

31.1.11 logging filter

【機能】

フィルタにマッチした動作の設定

【入力形式】

logging filter <シーケンス順番> <ログフィルタ名> {send-traps | change-level {<レベル名称> | <レベル番号>} | change-facility <ファシリティ名称> | event-action}

no logging filter <シーケンス順番> [<ログフィルタ名> [{send-traps | change-level {<レベル名称> | <レベル番号>} | change-facility <ファシリティ名称> | event-action}]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
シーケンス番号	シーケンス番号（フィルタの処理順）を指定します。	1～10	省略不可
ログフィルタ名	ログフィルタ名を指定します。	32文字以内のWORD型	
send-traps	フィルタにマッチしたログをTRAPとして送信する場合に指定します。	-	
レベル名称 レベル番号	レベル名称またはレベル番号を指定します。	レベル名称： emergencies alert critical errors warnings notifications informational debugging レベル番号： 0～7	

パラメタ	設定内容	設定範囲	省略時
ファシリティ名称	ファシリティ名称を指定します。	ファシリティ名称： user mail daemon auth syslog lpr news uucp cron authpriv ftp local0 local1 local2 local3 local4 local5 local6 local7	
event-action	フィルタにマッチしたログを emd に対して通知する場合に指定します。	-	省略不可

【動作モード】

基本設定モード

【説明】

フィルタにマッチした際の動作を設定します。

シーケンス番号で指定した順に処理されるため、レベル、ファシリティを変更している場合は最後の変更が有効となります。

"send-traps" を指定することで、フィルタにマッチしたログを TRAP として送信できます。

"change-level"、"change-facility" を指定することで、フィルタにマッチしたログのログレベル、ファシリティを変更できます。

【実行例】

フィルタにマッチした際の動作を設定します（シーケンス番号：3、ログフィルタ名：filter-A, send-traps）。

```
#configure terminal
(config)#logging filter 3 filter-A send-traps
```

【未設定時】

ログの操作を行いません。

31.1.12 logging fixed-facility

【機能】

ファシリティ名称またはファシリティ値の固定化

【入力形式】

logging fixed-facility [<ファシリティ名称> | <ファシリティ値>]

no logging fixed-facility [<ファシリティ名称> | <ファシリティ値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ファシリティ名称 ファシリティ値	装置が出力するログ情報のファシリティ名称またはファシリティ値を指定します。	ファシリティ名称または 0 ~ 127	省略不可

ファシリティ名称	ファシリティ値	ファシリティ名称	ファシリティ値
user	1	ftp	11
mail	2	local0	16
daemon	3	local1	17
auth	4	local2	18
syslog	5	local3	19
lpr	6	local4	20
news	7	local5	21
uucp	8	local6	22
cron	9	local7	23
authpriv	10	all	すべてのファシリティのログ情報を出力

【動作モード】

基本設定モード

【説明】

外部SYSLOGサーバへ送出するログ情報について、そのファシリティ名称またはファシリティ値を固定化します。

【実行例】

ファシリティ名称を固定化します（ファシリティ名称：local0）。

```
#configure terminal
(config)#logging fixed-facility local0
```

【未設定時】

ファシリティは各ログ情報のデフォルトで動作します。

31.1.13 logging host

【機能】

外部ログサーバへのログ情報出力の制御

【入力形式】

logging host <外部ログサーバ> [facility {all | <ファシリティ名称>} | level {<レベル名称> | <レベル番号>}] [linklocal-interface <インタフェース名> <インタフェース番号>]

no logging host <外部ログサーバ>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
外部ログサーバ	外部ログサーバを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 ホスト名： 254 文字以内の WORD 型	省略不可
ファシリティ名称 all	フィルタするファシリティ名称を指定します。	ファシリティ名称または all	
レベル名称 レベル番号	フィルタするレベル名称またはレベル番号を指定します。	レベル名称または 0～7	
インタフェース名	インタフェース名を指定します。	-	
インタフェース番号	インタフェース番号を指定します。	-	

【動作モード】

基本設定モード

【説明】

外部ログサーバへのログ情報出力を制御します。外部ログサーバに IPv6 リンクローカルアドレスを指定した場合は、送信インタフェースの設定が必要です。複数登録した場合には、show current.cfg(show running.cfg) コマンドで表示される上位 20 個までが有効となります。21 個以上は設定上、無効となります。

【実行例】

外部ログサーバへのログ情報出力を制御します（外部ログサーバ：192.0.2.1）。

```
#configure terminal
(config)#logging host 192.0.2.1
```

【未設定時】

外部ログサーバへのログ出力を行いません。

31.1.14 logging host-queue length

【機能】

最大メッセージ数の設定

【入力形式】

logging host-queue length <最大メッセージ数>

no logging host-queue length

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
最大メッセージ数	再送キューに保存するログメッセージの最大メッセージ数を指定します。	1～3000	省略不可

【動作モード】

基本設定モード

【説明】

再送キューに保存するログメッセージの最大メッセージ数を設定します。

【実行例】

最大メッセージ数を設定します（最大メッセージ数：3000）。

```
#configure terminal
(config)#logging host-queue length 3000
```

【未設定時】

最大メッセージ数は 1500 で動作します。

31.1.15 logging host-queue level

【機能】

再送キューに保存するログメッセージのレベル名称またはレベル番号の設定

【入力形式】

logging host-queue level {<レベル名称> | <レベル番号>}

no logging host-queue level

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
レベル名称 レベル番号	再送キューに保存するログメッセージのレベル名称またはレベル番号を指定します。	レベル名称または 0～7	省略不可

SYSLOG のレベルとは、ログメッセージの緊急度を表します。RFC3164 では、以下のように規定されています。

レベル名称	レベル番号
emergencies	0
alert	1
critical	2
errors	3
warnings	4
notifications	5
informational	6
debugging	7

【動作モード】

基本設定モード

【説明】

再送キューに保存するログメッセージのレベル名称またはレベル番号を設定します。設定されたレベル名称（番号の場合はより小さい）のログメッセージのみ、再送キューに保存します。

【実行例】

レベル番号を設定します（レベル番号：4）。

```
#configure terminal
(config)#logging host-queue level 4
```

【未設定時】

logging host コマンドの設定に従います。

31.1.16 logging host-queue timeout

【機能】

再送キューに保存するログメッセージの最大保存時間の設定

【入力形式】

logging host-queue timeout <最大保存時間>

no logging host-queue timeout

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
最大保存時間	再送キューに保存するログメッセージの最大保存時間（単位：秒）を指定します。	1～1000	省略不可

【動作モード】

基本設定モード

【説明】

再送キューに保存するログメッセージの最大保存時間（単位：秒）を設定します。

【実行例】

最大保存時間（単位：秒）を設定します（最大保存時間：1000 秒）。

```
#configure terminal
(config)#logging host-queue timeout 1000
```

【未設定時】

最大保存時間は 600 秒で動作します。

31.1.17 logging host-queue retry-interval

【機能】

再送キューに保存されたログメッセージの再送間隔の設定

【入力形式】

logging host-queue retry-interval <再送間隔>

no logging host-queue retry-interval

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
再送間隔	再送キューに保存されたログメッセージの再送間隔（単位：秒）を指定します。	1～1000	省略不可

【動作モード】

基本設定モード

【説明】

再送キューに保存されたログメッセージの再送間隔（単位：秒）を設定します。

【実行例】

再送間隔（単位：秒）を設定します（再送間隔：1000 秒）。

```
#configure terminal
(config)#logging host-queue retry-interval 1000
```

【未設定時】

再送間隔は 1 秒で動作します。

31.1.18 logging host facility

【機能】

ファシリティ名称の設定

【入力形式】

logging host <外部ログサーバ> facility {[no] <ファシリティ名称> | all} [linklocal-interface <インタフェース名> <インタフェース番号>]

no logging host <外部ログサーバ> [facility [[no] <ファシリティ名称>]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
外部ログサーバ	外部ログサーバを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 ホスト名： 254 文字以内の WORD 型	省略不可
ファシリティ名称 all	フィルタするファシリティ名称を指定します。	ファシリティ名称または all	
インタフェース名	出力インタフェース名を指定します。	-	実際に送信するインタフェース
インタフェース番号	出力インタフェース番号を指定します。	-	

ファシリティ名称	ファシリティ値	ファシリティ名称	ファシリティ値
user	1	ftp	11
mail	2	local0	16
daemon	3	local1	17
auth	4	local2	18
syslog	5	local3	19
lpr	6	local4	20
news	7	local5	21
uucp	8	local6	22
cron	9	local7	23
authpriv	10	all	すべてのファシリティのログ情報を出力

【動作モード】

基本設定モード

【説明】

外部ログサーバに出力するログ情報をフィルタする際のファシリティ名称を設定します。設定されたファシリティ名称のログ情報のみ出力します。ファシリティ名称の前に "no" を指定した場合には、そのファシリティのログ情報を出力しません。logging facility コマンドの設定よりも優先されます。

【実行例】

ファシリティ名称を設定します（外部ログサーバ：192.0.2.1、ファシリティ名称：all）。

```
#configure terminal
(config)#logging host 192.0.2.1 facility all
```

【未設定時】

logging facility コマンドの設定に従います。

31.1.19 logging host level

【機能】

外部ログサーバに出力するログ情報をフィルタする際のレベル名称またはレベル番号の設定

【入力形式】

logging host <外部ログサーバ> level {<レベル名称> | <レベル番号>} [linklocal-interface <インタフェース名> <インタフェース番号>]

no logging host <外部ログサーバ> level

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
外部ログサーバ	外部ログサーバを指定します。	IPv4 アドレス形式 IPv6 アドレス形式 ホスト名： 254 文字以内の WORD 型	省略不可
レベル名称 レベル番号	フィルタするレベル名称またはレベル番号を指定します。	レベル名称または 0～7	
インタフェース名	出力インタフェース名を指定します。	-	実際に送信するインタフェース
インタフェース番号	出力インタフェース番号を指定します。	-	

SYSLOG のレベルとは、ログメッセージの緊急度を表します。RFC3164 では、以下のように規定されています。

レベル名称	レベル番号
emergencies	0
alert	1
critical	2
errors	3
warnings	4
notifications	5
informational	6
debugging	7

【動作モード】

基本設定モード

【説明】

外部ログサーバに出力するログ情報をフィルタする際のレベル名称またはレベル番号を設定します。設定したレベル名称以上（番号の場合はより小さい）のログ情報のみ、出力します。logging level コマンドの設定よりも優先されます。

【実行例】

レベル名称を設定します（外部ログサーバ：192.0.2.1、レベル名称：errors）。

```
#configure terminal
(config)#logging host 192.0.2.1 level errors
```

【未設定時】

logging level コマンドの設定に従います。

31.1.20 logging level

【機能】

ログ情報をフィルタする際のレベル名称またはレベル番号の設定

【入力形式】

logging level {<レベル名称> | <レベル番号>}

no logging level

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
レベル名称 レベル番号	フィルタするレベル名称またはレベル番号を指定します。	レベル名称または0～7	省略不可

SYSLOGのレベルとは、ログメッセージの緊急度を表します。RFC3164では、以下のように規定されています。

レベル名称	レベル番号
emergencies	0
alert	1
critical	2
errors	3
warnings	4
notifications	5
informational	6
debugging	7

【動作モード】

基本設定モード

【説明】

ログ情報をフィルタする際のレベル名称またはレベル番号を設定します。設定されたレベル名称以上（番号の場合はより小さい）のログ情報のみ、出力します。

【実行例】

レベル番号を設定します（レベル番号：4）。

```
#configure terminal
(config)#logging level 4
```

【未設定時】

レベル名称は errors（レベル番号：3）で動作します。

31.1.21 logging source-interface

【機能】

ログ情報を送信する送信元アドレスとして使用するインタフェースの設定

【入力形式】

logging source-interface <インタフェース名> <インタフェース番号>

no logging source-interface

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース名	送信元アドレスとして使用するインタフェース名を指定します。	-	省略不可
インタフェース番号	送信元アドレスとして使用するインタフェース番号を指定します。	-	

