



Catalyst Supervisor Engine 32 PISA Cisco IOS ソフトウェア コマンド リファレンス

Catalyst Supervisor Engine 32 PISA Cisco IOS Software Command Reference

リリース 12.2(18)ZY およびそれ以降のリリース

【注意】シスコ製品をご使用になる前に、安全上の注意
(www.cisco.com/jp/go/safety_warning/)をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。
リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコシステムズおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコシステムズおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコシステムズまたはその供給者に知らされていても、それらに対する責任は一切負わないものとします。

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Catalyst Supervisor Engine 32 PISA Cisco IOS ソフトウェア コマンド リファレンス
Copyright © 2007–2009 Cisco Systems, Inc.
All rights reserved.

Copyright © 2007–2010, シスコシステムズ合同会社.
All rights reserved.



CONTENTS

はじめに	xxv
対象読者	xxv
マニュアルの構成	xxv
関連資料	xxvi
表記法	xxvi
マニュアルの入手方法およびテクニカル サポート	xxvii

CHAPTER 1

Supervisor Engine 32 PISA が設定された Catalyst 6500 シリーズ スイッチの コマンドライン インターフェイス	1-1
ヘルプの利用方法	1-1
コマンド オプションの検索	1-2
コマンド モードの概要	1-5
Cisco IOS ユーザ インターフェイス	1-5
コマンドの no 形式および default 形式の使用方法	1-7
CLI スtring検索の使用	1-7
正規表現	1-7
選択	1-10
位置指定	1-10
リコール機能用カッコ	1-11
設定変更の保存	1-11

CHAPTER 2

Supervisor Engine 32 Programmable Intelligent Services Accelerator (PISA) が設定された Catalyst 6500 シリーズ スイッチの Cisco IOS コマンド	2-1
action	2-2
apply	2-4
arp access-list	2-6
attach	2-9
auto-sync	2-11
bgp regexp deterministic	2-12
boot config	2-14
boot system	2-16
bridge-domain	2-19
cd	2-21

channel-group	2-22
channel-protocol	2-25
class-map	2-26
class-map type multicast-flows	2-29
class (policy-map)	2-31
clear cable-diagnostics tdr	2-35
clear catalyst6000 traffic-meter	2-36
clear counters	2-37
clear fm netflow counters	2-39
clear interface gigabitethernet	2-40
clear interface vlan	2-41
clear ip access-template	2-42
clear ip arp inspection log	2-43
clear ip arp inspection statistics	2-44
clear ip auth-proxy watch-list	2-45
clear ip cef epoch full	2-46
clear ip cef inconsistency	2-48
clear ip dhcp snooping	2-49
clear ip flow stats	2-50
clear ip igmp group	2-51
clear ip igmp snooping statistics	2-53
clear ip mroute	2-54
clear ip msdp peer	2-56
clear ip msdp sa-cache	2-57
clear ip msdp statistics	2-58
clear ip pim auto-rp	2-59
clear ip pim snooping statistics	2-60
clear ip pim snooping vlan	2-61
clear lacp counters	2-62
clear logging ip access-list cache	2-63
clear mac-address-table dynamic	2-64
clear mls acl counters	2-66
clear mls cef ip accounting per-prefix	2-68
clear mls cef ipv6 accounting per-prefix	2-69
clear mls ip multicast bidir-rpcache	2-70

clear mls ip multicast group	2-71
clear mls ip multicast statistics	2-72
clear mls nde flow counters	2-73
clear mls netflow	2-74
clear mls qos	2-77
clear mls statistics	2-79
clear mls stats	2-80
clear pagp	2-81
clear platform netint	2-82
clear platform pisa ixp counters	2-83
clear platform pisa np counters	2-85
clear port-security	2-87
clear spanning-tree detected-protocol	2-89
clear top counters interface report	2-91
clear vlan counters	2-92
clock	2-93
collect top counters interface	2-95
control-plane	2-97
copy /noverify	2-99
define interface-range	2-103
diagnostic bootup level	2-105
diagnostic cns	2-107
diagnostic event-log size	2-109
diagnostic monitor	2-110
diagnostic ondemand	2-113
diagnostic schedule test	2-114
diagnostic start	2-117
diagnostic stop	2-119
disconnect qdm	2-120
do	2-121
dot1x default	2-122
dot1x max-req	2-123
dot1x multi-hosts	2-124
dot1x port-control	2-125
dot1x reauthentication	2-127

dot1x system-auth-control	2-128
dot1x timeout	2-129
duplex	2-131
eigrp event-log-size	2-133
encapsulation dot1q	2-134
encapsulation isl	2-135
erase	2-136
errdisable detect cause	2-138
errdisable recovery	2-140
error-detection packet-buffer action	2-142
file verify auto	2-144
flowcontrol	2-145
format	2-147
fsck	2-150
hold-queue	2-153
hw-module boot	2-155
hw-module fan-tray version	2-157
hw-module oversubscription	2-159
hw-module reset	2-161
hw-module shutdown	2-162
hw-module simulate link-up	2-163
instance	2-164
interface	2-166
interface port-channel	2-169
interface range	2-171
interface vlan	2-173
inter-packet gap 6502-mode	2-174
ip access-list hardware permit fragments	2-175
ip arp inspection filter vlan	2-176
ip arp inspection limit	2-178
ip arp inspection log-buffer	2-180
ip arp inspection trust	2-182
ip arp inspection validate	2-183
ip arp inspection vlan	2-185
ip arp inspection vlan logging	2-186

ip auth-proxy max-login-attempts	2-188
ip auth-proxy watch-list	2-189
ip casa	2-191
ip cef load-sharing algorithm	2-192
ip cef table consistency-check	2-193
ip dhcp relay information option trust-all	2-195
ip dhcp relay information trust	2-196
ip dhcp route connected	2-197
ip dhcp snooping	2-198
ip dhcp snooping binding	2-199
ip dhcp snooping database	2-201
ip dhcp snooping information option	2-203
ip dhcp snooping limit rate	2-205
ip dhcp snooping packets	2-206
ip dhcp snooping verify mac-address	2-208
ip dhcp snooping vlan	2-210
ip flow-aggregation cache	2-212
ip flow-cache entries	2-214
ip flow-export	2-216
ip flow-export destination	2-217
ip flow-export hardware version	2-219
ip flow-export interface	2-220
ip flow-export source	2-221
ip flow-export version	2-223
ip flow ingress	2-225
ip flow layer2-switched	2-226
ip forward-protocol turbo-flood	2-227
ip igmp immediate-leave group-list	2-229
ip igmp last-member-query-interval	2-230
ip igmp snooping	2-231
ip igmp snooping explicit-tracking	2-232
ip igmp snooping fast-leave	2-234
ip igmp snooping flooding	2-236
ip igmp snooping I2-entry-limit	2-237
ip igmp snooping last-member-query-interval	2-238

ip igmp snooping limit track	2-240
ip igmp snooping mrouter	2-241
ip igmp snooping querier	2-243
ip igmp snooping rate	2-245
ip igmp snooping report-suppression	2-246
ip igmp snooping source-only-learning age-timer	2-247
ip igmp ssm-map	2-248
ip igmp tcn query	2-250
ip local-proxy-arp	2-251
ip mroute	2-252
ip msdp border	2-254
ip msdp cache-sa-state	2-256
ip msdp default-peer	2-257
ip msdp description	2-259
ip msdp filter-sa-request	2-260
ip msdp mesh-group	2-262
ip msdp originator-id	2-263
ip msdp peer	2-265
ip msdp redistribute	2-267
ip msdp sa-filter in	2-269
ip msdp sa-filter out	2-271
ip msdp sa-request	2-273
ip msdp shutdown	2-275
ip msdp ttl-threshold	2-276
ip multicast boundary	2-277
ip multicast cache-headers	2-279
ip multicast helper-map	2-281
ip multicast mrimo-filter	2-283
ip multicast multipath	2-284
ip multicast netflow	2-285
ip multicast route-limit	2-286
ip multicast-routing	2-287
ip multicast rpf backoff	2-288
ip multicast rpf interval	2-290
ip pim accept-register	2-291

ip pim accept-rp	2-292
ip pim bidir-enable	2-294
ip pim bsr-candidate	2-296
ip pim register-rate-limit	2-298
ip pim register-source	2-299
ip pim rp-announce-filter	2-300
ip pim rp-candidate	2-301
ip pim send-rp-announce	2-303
ip pim send-rp-discovery	2-305
ip pim snooping (global configuration mode)	2-306
ip pim snooping (interface configuration mode)	2-307
ip pim snooping dr-flood	2-308
ip pim snooping suppress sgr-prune	2-309
ip pim spt-threshold	2-310
ip pim ssm	2-311
ip pim state-refresh disable	2-312
ip rgmp	2-313
ip route-cache flow	2-315
ip sticky-arp (global configuration)	2-317
ip sticky-arp (interface configuration)	2-319
ip unnumbered	2-320
ipv6 mfib-cef	2-322
ipv6 mfib hardware-switching	2-323
ipv6 mld snooping	2-324
ipv6 mld snooping explicit-tracking	2-325
ipv6 mld snooping last-member-query-interval	2-327
ipv6 mld snooping limit	2-328
ipv6 mld snooping mrouter	2-330
ipv6 mld snooping querier	2-331
ipv6 mld snooping report-suppression	2-333
ip verify unicast reverse-path	2-334
ip verify unicast source reachable-via	2-336
ip wccp group-listen	2-338
ip wccp redirect	2-340
ip wccp web-cache accelerated	2-342

l2protocol-tunnel	2-344
l2protocol-tunnel cos	2-346
l2protocol-tunnel drop-threshold	2-347
l2protocol-tunnel global drop-threshold	2-349
l2protocol-tunnel shutdown-threshold	2-350
l2 vfi manual	2-352
lacp max-bundle	2-353
lacp port-priority	2-354
lacp rate	2-355
lacp system-priority	2-356
line	2-357
link debounce	2-359
load-interval	2-361
logging event link-status (global configuration)	2-363
logging event link-status (interface configuration)	2-365
logging event subif-link-status	2-366
logging ip access-list cache (global configuration mode)	2-368
logging ip access-list cache (interface configuration mode)	2-370
mac access-list extended	2-372
mac-address-table aging-time	2-375
mac-address-table learning	2-377
mac-address-table limit	2-379
mac-address-table notification mac-move	2-381
mac-address-table notification threshold	2-382
mac-address-table static	2-384
mac-address-table synchronize	2-387
mac packet-classify	2-388
mac packet-classify use vlan	2-390
match	2-391
match protocol	2-393
maxconns (real server configuration submode)	2-394
maximum-paths	2-395
mdix auto	2-396
mdt data	2-398
mdt default	2-399

mdt log-reuse	2-400
media-type	2-401
mkdir disk0:	2-402
mls aclmerge algorithm	2-403
mls acl tcam default-result	2-405
mls acl tcam share-global	2-406
mls aging fast	2-407
mls aging long	2-408
mls aging normal	2-409
mls cef maximum-routes	2-410
mls cef tunnel fragment	2-412
mls erm priority	2-413
mls exclude protocol	2-415
mls flow	2-417
mls ip	2-418
mls ip acl port expand	2-419
mls ip cef accounting per-prefix	2-420
mls ip cef load-sharing	2-421
mls ip cef rate-limit	2-423
mls ip cef rpf hw-enable-rpf-acl	2-425
mls ip cef rpf interface-group	2-426
mls ip cef rpf multipath	2-427
mls ip delete-threshold	2-428
mls ip directed-broadcast	2-429
mls ip inspect	2-431
mls ip install-threshold	2-432
mls ip multicast (global configuration mode)	2-433
mls ip multicast (interface configuration mode)	2-435
mls ip multicast bidir gm-scan-interval	2-436
mls ip multicast connected	2-437
mls ip multicast consistency-check	2-439
mls ip multicast flow-stat-timer	2-441
mls ip multicast replication-mode	2-442
mls ip multicast sso	2-443
mls ip multicast stub	2-444

mls ip multicast threshold	2-446
mls ip nat netflow-frag-l4-zero	2-447
mls ip pbr	2-448
mls ip reflexive ndr-entry tcam	2-449
mls ipv6 acl compress address unicast	2-450
mls ipv6 acl source	2-452
mls mpls (recirculation)	2-453
mls mpls (guaranteed bandwidth traffic engineering)	2-455
mls nde flow	2-457
mls nde interface	2-459
mls nde sender	2-460
mls netflow	2-461
mls netflow maximum-flows	2-462
mls netflow sampling	2-463
mls netflow usage notify	2-465
mls qos (global configuration mode)	2-466
mls qos (interface configuration mode)	2-468
mls qos aggregate-policer	2-469
mls qos bridged	2-471
mls qos channel-consistency	2-472
mls qos cos	2-473
mls qos cos-mutation	2-474
mls qos dscp-mutation	2-475
mls qos exp-mutation	2-476
mls qos loopback	2-477
mls qos map cos-dscp	2-478
mls qos map cos-mutation	2-479
mls qos map dscp-cos	2-481
mls qos map dscp-exp	2-482
mls qos map dscp-mutation	2-483
mls qos map exp-dscp	2-484
mls qos map exp-mutation	2-485
mls qos map ip-prec-dscp	2-487
mls qos map policed-dscp	2-489
mls qos marking ignore port-trust	2-491