【動作モード】

基本設定モード

【説明】

ログ情報を送信する際に、その送信元アドレスとして使用するインタフェースを設定します。

【実行例】

送信元アドレスとして使用するインタフェースを設定します（インタフェース名：loopback、インタフェース番号：1）。

```
#configure terminal
(config)#logging source-interface loopback 1
```

【未設定時】

送信元アドレスは送信インタフェースのアドレスで動作します。

31.1.22 logging suppress-repeated

【機能】

同一ログの繰り返し出力を抑制する設定

【入力形式】

logging suppress-repeated

no logging suppress-repeated

【動作モード】

基本設定モード

【説明】

同一のログが連続して出力される際、同一ログの繰り返し出力を抑制する場合に設定します。同一のログが 11 回以上連続した場合には、「syslogd: last message repeated [出力回数] times [繰り返したログ]」と出力されます（10 回以下は連続出力されます）。

【実行例】

同一ログの繰り返し出力を抑制します。

```
#configure terminal
(config)#logging suppress-repeated
```

【未設定時】

同一ログの繰り返し出力を抑制しません。

31.1.23 logging telnet

【機能】

TELNET へのログ情報出力の制御

【入力形式】

logging telnet


no logging telnet

【動作モード】

基本設定モード

【説明】

TELNET へのログ情報出力を制御します。TELNET 端末からは logging コマンドで出力を制御できます。

 参照 logging コマンドについては、マニュアル「コマンドリファレンス - 運用管理編 -」を参照してください。

【実行例】

TELNET へのログ情報出力を制御します。

```
#configure terminal
(config)#logging telnet
```

【未設定時】

TELNET へのログ情報出力を行いません。

31.1.24 logging telnet facility

【機能】

ファシリティ名称の設定

【入力形式】

logging telnet facility {[no] <ファシリティ名称> | all}

no logging telnet facility [[no] <ファシリティ名称>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ファシリティ名称 all	フィルタするファシリティ名称を指定します。	ファシリティ名称または all	省略不可

ファシリティ名称	ファシリティ値	ファシリティ名称	ファシリティ値
user	1	ftp	11
mail	2	local0	16
daemon	3	local1	17
auth	4	local2	18
syslog	5	local3	19
lpr	6	local4	20
news	7	local5	21
uucp	8	local6	22
cron	9	local7	23
authpriv	10	all	すべてのファシリティのログ情報を出力

【動作モード】

基本設定モード

【説明】

TELNET に出力するログ情報をファシリティでフィルタする場合に設定します。設定されたファシリティ名称のログ情報のみ出力します。ファシリティ名称の前に "no" を指定した場合には、そのファシリティのログ情報を出力しません。logging facility コマンドの設定よりも優先されます。

【実行例】

ファシリティ名称を設定します (all)。

```
#configure terminal
(config)#logging telnet facility all
```

【未設定時】

logging facility コマンドの設定に従います。

31.1.25 logging telnet level

【機能】

レベル名称の設定

【入力形式】

logging telnet level {<レベル名称> | <レベル番号>}

no logging telnet level

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
レベル名称 レベル番号	フィルタするレベル名称またはレベル番号を指定します。	レベル名称または 0～7	省略不可

SYSLOG のレベルとは、ログメッセージの緊急度を表します。RFC3164 では、以下のように規定されています。

レベル名称	レベル番号
emergencies	0
alert	1
critical	2
errors	3
warnings	4
notifications	5
informational	6
debugging	7

【動作モード】

基本設定モード

【説明】

TELNET に出力するログ情報をログレベル（プライオリティ）でフィルタする場合に設定します。設定したレベル名称以上（番号の場合はより小さい）のログ情報のみ、出力します。logging level コマンドの設定よりも優先されます。

【実行例】

レベル名称を設定します（レベル名称：errors）。

```
#configure terminal
(config)#logging telnet level errors
```

【未設定時】

logging level コマンドの設定に従います。

31.1.26 logging telnet timestamps msec

【機能】

TELNET に出力するログ情報のタイムスタンプの設定

【入力形式】

logging telnet timestamps msec

no logging telnet timestamps [msec]

【動作モード】

基本設定モード

【説明】

TELNET に出力するログ情報のタイムスタンプを、ミリ秒単位で出力する場合に設定します。

【実行例】

ミリ秒単位で出力します。

```
#configure terminal
(config)#logging telnet timestamps msec
```

【未設定時】

秒単位で出力します。

31.1.27 facility

【機能】

ログのファシリティ名称の設定

【入力形式】

facility <ファシリティ名称>

no facility [<ファシリティ名称>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ファシリティ名称	ファシリティ名称を指定します。	ファシリティ名称： user mail daemon auth syslog lpr news uucp cron authpriv ftp local0 local1 local2 local3 local4 local5 local6 local7	省略不可

【動作モード】

syslog filter 設定モード

【説明】

フィルタのマッチ条件とする、ログのファシリティ名称を設定します。
複数のファシリティが設定された場合は OR 条件として動作します。

【実行例】

ログのファシリティ名称を設定します（ファシリティ名称：user）。

```
#configure terminal
(config)#syslog filter filter-A
(config-syslog-filter)#facility user
```

【未設定時】

すべてのファシリティ名をマッチ条件とします。

31.1.28 level

【機能】

ログのレベル名称の設定

【入力形式】

level [<レベル名称> | <レベル番号>]

no level [<レベル名称> | <レベル番号>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
レベル名称 レベル番号	レベル名称またはレベル番号を指定します。	レベル名称： emergencies alert critical errors warnings notifications informational debugging レベル番号： 0～7	省略不可

【動作モード】

syslog filter 設定モード

【説明】

フィルタのマッチ条件とする、ログのレベル名称またはレベル番号を設定します。
複数のレベルが設定された場合は OR 条件として動作します。

【実行例】

ログのレベル名称を設定します（レベル名称：critical）。

```
#configure terminal
(config)#syslog filter filter-A
(config-syslog-filter)#level critical
```

【未設定時】

debugging(7)以外のレベルをマッチ条件とします。

31.1.29 message

【機能】

ホスト名以降のログメッセージに含まれるメッセージ文字列の設定

【入力形式】

message <メッセージ文字列>

no message [<メッセージ文字列>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
メッセージ文字列	メッセージ文字列を指定します。	254文字以内のSTRING型	省略不可

【動作モード】

syslog filter 設定モード

【説明】

フィルタのマッチ条件とする、ホスト名以降のログメッセージに含まれるメッセージ文字列を設定します。

メッセージ文字列は正規表現での指定も可能です。指定した正規表現に誤りがあった場合、該当の syslog filter 設定モードは無効となります。

指定したメッセージ文字列が 254 文字を超えた場合も、該当の syslog filter 設定モードが無効となります。

【実行例】

ホスト名以降のログメッセージに含まれるメッセージ文字列を設定します（メッセージ文字列：[Cc]onfiguration）。

```
#configure terminal
(config)#syslog filter filter-A
(config-syslog-filter)#message [Cc]onfiguration
```

【未設定時】

すべてのメッセージ文字列をマッチ条件とします。

31.1.30 dvpn client-log

【機能】

動的VPNクライアント機能のsyslog出力

【入力形式】

dvpn client-log

no dvpn client-log

【動作モード】

基本設定モード

【説明】

動的VPNクライアント機能の情報をsyslogに出力する場合に設定します。

【実行例】

動的VPNクライアント機能の情報をsyslogに出力します。

```
#configure terminal
(config)# dvpn client-log
```

【未設定時】

動的VPNクライアント機能の情報をsyslogに出力しません。

31.1.31 dvpn server-log

【機能】

動的VPNサーバ機能のsyslog出力

【入力形式】

dvpn server-log

no dvpn server-log

【動作モード】

基本設定モード

【説明】

動的VPN サーバ機能の情報を syslog に出力する場合に設定します。

【実行例】

動的VPN サーバ機能の情報を syslog に出力します。

```
#configure terminal
(config)# dvpn server-log
```

【未設定時】

動的VPN サーバ機能でのログを出力しません。

31.1.32 ip acl logging enable

【機能】

アクセスリストによる syslog 出力

【入力形式】

ip acl logging enable

no ip acl logging enable

【動作モード】

基本設定モード

【説明】

アクセスリストによるログの出力を有効にする場合に設定を行います。

【実行例】

アクセスリストによるログを syslog に出力します。

```
#configure terminal
(config)# ip acl logging enable
```

【未設定時】

アクセスリストによるログを出力しません。

31.1.33 ip nat table logging enable

【機能】

NAT によるパケット破棄の syslog 出力

【入力形式】

ip nat logging enable

no ip nat logging enable

【動作モード】

基本設定モード

【説明】

NAT によるパケット破棄のログの出力を有効にする場合に設定を行います。

【実行例】

NAT によるパケット破棄のログを syslog に出力します。

```
#configure terminal
(config)# ip nat logging enable
```

【未設定時】

NAT によるパケット破棄のログを出力しません。

31.1.34 ip nat table logging enable

【機能】

NAT 変換テーブルの作成による syslog 出力

【入力形式】

ip nat table logging enable

no ip nat table logging enable

【動作モード】

基本設定モード

【説明】

NAT 変換テーブルの作成によるログの出力を有効にする場合に設定を行います。

【実行例】

NAT 変換テーブルの作成によるログを syslog に出力します。

```
#configure terminal
(config)# ip nat table logging enable
```

【未設定時】

NAT 変換テーブルの作成によるログを出力しません。

31.1.35 ip vrrp mode logging-enable-all

【機能】

interface-delegation モードにおける vrrp の状態遷移による syslog 出力

【入力形式】

ip vrrp mode logging-enable-all

no ip vrrp mode logging-enable-all

【動作モード】

基本設定モード

【説明】

interface-delegation モードにおいて、非代表インタフェースを含めたすべてのインタフェースで vrrp の状態遷移 syslog を出力する場合に設定します。

【実行例】

```
#configure terminal
(config)#ip vrrp mode logging-enable-all
```

【未設定時】

代表インタフェースのみ状態遷移 syslog を出力します。

31.1.36 ipv6 vrrp mode logging-enable-all

【機能】

interface-delegation モードにおける vrrp の状態遷移による syslog 出力

【入力形式】

ipv6 vrrp mode logging-enable-all

no ipv6 vrrp mode logging-enable-all

【動作モード】

基本設定モード

【説明】

interface-delegation モードにおいて、非代表インタフェースを含めたすべてのインタフェースで vrrp の状態遷移 syslog を出力する場合に設定します。

【実行例】

```
#configure terminal
(config)#ipv6 vrrp mode logging-enable-all
```

【未設定時】

代表インタフェースのみ状態遷移 syslog を出力します。

31.1.37 monitor signal-quality logging usb-ethernet

【機能】

USB Ethernet デバイスの電波状態の syslog 出力

【入力形式】

monitor signal-quality logging usb-ethernet [interval <出力間隔>]

no monitor signal-quality logging usb-ethernet [interval <出力間隔>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
interval	電波状態を syslog に出力する間隔を設定する場合に指定します。	-	出力間隔は 60 秒となる
出力間隔	電波状態を syslog に出力する間隔（単位：秒）を指定します。	10～86400	省略不可

【動作モード】

基本設定モード

【説明】

USB Ethernet デバイスの電波状態を syslog に出力する際に設定します。

【実行例】

USB Ethernet デバイスの電波状態の syslog 出力を有効にします（出力間隔：60 秒）。

```
#configure terminal
(config)#monitor signal-quality logging usb-ethernet interval 60
```

【未設定時】

USB Ethernet デバイスの電波状態を syslog に出力しません。

31.1.38 ngn sip log

【機能】

データコネクト機能処理の syslog 出力

【入力形式】

ngn sip log {session | registrar | session-fail | limit}

no ngn sip log {session | registrar | session-fail | limit}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
session	SIP セッションの接続、切断に関わる情報を syslog に出力する際に指定します。	-	省略不可
registrar	SIP レジストラに関わる情報を syslog に出力する際に指定します。	-	省略不可
session-fail	SIP セッションの接続失敗に関わる情報を syslog に出力する際に指定します。	-	省略不可
limit	SIP の課金制御に関わる情報を syslog に出力する際に指定します。	-	省略不可

【動作モード】

基本設定モード

【説明】

データコネクト機能による SIP セッション接続や切断、SIP レジストラ、SIP セッション接続失敗、SIP の課金制御に関わる情報を syslog に出力する際に指定します。