mls qos marking statistics	2-492
mls qos mpls trust exp	2-493
mls qos police redirected	2-494
mls qos protocol	2-495
mls qos queueing-only	2-498
mls qos queue-mode mode-dscp	2-499
mls qos rewrite ip dscp	2-500
mls qos statistics-export (global configuration mode)	2-502
mls qos statistics-export (interface configuration mode)	2-503
mls qos statistics-export aggregate-policer	2-505
mls qos statistics-export class-map	2-507
mls qos statistics-export delimiter	2-510
mls qos statistics-export destination	2-511
mls qos statistics-export interval	2-513
mls qos trust	2-514
mls qos trust extend	2-516
mls qos vlan-based	2-518
mls rate-limit all	2-519
mls rate-limit layer2	2-520
mls rate-limit multicast ipv4	2-522
mls rate-limit multicast ipv6	2-524
mls rate-limit unicast acl	2-527
mls rate-limit unicast cef	2-529
mls rate-limit unicast ip	2-531
mls rate-limit unicast l3-features	2-534
mls rate-limit unicast vacl-log	2-535
mls rp ip (global configuration mode)	2-537
mls rp ip (interface configuration mode)	2-538
mls rp ipx (global configuration mode)	2-539
mls rp ipx (interface configuration mode)	2-540
mls rp management-interface	2-541
mls rp nde-address	2-542
mls rp vlan-id	2-543
mls rp vtp-domain	2-544
mls sampling	2-545

mls switching	2-547
mls switching unicast	2-548
mls verify	2-549
mobility	2-551
mode	2-553
mode dot1q-in-dot1q access-gateway	2-555
monitor event-trace (EXEC)	2-558
monitor event-trace (global configuration)	2-561
monitor permit-list	2-564
monitor session	2-566
monitor session type	2-571
mpls l2transport route	2-576
mpls load-balance per-label	2-578
mpls ttl-dec	2-579
mtu	2-580
name (MST configuration submode)	2-582
neighbor	2-584
net	2-585
nsf	2-587
pagp learn-method	2-590
pagp port-priority	2-591
platform ip features pisa	2-593
platform ip features sequential	2-596
platform ipv6 acl icmp optimize neighbor-discovery	2-598
platform scp retry interval	2-599
platform vfi dot1q-transparency	2-600
police (policy map)	2-601
police rate	2-604
policy-map	2-606
port access-map	2-609
port-channel load-balance	2-611
port-channel load-balance mpls	2-613
port-channel min-links	2-615
port-channel per-module load-balance	2-616
power enable	2-617

power inline	2-618
power redundancy-mode	2-620
priority-queue cos-map	2-621
priority-queue queue-limit	2-623
private-vlan	2-624
private-vlan mapping	2-627
private-vlan synchronize	2-629
process-min-time percent	2-630
rcv-queue bandwidth	2-633
rcv-queue cos-map	2-634
rcv-queue queue-limit	2-636
rcv-queue random-detect	2-637
rcv-queue threshold	2-639
reassign	2-641
redundancy	2-642
redundancy force-switchover	2-644
reload	2-645
remote command	2-647
remote login	2-648
remote-span	2-650
reset	2-651
retry	2-652
revision	2-653
rmon alarm	2-654
rmon event	2-656
route-converge-interval	2-658
router	2-659
scheduler allocate	2-660
service counters max age	2-661
service-policy	2-662
service-policy (control-plane)	2-663
session slot	2-665
set cos cos-inner (policy-map configuration)	2-666
set ip dscp (policy-map configuration)	2-668
set ip precedence (policy-map configuration)	2-670

set mpls experimental	2-672
set qos-group	2-673
show	2-674
show adjacency	2-676
show arp	2-678
show asic-version	2-679
show bootflash:	2-680
show bootvar	2-682
show cable-diagnostics tdr	2-685
show catalyst6000	2-687
show cdp neighbors	2-689
show cef interface policy-statistics	2-692
show class-map	2-693
show counters interface	2-694
show diagnostic	2-697
show diagnostic cns	2-702
show diagnostic sanity	2-703
show dot1q-tunnel	2-708
show dot1x	2-709
show dss log	2-712
show environment alarm	2-713
show environment cooling	2-716
show environment status	2-717
show environment temperature	2-720
show eobc	2-722
show erm statistics	2-725
show errdisable detect	2-726
show errdisable flap-value	2-727
show errdisable recovery	2-728
show etherchannel	2-729
show fm features	2-734
show fm inband-counters	2-736
show fm insp	2-737
show fm interface	2-738
show fm ipv6 traffic-filter	2-741

show fm nat netflow data	2-745
show fm reflexive	2-746
show fm summary	2-747
show fm vlan	2-748
show icc	2-750
show idprom	2-752
show interfaces	2-756
show interfaces accounting	2-759
show interfaces capabilities	2-761
show interfaces counters	2-763
show interfaces debounce	2-766
show interfaces description	2-768
show interfaces flowcontrol	2-769
show interfaces private-vlan mapping	2-771
show interfaces status	2-772
show interfaces summary	2-774
show interfaces switchport	2-775
show interfaces switchport backup	2-777
show interfaces transceiver	2-779
show interfaces trunk	2-782
show interfaces unidirectional	2-785
show interfaces vlan mapping	2-787
show ip arp inspection	2-788
show ip arp inspection log	2-791
show ip auth-proxy watch-list	2-793
show ipc	2-794
show ip cache flow	2-796
show ip cache verbose flow	2-800
show ip cef epoch	2-805
show ip cef inconsistency	2-807
show ip cef summary	2-809
show ip cef vlan	2-810
show ip dhcp relay information trusted-sources	2-811
show ip dhcp snooping	2-812
show ip dhcp snooping binding	2-814

show ip dhcp snooping database	2-817
show ip flow-export	2-819
show ip igmp groups	2-821
show ip igmp interface	2-824
show ip igmp snooping explicit-tracking	2-826
show ip igmp snooping mrouter	2-827
show ip igmp snooping rate-limit	2-828
show ip igmp snooping statistics	2-829
show ip igmp udlr	2-831
show ip interface	2-833
show ip mcache	2-836
show ip mds interface	2-838
show ip mpacket	2-840
show ip mroute	2-842
show ip mroute bidirectional	2-847
show ip msdp count	2-849
show ip msdp peer	2-851
show ip msdp sa-cache	2-853
show ip msdp summary	2-855
show ip nhrp	2-856
show ip pim bsr-router	2-859
show ip pim interface df	2-861
show ip pim mdt bgp	2-862
show ip pim mdt history	2-863
show ip pim mdt receive	2-864
show ip pim mdt send	2-866
show ip pim neighbor	2-867
show ip pim rp-hash	2-869
show ip pim rp mapping	2-871
show ip pim snooping	2-873
show ip rpf events	2-876
show ip wccp	2-877
show ipv6 mfib	2-879
show ipv6 mld snooping	2-885
show l2protocol-tunnel	2-887

show l3-mgr	2-889
show lacp	2-891
show logging ip access-list	2-894
show mac-address-table	2-896
show mac-address-table learning	2-902
show memory dead	2-906
show mls asic	2-908
show mls cef	2-909
show mls cef adjacency	2-914
show mls cef exact-route	2-919
show mls cef exception	2-920
show mls cef hardware	2-922
show mls cef inconsistency	2-924
show mls cef ip	2-926
show mls cef ip multicast	2-929
show mls cef ipv6	2-936
show mls cef logging	2-939
show mls cef lookup	2-940
show mls cef maximum-routes	2-941
show mls cef mpls	2-943
show mls cef rpf	2-944
show mls cef statistics	2-945
show mls cef summary	2-946
show mls cef vrf	2-948
show mls df-table	2-950
show mls ip	2-951
show mls ip cef rpf-table	2-954
show mls ip multicast	2-955
show mls ip multicast bidir	2-958
show mls ip multicast rp-mapping	2-959
show mls ip multicast sso	2-960
show mls ip non-static	2-962
show mls ip routes	2-963
show mls ip static	2-965
show mls ip statistics	2-966

show mls nde	2-967
show mls netflow	2-968
show mls netflow ip	2-971
show mls netflow ip sw-installed	2-976
show mls netflow ipv6	2-978
show mls qos	2-981
show mls qos free-agram	2-985
show mls qos maps	2-986
show mls qos mpls	2-988
show mls qos protocol	2-990
show mls qos statistics-export info	2-991
show mls rate-limit	2-993
show mls sampling	2-996
show mls statistics	2-997
show mls table-contention	2-999
show mpls igmp explicit-tracking	2-1001
show mpls msc	2-1002
show mobility	2-1007
show module	2-1009
show monitor permit-list	2-1012
show monitor session	2-1013
show mpls l2transport vc	2-1017
show mpls platform	2-1020
show mpls ttfib	2-1023
show pagp	2-1024
show platform	2-1026
show platform hardware capacity	2-1030
show platform pisa np	2-1036
show platform software ipv6-multicast	2-1043
show platform software pisa fm interface	2-1046
show platform software pisa split-vlan	2-1050
show policy-map	2-1051
show policy-map control-plane	2-1053
show policy-map interface	2-1055
show port-security	2-1057

show power	2-1059
show qdm status	2-1063
show qm-sp port-data	2-1064
show queueing interface	2-1067
show redundancy	2-1069
show rom-monitor	2-1072
show rpc	2-1073
show running-config	2-1075
show scp	2-1077
show snmp mib ifmib ifindex	2-1078
show spanning-tree	2-1080
show spanning-tree mst	2-1086
show standby delay	2-1090
show sup-bootflash	2-1091
show system jumbomtu	2-1094
show tcam counts	2-1095
show tcam interface	2-1097
show tech-support	2-1099
show top counters interface report	2-1102
show udd	2-1104
show version	2-1106
show vlan	2-1108
show vlan access-log	2-1112
show vlan access-map	2-1114
show vlan counters	2-1115
show vlan dot1q tag native	2-1116
show vlan filter	2-1117
show vlan internal usage	2-1119
show vlan mapping	2-1121
show vlan private-vlan	2-1122
show vlan remote-span	2-1124
show vlans	2-1125
show vlan virtual-port	2-1127
show vtp	2-1129
shutdown vlan	2-1133

snmp ifindex clear	2-1134
snmp ifindex persist	2-1136
snmp-server enable traps	2-1138
snmp-server enable traps transceiver type all	2-1140
snmp-server ifindex persist	2-1141
snmp-server source-interface	2-1143
snmp-server trap authentication unknown-context	2-1145
snmp-server trap link switchover	2-1146
spanning-tree backbonefast	2-1147
spanning-tree bpdufilter	2-1148
spanning-tree bpduguard	2-1150
spanning-tree cost	2-1151
spanning-tree etherchannel guard misconfig	2-1152
spanning-tree extend system-id	2-1154
spanning-tree guard	2-1155
spanning-tree link-type	2-1156
spanning-tree loopguard default	2-1157
spanning-tree mode	2-1158
spanning-tree mst	2-1159
spanning-tree mst configuration	2-1160
spanning-tree mst forward-time	2-1162
spanning-tree mst hello-time	2-1163
spanning-tree mst max-age	2-1164
spanning-tree mst max-hops	2-1165
spanning-tree mst pre-standard	2-1166
spanning-tree mst root	2-1168
spanning-tree pathcost method	2-1170
spanning-tree portfast (interface configuration mode)	2-1171
spanning-tree portfast bpdufilter default	2-1173
spanning-tree portfast bpduguard default	2-1175
spanning-tree portfast default	2-1176
spanning-tree port-priority	2-1177
spanning-tree transmit hold-count	2-1178
spanning-tree uplinkfast	2-1179
spanning-tree vlan	2-1180

speed	2-1182
squeeze	2-1185
stack-mib portname	2-1186
standby delay minimum reload	2-1187
standby track	2-1189
standby use-bia	2-1191
storm-control level	2-1192
switchport	2-1194
switchport access vlan	2-1196
switchport autostate exclude	2-1198
switchport backup	2-1200
switchport block unicast	2-1202
switchport capture	2-1203
switchport capture allowed vlan	2-1205
switchport dot1q ethertype	2-1207
switchport mode	2-1209
switchport port-security	2-1211
switchport port-security aging	2-1213
switchport port-security mac-address	2-1215
switchport port-security maximum	2-1217
switchport port-security violation	2-1219
switchport private-vlan host-association	2-1221
switchport private-vlan mapping	2-1222
switchport trunk	2-1224
switchport vlan mapping	2-1227
switchport vlan mapping enable	2-1229
switchport voice vlan	2-1231
sync-restart-delay	2-1233
system flowcontrol bus	2-1234
system jumbomtu	2-1235
tcam priority	2-1237
test cable-diagnostics	2-1239
time-range	2-1241
traceroute mac	2-1243
track interface	2-1247

transceiver type all monitoring	2-1249
tunnel udld address-resolution	2-1250
tunnel udld receive-only	2-1252
tunnel udld send-only	2-1254
udld	2-1256
udld port	2-1258
udld reset	2-1260
udp-port	2-1261
undelete	2-1262
unidirectional	2-1264
upgrade rom-monitor	2-1266
username secret	2-1268
verify	2-1269
vlan (config-VLAN submode)	2-1272
vlan (global configuration mode)	2-1276
vlan access-log	2-1278
vlan access-map	2-1280
vlan database	2-1282
vlan dot1q tag native	2-1284
vlan filter	2-1286
vlan internal allocation policy	2-1288
vlan mapping dot1q	2-1289
vtp	2-1291
wrr-queue	2-1294
wrr-queue cos-map	2-1297
wrr-queue dscp-map	2-1298
wrr-queue queue-limit	2-1299
wrr-queue random-detect	2-1301
wrr-queue shape	2-1303
wrr-queue threshold	2-1305

APPENDIX A

略語 A-1

APPENDIX B

オープンソースソフトウェアについて B-1

INDEX



はじめに

ここでは、このマニュアルの対象読者、構成、および表記法、そして関連資料の入手方法について説明します。

対象読者

このマニュアルは、Supervisor Engine 32 および Programmable Intelligent Services Adapter (PISA) が設定された Catalyst 6500 シリーズ スイッチの設定とメンテナンスを担当する、実務経験のあるネットワーク管理者を対象としています。

マニュアルの構成

このマニュアルは、次の章で構成されています。

章	タイトル	説明
第 1 章	Supervisor Engine 32 PISA が設定された Catalyst 6500 シリーズ スイッチの コマンドライン インターフェイス	Catalyst 6500 シリーズ スイッチの CLI について説明します。
第 2 章	Supervisor Engine 32 Programmable Intelligent Services Accelerator (PISA) が設定された Catalyst 6500 シリーズ スイッチの Cisco IOS コマンド	Supervisor Engine 32 および PISA が設定された Catalyst 6500 シリーズ スイッチ固有の Cisco IOS コマンドの詳細をアルファベット順に説明します。
付録 A	略語	このマニュアルで使用されている略語の定義を示します。
付録 B	オープン ソース ソフトウェアについて	Cisco IOS ソフトウェアの許諾を示します。

関連資料

Catalyst 6500 シリーズ スイッチの Cisco IOS には、次のマニュアルがあります。

- 『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Module Installation Guide*』
- 『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide*』
- 『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software System Message Guide*』
- 『*Release Notes for Cisco IOS Release 12.2ZY on the Supervisor Engine 32 PISA*』

Cisco IOS には、次のマニュアルがあります。

- 『*Configuration Fundamentals Configuration Guide*』
- 『*Command Reference*』

Management Information Base (MIB; 管理情報ベース) の詳細については、次の URL を参照してください。

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンド、コマンド オプションおよびキーワードは太字で示しています。
イタリック体	ユーザが値を指定する引数は、イタリック体で示しています。
[]	角カッコの中の要素は、省略可能です。
{ x y z }	必ずいずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。波カッコは、たとえば {interface interface type} のように、キーワードや引数を囲むのにも使われます。
[x y z]	いずれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
ストリング	引用符を付けない一組の文字。ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングと見なされます。
screen フォント	システムが表示する端末セッションおよび情報は、screen フォントで示しています。
boldface screen フォント	ユーザが入力しなければならない情報は、 boldface screen フォントで示しています。
イタリック体の screen フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
^	^ 記号は、Ctrl キーを表します。たとえば、画面に表示される ^D というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します。
< >	パスワードのように出力されない文字は、山カッコ (<>) で囲んで示しています。

表記法	説明
[]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!, #	コードの先頭に感嘆符 (!) またはポンド記号 (#) がある場合には、コメント行であることを示します。

(注) は、次のように表しています。



(注) 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意は、次のように表しています。



注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。



CHAPTER 1

Supervisor Engine 32 PISA が設定された Catalyst 6500 シリーズ スイッチの コマンド ライン インターフェイス

この章では、Supervisor Engine 32 および Programmable Intelligent Services Accelerator (PISA) の Command-Line Interface (CLI; コマンドライン インターフェイス) の概要と使用方法を説明します。内容は、次のとおりです。

この章は、次のセクションから構成されています。

- 「ヘルプの利用方法」(P.1-1)
- 「コマンド オプションの検索」(P.1-2)
- 「コマンド モードの概要」(P.1-5)
- 「コマンドの no 形式および default 形式の使用方法」(P.1-7)
- 「CLI スtring 検索の使用」(P.1-7)
- 「設定変更の保存」(P.1-11)

Catalyst 6500 シリーズ スイッチ Cisco IOS ソフトウェア コンフィギュレーションの概要については、『*Catalyst Supervisor Engine 32 PISA Cisco IOS ソフトウェア コンフィギュレーション ガイド*』を参照してください。

ヘルプの利用方法

システム プロンプトに疑問符 (?) を入力すると、各コマンド モードで使用できるコマンドのリストが表示されます。コンテキスト ヘルプ機能により、各コマンドの関連キーワードおよび引数のリストも表示できます。

表 1-1 に、コマンド モード、コマンド、キーワード、または引数に対して特定のヘルプ情報を表示できるコマンドの一覧を表示します。

表 1-1 ヘルプの利用方法

コマンド	目的
<code>abbreviated-command-entry?</code>	指定した文字ストリングで始まるコマンドのリストが表示されます (コマンドと疑問符の間にスペースを入れないでください)。
<code>abbreviated-command-entry<Tab></code>	指定したコマンド省略形から、完全なコマンド名が表示されます。

表 1-1 ヘルプの利用方法 (続き)

コマンド	目的
?	特定のコマンドモードで使用できるすべてのコマンドが一覧表示されます。
<i>command ?</i>	コマンドの関連キーワードが一覧表示されます。コマンドと疑問符の間にスペースを入れてください。
<i>command keyword ?</i>	キーワードの関連引数が一覧表示されます。キーワードと疑問符の間にスペースを入れてください。

コマンド オプションの検索

ここでは、コマンド構文を表示する例を示します。コマンド構文には、任意または必須のキーワードが含まれています。コマンドのキーワードを表示するには、コンフィギュレーション プロンプトで、またはコマンドの一部とスペースを入力したあとで、疑問符 (?) を入力します。Catalyst 6500 シリーズ スイッチ ソフトウェアにより、使用できるキーワードのリストと、キーワードの簡単な説明が表示されます。たとえば、グローバル コンフィギュレーション モードで **arap** コマンドの全キーワードを調べたい場合には、**arap ?** と入力します。

表 1-2 では、次のコマンド入力を例にして、コマンド入力の際の疑問符 (?) の使用法を示します。

- **interface gigabitethernet 1/1**
- **channel-group 1 mode auto**

表 1-2 コマンド オプションの検索

コマンド	コメント
Router> enable Password: <password> Router#	enable コマンドおよびパスワードを入力して、特権 EXEC コマンドを開始します。 特権 EXEC モードが開始されると、プロンプトが次のようになります。 Router#
Router# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#	グローバル コンフィギュレーション モードを開始します。 グローバル コンフィギュレーション モードが開始されると、プロンプトが次のようになります。 Router(config)#

表 1-2 コマンド オプションの検索 (続き)

コマンド	コメント
<pre>Router(config)# interface gigabitethernet ? <1-9> GigabitEthernet interface number Router(config)# interface gigabitethernet 1/1 Router(config-if)#</pre>	<p>interface gigabitethernet グローバル コンフィギュレーション コマンドを入力し、設定するギガビット イーサネット インターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。</p> <p>?を入力し、コマンドラインに次に入力する内容を調べます。この例では、<i>module-number/port-number</i> の形式で1~9のインターフェイス番号を入力する必要があります。</p> <p>インターフェイス コンフィギュレーション モードが開始されると、プロンプトが次のようになります。</p> <pre>Router(config-if)#</pre>
<pre>Router(config-if)#? Interface configuration commands: access-expression Build a bridge boolean access expression apollo Apollo interface subcommands appletalk Appletalk interface subcommands arp Set arp type (arpa, probe, snap) or timeout backup Modify backup parameters bandwidth Set bandwidth informational parameter bgp-policy Apply policy propogated by bgp community string bridge-group Transparent bridging interface parameters carrier-delay Specify delay for interface transitions cdp CDP interface subcommands channel-group Etherchannel/port bundling configuration clns CLNS interface subcommands cmns OSI CMNS custom-queue-list Assign a custom queue list to an interface decnet Interface DECnet config commands default Set a command to its defaults delay Specify interface throughput delay description Interface specific description dlsd DLSw interface subcommands dspu Down Stream PU exit Exit from interface configuration mode fair-queue Enable Fair Queuing on an Interface flowcontrol Configure flow operation. fras DLC Switch Interface Command help Description of the interactive help system hold-queue Set hold queue depth ip Interface Internet Protocol config commands ipx Novell/IPX interface subcommands isis IS-IS commands iso-igrp ISO-IGRP interface subcommands . . . Router(config-if)#</pre>	<p>?を入力し、ギガビット イーサネット インターフェイスに対して使用できるすべてのインターフェイス コンフィギュレーション コマンドのリストを表示します。</p>

表 1-2 コマンド オプションの検索 (続き)

コマンド	コメント
<pre>Router(config-if)# channel-group ? group channel-group of the interface Router(config-if)#channel-group</pre>	<p>コントローラを設定するコマンドを入力します。この例では、channel-group コマンドを入力します。</p> <p>? を入力し、コマンドラインに次に入力する内容を調べます。この例では、group キーワードを入力する必要があります。</p> <p><cr> が表示されていないので、コマンドを完成するためにはさらに情報を入力する必要があります。</p>
<pre>Router(config-if)# channel-group ? <1-256> Channel group number Router(config-if)#channel-group</pre>	<p>group キーワードを入力したら、? を入力し、コマンドラインに次に入力する内容を調べます。この例では、チャンネル グループ番号 1 ~ 256 を入力する必要があります。</p> <p><cr> が表示されていないので、コマンドを完成するためにはさらに情報を入力する必要があります。</p>
<pre>Router(config-if)# channel-group 1 mode ? mode Etherchannel Mode of the interface Router(config-if)#</pre>	<p>チャンネル グループ番号を入力したら、? を入力し、コマンドラインに次に入力する内容を調べます。この例では、mode キーワードを入力する必要があります。</p> <p><cr> が表示されていないので、コマンドを完成するためにはさらに情報を入力する必要があります。</p>
<pre>Router(config-if)# channel-group 1 mode ? auto Enable PAgP only if a PAgP device is detected desirable Enable PAgP unconditionally on Enable Etherchannel only Router(config-if)#</pre>	<p>mode キーワードを入力したら、? を入力し、コマンドラインに次に入力する内容を調べます。この例では、auto、desirable、または on キーワードを入力する必要があります。</p> <p><cr> が表示されていないので、コマンドを完成するためにはさらに情報を入力する必要があります。</p>

表 1-2 コマンドオプションの検索 (続き)

コマンド	コメント
Router (config-if) # channel-group 1 mode auto ? <cr> Router (config-if) #	この例では、 auto キーワードを使用します。 auto キーワードを入力したら、 ? を入力し、コマンドラインに次に入力する内容を調べます。 <cr> が表示されたので、 Return を押せばコマンドを完成できます。さらにキーワードを一覧表示する場合は、キーワードを追加して Return を押し、コマンドを完成させることができます。
Router (config-if) # channel-group 1 mode auto Router (config-if) #	この例では、 Return を押して、コマンドを完成します。

コマンドモードの概要

ここでは、Cisco IOS ユーザ インターフェイスのコマンドモードについて説明します。

Cisco IOS ユーザ インターフェイス

Cisco IOS のユーザ インターフェイスは、いくつかの異なるモードに分けられます。現在実行しているモードによって、使用できるコマンドが異なります。システムプロンプトに疑問符 (?) を入力すると、各コマンドモードで使用できるコマンドのリストを表示できます。

Catalyst 6500 シリーズ スイッチ上でセッションを開始するときには、ユーザモード (ユーザ EXEC モードとも呼ばれる) から始めます。EXEC モードで使用できるコマンドサブセットは限定されています。すべてのコマンドにアクセスするには、特権 EXEC モードを開始する必要があります。特権 EXEC モードを開始するには、通常、パスワードを入力する必要があります。特権 EXEC モードからは、任意の EXEC コマンドを実行できるほか、グローバル コンフィギュレーション モードを開始できます。ほとんどの EXEC コマンドは、ある項目の現在のステータスを表示する **show** コマンドや、カウンタまたはインターフェイスをクリアする **clear** コマンドなどの 1 回限りのコマンドです。Catalyst 6500 シリーズ スイッチを再起動した場合、EXEC コマンドは保存されません。

コンフィギュレーション モードでは、実行コンフィギュレーションを変更できます。変更したコンフィギュレーションを保存しておけば、Catalyst 6500 シリーズ スイッチの再起動後も、コマンドが保存されます。コンフィギュレーション モードを使用するには、最初にグローバル コンフィギュレーション モードを開始します。グローバル コンフィギュレーション モードから、インターフェイス コンフィギュレーション モード、サブインターフェイス コンフィギュレーション モード、および各種のプロトコル特定のモードを開始できます。

ROM モニタ モードは、Catalyst 6500 シリーズ スイッチが正常に起動しないときに使用する独立したモードです。Catalyst 6500 シリーズ スイッチまたはアクセス サーバの起動時に、有効なシステムイメージが検出されない場合、またはスタートアップ時にコンフィギュレーション ファイルが破壊されている場合、ROM モニタ モードが開始されることがあります。

表 1-3 に、Cisco IOS ソフトウェアの主要なコマンドモードの概要を示します。

表 1-3 主要コマンド モードの概要

コマンド モード	アクセス方式	プロンプト	終了方法
ユーザ EXEC	ログインします。	Router>	logout コマンドを入力します。
特権 EXEC	ユーザ EXEC モードで、 enable EXEC コマンドを入力します。	Router#	ユーザ EXEC モードに戻るには、 disable コマンドを入力します。 グローバル コンフィギュレーション モードを開始するには、 configure terminal 特権 EXEC コマンドを入力します。
グローバル コンフィギュレーション	特権 EXEC モードで、 configure terminal 特権 EXEC コマンドを入力します。	Router(config)#	特権 EXEC モードに戻るには、 exit コマンドまたは end コマンドを入力するか、 Ctrl+Z キーを押します。 インターフェイス コンフィギュレーション モードを開始するには、 interface コンフィギュレーション コマンドを入力します。
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードで、 interface コマンドを入力し、インターフェイスを指定します。	Router(config-if)#	グローバル コンフィギュレーション モードに戻るには、 exit コマンドを入力します。 特権 EXEC モードに戻るには、 exit コマンドを入力するか、 Ctrl+Z キーを押します。 サブインターフェイス コンフィギュレーション モードを開始するには、 interface コマンドを入力し、サブインターフェイスを指定します。
サブインターフェイス コンフィギュレーション	インターフェイス コンフィギュレーション モードで interface コマンドを入力し、サブインターフェイスを指定します。	Router(config-subif)#	グローバル コンフィギュレーション モードに戻るには、 exit コマンドを入力します。 特権 EXEC モードに戻るには、 end コマンドを入力するか、 Ctrl+Z キーを押します。
ROM モニタ	特権 EXEC モードで、 reload EXEC コマンドを入力します。システムの起動後、60 秒以内に Break キーを押します。	Rommon>	ROM モニタ モードを終了するには、 boot コマンドを入力してイメージをリロードする必要があります。ファイル名または他の起動命令を指定せずに boot コマンドを使用すると、システムはデフォルトのフラッシュ イメージ (オンボード フラッシュ メモリ上の最初のイメージ) から起動します。また、特定のフラッシュ イメージから起動するように指定することもできます (boot system flash filename コマンドを使用)。