【実行例】

データコネクト機能の syslog 出力を有効にします。

```
#configure terminal
(config)#ngn sip log session
(config)#ngn sip log registrar
(config)#ngn sip log session-fail
(config)#ngn sip log limit
```

【未設定時】

SIP セッション接続や切断、SIP レジストラ、SIP セッション接続失敗、SIP の課金制御に関わる情報を syslog に出力しません。

31.1.39 process

【機能】

ログメッセージに含まれるプロセス名の設定

【入力形式】

process <プロセス名>

no process [<プロセス名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
プロセス名	プロセス名を指定します。	32 文字以内の WORD 型	省略不可

【動作モード】

syslog filter 設定モード

【説明】

フィルタのマッチ条件とする、ログメッセージに含まれるプロセス名を設定します。
大文字、小文字は区別され、プロセス名が完全一致する場合にマッチします。

【実行例】

ログメッセージに含まれるプロセス名を設定します（プロセス名：M-sh）。

```
#configure terminal
(config)#syslog filter filter-A
(config-syslog-filter)#process M-sh
```

【未設定時】

すべてのプロセス名をマッチ条件とします。

第32章 アラームの設定



この章では、アラームの設定に関するコマンドについて説明します。

32.1 アラームの設定

32.1.1 environment profile

【機能】

environment プロファイル設定モードへの移行

【入力形式】

environment profile

no environment profile

【動作モード】

基本設定モード

【説明】

environment プロファイル設定モードに移行します。コマンドの先頭に "no" を指定することで、environment プロファイル設定モードの内容がすべて消去されます。

【実行例】

environment プロファイル設定モードに移行します。

```
#configure terminal
(config)#environment profile
(config-env-profile)#
```

32.1.2 cpu utilization

【機能】

CPU 使用率に対する警報発生しきい値の設定

【入力形式】

cpu utilization <警告レベル> threshold percent <警報発生値> hysteresis <オフセット値>

no cpu utilization <警告レベル> threshold [percent <警報発生値> hysteresis <オフセット値>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
警告レベル	警告レベルを指定します。	1～3	省略不可
警報発生値	警報発生値（単位：%）を指定します。	0～100	省略不可
オフセット値	警報復帰値までのオフセット値（単位：%）を指定します。	0～100	省略不可

【動作モード】

environment プロファイル設定モード

【説明】

5 分間の平均 CPU 使用率に対する、警報発生しきい値を設定します。警報復帰値が 0 以下の場合は、警報復帰値は 0 で動作します。

【実行例】

5 分間の平均 CPU 使用率に対する、警報発生しきい値を設定します（警告レベル：1、警報発生値：100%、オフセット値：10%）。

```
#configure terminal
(config)#environment profile
(config-env-profile)#cpu utilization 1 threshold percent 100 hysteresis 10
```

【未設定時】

警報動作機能は動作しません。

32.1.3 temp-sensor expected temperature

【機能】

アラーム発出しきい値の設定

【入力形式】

temp-sensor <センサー番号> expected temperature {<しきい値> | implicit}

no temp-sensor <センサー番号> expected temperature [{<しきい値> | implicit}]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
センサー番号	温度センサー番号を指定します。	1～4	省略不可
しきい値 implicit	しきい値（単位：℃）またはデフォルトを指定します。	しきい値：0～125 implicit: デフォルト	

【動作モード】

environment プロファイル設定モード

【説明】

温度センサーに対する、温度アラームしきい値を設定します。
温度アラームしきい値設定はセンサーごとに行い、温度アラームしきい値と現在温度で判断します。

【温度しきい値について】

各センサーのデフォルト値を以下に示します。

温度センサー	発生しきい値
#1 装置内部温度	74℃
#2 吸気温度	60℃
#3 装置内部温度	69℃
#4CPU 温度	99℃

【実行例】

アラーム発出しきい値を設定します（センサー番号：1、しきい値：60℃）。

```
#configure terminal
(config)#environment profile
(config-env-profile)#temp-sensor 1 expected temperature 60
```

【未設定時】

デフォルトの温度しきい値を使用します。

32.1.4 physical memory

【機能】

メモリ使用量に対する、警報発生しきい値の設定

【入力形式】

physical memory <警告レベル> threshold {percent | size} <警報発生値> hysteresis <オフセット値> [remain]

no physical memory <警告レベル> threshold [{percent | size} <警報発生値> hysteresis <オフセット値> [remain]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
警告レベル	警告レベルを指定します。	1～3	省略不可
percent size	割合で指定するか、サイズで指定するかを指定します。	-	省略不可
警報発生値	警報発生値（単位：%またはbytes）を指定します。	%：0～100 bytes：0～4294967295	省略不可
オフセット値	警報復帰値までのオフセット値（単位：%またはbytes）を指定します。	%：0～100 bytes：0～4294967295	省略不可
remain	未使用量に対するしきい値を設定する場合に指定します。	-	使用量に対するしきい値

【動作モード】

environment プロファイル設定モード

【説明】

メモリ使用量に対する、警報発生しきい値を設定します。設定したしきい値を5分間継続して超えた場合に警報発生します。警報復帰値が0以下の場合には、警報復帰値は0で動作します。

【実行例】

警報発生しきい値を設定します（警告レベル：1、警報発生値：100%、オフセット値：10%）。

```
#configure terminal
(config)#environment profile
(config-env-profile)#physical memory 1 threshold percent 100 hysteresis 10
```

【未設定時】

警報動作機能は動作しません。

32.1.5 psu-output-error timer

【機能】

電源の出力異常を検出し電源異常と判断するまでの時間の設定

【入力形式】

psu-output-error timer [<検出時間>]

no psu-output-error timer [<検出時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
検出時間	電源出力異常を検出してから電源異常と判断するまでの時間（分）を指定する	0～60	省略不可

【動作モード】

environment プロファイル設定モード

【説明】

電源の出力異常を検出し電源異常と判断するまでの時間を設定します。

実装した電源の故障以外に電源を実装した状態で電源スイッチ OFF にしている場合も、ここで指定された時間を経過すると電源異常と判断します。

【実行例】

電源の出力異常を検出し電源異常と判断するまでの時間を設定します（検出時間：60 分）。

```
#configure terminal
(config)#environment profile
(config-env-profile)#psu-output-error timer 60
```

【未設定時】

電源出力異常を検出してから 1 分間経過で電源異常と判断します。

32.1.6 psu-temp-sensor safety control power-down

【機能】

電源冗長時に電源内部が装置危険温度のしきい値を超えた場合に電源を off にする設定

【入力形式】

psu-temp-sensor safety control power-down [redundancy]

no psu-temp-sensor safety control [power-down [redundancy]]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
power-down	電源を OFF する	-	省略不可
redundancy	電源冗長時のみ保護動作を行う場合に指定します。	-	電源冗長状態に関係なく保護動作を行う

【動作モード】

environment プロファイル設定モード

【説明】

電源内部の温度センサーが装置危険温度のしきい値を超えた場合の電源保護動作を選択します。

【実行例】

電源冗長時に電源内部が装置危険温度のしきい値を超えた場合の電源を off にします。

```
#configure terminal
(config)#environment profile
(config-env-profile)#psu-temp-sensor safety control power-down redundancy
```

【未設定時】

電源保護動作を行いません。

32.1.7 temp-sensor safety control

【機能】

装置内部が装置危険温度のしきい値を超えた場合に電源を off にする設定

【入力形式】

temp-sensor safety control [保護動作]

no temp-sensor safety control [保護動作]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
保護動作	危険温度検出時の保護動作を指定します。	fallback: 縮退モードに移行する power-down: 装置電源を OFF する	省略不可

【動作モード】

environment プロファイル設定モード

【説明】

装置内部の温度センサーが装置危険温度のしきい値を超えた場合の装置保護動作を選択します。

【実行例】

装置内部が装置危険温度のしきい値を超えた場合の電源を off にします。

```
#configure terminal
(config)#environment profile
(config-env-profile)#temp-sensor safety control power-down
```

【未設定時】

装置保護動作を行いません。

第33章 ハードウェア 故障検出の設定



この章では、ハードウェア故障検出の設定に関するコマンドについて説明します。

33.1 ハードウェア故障検出の設定

33.1.1 hardware-fault-detection action

【機能】

ハードウェア故障を検出した場合の動作の設定

【入力形式】

hardware-fault-detection action {fallback | none | reboot}

no hardware-fault-detection action

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
fallback none reboot	ハードウェア故障を検出した場合の動作を指定します。	以下の表を参照してください。	省略不可

fallback	装置を fallback 状態に遷移させます。
none	なにもしません。
reboot	自動で装置を再起動させます。

【動作モード】

基本設定モード

【説明】

ハードウェア故障を検出した場合の装置動作を設定します。

fallback に設定すると、管理ポート以外の Ethernet インタフェースを遮断し、装置管理ができる最低限の動作をするモードに切り替えます。none に設定すると、装置動作をそのまま継続します。reboot に設定すると、装置を再起動します。

弊社の技術員または弊社が認定した技術員からの指示がなければ、設定変更する必要はありません。

【実行例】

ハードウェア故障を検出した場合に、動作を継続するように設定します (none)。

```
#configure terminal
(config)#hardware-fault-detection action none
```

【未設定時】

fallback で動作します。

33.1.2 hardware-fault-detection level-up

【機能】

装置動作に影響を与えるハードウェア異常が間欠的に発生した場合に、ハードウェア故障と判定する条件の設定

【入力形式】

hardware-fault-detection level-up interval <監視間隔> iteration <連続検出回数>

no hardware-fault-detection level-up

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
監視間隔	装置動作に影響を与える異常発生 の監視間隔（単位：秒）を指定しま す。	1～10	省略不可
連続検出回数	装置動作に影響を与える異常発生 の連続発生回数を指定します。	3～60	

【動作モード】

基本設定モード

【説明】

装置動作に影響を与えるハードウェア異常の発生が間欠的な場合に、ハードウェア故障と判定するための異常発生
の監視間隔と連続発生回数を設定します。

監視間隔を狭くすると、短期間の異常発生時に故障と判定しやすく、逆に広くすると、長期間の異常発生
時に故障と判定しやすくなります。

連続発生回数を少なく設定すると、異常発生初期に故障と判定しますが、一時的な異常で復旧が見込める
ような事象でも敏感に故障と判定するようになります。

弊社の技術員または弊社が認定した技術員からの指示がなければ、設定変更する必要はありません。

【実行例】

装置動作に影響を与えるハードウェア異常の発生が間欠的な場合に、ハードウェア故障と判定する条件を
設定します（監視間隔：5 秒、連続検出回数：30）。

```
#configure terminal
(config)#hardware-fault-detection level-up interval 5 iteration 30
```

【未設定時】

以下の値で動作します。

監視間隔： 10 秒

連続検出回数： 60 回

第34章 イベントアクション 機能の設定



この章では、イベントアクション機能の設定に関するコマンドについて説明します。

34.1 イベントアクション機能の設定

34.1.1 event-action

【機能】

イベントアクション設定モードへの移行

【入力形式】

event-action <モード番号>

no event-action <モード番号>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
モード番号	イベントアクションモードの番号を指定します。	1～100	省略不可

【動作モード】

基本設定モード

【説明】

イベントアクション設定モードに移行します。"no"を指定した場合は、該当イベントアクション設定モードの内容がすべて消去されます。

モード内に設定されたイベントとアクションを関連付けます。

モードが削除された場合や、モード内に設定されたイベントとアクションが変更された場合、該当モードの情報は初期化されます。

モード内の設定に誤りがあった場合、該当のモードに設定されたイベントアクションは登録されません。

【実行例】

イベントアクション設定モードに移行します（モード番号：1）。

```
#configure terminal
(config)#event-action 1
(config-event-action)#
```

34.1.2 description

【機能】

説明書きの設定

【入力形式】

description <説明>

no description <説明>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
説明	説明を指定します。	254 文字以内の WORD 型 (*1)	省略不可

*1) 1 文字の空白（スペース）は使用可能です。複数の空白（スペース）は 1 文字にまとめられます。

【動作モード】

イベントアクション設定モード

【説明】

説明書きを設定します。わかりやすい名称を割り当ててください。

show event-action entry コマンドで、イベントアクション設定モードの説明が表示されます。

【実行例】

説明書きを設定します（説明：test message）。

```
#configure terminal
(config)#event-action 1
(config-event-action)#description test message
```