コマンド モードの詳細については、『*Configuration Fundamentals Configuration Guide*』の「Using the Command Line Interface」の章を参照してください。



(注)

グローバル コンフィギュレーション モードまたは他のモードで、EXEC レベルの Cisco IOS コマンド (**show**、**clear**、**debug** コマンド) を入力するには、EXEC コマンドの前に **do** コマンドを入力します。このコマンドの使用方法については、**do** コマンドを参照してください。

コマンドの no 形式および default 形式の使用法

ほとんどすべてのコンフィギュレーション コマンドには **no** 形式があります。通常、コマンドの機能をディセーブルにする場合に **no** 形式のコマンドを指定します。ディセーブルにした機能を再びイネーブルにしたり、デフォルトでディセーブルに設定されている機能をイネーブルにしたりするには、**no** キーワードを付けないコマンドを使用します。たとえば、IP ルーティングはデフォルトでイネーブルに設定されています。IP ルーティングをディセーブルにするには、**noiprouting** コマンドを指定します。IP ルーティングを再びイネーブルにするには、**ip routing** コマンドを指定します。このマニュアルでは、コンフィギュレーション コマンドの完全な構文およびコマンドの **no** 形式について説明します。

コンフィギュレーション コマンドには **default** 形式もあります。**default** 形式のコマンドは、コマンドの機能をデフォルト設定に戻します。ほとんどのコマンドはデフォルトでディセーブルに設定されているので、**default** 形式は **no** 形式と同じ結果になります。ただし、一部のコマンドはデフォルトでイネーブルに設定され、変数にデフォルト値が割り当てられています。このようなコマンドを **default** 形式で実行すると、コマンドの変数にデフォルト値が再設定されます。このマニュアルでは、コマンドが **no** 形式と異なる場合のコマンドの **default** 形式について説明します。

CLI スtring検索の使用

コマンド出力のパターンは String と呼ばれます。CLI String 検索機能を使用すれば、**show** または **more** コマンド出力の検索およびフィルタリングを行うことができます。また、**--More--** プロンプトで検索およびフィルタリングを行うことができます。この機能は、大量の出力をソートする必要がある場合や、出力から不要な情報を除外する場合に役立ちます。

検索機能を使用すれば、フィルタリングされていない出力で、指定された正規表現を含むものを最初の行から始めることができます。コマンド 1 つあたり、最大 1 つのフィルタを指定できます。または **--More--** プロンプトから新しい検索を開始できます。

正規表現は、ソフトウェアが **show** または **more** コマンド出力のマッチングを行うために使うパターン（句、番号、またはより複雑なパターン）です。正規表現は、大文字と小文字を区別し、複雑な一致要件を可能にします。単純な正規表現の例は、**Serial**、**misses**、**138** などです。複合正規表現の例は、**00210...**、**(is)**、**[Oo]utput** などです。

3 種類のフィルタリングを行うことができます。

- 指定した正規表現を含む行で出力を始めるには、**begin** キーワードを使用します。
- 指定した正規表現を含む出力行を含めるには、**include** キーワードを使用します。
- 指定した正規表現を含む出力行を除外するには、**exclude** キーワードを使用します。

次に、このフィルタリングされた出力を **--More--** プロンプトで検索できます。



(注)

CLI String 検索機能を使用しても、以前の出力へ逆方向に検索またはフィルタリングできません。フィルタリングは、CLI への HTTP アクセスで指定できません。

正規表現

正規表現は、コマンド出力内の同じ 1 つの文字に一致する 1 つの文字でもかまいませんし、コマンド出力内の同じ複数の文字に一致する複数の文字でもかまいません。このセクションでは、単一文字パターンおよび複数文字パターンを作成する方法、および繰り返し指定、選択、位置指定、およびカッコを用いたより複雑な正規表現を作成する方法について説明します。

単一文字パターン

最も単純な正規表現は、コマンド出力の同じ 1 つの文字と一致する単一文字です。単一文字パターンとしては任意の文字 (A ~ Z, a ~ z) または数字 (0 ~ 9) を使用できます。他のキーボード文字 (! や ~ など) も単一文字パターンとして使用できますが、正規表現として用いられた場合に特別な意味を持つキーボード文字もあります。表 1-4 に特別な意味を持つキーボード文字を一覧表示します。

表 1-4 特別な意味を持つ文字

文字	特別な意味
.	スペースを含む任意の単一文字と一致します。
*	0 個または複数のパターンのシーケンスに一致します。
+	1 個または複数のパターンのシーケンスに一致します。
?	0 または 1 回のパターンと一致します。
^	ストリングの最初と一致します。
\$	ストリングの最後と一致します。
_ (アンダースコア)	カンマ (,), 左波カッコ ({), 右波カッコ (}), 左カッコ ([), 右カッコ (]), ストリングの最初、ストリングの最後、またはスペースと一致します。

これらの特殊文字を単一文字パターンとして入力する場合は、各文字の前にバックスラッシュ (\) を置いて特別な意味を持たないようにしてください。次の例は、それぞれドル記号、アンダースコア、プラス記号に一致する単一文字パターンです。

`\$ _ \+`

一連の単一文字パターンを指定して、コマンド出力とのマッチングを行うことができます。たとえば、a、e、i、o、u のうちの 1 つを含むストリングに一致する正規表現を作成できます。パターンマッチングが成功するには、これらの文字のうちの 1 つだけがストリングに存在しなくてはなりません。一連の単一文字パターンを指定するには、単一文字パターンを角カッコ ([]) で囲みます。たとえば、

`[aeiou]`

小文字アルファベットの 5 つの母音のうちの任意の 1 文字と一致します。

`[abcdABCD]`

小文字または大文字アルファベットの最初の 4 文字のうち、任意の 1 文字と一致します。

ダッシュ (-) で区切って範囲の終点だけを入力することにより、範囲を簡略化できます。上記の範囲は次のように簡略化できます。

`[a-dA-D]`

範囲に単一文字パターンとしてダッシュを追加する場合は、もう 1 つダッシュを追加して、その前にバックスラッシュを入力します。

`[a-dA-D\-]`

範囲に単一文字パターンとして右角カッコ (]) を含めることもできます。次のように入力してください。

`[a-dA-D\-])]`

上記の例は、大文字または小文字のアルファベットの最初の 4 文字のうち、任意の 1 文字、ダッシュ、または右角カッコに一致します。

範囲の最初にカレット (^) を含めることにより、範囲の一致を逆にできます。次の例では、列挙された文字以外の任意の文字に一致します。

`[^a-dqsv]`

次の例では、右角カッコ (]) または `d` という文字以外の任意の文字に一致します。

`[^\d]`

複数文字パターン

正規表現を作成する場合、複数の文字を含むパターンを指定することもできます。文字、数字、または特別な意味を持たないキーボード文字を組み合わせて複数文字パターン正規表現を作成できます。たとえば、`a4%` は複数文字正規表現です。特別な意味を持つキーボード文字に、その特別な意味を持たせないようにする場合には、キーボード文字の前にバックスラッシュを入力します。

複数文字パターンでは、順序が大切です。正規表現 `a4%` は、`a` という文字のあとに `4` が続き、そのあとに `%` 記号が続く文字と一致します。String に `a4%` という文字がその順序で含まれていない場合、パターン マッチングは失敗となります。この複数文字正規表現において、

`a.`

は、ピリオド文字の特別な意味を使用し、`a` という文字のあとに任意の文字が 1 つ来る String と一致します。この例では、`ab`、`a!`、または `a2` という String はすべてこの正規表現での有効な一致となります。

ピリオド文字の前にバックスラッシュを入力することにより、ピリオド文字に特別な意味を持たせないようにできます。次の表現では、

`a\.`

という String だけが、この正規表現に一致します。

すべての文字、すべての数字、すべてのキーボード文字、または文字、数字、および他のキーボード文字の組み合わせを含む、複数文字正規表現を作成できます。次の例はすべて有効な正規表現です。

`telebit 3107 v32bis`

繰り返し指定

ある特殊文字を単一および複数文字パターンとともに使用することにより、指定された正規表現の繰り返しと一致する複雑な正規表現を作成できます。表 1-5 に、正規表現の「繰り返し」を指定する特殊文字を一覧表示します。

表 1-5 繰り返し指定として使用される特殊文字

文字	説明
*	0 個以上の単一または複数文字パターンに一致します。
+	1 つ以上の単一または複数文字パターンに一致します。
?	単一または複数文字パターンの 0 回または 1 回の繰り返しに一致します。

次の例は、`a` という文字の任意の回数 (0 を含む) に一致します。

`a*`

次のパターンでは、String 内で最低 1 つの `a` という文字が一致している必要があります。

`a+`

次のパターンでは、String `bb` または `bab` に一致します。

`ba?b`

次の String では、任意の数の アスタリスク (*) に一致します。

`**`

複数文字パターンで繰り返し指定を使用する場合は、パターンをカッコで囲みます。次の例では、パターンは任意の数の複数文字 String `ab` に一致します。

`(ab)*`

より複雑な例として、次のパターンは、1 つまたは複数の英数字ペアに一致します (ただし、0、つまり空 String には一致しません)。

`([A-Za-z][0-9])+`

繰り返し指定 (*、+、または ?) を使用している一致の記述順序では、最も長い構造から先に一致します。ネストされた構造でのマッチングは外側から内側へ行われます。連結構造では、構造の左側からマッチングされます。この正規表現は番号の前に文字が指定されるため、`A9b3` には一致しますが、`9Ab3` には一致しません。

選択

選択を使用すると、String とのマッチングに選択パターンを指定できます。選択パターンは、縦棒 (|) で分離します。選択肢のうちの 1 つだけが、String と一致できます。たとえば、正規表現

`codex | telebit`

は、`codex` または `telebit` という String と一致させることができますが、`codex` と `telebit` の両方とは一致しません。

位置指定

String の最初または最後に対して正規表現パターンのマッチングを行うことができます。つまり、String の最初または最後に固有のパターンが含まれるよう指定できます。表 1-6 に示す特殊文字を用いた String の一部に対して、これらの正規表現の「位置指定」を行います。

表 1-6 位置指定に用いられる特殊文字

文字	説明
<code>^</code>	String の最初と一致します。
<code>\$</code>	String の最後と一致します。

次の正規表現が String と一致するのは、String が `abcd` で始まるときだけです。

`^abcd`

対照的に、次の表現は、`a`、`b`、`c`、`d` という文字以外のすべての単一文字に一致します。

`[^abcd]`

次の例では、正規表現は `.12` で終わる String と一致します。

`$.12`

これらの位置指定文字を特殊文字アンダースコア (`_`) と対比させてください。アンダースコアは、String の始め (^)、String の終わり (\$)、カッコ ()、スペース ()、波カッコ ({ })、カンマ (,)、またはアンダースコア (_) と一致します。アンダースコア文字を使用した場合、パターンは String のどの位置に存在していてもかまわないという指定になります。

たとえば、

```
_1300_
```

は、文字列内の任意の位置に 1300 が含まれる文字列に一致します。文字列の 1300 の前後にスペース、波カッコ、カンマ、またはアンダースコアを置くことができます。たとえば、

```
{1300_
```

は、正規表現に一致しますが、21300 および 13000 は一致しません。

アンダースコア文字を用いれば、

```
^1300$ ^1300(space) (space)1300 {1300 ,1300, {1300} ,1300, (1300
```

のような長い正規表現リストを以下に置き換えることができます。

```
_1300_
```

リコール機能用カッコ

「繰り返し指定」(P.1-9) に示すように、カッコを複数文字正規表現とともに使用して、パターンを繰り返すことができます。また、単一文字パターンまたは複数文字パターンを囲むカッコを使用して、正規表現の他の場所で使用するパターンを記憶させることができます。

以前のパターンをリコールするための正規表現を作成するには、リコールする特定のパターンを示すカッコ、バックスラッシュ (\)、整数という順序で入力します。これにより、記憶されたパターンを再び使用できます。整数は、正規表現パターン内のカッコの繰り返し数を示します。正規表現内に複数のリコールパターンがある場合、\1 は最初のリコールパターン、\2 は 2 番めのリコールパターン、というようになります。

次の正規表現は、リコール機能用カッコを使用します。

```
a(.)bc(.)\1\2
```

この正規表現は、a のあとに任意の文字が来て (文字 1 と呼ぶ)、その次に bc が来て、その次に任意の文字 (文字 2 と呼ぶ) が来て、その次に再び文字 1 が来て、その次に再び文字 2 が来る文字列と一致します。この正規表現は aZbcTZT と一致します。ソフトウェアは、文字 1 が Z で文字 2 が T で、正規表現のあとに再び Z および T が使用されることを記憶します。

設定変更の保存

設定変更をスタートアップ コンフィギュレーションに保存して、システムのリロードの際や停電時に設定変更が失われないようにするには、次のコマンドを入力します。

```
Router# copy system:running-config nvram:startup-config  
Building configuration...
```

設定を保存するには 1 ~ 2 分かかります。設定が保存されたあと、次の出力が表示されます。

```
[OK]  
Router#
```

通常のプラットフォームでは、この手順により設定が NVRAM に保存されます。クラス A フラッシュファイル システム プラットフォームでは、この手順により、COkuNFIG_FILE 環境変数で指定された場所に設定が保存されます。CONFIG_FILE 環境変数のデフォルトは NVRAM です。



CHAPTER 2

Supervisor Engine 32 Programmable Intelligent Services Accelerator (PISA) が設定された Catalyst 6500 シリーズ スイッチの Cisco IOS コマンド

この章では、Supervisor Engine 32 および PISA が設定された Catalyst 6500 シリーズ スイッチ固有の Cisco IOS コマンド一覧をアルファベット順に紹介します。このマニュアルに記載されていない Cisco IOS コマンドの詳細については、次の最新の CiscoIOS マニュアルを参照してください。

- 『*Cisco IOS Release 12.2 Configuration Fundamentals Configuration Guide*』
- 『*Cisco IOS Release 12.2 Command Reference*』

action

パケットの **action** 句を設定するには、**action** コマンドを使用します。action 句を削除するには、このコマンドの **no** 形式を使用します。

```
action {{drop [log]} | {forward [capture]} | {redirect {interface interface-number}} |
      {port-channel channel-id} {interface interface-number} | {port-channel channel-id}
      ...}
```

```
no action {{drop [log]} | {forward [capture]} | {redirect {interface interface-number}} |
          {port-channel channel-id} {interface interface-number} | {port-channel channel-id}
          ...}
```

シンタックスの説明

drop	パケットを廃棄します。
log	(任意) 廃棄されたパケットをソフトウェアに記録します。
forward	パケットを宛先に転送します (ハードウェアによりスイッチングされます)。
capture	(任意) 転送されたパケットのキャプチャ ビットを設定し、キャプチャ機能がイネーブルであるポートでもパケットを受信できるようにします。
redirect interface	指定したインターフェイスにパケットをリダイレクトします。有効値は、 fastethernet 、 gigabithernet 、および tengigabithernet です。その他の有効値については、「使用上のガイドライン」を参照してください。
interface-number	モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
port-channel channel-id	トラフィックをリダイレクトするポート チャンネルを指定します。有効値は 1 ~ 256 の範囲の最大 64 個の値です。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

virtual LAN (VLAN; 仮想 LAN) アクセス マップ サブモード

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

interface-number 引数はモジュールおよびポート番号を指定します。**interface-number** の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

各リダイレクト アクションにより、最大 5 つの宛先インターフェイスのリストを指定できます。リダイレクト アクションで使用できるインターフェイス リストも、最大 255 個に制限されています。

リダイレクト アクションは、次の例に示すように、単一のインターフェイスではなくインターフェイスのリストをサポートします。

```
[...] {redirect {{ethernet | gigabitethernet | tengigabitethernet} slot/port} | {port-channel
channel-id}}
```

action 句は、マッチングが行われるときに実施すべきアクションを指定します。

転送されたパケットは、適用された Cisco IOS access control list (ACL; アクセス制御リスト) による制約を受けます。**capture** キーワードは、VLAN access control list (VACL; VLAN アクセス制御リスト) によって転送されたパケットにキャプチャ ビットを設定します。キャプチャ機能がイネーブルであるポートは、VACL によって転送され、キャプチャ ビットが設定されたパケットを受信できます。キャプチャできるのは、VACL によって転送され、キャプチャ ビットが設定されたパケットだけです。

log キーワードが指定されている場合、廃棄されたパケットがソフトウェアで記録されます。記録できるのは廃棄された Internet Protocol (IP) パケットだけです。**redirect** キーワードでは、物理インターフェイスまたは EtherChannel インターフェイスのいずれかを 5 つまで指定できます。EtherChannel メンバーをリダイレクト インターフェイスに指定できません。

WAN インターフェイスの VACL がサポートしているのは、**action forward capture** コマンドだけです。

VACL 内で有効な action 句は、転送、廃棄、キャプチャ、またはリダイレクトです。トラフィックのロギングもできます。WAN インターフェイスに適用された VACL は、リダイレクトアクションまたはログアクションをサポートしません。

リダイレクト インターフェイスは VACL マップが設定されている VLAN 内になくはなりません。

VLAN アクセス マップでは、パケット タイプ (IP、Internetwork Packet Exchange (IPX)、または Media Access Control (MAC; メディア アクセス制御)) が設定された ACL が 1 つでもあれば、そのパケット タイプのデフォルトアクションは **drop** (拒否) です。

ACL にパケット タイプが設定されていない場合は、そのパケット タイプのデフォルトアクションは **forward** (許可) です。

ACL にパケット タイプが設定されており、ACL が空または未定義の場合、設定されたアクションが、そのパケット タイプに適用されます。

例

次に、廃棄およびログ アクションを定義する例を示します。

```
Router(config-access-map)# action drop log
Router(config-access-map)#
```

次に、転送アクションを定義する例を示します。

```
Router(config-access-map)# action forward
Router(config-access-map)#
```

関連コマンド

コマンド	説明
match	VLAN アクセス マップ シーケンスの ACL を 1 つまたは複数選択して、 match 句を指定します。
show vlan access-map	VLAN アクセス マップの内容を表示します。
vlan access-map	VLAN アクセス マップを作成するか、VLAN アクセス マップ コマンド モードを開始します。

apply

提示された新規 VLAN データベースの実装、データベース設定番号の増分、nonvolatile RAM (NVRAM; 不揮発性 RAM) への設定番号の保存、および管理ドメイン全体への設定番号の伝播を行うには、**apply** コマンドを使用します。

apply

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

VLAN コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

apply コマンドは、VLAN データベース モードを開始したあとに行った設定変更を実装し、これを実行コンフィギュレーションに使用します。このコマンドにより、VLAN データベース モードが開始されます。

Catalyst 6500 シリーズ スイッチが VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) クライアント モードである場合、このコマンドは使用できません。

VLAN データベース変更が行われたかどうかを確認するには、特権 EXEC モードで **show vlan** コマンドを入力します。

例

次に、提示された新規の VLAN データベースを実装し、これを現在のデータベースとして認識する例を示します。

```
Router(config-if-vlan)# apply
Router(config-if-vlan)#
```

関連コマンド

コマンド	説明
abort	提示された新しい VLAN データベースを放棄します。
exit	提示された新しい VLAN データベースを実装します。
reset	提示された新しい VLAN データベースを放棄し、VLAN コンフィギュレーション モードのまま新しいデータベースをリセットして、現在の VLAN データベースに一致させます。
show vlan	VLAN 情報を表示します。

コマンド	説明
<code>shutdown vlan</code>	指定 VLAN でローカルトラフィックをシャットダウンします。
<code>vtp</code>	グローバル VTP ステートを設定します。

arp access-list

Address Resolution Protocol (ARP; アドレス解決プロトコル) インスペクションおよび Quality of Service (QoS; サービス品質) フィルタリング用に ARP ACL を設定し、ARP ACL コンフィギュレーション サブモードを開始するには、**arp access-list** コマンドを使用します。ARP ACL を削除するには、このコマンドの **no** 形式を使用します。

arp access-list *name*

no arp access-list *name*

シンタックスの説明

<i>name</i>	アクセス リストの名前
-------------	-------------

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ARP ACL コンフィギュレーション サブモードが開始されると、**permit** または **deny** 句を追加して、フローに対する QoS を許可または拒否できます。次の構文は、QoS フィルタリングの ARP QoS ACL コンフィギュレーション サブモードで使用できます。ポリシーマップがインターフェイスに付加されると、他のすべての設定は拒否されます。

{permit | deny} {ip {any | {host sender-ip [sender-ip-mask]}}} {mac any}

no {permit | deny} {ip {any | {host sender-ip [sender-ip-mask]}}} {mac any}

permit	QoS をフローに適用するように指定します。
deny	この access control entry (ACE; アクセス制御エントリ) に一致するトラフィックに設定された QoS アクションを省略します。
ip	IP ARP パケットを指定します。
any	任意の IP ARP パケットを指定します。
host sender-ip	ホストの送信側の IP アドレスを指定します。
sender-ip-mask	(任意) ホストの送信側のワイルドカード マスク
mac any	MAC レイヤの ARP トラフィックを指定します。
no	ARP ACL から ACE を削除します。

ARP ACL コンフィギュレーション サブモードを開始すると、ARP インспекションで次のコンフィギュレーション コマンドが使用可能になります。

- **default** : コマンドをデフォルトに設定します。デフォルト設定を設定するには、**deny** および **permit** キーワードおよび引数を使用できます。
- **deny** : 拒否するパケットを指定します。
- **exit** : ACL コンフィギュレーション モードを終了します。
- **no** : コマンドを否定するか、またはデフォルトを設定します。
- **permit** : 転送するパケットを指定します。

一部の一致基準に基づいて、ARP パケットを転送または廃棄する **permit** 句または **deny** 句を設定するには、**permit** または **deny** キーワードを入力します。**permit** および **deny** キーワードの構文は、次のとおりです。

```
{permit | deny} ip {any | {host {sender-ip | {sender-ip sender-ip-mask}}}} mac {any | {host {sender-mac | {sender-mac sender-mac-mask}}}} [log]
```

```
{permit | deny} request ip {any | {host {sender-ip | {sender-ip sender-ip-mask}}}} mac {any | {host {sender-mac | {sender-mac sender-mac-mask}}}} [log]
```

```
{permit | deny} response ip {any | {host {sender-ip | {sender-ip sender-ip-mask}}}} [{any | {host {target-ip | {target-ip target-ip-mask}}}}] mac {any | {host {sender-mac | {sender-mac sender-mac-mask}}}} [any | {host {target-mac | {target-mac target-mac-mask}}}}] [log]
```

permit	転送するパケットを指定します。
deny	拒否するパケットを指定します。
ip	送信側の IP アドレスを指定します。
any	任意の送信側の IP アドレスを指定します。
host	単一の送信側ホストを指定します。
<i>sender-ip</i>	ホストの送信側の IP アドレス
<i>sender-ip-mask</i>	ホストの送信側のワイルドカード マスク
mac any	任意の MAC アドレスを指定します。
mac host	単一の送信側ホストの MAC アドレスを指定します。
<i>sender-mac</i>	ホストの送信側の MAC アドレス
<i>sender-mac-mask</i>	ホストの送信側のワイルドカード マスク
log	(任意) 一致するログを指定します。
request	ARP 要求を指定します。
response	ARP 応答を指定します。
any	(任意) 任意のターゲット アドレスを指定します。
host	(任意) 単一のターゲット ホストを指定します。
<i>target-mac</i>	ターゲット ホストの MAC アドレス
<i>target-mac-mask</i>	ターゲット ホストのサブネット マスク

request または **response** キーワードを指定せずに **ip** キーワードを入力すると、この設定は要求および応答の両方に適用されます。

ARP ACL を定義すると、**ip arp inspection filter** コマンドを使用する VLAN の ARP インспекションに ARP ACL を適用できます。

着信 ARP パケットは ARP アクセス リストと比較され、このアクセス リストが許可した場合にだけ許可されます。アクセス リストが明示的な拒否によりパケットを拒否した場合、これらのパケットは廃棄されます。パケットが暗黙的な拒否により拒否された場合、これらのパケットは **Dynamic Host Configuration Protocol (DHCP) バインディング** のリストに照合されます。ただし、アクセス リストがスタティックであるか、またはパケットがバインディングと比較されない場合は除きます。

ARP アクセス リストが **Dynamic ARP Inspection (DAI; ダイナミック ARP インспекション)** の VLAN に適用される場合、IP と Ethernet 間の MAC バインディングだけを含む ARP パケットが ACL と比較されます。他のすべてのパケット タイプは、確認されずに着信 VLAN でブリッジされます。

ACL エントリは入力順にスキャンされます。最初に一致したエントリが使用されます。パフォーマンスを高めるには、ACL の始めの方に、最もよく使用されるエントリを置きます。

リストの最後に明示的な **permit ip any mac any** エントリを含めなかった場合、ACL の最後には暗黙的な **deny any ip mac any** エントリが存在します。

新しいエントリはすべて既存のリストの最後に置かれます。リストの中間にエントリを追加できません。

例

次に、新しい ARP ACL を作成するか、または既存の ARP ACL のサブモードを開始する例を示します。

```
Router(config)# arp access-list arpacl22
Router(config-arp-nacl)#
```

次に、QoS を拒否し、MAC レイヤの ARP トラフィックを許可する、**arp_filtering** と名付けられた ARP ACL を作成する例を示します。

```
Router(config)# arp access-list arp_filtering
Router(config-arp-nacl)# permit ip host 1.1.1.1 mac any
Router(config-arp-nacl)# deny any ip mac any
Router(config-arp-nacl)#
```

関連コマンド

コマンド	説明
show arp	ARP テーブルに関する情報を表示します。

attach

リモートから特定のモジュールに接続するには、**attach** コマンドを使用します。

attach *num*

シンタックスの説明	<i>num</i> モジュール番号。有効値については、「使用上のガイドライン」を参照してください。				
デフォルト	このコマンドにはデフォルト設定がありません。				
コマンドモード	特権 EXEC				
コマンドの履歴	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>12.2(18)ZY</td> <td>このコマンドのサポートが追加されました。</td> </tr> </tbody> </table>	リリース	変更内容	12.2(18)ZY	このコマンドのサポートが追加されました。
リリース	変更内容				
12.2(18)ZY	このコマンドのサポートが追加されました。				

使用上のガイドライン



注意

attach または **remote login** コマンドを入力し、スイッチから別のコンソールにアクセスする場合、グローバルまたはインターフェイス コンフィギュレーション モードのコマンドを入力すると、スイッチがリセットすることがあります。

num に指定できる値は、使用するシャーシによって変わります。たとえば、13 スロット シャーシを使用している場合、モジュール番号の有効値は 1 ~ 13 です。