【未設定時】

説明書きは設定されません。

34.1.3 event-condition

【機能】

イベント発生判定のマッチタイプの設定

【入力形式】

event-condition {match-all | match-any}

no event-condition {match-all | match-any}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
match-all match-any	マッチタイプを指定します。	match-all : and match-any : or	省略不可

【動作モード】

イベントアクション設定モード

【説明】

イベント発生判定のマッチタイプを設定します。

match-all が指定された場合は、該当イベントアクションモードに設定されたすべてのイベントが発生した場合にアクションを実施します。

match-any が指定された場合は、該当イベントアクションモードに設定されたイベントのうち 1 つでも発生した場合にアクションを実施します。

【実行例】

イベント発生判定のマッチタイプを設定します (match-all)。

```
#configure terminal
(config)#event-action 1
(config-event-action)#event-condition match-all
```

【未設定時】

match-any で動作します。

34.1.4 replay-action

【機能】

アクションを繰り返し実施するか、一度だけ実施するかの設定

【入力形式】

replay-action {on | off}

no replay-action {on | off}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
on off	アクションを繰り返し実施するかどうかを指定します。	on: アクションを繰り返し実施 off: アクションを一度だけ実施	省略不可

【動作モード】

イベントアクション設定モード

【説明】

アクションを繰り返し実施するか、一度だけ実施するかを設定します。

"on" を指定した場合は、イベントが発生する都度アクションを実施します。

"off" を指定した場合は、アクションを一度だけ実施し、以降イベントの発生状態を監視しません。

【実行例】

アクションを繰り返し実施するか、一度だけ実施するかを設定します (off)。

```
#configure terminal
(config)#event-action 1
(config-event-action)#replay-action off
```

【未設定時】

on で動作します。

34.1.5 retry

【機能】

リトライ回数の上限の設定

【入力形式】

```
retry { <リトライ回数> [interval <リトライ間隔>] | interval <リトライ間隔> }
```

```
no retry { <リトライ回数> [interval <リトライ間隔>] | interval <リトライ間隔> }
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
リトライ回数	リトライ回数を指定します。	0～60	3
リトライ間隔	リトライ間隔（単位：秒）を指定します。	1～60	1

【動作モード】

イベントアクション設定モード

【説明】

リトライ回数の上限を指定します。

リトライ回数の上限を超えた場合、アクションの実施状態は "ERROR FINISH" に遷移します。"ERROR FINISH" はアクションを完了できなかったことを示します。"ERROR FINISH" になった場合、イベントの状態が True から False になった際にアクションの実施状態は "INACTIVE" になり、再度 False から True になった際にアクションを実施します。リトライを繰り返している間に、イベントの状態が True から False に遷移した場合、以降のリトライは実施しません。

interval 設定はアクションの実施に失敗した際、再度アクションを実施するまでの間隔を指定します。指定した interval の間に、イベントの状態が True から False に遷移した場合、リトライは実施しません。

【実行例】

リトライ回数の上限を指定します（リトライ回数：5 回、interval：60 秒）。

```
#configure terminal
(config)#event-action 1
(config-event-action)#retry 5 interval 60
```

【未設定時】

リトライ回数は 3 回として動作します。

リトライ間隔は 1 秒として動作します。

34.1.6 event interface

【機能】

インタフェースの UP/DOWN をイベントとして監視する設定

【入力形式】

event interface <インタフェース名> <インタフェース番号> {up | down} [time-threshold <経過時間>]

no event interface <インタフェース名> <インタフェース番号> {up | down} [time-threshold <経過時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース名	インタフェース名を指定します。	-	省略不可
インタフェース番号	インタフェース番号を指定します。	-	省略不可
up down	インタフェースの UP/DOWN を指定します。	-	省略不可
経過時間	経過時間（単位：秒）を指定します。	0～2147483647	0

【動作モード】

イベントアクション設定モード

【説明】

インタフェースの UP/DOWN をイベントとして監視する場合に設定します。

インタフェースの UP 状態または DOWN 状態が、指定した経過時間の間、指定した状態を維持した場合にイベント発生と判断します。経過時間で指定した時間に満たないうちにインタフェースの状態が変化した場合は、イベント未発生と判断します。

指定したインタフェースの設定がない場合は、インタフェースの状態を "DOWN" として扱います。

【実行例】

インタフェースの UP/DOWN をイベントとして監視します（インタフェース名：gigaethernet、インタフェース番号：1/1、down）。

```
#configure terminal
(config)#event-action 1
(config-event-action)#event interface gigaethernet 1/1 down
```

【未設定時】

インタフェースの UP/DOWN をイベントとして監視しません。

34.1.7 event interface counter

【機能】

カウンタ値の条件比較結果をイベントとして監視する設定

【入力形式】

event interface <インタフェース名> <インタフェース番号> counter <カウンタ名>
{eq | ne | gt | ge | lt | le} <カウンタ値>

no event interface <インタフェース名> <インタフェース番号> counter <カウンタ名>
{eq | ne | gt | ge | lt | le} <カウンタ値>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
インタフェース名	インタフェース名を指定します。	-	省略不可
インタフェース番号	インタフェース番号を指定します。	-	省略不可
カウンタ名	show interface コマンドで確認できるカウンタ名を指定します。	カウンタ名一覧を参照	省略不可
eq ne gt ge lt le	数値の比較条件を指定します。	eq : 等しい ne : 等しくない gt : 超える ge : 以上 lt : 未満 le : 以下	省略不可
カウンタ値	カウンタ値を指定します。	0～4294967295	省略不可

【カウンタ名一覧】

カウンタ名	内容
bit_rate_input	平均入力ビットレート
bit_rate_output	平均出力ビットレート
broadcasts_input	受信したブロードキャストパケット数
broadcasts_output	送信したブロードキャストパケット数
bytes_input	受信した bytes 数
bytes_output	送信した bytes 数
crc_errors_input	CRC（巡回冗長検査）エラーした受信パケット
discards_input	受信したフレームのうち廃棄したフレーム数
discards_output	送信したフレームのうち廃棄したフレーム数
dropped_input	受信があふれた回数
dropped_output	送信があふれた回数
errors_input	受信時にエラー廃棄したパケット数
errors_output	送信時にエラー廃棄したパケット数
inactive_discards_input	受信時に Inactive セッション時のパケットフィルタ機能により破棄したパケット数
inactive_discards_output	送信時に Inactive セッション時のパケットフィルタ機能により破棄したパケット数

カウンタ名	内容
ip_broadcasts_input	受信した IP ブロードキャストパケット数
ip_broadcasts_output	送信した IP ブロードキャストパケット数
ip_multicasts_input	受信した IP マルチキャストパケット数
ip_multicasts_output	送信した IP マルチキャストパケット数
ip_unicasts_input	受信した IP ユニキャストパケット数
ip_unicasts_output	送信した IP ユニキャストパケット数
l2_broadcasts_input	受信した L2 ブロードキャストフレーム数
l2_broadcasts_output	送信した L2 ブロードキャストフレーム数
l2_multicasts_input	受信した L2 マルチキャストフレーム数
l2_multicasts_output	送信した L2 マルチキャストフレーム数
l2_unicasts_input	受信した L2 ユニキャストパケットの内、出力ポートの学習が既に行われたもののフレーム数
l2_unicasts_output	送信した L2 ユニキャストパケットの内、出力ポートの学習が既に行われたもののフレーム数
l2_unknown_unicasts_input	受信した L2 ユニキャストパケットの内、出力ポートが未学習のもののフレーム数
l2_unknown_unicasts_output	送信した L2 ユニキャストパケットの内、出力ポートが未学習のもののフレーム数
multicasts_input	受信したマルチキャストパケット数
multicasts_output	送信したマルチキャストパケット数
overrun_input	フレームの受信レートがハードウェアの受信能力を超えたため、受け取れなかった回数
oversized_input	規程より長いフレームの受信パケット数
packet_rate_input	平均入力パケットレート
packet_rate_output	平均出力パケットレート
packets_input	受信したパケット数
packets_output	送信したパケット数
pause_frames_input	受信した Pause フレーム数
undersized_input	フレーム長が 64 より短いフレームの受信パケット数
unicasts_input	受信したユニキャストパケット数
unicasts_output	送信したユニキャストパケット数
unknown_protocol_input	プロトコル不明のため処理できなかったパケット数

【動作モード】

イベントアクション設定モード

【説明】

show interface コマンドで確認できるカウンタ値の条件比較結果をイベントとして監視する場合に設定します。

カウンタの監視可能な上限は 10 件となります。10 件を超えた場合はエラーとなります。

設定されていないインタフェースに対する監視設定も件数に含みます。

【実行例】

show interface コマンドで確認できるカウンタ値の条件比較結果をイベントとして監視します（インタフェース名：gigaetherenet、インタフェース番号：1/1、カウンタ名：bit_rate_input、gt、カウンタ値：100）。

```
#configure terminal
(config)#event-action 1
(config-event-action)#event interface gigaetherenet 1/1 counter bit_rate_input gt 100
```

【未設定時】

条件比較結果をイベントとして監視しません。

34.1.8 event manual

【機能】

実行コマンドとしてアクションを実施するためのタグ名の設定

【入力形式】

event manual <アクションタグ名>

no event manual [<アクションタグ名>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
アクションタグ名	実行コマンドとしてアクションを実施するための識別タグ名を指定します。	32 文字以内の WORD 型	省略不可

【動作モード】

イベントアクション設定モード

【説明】

実行コマンドとしてアクションを実施するためのタグ名を設定します。

再起呼び出しになってしまうため、自身のタグ名は設定しないでください。

【実行例】

実行コマンドとしてアクションを実施するためのアクションタグ名を設定します（アクションタグ名：sample-A）。

```
#configure terminal
(config)#event-action 1
(config-event-action)#event manual sample-A
```

【未設定時】

アクションを実施しません。

34.1.9 event ping

【機能】

ping による宛先監視の設定

【入力形式】

event ping <宛先> [repeat <送信回数>] [timeout <タイムアウト時間>] [event-interval <実行間隔>]
[invert]

no event ping <宛先> [repeat <送信回数>] [timeout <タイムアウト時間>] [event-interval <実行間隔>]
[invert]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
宛先	宛先を指定します。	ホスト名：254文字以内のWORD型 IPv4 アドレス形式 IPv6 アドレス形式	省略不可
送信回数	ping の送信回数を指定します。	1～10	5
タイムアウト時間	ping のタイムアウト時間（単位：秒）を指定します。	1～10	2
実行間隔	ping イベント実行間隔（単位：分）を指定します。	1～1440	1
invert	True と False の状態を反転させて通知する場合に指定します。	-	True と False の状態をそのまま通知する

【動作モード】

イベントアクション設定モード

【説明】

ping による宛先監視を行う場合に設定をします。

疎通可能であれば True、疎通不可の場合は False となります。

invert 指定している場合は、逆に疎通可能であれば False、疎通不可の場合は True となります。

実行間隔は、前回 ping イベント実行開始時間から指定された時間経過したタイミングとなりますので、たとえば実行間隔：1分（60秒）、送信回数：10回、タイムアウト時間：10秒と設定にすると ping の実行～終了までが100秒となり、実行間隔を超えるケースがあります。

この場合は、100秒経過後に次の ping が実行されることとなります。

送信する ping のパラメタは以下のようになります。

送信回数： 1～10回（設定により変更、省略時は5回）
 データサイズ： 100bytes
 タイムアウト時間： 1～10秒（設定により変更、省略時は2秒）
 df-bit： DFbitをセットしない
 TTL： 255
 Hop Limit： 64

疎通可能の判定は、送信回数で指定された回数送信し、そのうち 1 回でも送信の応答があれば疎通可能と判定します。

例) 送信回数 5 回、応答数 1～5 回：疎通可能判定

送信回数 5 回、応答数 0 回：疎通不可判定

event-action 機能による ping の宛先監視は、装置全体で 10 個まで設定可能です。

【実行例】

ping による宛先監視を行います（宛先：192.168.0.1）。