このコマンドは、スーパーバイザ エンジンだけでサポートされています。

attach num コマンドを実行すると、プロンプトは **Switch-sp#** に変更されます。

attach コマンドは、**remote login module num** コマンドと同一のものです。

このセッションを終了する方法は 2 通りあります。

- 次のように、**exit** コマンドを入力します。

```
Switch-sp# exit
```

```
[Connection to Switch closed by foreign host]
```

```
Router#
```

- 次のように、**Ctrl-C** を 3 回押します。

```
Switch-sp# ^C
```

```
Switch-sp# ^C
```

```
Switch-sp# ^C
```

```
Terminate remote login session? [confirm] y
```

```
[Connection to Switch closed by local host]
```

```
Router#
```

attach

例

次に、スーパーバイザ エンジンにリモートからログインする例を示します。

```
Router# attach 5
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C" to end this session
Terminate remote login session? [confirm] yes
[Connection to Switch closed by local host]

Switch-sp#
```

関連コマンド

コマンド	説明
remote login	Catalyst 6500 シリーズ スイッチ コンソールまたは特定のモジュールにアクセスします。

auto-sync

NVRAM 内のコンフィギュレーション ファイルの自動同期化をイネーブルにするには、**auto-sync** コマンドを使用します。自動同期化をディセーブルにするには、このコマンドの **no** 形式を使用します。

auto-sync {**startup-config** | **config-register** | **bootvar** | **running-config** | **standard**}

no auto-sync {**startup-config** | **config-register** | **bootvar** | **standard**}

シンタックスの説明

startup-config	スタートアップ コンフィギュレーションの自動同期化を指定します。
config-register	コンフィギュレーション レジスタ設定の自動同期化を指定します。
bootvar	BOOTVAR コンフィギュレーションの自動同期化を指定します。
running-config	実行コンフィギュレーションの自動同期化を指定します。
standard	スタートアップ コンフィギュレーション、BOOTVAR、およびコンフィギュレーション レジスタの自動同期化を指定します。

デフォルト

実行コンフィギュレーションの自動同期化。

コマンド モード

メイン CPU 冗長モード

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

no auto-sync standard コマンドを入力すると、自動同期化は行われません。イネーブルにするキーワードがある場合、各キーワードに該当するコマンドを入力する必要があります。

例

次に（デフォルト設定から）メイン CPU のコンフィギュレーション レジスタの自動同期化をイネーブルにする例を示します。

```
Router# configure terminal
Router (config)# redundancy
Router (config-r)# main-cpu
Router (config-r-mc)# no auto-sync standard
Router (config-r-mc)# auto-sync config-register
Router (config-r-mc)#
```

関連コマンド

コマンド	説明
redundancy	冗長コンフィギュレーション モードを開始します。

bgp regexp deterministic

決定性処理時間の正規表現エンジンを使用するように Cisco IOS ソフトウェアを設定するには、**bgp regexp deterministic** コマンドを使用します。デフォルトの正規表現エンジンを使用するように Cisco IOS ソフトウェアを設定するには、このコマンドの **no** 形式を使用します。

bgp regexp deterministic

no bgp regexp deterministic

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

デフォルト

デフォルトの正規表現エンジンが有効です。

コマンド モード

ルータ コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

デフォルトの Cisco IOS 正規表現エンジンでは、再帰アルゴリズムが使用されます。このエンジンは効果的ですが、正規表現の複雑さが増すにつれて、より多くのシステム リソースが使用されるようになります。再帰アルゴリズムは単純な正規表現で適切に動作しますが、非常に複雑な正規表現の処理時には、デフォルト エンジンで部分一致の処理にバックトラッキングが必要になるため、能率が下がります。場合によっては、デフォルト エンジンで非常に複雑な正規表現の処理に要する時間が長過ぎて、CPU のウォッチドッグ タイムアウトとスタック オーバーフロー トレースが発生することもあります。

決定性処理時間の正規表現エンジンは、デフォルトの正規表現エンジンに置き換わるものではありません。この新しいエンジンでは、アルゴリズムが改善されて余分なバックトラッキングがなくなり、複雑な正規表現の処理時のパフォーマンスが大きく改善されます。新しいエンジンをイネーブルにすると、複雑な正規表現がより迅速に評価されるため、CPU のウォッチドッグ タイムアウトおよびスタック オーバーフロー トレースが発生しません。ただし、新しい正規表現エンジンでは、単純な正規表現の処理に、デフォルト エンジンよりも長い時間がかかります。

複雑な正規表現を評価する必要がある場合、または正規表現の評価に関連して問題があった場合は、新しい正規表現エンジンの使用を推奨します。単純な正規表現だけを使用する場合は、デフォルトの正規表現エンジンの使用を推奨します。**bgp regexp deterministic** コマンドを Border Gateway Protocol (BGP) ルーティング プロセスで入力すると、新しいエンジンをイネーブルにできます。デフォルトの正規表現エンジンをイネーブルに戻すには、このコマンドの **no** 形式を入力します。

例 次に、決定性処理時間の正規表現エンジンを使用するように Cisco IOS ソフトウェアを設定する例を示します。

```
Router(config)# router bgp 1  
Router(config-router)# bgp regexp deterministic  
Router(config-router)#
```

次に、デフォルトの正規表現エンジンを使用するように Cisco IOS ソフトウェアを設定する例を示します。

```
Router(config)# router bgp 1  
Router(config-router)# no bgp regexp deterministic  
Router(config-router)#
```

boot config

システムが初期化（スタートアップ）時の自身の設定に使用するコンフィギュレーション ファイルの装置およびファイル名を指定するには、**boot config** コマンドを使用します。指定内容を削除するには、このコマンドの **no** 形式を使用します。

boot config {*device:file-name*}

no boot config

シンタックスの説明

<i>device:</i>	装置 ID。有効値の一覧については、「使用上のガイドライン」を参照してください。
<i>file-name</i>	コンフィギュレーション ファイル名

デフォルト

コンフィギュレーション ファイルは NVRAM に保存されます。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

device: の有効値は次のとおりです。

- **disk0:**
 - 外部 CompactFlash Type II スロット×1
 - CompactFlash Type II フラッシュ Personal Computer (PC) カードをサポート
- **sup-bootdisk:**
 - Supervisor Engine 32 256-MB 内部 CompactFlash フラッシュ メモリ
 - Supervisor Engine 32 ROM monitor (ROMMON; ROM モニタ) からの場合は、bootdisk:
- **bootdisk:**
 - PISA 256-MB 内部 CompactFlash フラッシュ メモリ
 - Supervisor Engine 32 ROMMON からはアクセス不能

boot config コマンドを使用する場合、影響を受けるのは実行コンフィギュレーションだけです。環境変数の設定値を ROM モニタ管理下に置き、環境変数を正常に機能させるには、この設定値をスタートアップ コンフィギュレーションに保存する必要があります。環境変数を実行コンフィギュレーションからスタートアップ コンフィギュレーションに保存するには、**copy system:running-config nvram:startup-config** コマンドを使用します。

次の場合、ソフトウェアがエラー メッセージを表示し、CONFIG_FILE 環境変数を更新しません。

- ファイルシステムとして **nvr**am を指定し、そこにコンフィギュレーションの抽出バージョンしか含まれていなかった場合（抽出コンフィギュレーションには、アクセス リストが含まれません）
- 存在しない、または無効なコンフィギュレーション ファイルをファイル名引数に指定した場合

CONFIG_FILE 環境変数が存在しない場合、または（初回起動時のように）この変数がヌルである場合には、NVRAM 内のコンフィギュレーションが初期化に使用されます。ソフトウェアによって NVRAM に問題が検出された場合、または NVRAM 内のコンフィギュレーションに問題があった場合、装置は **setup** モードを開始します。

このコマンドの **no** 形式を使用した場合、スタートアップ コンフィギュレーションとして NVRAM コンフィギュレーションが使用されます。

BOOT、BOOTLDR、および CONFIG_FILE 環境変数の内容を表示するには、**show bootvar** コマンドを使用します。このコマンドは、スタートアップ コンフィギュレーション内のこれらの変数の設定値を表示しますが、実行コンフィギュレーションがスタートアップ コンフィギュレーションと異なっている場合には、実行コンフィギュレーション内の設定値も表示します。

例

次に、初期化中に内部フラッシュ メモリ内のコンフィギュレーション ファイルが自動的に設定されるように設定する例を示します。3 行めでは、指定内容をスタートアップ コンフィギュレーションにコピーし、この指定内容が次のリロード時に実施されるようにしています。

```
Router (config)# boot config disk0:router-config
Router (config)# end
Router# copy system:running-config nvram:startup-config
Router#
```

関連コマンド

コマンド	説明
copy system:running-config nvram:startup-config	実行コンフィギュレーションからスタートアップ コンフィギュレーションに環境変数を保存します。
show bootvar	BOOT 環境変数に関する情報を表示します。

boot system

起動時に読み込むシステム イメージを指定するには、**boot system** コマンドを使用します。起動システム イメージの指定を削除するには、このコマンドの **no** 形式を使用します。

boot system filename

boot system flash [*flash-fs:*][*partition-number:*][*filename*]

no boot system [*filename*]

no boot system flash [*flash-fs:*][*partition-number:*][*filename*]

シンタックスの説明

<i>filename</i>	システムの起動時に読み込むシステム イメージのコンフィギュレーション ファイル名を指定します。
flash	内部フラッシュ メモリから起動します。
<i>flash-fs:</i>	(任意) 起動時に読み込むシステム イメージが格納されたフラッシュ ファイル システム。有効値は、 flash: 、 bootflash 、 slot0 、および slot1 です。
<i>partition-number:</i>	(任意) 起動するシステム イメージ (任意の <i>filename</i> 引数で指定) が格納されたフラッシュ メモリ パーティション番号
<i>filename</i>	(boot system flash コマンドを使用する場合に任意) 起動時に読み込むシステム イメージ名 (大文字と小文字を区別します)

デフォルト

ネットワーク サーバから起動するようにスイッチを設定していても、**boot system** コマンドでシステム イメージ ファイルを指定しないと、スイッチはコンフィギュレーション レジスタ設定を使用してデフォルトのシステム イメージ ファイルを決定します。スイッチは、*cisco* の後ろに、コンフィギュレーション レジスタ内のブート フィールド番号と同等の 8 進数、ハイフン (-)、プロセッサ タイプ名 (*cisconn-cpu*) を付加してデフォルトの起動ファイル名を形成します。コンフィギュレーション レジスタおよびデフォルト ファイル名の詳細については、該当するハードウェア インストールガイドを参照してください。**config-register** または **confreg** コマンドも参照してください。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

config-register コマンドを正しく設定しないと、このコマンドは機能しません。

Catalyst 6500 シリーズ スイッチでは Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) ブートがサポートされません。

ip-address 引数を指定しない場合、この値はデフォルトで IP ブロードキャスト アドレス (255.255.255.255) になります。

flash-fs: 引数を入力するときは、コロンが必要です。

flash キーワードの後ろの引数をすべて省略すると、システムは内部フラッシュ メモリから、起動可能な最初のイメージを検索します。

partition-number: 引数を使用する場合、ファイル名を指定しないと、Route Processor (RP; ルート プロセッサ) はフラッシュ メモリの指定されたパーティションにある最初の有効なファイルを読み込みます。この引数は、パーティション分割が可能なルート プロセッサ上だけで有効です。

filename 引数は、大文字と小文字を区別します。**filename** を指定しないと、スイッチは次の場所にある最初の有効なファイルを読み込みます。

- 指定されたフラッシュ ファイル システム
- フラッシュ メモリの指定されたパーティション
- **flash-fs:** 引数を省略する場合もデフォルトのフラッシュ ファイル システム

ルート プロセッサの起動にフェールセーフ方式を適用するには、複数の **boot system** コマンドを入力します。ルート プロセッサは **boot system** コマンドを、コンフィギュレーション ファイルに入力した順に、保存および実行します。同じ種類の **boot** コマンドをいくつか使用すると (たとえば、2 つのコマンドを使用して、異なるネットワーク サーバからの起動をルート プロセッサに命令するなど)、ルート プロセッサはこれらのコマンドをコンフィギュレーション ファイル内の順番で実行します。その中に無効な装置を指定する **boot system** コマンド エントリがある場合、ルート プロセッサはそのエントリを省略します。Read-Only Memory (ROM; 読み出し専用メモリ) のシステム イメージを、コンフィギュレーション内の他の **boot** コマンドのバックアップとして指定するには、**boot system rom** コマンドを使用します。

一部のプラットフォームでは、システム イメージを読み込む前に起動イメージを読み込む必要があります。ただし、多くのプラットフォームでは、ルート プロセッサがネットワーク サーバから起動する場合またはフラッシュ ファイル システムを指定しない場合にだけ、指定した起動イメージが読み込まれます。ファイル システムを指定すると、起動イメージを最初に読み込む必要がないので、ルート プロセッサの起動が速くなります。

詳細については、『Cisco IOS Release 12.2 Command Reference』を参照してください。



(注)

boot system コマンドによって影響を受けるのは実行コンフィギュレーションだけです。BOOT 変数の設定値を ROM モニタ管理下に置き、BOOT 変数を正常に機能させるには、この設定値をスタートアップ コンフィギュレーションに保存する必要があります。BOOT 変数を実行コンフィギュレーションからスタートアップ コンフィギュレーションに保存するには、**copy system:running-config nvram:startup-configEXEC** コマンドを使用します。