```
#configure terminal
(config)#event-action 1
(config-event-action)# event ping 192.168.0.1
```

【未設定時】

ping による宛先監視を行いません。

34.1.10 event syslog filter

【機能】

フィルタにマッチするログ出力をイベントとして監視する設定

【入力形式】

event syslog filter <ログフィルタタグ名> [effective-time <継続時間>]

no event syslog filter <ログフィルタタグ名> [effective-time <継続時間>]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
ログフィルタタグ名	ログフィルタの識別タグ名を指定します。	32 文字以内の WORD 型	省略不可
継続時間	イベント発生を継続する時間（単位：秒）を指定します。	0～300	300

【動作モード】

イベントアクション設定モード

【説明】

フィルタにマッチするログ出力をイベントとして監視する場合に設定します。

イベントが発生してからアクションが実施されなかった場合、effective-time で指定した時間分、イベント発生状態を継続します（時間経過後はイベント未発生に戻ります）。

effective-time で指定した時間以内に再度イベントが発生（フィルタにマッチするログが出力）した場合、継続時間は延長されます。

effective-time で 0 を指定した場合、ログ出力の瞬間のみイベント発生となります。

動作には、本コマンド、logging filter コマンド、syslog filter 設定モードの各設定が必要となります。

【実行例】

フィルタにマッチするログ出力をイベントとして監視します（ログフィルタタグ名：filter-A）。

```
#configure terminal
(config)#event-action 1
(config-event-action)#event syslog filter filter-A
```

【未設定時】

ログ出力をイベントとして監視しません。

34.1.11 event timer countdown

【機能】

refresh コマンド実行からの経過時間をイベントとして監視する設定

【入力形式】

event timer countdown <継続時間> [replay]

no event timer countdown <継続時間> [replay]

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
継続時間	refresh コマンド実行からの経過時間（単位：秒）を指定します。	0～2147483647	300

【動作モード】

イベントアクション設定モード

【説明】

refresh コマンド実行からの経過時間をイベントとして監視する場合に設定します。

refresh コマンド実行後、指定時間経過後にイベント発生とし、そのままイベント発生状態を継続します。
"replay" を指定した場合は、イベントが発生しアクションを実施したあと、指定時間経過後にイベント未発生状態となります。

【実行例】

refresh コマンド実行からの経過時間をイベントとして監視します（継続時間：60 秒、replay）。

```
#configure terminal
(config)#event-action 1
(config-event-action)#event timer countdown 60 replay
```

【未設定時】

refresh コマンド実行からの経過時間をイベントとして監視しません。

34.1.12 event timer uptime

【機能】

システムが起動してからの経過時間をイベントとして監視する設定

【入力形式】

event timer uptime <日数> <時間>

no event timer uptime <日数> <時間>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
日数	日数を指定します。	0～24854	省略不可
時間	時間を指定します。	0:0～23:59	省略不可

【動作モード】

イベントアクション設定モード

【説明】

システムが起動してからの経過時間をイベントとして監視する場合に設定します。

システム起動後、指定時間経過後にイベント発生とし、そのままイベント発生状態を継続します。設定投入時点ですでに指定時間を経過していた場合もイベント発生となります。

【実行例】

システムが起動してからの経過時間をイベントとして監視します（日数：1日、時間：0:0）。

```
#configure terminal
(config)#event-action 1
(config-event-action)#event timer uptime 1 0:0
```

【未設定時】

システムが起動してからの経過時間をイベントとして監視しません。

34.1.13 event timer schedule

【機能】

装置に設定された日時の監視の設定

【入力形式】

event timer schedule <日> <時:分>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
日	日にち、またはanyを指定します。anyを指定することにより毎日として扱われます。	1～31,any	省略不可
時:分	時刻を指定します。	時:0～23 分:0～59	省略不可

【動作モード】

イベントアクション設定モード

【説明】

装置に設定された日時を監視する設定をします。

監視は分単位で行います。

装置に設定された日時が、指定日時になったことを契機に True となります。

装置に設定された日時が、指定日時から外れた場合、False に遷移します。

【注意】

複数の event timer schedule を 2 分以上の間隔を空けず、連続した時刻で指定した場合、最初のイベントのみ有効となります。

例) 1 分間隔で連続したイベントを設定

```
(config-event-action)#event timer schedule any 12:00
```

```
(config-event-action)#event timer schedule any 12:01
```

```
(config-event-action)#event timer schedule any 12:02
```

この場合、アクションは 12:00 のみ有効となります。

特定のイベントを契機に 1 分間隔でアクションを実行させる場合は、action 設定に wait time を指定してください。

例) イベントを契機に 1 分間隔でアクションを実行させる設定

```
(config-event-action)#event timer schedule any 12:00
```

```
(config-event-action)#action 1.0 <アクション>
```

```
(config-event-action)#action 1.1 wait time 60
```

```
(config-event-action)#action 2.0 <アクション>
```

```
(config-event-action)#action 2.1 wait time 60
```

```
(config-event-action)#action 3.0 <アクション>
```

【実行例】

装置に設定された日時を監視する設定をします (日: any、時: 分: 12:00)。

```
#configure terminal
(config)#event-action 1
(config-event-action)#event timer schedule any 12:00
```

【未設定時】

装置に設定された日時の監視をしません。

34.1.14 action cli exec command

【機能】

アクションとして実行するコマンド（CLI アクション）の設定

【入力形式】

```
action < 実行順序 > cli exec command {<実行コマンド> | {<load コマンド> | <commit コマンド> |
<refresh コマンド> | <discard コマンド> | <restore コマンド> | <save コマンド> | <tech-support コマン
ド> | <report-all コマンド>}}
```

```
no action < 実行順序 > cli exec command {<実行コマンド> | {<load コマンド> | <commit コマンド> |
<refresh コマンド> | <discard コマンド> | <restore コマンド> | <save コマンド> | <tech-support コマン
ド> | <report-all コマンド>}}
```

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
実行順序	アクションの実行順序を指定します。	0.0 ～ 99.9	省略不可
実行コマンド	実行コマンドを指定します。	512文字以内のSTRING型	省略不可
load コマンド	load コマンド書式を指定します。	-	省略不可
commit コマンド	commit コマンド書式を指定します。	-	省略不可
refresh コマンド	refresh コマンド書式を指定します。	-	省略不可
discard コマンド	discard コマンド書式を指定します。	-	省略不可
restore コマンド	restore コマンド書式を指定します。	-	省略不可
save コマンド	save コマンド書式を指定します。	-	省略不可
tech-support コマンド	tech-support コマンド書式を指定します。	-	省略不可
report-all コマンド	report-all コマンド書式を指定します。	-	省略不可

【動作モード】

イベントアクション設定モード

【説明】

アクションとして実行するコマンド（CLI アクション）を設定します。

configure terminal コマンドは使用できません。

イベント契機で実行する場合、実行するコマンドのユーザ名は"event-manager"になり、ユーザレベルは15となります。

event manual run コマンドで実行する場合、実行するコマンドのユーザ名とユーザレベルは実行ユーザと同一となります。

実行の可否を "[y/N]" で問うコマンドの場合は 'N' が選択されます。そのほかの問い合わせを行うコマンドはエラーとなります。

CLI アクションの同時実行数は最大 10 件となります。

【実行例】

アクションとして実行するコマンド（CLI アクション）を設定します（実行順序：1.0、実行コマンド：show command-log）。

```
#configure terminal
(config)#event-action 1
(config-event-action)#action 1.0 cli exec command show command-log
```

【未設定時】

CLI アクションを実施しません。

34.1.15 action snmp-trap message

【機能】

SNMP Trap で送信するメッセージ（SNMP Trap アクション）の設定

【入力形式】

action <実行順序> snmp-trap message <送信メッセージ>

no action <実行順序> snmp-trap message <送信メッセージ>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
実行順序	アクションの実行順序を指定します。	0.0 ～ 99.9	省略不可
送信メッセージ	SNMP Trap で送信するメッセージを指定します。	254 文字以内の WORD 型(*1)	省略不可

*1) 1 文字の空白（スペース）は使用可能です。複数の空白（スペース）は 1 文字にまとめられます。

【動作モード】

イベントアクション設定モード

【説明】

SNMP Trap で送信するメッセージ（SNMP Trap アクション）を設定します。

本機能の動作には、snmp-server 設定も必要です。

【実行例】

SNMP Trap で送信するメッセージ（SNMP Trap アクション）を設定します（実行順序：1.0、送信メッセージ：Test message）。

```
#configure terminal
(config)#event-action 1
(config-event-action)#action 1.0 snmp-trap message Test message
```

【未設定時】

SNMP Trap アクションを実施しません。

34.1.16 action syslog

【機能】

送信するログメッセージ（SYSLOG アクション）の設定

【入力形式】

action <実行順序> syslog [level {<レベル番号> | <レベル名>}] message <送信メッセージ>

no action <実行順序> syslog [level {<レベル番号> | <レベル名>}] message <送信メッセージ>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
実行順序	アクションの実行順序を指定します。	0.0～99.9	省略不可
レベル番号 レベル名	ログレベルを指定します。	レベル番号：0～7 レベル名：emergencies, alert, critical, errors, warnings, notifications, informational, debugging	informational
送信メッセージ	SNMP Trap で送信するメッセージを指定します。	254文字以内の WORD 型(*1)	省略不可

*1) 1文字の空白（スペース）は使用可能です。複数の空白（スペース）は1文字にまとめられます。

【動作モード】

イベントアクション設定モード

【説明】

送信するログメッセージ（SYSLOG アクション）を設定します。

【実行例】

送信するログメッセージ（SYSLOG アクション）を設定します（実行順序：1.0、送信メッセージ：SYSLOG MESSAGE）。

```
#configure terminal
(config)#event-action 1
(config-event-action)#action 1.0 syslog level 0 message SYSLOG MESSAGE
```

【未設定時】

SYSLOG アクションを実施しません。

34.1.17 action interface

【機能】

変更するインタフェースの状態（インタフェースアクション）の設定

【入力形式】

action <実行順序> interface <インタフェース名> {<インタフェース番号> | all} {up | down}

no action <実行順序> interface <インタフェース名> {<インタフェース番号> | all} {up | down}

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
実行順序	アクションの実行順序を指定します。	0.0～99.9	省略不可
インタフェース名	インタフェース名を指定します。	-	省略不可
インタフェース番号	インタフェース番号を指定します。	インタフェース番号 all	省略不可
up down	インタフェースの UP/DOWN を指定します。	-	省略不可

【動作モード】

イベントアクション設定モード

【説明】

変更するインタフェースの状態（インタフェースアクション）を設定します。

【実行例】

変更するインタフェースの状態（インタフェースアクション）を設定します（実行順序：1.0、インタフェース名：tunnel、インタフェース番号：all、down）。

```
#configure terminal
(config)#event-action 1
(config-event-action)#action 1.0 interface tunnel all down
```

【未設定時】

インタフェースアクションを実施しません。

34.1.18 action wait time

【機能】

次のアクション実行までの待ち時間（単位：秒）の設定

【入力形式】

action <実行順序> wait time <待ち時間>

no action <実行順序> wait time <待ち時間>

【パラメタ】

パラメタ	設定内容	設定範囲	省略時
実行順序	アクションの実行順序を指定します。	0.0～99.9	省略不可
待ち時間	次のアクション実行までの待ち時間（単位：秒）を指定します。	0～65535	省略不可

【動作モード】

イベントアクション設定モード

【説明】

次のアクション実行までの待ち時間（単位：秒）を設定します。

【実行例】

次のアクション実行までの待ち時間（単位：秒）を設定します（実行順序：1.0、待ち時間：100 秒）。

```
#configure terminal
(config)#event-action 1
(config-event-action)#action 1.0 wait time 100
```

【未設定時】

すぐに次のアクションを実行します。

第 35 章 付録



35.1	正規表現について	968
35.2	VRF 設定の関連付け動作について	970

35.1 正規表現について

本装置の一部コマンドでは、正規表現を用いた文字列検索に対応しています。半角英数字などの通常文字やメタ文字で構成されたパターンを表記することにより、対象となる文字列の集合を 1 つのコマンドで指定することが可能です。

本装置で使用可能なメタ文字の種類と用法については、以下を参照してください。

表 35-1 本装置で使用可能なメタ文字の種類と用法

正規表現で使用可能なメタ文字		意味	使用例	
.	ピリオド	任意の 1 文字を意味します (スペースを含む)	1.	"10", "19", "1a" などの文字列が該当
*	アスタリスク	直前の 1 文字、またはグループ化された文字列の 0 回以上の繰り返しを意味します (スペースを除く)	12*	"1", "12", "122" など、直前にある文字 "2" を 0 回以上繰り返した文字列が該当
+	プラス	直前の 1 文字、またはグループ化された文字列の 1 回以上の繰り返しを意味します (スペースを除く)	12+	"12", "122" など、直前にある文字 "2" を 1 回以上繰り返した文字列が該当
^	キャレット	文字列の先頭を意味します	^11	"11", "1123" など、先頭が "11" から始まる文字列が該当
\$	ドル	文字列の末尾を意味します	11\$	"11", "3211" など、末尾が "11" で終わる文字列が該当
_	アンダースコア	次の中の 1 文字 スペース " カンマ "," 中括弧 "{", "}" 括弧 "(", ")" あるいは次の位置指定を意味するメタ文字の代用を意味します 文字列の先頭 (^) 文字列の末尾 (\$)	_12_	"12", "0 12", "12,3", "0{12}", "(12)3" など、"12" の前後に代用文字が入る文字列、または "12" で始まる (終わる) 文字列が該当
()	括弧	グループ化を意味します	(12)+	"12", "1212", "121212" など "12" を 1 回以上繰り返した文字列が該当
{ }	中括弧	繰り返し回数を指定します	1{2}	"11", "211", "11222" など、"1" を 2 回繰り返した文字列が該当
			1{2,}	"11", "111", "211", "1112", "1111" など、"1" を 2 回以上繰り返した文字列が該当
			1{2,3}	"11", "111", "211", "1112" など、"1" を 2 回以上 3 回以下繰り返した文字列が該当
[]	大括弧	文字の範囲を意味します	[1234]	"1", "2", "3", "4" が該当
			[13]	"1", "3" が該当
-	ハイフン		[1-4]	"1", "2", "3", "4" が該当
			[a-cA-C]	"a", "b", "c", "A", "B", "C" が該当
	パイプ	「または」を意味します	^1 ^2	1 文字目が "1" または "2" の文字列が該当
			^1 2\$	1 文字目が "1" または最後の文字が "2" の文字列が該当

正規表現で使用可能な メタ文字		意味	使用例	
\	バックスラッシュ	正規表現の文字の特殊な意味を取り除きます	1\1	"1.1" が該当

35.1.1 使用例

【使用例 1) AS パスリストの指定】

BGP で通知する／受け入れるプレフィックスの AS パスリストによるフィルタリングを行う際に、AS パス値として正規表現を利用します。

AS-PATH 属性に 10000、10001、10002、10003 のどれかが含まれるプレフィックス情報のみを受け入れる場合には、以下のように設定します。

```
ip as-path access-list 1 permit 1000[0-3]
router bgp 60000
 neighbor 10.0.0.1 remote-as 60000
 address-family ipv4 unicast
   neighbor 10.0.0.1 filter-list 1 in
 exit
 exit
```

【使用例 2) コミュニティリストの指定】

BGP で通知する／受け入れるコミュニティ属性によるフィルタリングを行う際に、コミュニティ属性値として正規表現を利用します。

コミュニティ属性に 60001:1～60009:1 のどれかが含まれるプレフィックス情報のみを受け入れる場合には、以下のように設定します。

```
ip community-list expanded com1 permit ^6000[1-9]:1
route-map MAP_COM1 permit 1
 match community com1
 exit
router bgp 60000
 neighbor 10.0.0.1 remote-as 60000
 address-family ipv4 unicast
   neighbor 10.0.0.1 route-map MAP_COM1 in
 exit
 exit
```

【使用例 3) 拡張コミュニティリストの指定】

BGP で通知する／受け入れる拡張コミュニティ属性によるフィルタリングを行う際に、拡張コミュニティ属性値として正規表現を利用します。

拡張コミュニティ属性に route-target 60001:1～60009:1 のどれかが含まれるプレフィックス情報のみを受け入れる場合には、以下のように設定します。

```
ip extcommunity-list expanded ecom1 permit RT:6000[1-9]:1
route-map MAP_ECOM1 permit 1
 match extcommunity ecom1
 exit
router bgp 60000
 neighbor 10.0.0.1 remote-as 60000
 address-family vpnv4
   neighbor 10.0.0.1 route-map MAP_ECOM1 in
 exit
 exit
```

35.2 VRF 設定の関連付け動作について

本装置では VRF 設定を行うと自動で関連設定の追加及び削除が行われます。

35.2.1 vrf 設定モード追加時の関連付け動作

vrf 設定モードを追加した場合、BGP サービス設定モードに 同一 VRF 名の address-family ipv4 VRF 設定モードを自動で追加します。

【実行例】

- 設定前コンフィグ

```
!  
router bgp 1  
exit  
!
```

- 設定後コンフィグ

"ip vrf vrf-A" を追加した場合、BGP サービス設定モードに "address-family ipv4 vrf vrf-A" を自動で追加します。

```
!  
ip vrf vrf-A  
exit  
!  
router bgp 1  
!  
address-family ipv4 vrf vrf-A  
exit  
!  
exit  
!
```

35.2.2 vrf 設定モード削除時の関連付け動作

vrf 設定モードを削除した場合、自動で下記の関連設定を削除します。

- BGP サービス設定モード内の同一 VRF 名を指定した address-family ipv4 VRF 設定モードと address-family ipv6 VRF 設定モード
- 同一 VRF 名の ip vrf forwarding 設定がある loopback インタフェース設定モード
- 同一 VRF 名の ip vrf forwarding 設定がある tunnel インタフェース設定モード
- 同一 VRF 名の ip vrf forwarding 設定がある port-channel インタフェース設定モードと削除した port-channel と同一チャンネル番号の channel-group 設定
- 下記の同一 VRF 名の設定を削除
 - OSPF-VRF サービス設定モード
 - ip route vrf 設定
 - ip route ~ survey vrf 設定
 - ipv6 route vrf 設定
 - ipv6 route ~ survey vrf 設定
 - ip icmp vrf 設定
 - ipv6 icmp vrf 設定
 - survey vrf 設定

【実行例】

- 削除前コンフィグ

```

!
ip route 15.15.15.0 255.255.255.0 150.150.150.150 survey vrf vrf-A 10.10.10.10
ip route vrf vrf-A 10.10.10.0 255.255.255.0 100.100.100.100
ip icmp vrf vrf-A source address 10.10.10.10
!
ip vrf vrf-A
  rd 1:1
exit
!
survey vrf vrf-A 10.10.10.10
!
interface GigaEthernet 1/1
  channel-group 10
exit
!
interface Loopback 10
  ip vrf forwarding vrf-A
  ip address 192.168.10.10
exit
!
interface Port-channel 10
  ip vrf forwarding vrf-A
  ip address 192.166.10.10 255.255.255.0
exit
!
router ospf-vrf vrf-A 1 daemon-id 1
exit
!
router bgp 1
!
  address-family ipv4 vrf vrf-A
  exit
!
exit
!

```

- 削除後コンフィグ

"ip vrf vrf-A" を削除した場合、関連設定を自動で削除します。

```

!
interface GigaEthernet 1/1
exit
!
router bgp 1
exit
!

```

35.2.3 router bgp 設定追加時の関連付け動作

BGP サービス設定モードを追加した場合、設定済みの vrf 設定モードと同一 VRF 名の address-family ipv4 VRF 設定モードを BGP サービス設定モードに自動で追加します。

【実行例】

- 削除前コンフィグ

```

!
ip vrf vrf-A
exit
!

```

- 削除後コンフィグ

"router bgp 1" を追加した場合、router bgp 1 モードに "address-family ipv4 vrf vrf-A" を自動で追加します。

```
!  
ip vrf vrf-A  
exit  
!  
router bgp 1  
!  
address-family ipv4 vrf vrf-A  
exit  
!  
exit  
!
```

35.2.4 ip vrf forwarding 設定追加時の関連付け動作

ip vrf forwarding 設定を追加するインタフェース設定モード内の ip address 設定、ipv6 address 設定を自動で削除します。

【実行例】

- 削除前コンフィグ

```
!  
ip vrf vrf-A  
rd 1:1  
exit  
!  
interface Port-channel 1  
ip address 192.168.0.1 255.255.255.0  
ip address secondary 192.168.2.2 255.255.255.0  
ipv6 address 2001:db8::3/64  
exit  
!
```

- 削除後コンフィグ

port-channel インタフェース設定モード内に "ip vrf forwarding vrf-A" を追加した場合、port-channel インタフェース設定モード内の ip address 設定と ipv6 address 設定を自動で削除します。

```
!  
ip vrf vrf-A  
rd 1:1  
exit  
!  
interface Port-channel 1  
ip vrf forwarding vrf-A  
exit  
!
```


35.2.5 ip vrf forwarding 設定削除時の関連付け動作

ip vrf forwarding 設定を削除するインタフェース設定モード内の ip address 設定、ipv6 address 設定を自動で削除します。

【実行例】

- 削除前コンフィグ

```
!  
ip vrf vrf-A  
  rd 1:1  
exit  
!  
interface Port-channel 1  
  ip vrf forwarding vrf-A  
  ip address 192.168.0.1 255.255.255.0  
  ip address secondary 192.168.2.2 255.255.255.0  
  ipv6 address 2001::db8::3/64  
exit  
!
```

- 削除後コンフィグ

port-channel インタフェース設定モード内の "ip vrf forwarding vrf-A" を削除した場合、port-channel インタフェース設定モード内の ip address 設定と ipv6 address 設定を自動で削除します。