BOOT 変数の内容を確認するには、**show bootenv EXEC** コマンドを使用します。

例

次に、ROM ソフトウェアをバックアップにしているシステム ファイル名の例を示します。

```
Router(config)# boot system flash config1
Router(config)# boot system rom
```

次に、システム イメージ ファイル (igs-bpx-1) を、フラッシュ装置のパーティション 2 から起動する例を示します。

```
Router(config)# boot system flash:2:igs-bpx-1
Router(config)#
```

関連コマンド

コマンド	説明
<code>config-register</code>	コンフィギュレーションレジスタ設定を変更します。
<code>copy /noverify</code>	現在のコピー操作の自動イメージ確認をディセーブルにします。
<code>ip rcmd remote username</code>	<code>rcp</code> を使用してリモートコピーを要求するときに使用するリモートユーザ名を設定します。
<code>show bootvar</code>	BOOT 環境変数に関する情報を表示します。

bridge-domain

Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) 変換をイネーブルにするには、**bridge-domain** コマンドを使用します。

```
bridge-domain {vlan | {PE-vlan dot1qtunnel}} [ignore-bpdu-pid] {pvst-tlv CE-vlan}
```

シンタックスの説明

<i>vlan</i>	バックツーバック トポロジーの VLAN 番号
<i>PE-vlan</i> dot1qtunnel	レイヤ 2 トポロジーで Provider Edge (PE; プロバイダーエッジ) の VLAN 番号を指定します。
ignore-bpdu-pid	(任意) 通常は RFC 1483 データ用に確保されている PID 0x00-07 を使用して、Institute of Electrical and Electronics Engineers (IEEE; 米国電気電子学会) BPDU を送信します。
pvst-tlv	送信時に Per-VLAN Spanning Tree+(PVST+) BPDU を IEEE BPDU に変換します。 受信時に IEEE BPDU を PVST+ BPDU に変換します。
<i>CE-vlan</i>	IEEE BPDU/PVST+ BPDU 変換で挿入される、Shared Spanning Tree Protocol (SSTP) Type-Length-Value (TLV) のカスタマーエッジ VLAN

デフォルト

ディセーブル

コマンド モード

VC または Data Link Switching (DLCI; データ リンク スイッチング) コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

CE-vlan 引数が *PE-vlan* 引数と同じである必要はありません。

RFC 1483 に完全に準拠しているデバイスに接続し、PID 0x000E を使用して IEEE BPDU が送信される場合は、**bridge-domain** コマンドで **ignore-bpdu-pid** キーワードを使用する必要があります。

ignore-bpdu-pid キーワードを入力すると、デバイス間の PVC は RFC 1483 に準拠したトポロジーで動作し、これは完全モードと呼ばれます。**ignore-bpdu-pid** キーワードを入力すると、ルース モードが開始されます。両方のモードについて以下で説明します。

- **ignore-bpdu-pid** キーワードを指定しない場合は完全モードになり、PID 0x00-0E を使用して IEEE BPDU が送信されます。これは RFC 1483 に準拠します。
- **ignore-bpdu-pid** キーワードを指定した場合はルース モードになり、通常は RFC 1483 データ用に確保されている PID 0x00-07 を使用して IEEE BPDU が送信されます。

Cisco 独自の PVST+ BPDU は、**ignore-bpdu-pid** キーワードを入力したかどうかに関わらず、常に PID 0x00-07 を使用してデータ フレームで送信されます。

PID 00-07 で PVST (または 802.1D) BPDU を送信するデバイス (Asynchronous Transfer Mode (ATM; 非同期転送モード) DSL モデムなど) に接続する場合は、**ignore-bpdu-pid** キーワードを使用します。

PVST または IEEE Spanning Tree Protocol (STP; スパニング ツリー プロトコル) だけを認識するデバイスと相互運用するときは、**pvst-tlv** キーワードによって BPDU 変換がイネーブルになります。Catalyst 6500 シリーズ スイッチ ATM モジュールでは PVST+ だけがサポートされるので、ATM モジュールで PVST だけを認識する Catalyst 5000 ファミリー スイッチに接続するとき、または IEEE 形式だけを認識するその他の Cisco IOS ルート プロセッサと接続するときは **pvst-tlv** キーワードを使用する必要があります。

送信時に、**pvst-tlv** キーワードによって PVST+ BPDU は IEEE BPDU に変換されます。

受信時に、**pvst-tlv** キーワードによって IEEE BPDU は PVST+ BPDU に変換されます。

例

次に、RFC 1483 準拠トポロジーで IEEE BPDU だけを認識するデバイスに Catalyst 6500 シリーズ スイッチを接続するとき、BPDU 変換をイネーブルにする例を示します。

```
Router(config-if-atm-vc)# bridge-domain 100 pvst-tlv 150  
Router(config-if-atm-vc)#
```

デバイスは IEEE BPDU 用の RFC 1483 準拠トポロジーで動作するため、**ignore-bpdu-pid** キーワードは使用しません。

次に、Catalyst 5500 ATM モジュールが RFC 1483 非準拠トポロジーで PVST BPDU だけを認識するデバイスである場合、BPDU 変換をイネーブルにする例を示しています。Catalyst 6500 シリーズ スイッチを Catalyst 5500 ATM モジュールに接続するときは、両方のキーワードを入力する必要があります。

```
Router(config-if-atm-vc)# bridge-domain 100 ignore-bpdu-pid pvst-tlv 150  
Router(config-if-atm-vc)#
```

Layer 2 Protocol Tunneling (L2PT; レイヤ 2 プロトコル トンネリング) トポロジーの BPDU 変換をイネーブルにするには、次のコマンドラインを使用します。

```
Router(config-if-atm-vc)# bridge-domain 100 dot1qtunnel ignore-bpdu-pid pvst-tlv 150  
Router(config-if-atm-vc)#
```

cd

デフォルトのディレクトリまたはファイル システムを変更するには、**cd** コマンドを使用します。

```
cd [filesystem:][directory]
```

シンタックスの説明

<i>filesystem:</i>	(任意) ディレクトリまたはファイル システムの URL またはエイリアス。直後にコロンを入力します。有効値のリストについては、「使用上のガイドライン」を参照してください。
<i>directory</i>	(任意) ディレクトリ名

デフォルト

初期デフォルトのファイル システムは、**disk0:** です。

コマンド モード

EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

filesystem: に有効な値は **bootflash:**、**disk0:**、および **disk1:** です。

任意の *filesystem* 引数を持つすべての EXEC コマンドでは、任意の *filesystem* 引数が省略されると、**cd** コマンドで指定されたファイル システムが使用されます。たとえば、ファイル システムのファイル リストを表示する **dir** コマンドには、任意の *filesystem* 引数が含まれます。この引数を省略した場合、システムは **cd** コマンドで指定されたファイル システムのファイルを一覧表示します。

ファイル システムにディレクトリを指定しない場合、デフォルトはそのファイル システムのルート ディレクトリとなります。

例

次に、disk 0: に挿入されたフラッシュ PC カードにデフォルトのファイル システムを設定する例を示します。

```
Router# cd disk0:
Router# pwd
disk0:/
```

関連コマンド

コマンド	説明
dir	ファイル システムのファイル リストを表示します。
mkdir disk0:	フラッシュ ファイル システムに新しいディレクトリを作成します。
pwd	cd コマンドの現在の設定を表示します。
show file system	使用可能なファイル システムを表示します。
undelete	フラッシュ ファイル システムで [delete] マークが付いたファイルを回復します。

channel-group

EtherChannel インターフェイスの EtherChannel グループへの割り当ておよび設定を行うには、**channel-group** コマンドを使用します。インターフェイスからチャネル グループ設定を削除するには、このコマンドの **no** 形式を使用します。

```
channel-group number mode {active | on | {auto [non-silent]} | {desirable [non-silent]} | passive}
```

```
no channel-group number
```

シンタックスの説明

number	チャネル グループ番号。有効値は 1 ～ 256 の範囲の最大 64 個の値です。
mode	インターフェイスの EtherChannel モードを指定します。
active	無条件に Link Aggregation Control Protocol (LACP) をイネーブルにします。
on	EtherChannel だけをイネーブルにします。
auto	ポートをパッシブ ネゴシエーション ステートにします。ポートは受信した Port Aggregation Protocol (PAgP; ポート集約プロトコル) パケットには応答しますが、PAgP パケット ネゴシエーションは開始しません。
non-silent	(任意) トラフィックが他の装置から送信されることが予想される場合に auto または desirable モードとともに使用されます。
desirable	ポートをアクティブ ネゴシエーション ステートにします。ポートは PAgP パケットを送信して、他のポートとのネゴシエーションを開始します。
passive	LACP 装置が検出された場合にだけ、LACP をイネーブルにします。

デフォルト

チャネル グループは割り当てられません。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



(注) Supervisor Engine 32 PISA EtherChannel のコンフィギュレーションを変更できません。



(注) ポートが Supervisor Engine 32 PISA EtherChannel のメンバーになると、**no channel-group 256 mode on** コマンドだけがポートに影響します (ポートがメンバーである間)。ポートが PISA EtherChannel のメンバーである間、**no channel-group 256 mode on** コマンド以外のすべてのポートのコンフィギュレーション コマンドが無視されます。

デフォルトでは、Supervisor Engine 32 PISA EtherChannel (ポート チャネル インターフェイス 256。 **pisa-channel** コマンドを使用して自動的に設定) は、1 Gps EtherChannel です。



(注)

pisa-channel コマンドはコンフィギュレーション ファイルには表示されますが、ユーザは設定できません。

チャンネル グループ番号はグローバルであり、すべてのチャンネル プロトコル間で共有されます。特定のチャンネル番号が、あるチャンネル グループの PAgP がイネーブルのインターフェイスに使用された場合、LACP がイネーブルのインターフェイスを持つチャンネルの設定に同一のチャンネル番号を使用できません (その逆の場合も同様です)。

auto または **desirable** キーワードを入力すると、指定されたインターフェイスで PAgP がイネーブルになります。LACP がイネーブルのインターフェイスで入力すると、このコマンドは拒否されます。

active および **passive** キーワードが有効なのは、PAgP がディセーブルのインターフェイスだけです。特定のチャンネル グループに指定されたインターフェイスである場合だけ、インターフェイスのモードを変更できます。

on キーワードは、ネゴシエーションなしでチャンネルのインターフェイスを強制的にバンドルします。

on モードでは、スイッチの片側に PAgP、反対側に LACP を手動で設定できます。

on モードの場合、**on** モードのポート グループが他の **on** モードのポート グループに接続されている場合にだけ、使用可能な EtherChannel が成立します。

入力するプロトコルと別のプロトコルでチャンネルに追加されたインターフェイスに **channel group** コマンドを入力する場合、このコマンドは拒否されます。

インターフェイスがチャンネルに属する場合、このコマンドの **no** 形式は拒否されます。

同じチャンネル グループ内のすべてのポートは、同じプロトコルを使用する必要があります。1 つのチャンネル グループ上では、2 つのプロトコルを実行できません。

PAgP と LACP 間に互換性はありません。チャンネルの両側で同一のプロトコルを使用する必要があります。

プロトコルは常時変更できますが、変更すると、既存のすべての EtherChannel が新しいプロトコルのデフォルト チャンネル モードにリセットされます。

EtherChannel 内のすべてのポートを、同じ速度およびデュプレックス モード (LACP モードでは全二重だけ) で動作するように設定してください。

物理インターフェイスをチャンネル グループに割り当てる前にポート チャネル インターフェイスを作成する必要はありません。チャンネル グループが最初の物理インターフェイスを取得したときに、ポート チャネル インターフェイスは自動的に作成されます (まだ作成されていない場合)。

チャンネル グループの一部である物理インターフェイスに割り当てられた IP アドレスをディセーブルにする必要はありませんが、ディセーブルにすることを強く推奨します。

interface port-channel コマンドを入力することによって、またはチャンネル グループが最初の物理インターフェイスを割り当てられたときに、レイヤ 2 およびレイヤ 3 の両方のポート チャネルを作成できます。ポート チャネルは稼働中に、またはダイナミックに作成できません。

ポート チャネル インターフェイスに行われた設定変更または属性変更は、ポート チャネルとして同じチャンネル グループ内のすべてのインターフェイスに伝播されます (たとえば、設定変更は、そのポート チャネルの一部ではないが、そのチャンネル グループの一部である物理インターフェイスにも伝えられます)。

レイヤ 2 EtherChannel の設定時に、手動で作成したポート チャネル論理インターフェイスにレイヤ 2 LAN ポートを追加できません。

channel-group

Multiprotocol Label Switching (MPLS; マルチプロトコル ラベル スイッチング) が設定されている場合も、Gigabit Ethernet WAN (GE-WAN; ギガビット イーサネット WAN) インターフェイス上で **channel-group** コマンドを使用できません。GE-WAN インターフェイスで **channel-group** コマンドを使用する前に、IP、MPLS、およびその他のレイヤ 3 コンフィギュレーション コマンドをすべて削除する必要があります。



(注)

channel-group コマンドを再入力して、以前のグループからインターフェイスを削除し、新しいグループに移動します。一方、GE-WAN ポートの場合は、新しいグループにインターフェイスを割り当てる前に、**no channel-group** コマンドを入力してグループからインターフェイスを手動で削除する必要があります。



注意

物理 EtherChannel インターフェイスでレイヤ 3 アドレスをイネーブルにしないでください。物理 EtherChannel インターフェイス上でブリッジ グループを割り当てると、ネットワーク上にループが発生します。

注意事項の一覧については、『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*』の「Configuring EtherChannel」を参照してください。

例

次に、インターフェイス EtherChannel 1/0 をポート チャネル 1 に指定された EtherChannel グループに追加する例を示します。

```
Router(config-if)# channel-group 1 mode on
Router(config-if)#
```