```
!  
ip vrf vrf-A  
  rd 1:1  
exit  
!  
interface Port-channel 1  
exit  
!
```

35.2.6 ip vrf 設定の確認

以下の設定は、コマンド入力時に指定した <VRF 名> を持つ VRF インスタンスが設定されているかを確認します。指定した VRF インスタンスがなかった場合は設定エラーとなり、入力した設定は反映されません。

- BGP サービス設定モード内の address-family ipv4 VRF 設定モード
- BGP サービス設定モード内の address-family ipv6 VRF 設定モード
- OSPF-VRF サービス設定モード
- ip vrf forwarding 設定

索引

A

aaa accounting commands	104
aaa accounting connection	105
aaa accounting exec	105
aaa accounting network	706
aaa accounting ngn-sip start-stop group	715
aaa accounting send stop-record authentication failure	107
aaa accounting suppress null-username	107
aaa accounting system default	108
aaa authentication enable	86
aaa authentication ike-client	583
aaa authentication login	87
aaa authentication login-prompt	88
aaa authentication ngn-sip group	715
aaa authentication password-prompt	88
aaa authentication server-fail-message	89
aaa authentication suppress-log	90
aaa authorization commands	91
aaa authorization exec	92
aaa authorization network	590
aaa group server radius	721
aaa local group	577
access-list	376
access-list description	383
access-list (IPv4 拡張設定)	377
access-list (IPv4 標準設定)	376
access-list (IPv6 拡張設定)	380
access-list (IPv6 標準設定)	379
access-list (MAC アドレス設定)	381
account	156, 729
accounting	109, 561, 716
action	833
action cli exec command	962
action interface	965
action snmp-trap message	963
action syslog	964
action wait time	965
address	424, 452
address-family ipv4 unicast	309
address-family ipv4 vrf	351
address-family ipv6 unicast	330
address-family ipv6 vrf	352
aggregate-address	309, 330
alias	51
always-up	764
area authentication	193
area default-cost	194, 242
area export-list	195
area import-list	196
area nssa	196

area range	198, 243
area shortcut	199
area stub	199, 244
area virtual-link	235, 259
area virtual-link authentication	235
area virtual-link authentication-key	236
area virtual-link dead-interval	237, 259
area virtual-link hello-interval	238, 260
area virtual-link message-digest-key	239
area virtual-link retransmit-interval	239, 261
area virtual-link transmit-delay	240, 262
arp	402
arp vrf	739
attribute 31 extend-with-prefixlen	710
attribute 31 include-in-access-req	708
attribute 31 include-in-acct-req	709
attribute 81 include-in-access-req	710
attribute 81 include-in-acct-req	711
attribute ignore	708
authentication	535
authentication accept	157, 731
authorization	95
auto config save enable	113
auto connect	730
auto-cost reference-bandwidth	200

B

bandwidth	790
bandwidth profile	804
bandwidth scale	815
banner motd enable	111
banner motd text	111
bfd all-interface	528
bfd-map	517
bgp aggregate-nexthop-check	265
bgp always-compare-med	272
bgp anvl-dampening-config	266
bgp bestpath as-path ignore	272
bgp bestpath compare-routerid	273
bgp bestpath igp-metric ignore	273
bgp bestpath med	274
bgp bundle-time	276
bgp cluster-id	277
bgp dampening	278
bgp default local-preference	279
bgp deterministic-med	280
bgp enforce-first-as	280
bgp listen range	281
bgp local-as	744
bgp log-neighbor-changes	282
bgp log-update-error	283

bgp multi-path	283
bgp network import-check	284
bgp nexthop-validation-timer	285
bgp rfc1771-path-select	267
bgp rfc1771-strict	267
bgp router-id	286
bridge loop-detect-disable	770
bridge loop-detect-time	771
bridge transparent bpdu	772
bridge transparent eap	772
bridge transparent lacp	773
bridge transparent other	774
bridge-group	130, 164, 770
burst	823

C

ca trustpoint	593
capability restart graceful	201
changeback-time	721
channel-group	132
class	789, 831
class-map	779
client authentication eap-identity request	586
client authentication list	584
client authentication my-name	584
client authentication type	585, 717
client configuration address	591
client-id	422
client-priority	670
clock summer-time	54
clock timezone	55
compatible rfc1583	201
config comment	113
configure terminal	44
continue	354
cookie size	764
count	791, 833
cpu utilization	939
crypto ip dns-params	632
crypto ip dns-query auto-refresh	633
crypto ip dns-query negotiation	633
crypto ip dns-query timeout	634
crypto ip domain-name	635
crypto ip name-server	636
crypto ipsec esn	612
crypto ipsec ikev2 delay old-sa-delete	636
crypto ipsec ikev2 delay old-sa-delete-ack	637
crypto ipsec policy	548
crypto ipsec qm-addr-zero-any	642
crypto ipsec replay-check disable	605
crypto ipsec responder udp-encapsulation spoofed	613
crypto ipsec security-association lifetime seconds	550
crypto ipsec security-association softlimit	551
crypto ipsec selector	558
crypto ipsec selector-check	604
crypto ipsec sequence-overflow disable	607
crypto ipsec udp-encapsulation	612
crypto ipsec udp-encapsulation-force	534
crypto ipsec-tunnel ike limit	619
crypto ipsec-tunnel ike threshold	619
crypto ipsec-tunnel ipsec-in limit	620
crypto ipsec-tunnel ipsec-in threshold	621
crypto ipsec-tunnel session limit	622
crypto ipsec-tunnel session threshold	622
crypto isakmp client configuration group	588
crypto isakmp keepalive	598
crypto isakmp keepalive-icmp	599
crypto isakmp keepalive-params no-reconnect	531
crypto isakmp log	658
crypto isakmp negotiation always-up-params	638
crypto isakmp negotiation cookie-req	631
crypto isakmp negotiation expire-time	639
crypto isakmp negotiation limit	630
crypto isakmp negotiation protected-rekey-interval	640
crypto isakmp negotiation retry	641
crypto isakmp policy	531
crypto isakmp profile	561
crypto isakmp rekey continuous-channel	532
crypto isakmp security-association softlimit	533
crypto isakmp tos	533
crypto keyring	540
crypto map	572
crypto pki startup-import delete other-certificate	597
crypto pki startup-import pkcs12	596
crypto pki startup-import store file	595
crypto session identification address	642
crypto session reject-duplicated-request	643
crypto session release idle-time	644
crypto session release ipsec-lost-time	645
crypto session release isakmp-lost-time	646
crypto session release reset acct-stop-send	647
crypto session release reset delay	648
crypto session release reset delete-send	647
crypto session release session-time	648

D

dataconnect-policy-map	823
default-information originate ...	178, 202, 310, 331
default-metric	179, 203, 245
description	134, 623, 662, 745, 949

designated-source	521
destination address	510
digest type	754
disable	45
distance	180, 204, 245, 286
distance bgp	287
distance ospf	205
distribute-list	181, 205
dns	425, 453, 588
dns-server access-class	81
dns-server enable	80
domain	426, 454, 671
dont-route	536, 881
dot1q tunnel tpid	120
drop	791
dscp	881
dst	559
duid	455
dvpn autoignore	660
dvpn client	670
dvpn client-log	931
dvpn ip	660
dvpn profile	662
dvpn server auth aaa	681
dvpn server auth use	681
dvpn server domain	682
dvpn server sips max-sessions	682
dvpn server use enable	683
dvpn server-log	931
dvpn sip encode-off	674
dvpn-interface	663
dvpn-server address	672
dvpn-server username	673

E

eee	121
enable	45
encryption	536
encryption-keysize	537
end	46
environment profile	939
ether-ip tunnel-profile	503
ethernet linkdown-delay-time	147
ethernet linkup-delay-time	147
event interface	953
event interface counter	954
event manual	956
event ping	957
event syslog filter	958
event timer countdown	959
event timer schedule	960
event timer uptime	960
event-action	949
event-condition	950

exec-timeout	65
exit	46
extended-queue	792

F

facility	928
flowcontrol	136
frame-overhead	812, 818
frequency	882
ftp-server access-class	76
ftp-server exec-timeout	76
ftp-server shutdown	77
fvrf	562

G

gateway	426
group	538

H

hardware-fault-detection action	946
hardware-fault-detection level-up	947
hash	539
hello interval	755
help	48
hidden	756
hop-limit	883
host	431, 462
hostname	35
hostname local	756
hostname remote	757

I

iaid	449
ids profile	837
ike-version	563
incoming-call disable	686
initiate-mode	543
instance-metric	206
interface gigabitEthernet	122
interface loopback	123
interface management	123
interface port-channel	124
interface trunk-channel	125
interface tunnel	124
interface usb-ethernet	126
interval	522
ip access-group	383
ip access-group default spi	386
ip access-group spi ftp-data enable	387
ip access-group spi timeout	388
ip acl logging enable	932

ip address	416	ip ospf network	213
ip arp max-request	404	ip ospf priority	214
ip arp packet-hold	402	ip ospf retransmit-interval	215
ip arp polling disable	403	ip ospf transmit-delay	215
ip arp pre-solution disable	404	ip prefix-list	411
ip as-path access-list	268	ip prefix-list description	412
ip community-list	269	ip proxy-arp	417
ip dhcp client-profile	420, 421	ip rip authentication mode	182
ip dhcp host-database	421	ip rip authentication string	182
ip dhcp server-profile	420, 423	ip rip split-horizon	184
ip dhcp service	419	ip route	414
ip domain-name	406	ip route bfd-map	517
ip extcommunity-list	270	ip route survey	871
ip finger	109	ip route vrf	741
ip fragment- cache disable	135	ip route vrf bfd-map	519
ip host	406	ip route vrf survey	872
ip icmp disable-sending-errors	408	ip scp server enable	73
ip icmp source	409	ip sftp server enable	73
ip ids	837	ip spi entry icmp-timeout	397
ip local pool	410	ip spi entry others-timeout	398
ip name-server	79	ip spi entry tcp-fin-timeout	392
ip name-server source-interface	80	ip spi entry tcp-idle-timeout	394
ip nat acl	495	ip spi entry tcp-syn-timeout	391
ip nat acl permit	496	ip spi entry udp-idle-timeout	395
ip nat default action	501	ip ssh authentication-retries	71
ip nat inside destination static	489	ip ssh port	71
ip nat inside destination static-subnet	490	ip ssh time-out	72
ip nat inside source list interface	486	ip unnumbered	418
ip nat inside source list pool	484	ip vrf	739
ip nat inside source static	487	ip vrf forwarding	707, 744
ip nat inside source static-subnet	488	ip vrrp advertise_delay_timer	849
ip nat list	483	ip vrrp enable	842
ip nat outside destination static	493	ip vrrp initialize_delay_time	850
ip nat outside destination static-subnet	494	ip vrrp mode interface-delegation	851
ip nat outside source static	491	ip vrrp mode logging-enable-all	934
ip nat outside source static-subnet	492	ip vrrp mode trap-enable-all	852
ip nat pool	483	ip vrrp np_delay_timer	850
ip nat table logging enable	933	ipinip fragment	511
ip nat translation finrst-timeout	497	ipinip propagate-tos	514
ip nat translation icmp-timeout	497	ipinip propagate-ttl	514
ip nat translation tcp-timeout	498	ipinip tunnel-profile	509
ip nat translation timeout	499	ipsec-timeout	686
ip nat translation udp-timeout	499	ipv6 access-group	384
ip nat wellknown	500	ipv6 access-group default spi	386
ip ospf authentication	207	ipv6 access-group spi ftp-data enable	388
ip ospf authentication-key	208	ipv6 access-group spi timeout	389
ip ospf bfd	526	ipv6 address	443
ip ospf cost	208	ipv6 address dhcp	444
ip ospf database-filter all out	209	ipv6 dhcp client-profile	447, 449
ip ospf dead-interval	210	ipv6 dhcp host-database	448
ip ospf disable all	210	ipv6 dhcp server-profile	447, 451
ip ospf hello-interval	211	ipv6 dhcp service	446
ip ospf message-digest-key	212	ipv6 enable	463
ip ospf mtu	212	ipv6 hop-limit	464

ipv6 hoplimit-receive-enable	467
ipv6 host	434
ipv6 icmp disable-sending-errors	435
ipv6 icmp source	436
ipv6 ids	838
ipv6 local pool	437
ipv6 mtu-receive-enable	467
ipv6 nd curhoplimit	478
ipv6 nd managed-config-flag	468
ipv6 nd max-solicit	464
ipv6 nd mtu	479
ipv6 nd ns-interval	468
ipv6 nd other-config-flag	469
ipv6 nd packet-hold	465
ipv6 nd prefix-advertisement	470
ipv6 nd pre-resolution disable	471
ipv6 nd ra-delay	471
ipv6 nd ra-interval	472
ipv6 nd ra-lifetime	473
ipv6 nd reachable-time	473
ipv6 nd receive-ra	475
ipv6 nd rs-delay	476
ipv6 nd rs-times	476
ipv6 nd send-ra	477
ipv6 neighbor	466
ipv6 neighbor vrf	742
ipv6 ns-interval-receive-enable	479
ipv6 ospf bfd	527
ipv6 ospf cost	246
ipv6 ospf dead-interval	247
ipv6 ospf display route single-line	248
ipv6 ospf hello-interval	248
ipv6 ospf priority	249
ipv6 ospf retransmit-interval	250
ipv6 ospf transmit-delay	250
ipv6 prefix-list	438
ipv6 prefix-list description	439
ipv6 reachable-time-receive-enable	474
ipv6 route	441
ipv6 route bfd-map	518
ipv6 route survey	873
ipv6 route vrf	743
ipv6 route vrf bfd-map	520
ipv6 route vrf survey	875
ipv6 router ospf area	251
ipv6 router-lifetime-receive-enable	480
ipv6 spi entry icmp-timeout	397
ipv6 spi entry others-timeout	399
ipv6 spi entry tcp-fin-timeout	393
ipv6 spi entry tcp-idle-timeout	394
ipv6 spi entry tcp-syn-timeout	391
ipv6 spi entry udp-idle-timeout	396
ipv6 unnumbered	481
ipv6 vrrp address	861

ipv6 vrrp adver-interval	862
ipv6 vrrp advertise_delay_timer	859
ipv6 vrrp delegated-interface	863
ipv6 vrrp initialize_delay_time	860
ipv6 vrrp mode interface-delegation	863
ipv6 vrrp mode logging-enable-all	934
ipv6 vrrp mode trap-enable-all	864
ipv6 vrrp np_delay_timer	860
ipv6 vrrp preempt	864
ipv6 vrrp priority	865
ipv6 vrrp track	866
isakmp authorization list	563

K

keep connect	664
keepalive	600
keepalive-icmp	601
keyring	564

L

l2-encapsulation map cos-dscp	503, 748
l2tpv3 always-up	750
l2tpv3 always-up-params	750
l2tpv3 hello interval	751
l2tpv3 log	752
l2tpv3 pseudowire	749
l2tpv3 retransmit retries	752
l2tpv3 retransmit timer	753
l2tpv3 tunnel-profile	748
lease-time	427
level	929
lifetime	540
line	65
link-state	572, 649
link-state always-up	145
load-interval	137
local policy-route	830
local-address	565
local-address-icmp	601
localid	675
local-key	566
localnet	674
log-adjacency-changes	216, 252
logging buffer facility	907
logging buffer level	908
logging buffer timestamps msec	909
logging console facility	910
logging console level	911
logging console timestamps msec	912
logging facility	913
logging filter	914
logging fixed-facility	916
logging host	917

logging host facility	921
logging host level	922
logging host-queue length	918
logging host-queue level	918
logging host-queue retry-interval	920
logging host-queue timeout	919
logging level	923
logging source-interface	924
logging suppress-repeated	925
logging telnet	925
logging telnet facility	926
logging telnet level	927
logging telnet timestamps msec	928
login authentication	66

M

mac access-group	399
mac-address	138
mac-address-table aging-time	127
mac-address-table cvid-enable	775
mac-address-table max-entry	774
mac-address-table static	129
mac-address-table total-max-entry	128
match 802.1p priority	780
match address	573
match any	781
match as-path	355
match community	356
match identity	567
match interface	357
match ip access-group	782
match ip address	357
match ip dscp	782
match ip next-hop	358
match ip precedence	783
match ip tos	784
match ipv6 access-group	785
match ipv6 address	359
match ipv6 next-hop	360
match local-source	785
match mac access-group	786
match mac ctg-priority	788
match mac stag-priority	787
match mac unknown-unicast	787
match metric	360
match origin	361
match route-type external	362
match tag	362
match-all	779
match-any	780
match-list	826
max-call	731
maximum-paths	217
maximum-prefix	185

max-metric router-lsa	218
media	139
message	930
min_rx	523
mode	758
modem out-strings init	732
modem profile	727
monitor signal-quality enable level	735
monitor signal-quality interval	736
monitor signal-quality logging usb-ethernet ...	935
mss	141
mtu	140
multi-hop ttl-drop-threshold	523
multiplier	524

N

nas-ip-address	722
nas-port-type	712
ncp	157
negotiation protected-rekey-interval	651
neighbor	186, 218, 525
neighbor activate	311, 332
neighbor advertisement-interval	288
neighbor advertisement-limit	289
neighbor allowas-in	312, 333
neighbor attribute-unchanged	312, 333
neighbor capability graceful-restart	313, 334
neighbor capability route-refresh	290
neighbor default-originate	314, 335
neighbor description	291
neighbor disable-nexthop-validation	315, 336
neighbor distribute-list	316, 337
neighbor dont-capability-negotiate	292
neighbor ebgp-multihop	293
neighbor enforce-multihop	293
neighbor filter-list	317, 338
neighbor interface	294
neighbor maximum-prefix	318, 339
neighbor next-hop-self	319, 340
neighbor override-capability	295
neighbor passive	296
neighbor password	296
neighbor peer-group	297, 298
neighbor port	299
neighbor prefix-list	319, 340
neighbor remote-as	299
neighbor remove-private-as	320, 341
neighbor retain-stale time	300
neighbor route-map	321, 342
neighbor route-reflector-client	343
neighbor route-server-client	322, 344
neighbor send-community	323, 344
neighbor shutdown	301
neighbor soft-reconfiguration inbound	324, 345

neighbor soo 324, 346
neighbor start-interval 302
neighbor strict-capability-match 303
neighbor surveillance down-action 880
neighbor surveillance nexthop-validation-check
..... 878
neighbor surveillance peer-address 879
neighbor timers 303
neighbor update-source 304
neighbor version 305
neighbor weight 306
network 186, 219, 325, 347
ngn enable 687
ngn sip agent bind port-channel 688
ngn sip agent call-timeout 689
ngn sip agent charge-setting 689
ngn sip agent control session 690
ngn sip agent ipsec-timeout 691
ngn sip agent limit 692
ngn sip agent proxy server address 693
ngn sip agent proxy server domain 694
ngn sip agent registrar expire 694
ngn sip agent registrar retry 695
ngn sip agent registrar server address 696
ngn sip agent service-policy 822
ngn sip agent sessiontimer default 697
ngn sip agent sessiontimer use disable 698
ngn sip agent survey sip-server invite 698
ngn sip agent user 699
ngn sip log 936
ngn sip profile 700
ngn sip profile-radius 718
ngn sip radius acct 719
ngn sip radius auth 719
ngn sip use enable 700
no aaa authorization config-commands 92
no bgp client-to-client reflection 276
no bgp default ipv4-unicast 278
no bgp extended-asn-cap 266
no bgp fast-external-failover 281
no bgp lookup default-information 326, 348
no ip rip receive-packet 183
no ip rip send-packet 184
no logging buffer 907
no logging console 910
no snmp trap link-status 898
notify-nhid-usage 117
ntp authenticate 56
ntp authentication-key 56
ntp server 57
ntp source 58
ntp trusted-key 59
ntp-server 428
ntp-server enable 78

O

offset-list 187
opaque-lsa-capable 220
option 428, 456
option-request 450
ospf abr-type 220
ospf restart helper max-grace-period 222
ospf restart helper policy 222
outgoing-call disable 701
overflow database external 223, 253

P

passive-interface 188, 224, 253
password 67, 717
password enable 63
password login 64
periodic-log 118
physical memory 941
pki revocation-check 593
pki validity-check 594
police 793
policing-header 794
policy-map 789
policy-route input 829
policy-route-map 831
pool 589
port profile 804, 817
port scheduler 805, 806
pppoe enable 158
pppoe interface 159
pppoe profile 159
preference 457
prefix 457
pre-shared-key 541
privilege 36
process 936
profile-mode 511
prompt timestamp 67
proxysql address 83
proxysql domain 82
psu-output-error timer 942
psu-temp-sensor safety control power-down
..... 942
pw-type 765

Q

queue 794
queue limit 817, 819, 824
queue normal rate 816, 825
queue shape 820
queue-length update 225

R

radius-server host	97
radius-server retransmit-count	98
radius-server source-interface	98
radius-server timeout	99
rd	746
recv-buffer-size	189
redistribute	190, 226, 254, 327, 348
refresh timer	227
remote dial number	702, 728
remote dial speed	702
remote-address-icmp	602
remote-end-id ascii	766
remoteid	666
remotenet	665
replay-action	951
retransmit	723
retransmit retries	758
retransmit timer	759
retries infinity	423, 451
retry	883, 952
route-map	354
router bgp	265
router ipv6 ospf	242
router ospf	193
router ospf-vrf	263
router rip	178
router-id	228, 256
router-id local	760
router-id remote	761

S

sa-up route	615
sa-up route-dvnpn	616
sa-up route-radius	617
sa-up route-sip-radius	618
search-sequence	795, 832
self-identity	568
sequencing both	766
server-name	160
server-private	723
service-name	161
service-policy	142, 796
service-type	712
session-mode	525
set 802.1p priority	797
set aggregator	363
set as-path prepend	364
set atomic-aggregate	364
set community	365
set dscp	827
set dvnpn client	667

set esn	556
set extcommunity	366
set ikev2 delay old-sa-delete-ack	655
set ip df-bit	513, 610
set ip dscp	797
set ip fragment	611
set ip next-hop	367
set ip prec	798
set ip tos	609, 799
set ipsec-policy	569
set ipsec-tunnel ike limit	624
set ipsec-tunnel ike threshold	625
set ipsec-tunnel index	627
set ipsec-tunnel ipsec-in limit	625
set ipsec-tunnel ipsec-in threshold	626
set ipsec-tunnel name	628
set ipsec-tunnel session limit	628
set ipsec-tunnel session threshold	629
set ipv6 dscp	799
set ipv6 next-hop	367
set ipv6 traffic-class	800
set isakmp-policy	570
set isakmp-profile	574
set local-preference	368
set mac stag-priority	801
set metric	369
set metric-type	370
set mss	143, 734
set mtu	161, 504, 512, 608, 733, 767
set negotiation expire-time	543
set negotiation retry	544
set next-hop	370
set origin	371
set originator-id	372
set peer	570
set pfs	548
set profile	768
set rekey continuous-channel	545
set rekey dont-initiate	650
set replay-check	606
set security-association always-up	549
set security-association lifetime seconds	551
set security-association rekey	656
set security-association softlimit	546, 553
set security-association transform	555
set security-association transform-keysize aes	554
set selector-check	604
set sequence-overflow	607
set service-policy	821
set session identification address	651
set session reject-duplicated-request	652
set session release idle-time	654, 735
set session release ipsec-lost-time	653
set session release isakmp-lost-time	654

set tag	372
set udp-encapsulation	556
set udp-encapsulation-force	547
set weight	373
shape	813, 814
show alias	51
show command-log	50
show history	49
show privilege	37
shutdown	145
sip encrypt-enable	678
sip expire-register	677
sip expire-session	677
sip expire-session-disable	678
sip limit	703
sip local-address	679
sip-server	429
sip-server address	459
sip-server domain	460
size	884
snmp-server community	890
snmp-server contact	890
snmp-server enable traps	891
snmp-server engine-id	900
snmp-server group	900
snmp-server host	892, 901
snmp-server host-queue timeout	893
snmp-server location	894
snmp-server name	895
snmp-server queue-length	895
snmp-server source-interface	896
snmp-server trap-timeout	897
snmp-server user	903
snmp-server view	904
sntp poll-interval	59
sntp retry	60
sntp server	61
sntp-server	461
source address	509
source-address	724
speed-duplex	149
src	558
ssh-server access-class	74
ssh-server version	74
stability	885
summary-address	228
summary-prefix	256
survey	876
survey-map	870
switchport mode dot1q tunnel	165
switchport passthrough	166
switchport transparent	167
syslog filter	906

T

table-map	328, 349
tacacs-server host	100
tacacs-server key	101
tacacs-server source-interface	101
tacacs-server timeout	102
telnet-server access-class	69
telnet-server shutdown	69
temp-sensor expected temperature	940
temp-sensor safety control	943
timeout	725, 886
timers basic	190
timers bgp	307
timers lsa arrival	229
timers spf	257
timers throttle lsa	230
timers throttle spf	231
time-server	430
to-host police	809
to-host protocol	807
to-host reason	810
track down-action	842
track ip	852
track ipv6	867
track management	843
track port-channel	844
track survey	845
track vhost	846
traffic-class	886
traffic-manager extended	803
traffic-manager network	803
transmit	801
trap lsa maxage	232
trap lsa originate	232
trap tx-retransmit	233
trap vlink-tx-retransmit	234
trunk-group	167
trunk-group collector-max-delay	175
trunk-group fall-over bfd-map	528
trunk-group lacpdu-dst-mac	171
trunk-group lacpdu-timeout	170
trunk-group load-balance	176
trunk-group max-active-port	171
trunk-group min-active-port	172
trunk-group mode	169
trunk-group standby-no-receive	173
trunk-group system-priority	173
trunk-group transmit-pause-time	174
trunk-member port-priority	168
ttl	887
tunnel destination	505, 761
tunnel mode	150, 575
tunnel mode modem profile	727

tunnel protection	506, 762
tunnel source	506, 763
tunnel-unused	888
type	839

U

update firmware	115
updateinfo	115
user session-limit	93
username	94, 577
username interface tunnel	578
username isakmp keepalive	579
username isakmp negotiation expire-time	581
username isakmp negotiation retry	580
user-password	713

V

vlan-id	152, 153
vrf	576
vrf-icmp	603
vrrp address	853
vrrp adver-interval	854
vrrp delegated-interface	855
vrrp preempt	855
vrrp priority	856
vrrp track	857
vrrp version	847

W

watch	668, 834
wins-server	431

Si-R GX500 コマンドリファレンス -構成定義編-

P3NK-5912-07Z0

発行日 2023年6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。