関連コマンド

コマンド	説明
interface port-channel	ポート チャネル仮想インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
show etherchannel	チャネルの EtherChannel 情報を表示します。
show interfaces port-channel	特定のポート チャネルが認識するトラフィックを表示します。

channel-protocol

チャンネルを管理するためにインターフェイスで使用するプロトコルを設定するには、**channel-protocol** コマンドを使用します。プロトコルの選択を解除するには、このコマンドの **no** 形式を使用します。

channel-protocol {lACP | pagp}

no channel-protocol

シンタックスの説明

lACP	チャンネルの管理に LACP を指定します。
pagp	チャンネルの管理に PAgP を指定します。

デフォルト

pagp

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

channel-group コマンドを使用して、プロトコルを選択することもできます。

インターフェイスがチャンネルに属する場合、このコマンドの **no** 形式は拒否されます。

EtherChannel のすべてのポートで同じプロトコルを使用する必要があります。

PAgP と LACP 間に互換性はありません。チャンネルの両側で同一のプロトコルを使用する必要があります。

channel-protocol コマンドは、チャンネル グループ単位で実行され、再設定されたチャンネル グループ内のポートにだけ影響します。**channel-protocol** コマンドを使用して、選択したプロトコルに適応しないモードが選択されないように制限できます。

EtherChannel 内のすべてのポートを、同じ速度およびデュプレックス モード (LACP モードでは全二重だけ) で動作するように設定してください。注意事項の一覧については、『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*』の「Configuring EtherChannel」を参照してください。

例

次に、インターフェイスのチャンネル管理に LACP を選択する例を示します。

```
Router(config-if)# channel-protocol lACP
Router(config-if)#
```

関連コマンド

コマンド	説明
channel-group	EtherChannel インターフェイスの EtherChannel グループへの割り当ておよび設定を行います。
show etherchannel	チャンネルの EtherChannel 情報を表示します。

class-map

QoS クラス マップを設定するための QoS クラス マップ コンフィギュレーション モードにアクセスするには、**class-map** コマンドを使用します。クラス マップを削除するには、このコマンドの **no** 形式を使用します。

```
class-map name [match-all | match-any]
```

```
no class-map name [match-all | match-any]
```

シンタックスの説明

<i>name</i>	クラス マップ名
match-all	(任意) クラス マップのすべての一致基準に一致します。
match-any	(任意) 1 つまたは複数の一致基準に一致します。

デフォルト

match-all または **match-any** キーワードを指定しない場合、デフォルトは **match-all** となります。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

個々のインターフェイスに **class-map** コマンドおよびそのサブコマンドを適用して、グローバルに名付けられたサービス ポリシーの一部としてパケットの分類、マーキング、集約、およびフロー ポリッシングを定義します。

サービス ポリシーは EtherChannel に付加できます。EtherChannel のメンバーであるポートにサービス ポリシーを付加しないでください。

QoS クラス マップ コンフィギュレーション モードでは、次のコンフィギュレーション コマンドが利用できます。

- **exit** : QoS クラス マップ コンフィギュレーション モードを終了するのに使用します。
- **no** : クラスマップから一致ステートメントを削除するのに使用します。
- **match** : 分類基準を設定するのに使用します。次の任意の **match** サブコマンドを利用できます。
 - **access-group** {*acl-index* | *acl-name*}
 - **ip** {*dscp* | *precedence*} *value1 value2 ... value8*

次のサブコマンドは Command-Line Interface (CLI; コマンドライン インターフェイス) ヘルプに表示されますが、Optical Service Module (OSM; オプティカル サービス モジュール) 上の LAN インターフェイスまたは WAN インターフェイスではサポートされません。

- **input-interface** {{*interface interface-number*} | {**null** *number*} | {**vlan** *vlan-id*}}
- **protocol** *linktype*
- **destination-address** **mac** *mac-address*

- **source-address mac** *mac-address*

Policy Feature Card (PFC; ポリシー フィーチャ カード) の QoS は、次のサブコマンドをサポートしません。

- **input-interface** *{{interface interface-number} | {null number} | {vlan vlan-id}}*
- **protocol** *linktype*
- **destination-address mac** *mac-address*
- **source-address mac** *mac-address*
- **qos-group** *group-value*

これらのサブコマンドを入力した場合、インターフェイスにポリシー マップが付加されないと、PFC QoS はサポートされていないキーワードを検出しません。インターフェイスにポリシー マップを付加しようとする、エラー メッセージが表示されます。詳細については、『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*』および『*Cisco IOS Release 12.2 Command Reference*』を参照してください。

クラスマップ名を設定し、クラスマップ コンフィギュレーション モードを開始すると、**match** サブコマンドを入力できます。これらのサブコマンドの構文は次のとおりです。

```
match {{access-group acl-index} | acl-name} | {{ip dscp} | {precedence value}}
```

match サブコマンドの構文説明についてはを参照してください。表 2-1

表 2-1 match 構文説明

任意サブコマンド	説明
access-group <i>acl-index</i> <i>acl-name</i>	アクセス リスト インデックスまたはアクセス リスト名を指定します。有効なアクセス リスト インデックスの値は 1 ~ 2699 です。
access-group <i>acl-name</i>	名前付きアクセス リストを指定します。
ip dscp <i>value1 value2 ... value8</i>	対応する IP differentiated services code point (DSCP) 値。有効値は、0 ~ 63 です。スペースで区切るにより最大 8 つの DSCP 値を入力できます。
ip precedence <i>value1 value2 ... value8</i>	対応する IP precedence 値を指定します。有効値は、0 ~ 7 です。スペースで区切るにより最大 8 つの precedence 値を入力できます。

例 次に、**class-map** コマンドおよびサブコマンドにアクセスして、ipp5 という名前のクラスマップを設定し、IP precedence 5 の一致ステートメントを入力する例を示します。

```
Router(config)# class-map ipp5
Router(config-cmap)# match ip precedence 5
Router(config-cmap)#
```

次に、すでに設定されたアクセス リストに一致するクラスマップを設定する例を示します。

```
Router(config-cmap)# match access-group IPacl1
Router(config-cmap)#
```

関連コマンド

コマンド	説明
policy-map	QoS ポリシー マップを設定するための QoS ポリシー マップ コンフィギュレーション モードにアクセスします。

コマンド	説明
show class-map	クラス マップ情報を表示します。
show policy-map interface	インターフェイスに対応付けられた入力および出力ポリシーの統計情報およびコンフィギュレーションを表示します。

class-map type multicast-flows

マルチキャスト クラス マップを作成してマルチキャスト クラスマップ コンフィギュレーション モードを開始するには、**class-map type multicast-flows** コマンドを使用します。クラス マップを削除するには、このコマンドの **no** 形式を使用します。

class-map type multicast-flows *name*

no class-map type multicast-flows *name*

シンタックスの説明

<i>name</i>	クラスマップ名
-------------	---------

デフォルト

クラスは指定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

マルチキャスト クラスマップ コンフィギュレーション モードを開始すると、次のコンフィギュレーション コマンドが利用できます。

- **exit** : マルチキャスト クラスマップ コンフィギュレーション モードを終了するのに使用します。
- **group** : マルチキャスト グループの範囲を設定するために使用します。これらのサブコマンドの構文は次のとおりです。

group *group-addr* [*source addr* | *to addr*]

group サブコマンドの構文説明については表 2-2 を参照してください。

表 2-2 group 構文説明

サブコマンド	説明
<i>group-addr</i>	マルチキャスト グループ アドレス
<i>source addr</i>	(任意) チャネル送信元アドレスを指定します。
<i>to addr</i>	(任意) マルチキャスト グループ範囲の終了アドレスを指定します。

- **no** : コマンドを無効にする、またはデフォルトを設定するために使用します。

■ class-map type multicast-flows

例

次に、マルチキャスト クラス マップを作成する例を示します。

```
Router(config)# class-map type multicast-flows static2  
Router(config-mcast-flows-cmap)#
```

次に、マルチキャスト グループ範囲の設定例を示します。

```
Router(config-mcast-flows-cmap)# group 192.0.2.0 source 192.0.2.10  
Router(config-mcast-flows-cmap)#
```

class (policy-map)

作成または変更を行うポリシーを含むクラスの名前を指定する前、またはポリシーを設定する前にデフォルト クラス（一般的には **class-default** クラス）を指定するには、QoS ポリシーマップ コンフィギュレーション モードで **class** コマンドを使用します。ポリシー マップからクラスを削除するには、このコマンドの **no** 形式を使用します。

```
class {class-name | class-default}
```

```
no class {class-name | class-default}
```

シンタックスの説明

<i>class-name</i>	ポリシーの設定または修正を行うクラスの名前
class-default	デフォルト クラスを指定します。

デフォルト

クラスは指定されていません。

コマンド モード

QoS ポリシーマップ コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

作成または変更を行うポリシーのクラス名を指定するには、**class**（ポリシーマップ）コマンドを使用できます。最初にポリシー マップを指定する必要があります。

ポリシー マップを指定して必要な QoS ポリシーマップ コンフィギュレーション モードを開始するには、**class**（ポリシー マップ）コマンドを使用する前に **policy-map** コマンドを使用します。ポリシー マップを指定したら、新しいクラスにポリシーを設定したり、そのポリシー マップの既存クラスのポリシーを修正したりすることができます。

クラス特性を定義する場合は、次の注意事項に従ってください。

- ポリシー マップで指定するクラス名により、そのクラスの特性（つまりポリシー）が、**class-map** コマンドを使用して設定したとおりに、クラス マップおよびその一致基準に関連付けられます。
- クラスのポリシーを設定し、帯域幅を指定してポリシーマップをインターフェイスに付加するとき、クラスの帯域幅要件が満たされるかどうか、**Class-Based Weighted Fair Queuing** (CBWFQ; クラス ベース均等化キューイング) によって判断されます。要件が満たされる場合、CBWFQ は帯域幅要件にキューを割り当てます。
- クラスを削除すると、インターフェイスの使用可能帯域幅は、そのクラスに割り当てられていた量だけ増加します。
- ポリシー マップに設定できるクラスの最大数は 64 です。

class-default という定義済みデフォルト クラスを指定するには、**class-default** キーワードを使用します。**class-default** という定義済みデフォルト クラスは、トラフィックが設定済みクラス マップの一致基準に一致しない場合、そのトラフィックが転送されるクラスです。

queue-limit コマンドを使用してテール ドロップを使用するか、**random-detect** コマンドを使用して Weighted Random Early Detection (WRED; 重み付けランダム早期検出) を使用するように、クラス ポリシーを定義できます。テール ドロップまたは WRED のどちらかを使用する場合は、次の注意事項に従ってください。

- **queue-limit** コマンドおよび **random-detect** コマンドは、同一クラス ポリシーでは使用できませんが、同一ポリシー マップの 2 つのクラス ポリシーでは使用できます。
- **queue-limit** コマンドまたは **random-detect** コマンドのどちらかをクラス ポリシーで設定するとき、**bandwidth** コマンドを使用できます。**bandwidth** コマンドでは、クラスに割り当てる帯域幅を指定します。
- 定義済みデフォルト クラスには、**fair-queue** (class-default) コマンドを使用できます。**fair-queue** コマンドでは、デフォルト クラスのダイナミック キューの数を指定します。**fair-queue** コマンドは、**queue-limit** コマンドまたは **random-detect** コマンドのどちらかと同じクラス ポリシーで使用できます。**bandwidth** コマンドとの併用はできません。

例

次に、policy1 というポリシー マップに含まれる 3 つのクラス ポリシーを設定する例を示します。class1 は、アクセス制御リスト 136 と一致するトラフィックのポリシーを指定します。class2 は、インターフェイス ethernet101 のトラフィックのポリシーを指定します。3 番目のクラスはデフォルト クラスであり、設定済み一致基準を満たさないパケットがこれに転送されます。

```
Router(config)# policy-map policy1
Router(config-pmap)# class-map class1
Router(config-pmap-c)# match access-group 136
Router(config-pmap)# class-map class2
Router(config-pmap-c)# match input-interface ethernet101
```

次に、class1、class2、デフォルト クラスのポリシー指定を含むポリシー マップを作成する例を示します。

```
Router(config)# policy-map policy1
Router(config-pmap)# class-map class1
Router(config-pmap-c)# bandwidth 2000
Router(config-pmap-c)# queue-limit 40

Router(config-pmap)# class class2
Router(config-pmap-c)# bandwidth 3000
Router(config-pmap-c)# random-detect
Router(config-pmap-c)# random-detect exponential-weighting-constant 10

Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue 16
Router(config-pmap-c)# queue-limit 20
```



(注)

このクラスを含むポリシー マップをインターフェイスに付加して、そのインターフェイスのサービス ポリシーを規定するとき、設定されるすべてのクラス ポリシーおよび Resource Reservation Protocol (RSVP) を含めて、使用可能な帯域幅が評価されます。

次に、policy8 というポリシー マップに組み込まれるデフォルト クラス **class-default** のポリシーを設定する例を示します。デフォルト クラス **class-default** には、その他のクラスの一貫基準を満たさないトラフィック用に 20 個のハッシュ キューが含まれます。このクラスのポリシーは、policy8 というポリシー マップ、および平均キュー サイズの計算に使用される加重係数 14 によって定義されます。輻輳回避のために、テール ドロップではなく、WRED パケット ドロップが使用されます。

```
Router(config)# policy-map policy8
Router(config-pmap)# class class-default
```

```
Router(config-pmap-c)# fair-queue 20
Router(config-pmap-c)# random-detect exponential-weighting-constant 14
```

関連コマンド

コマンド	説明
class-map	QoS クラス マップを設定するための QoS クラス マップ コンフィギュレーション モードにアクセスします。
fair-queue	デフォルト クラス ポリシーの一部として、class-default クラスが使用するために確保するダイナミック キューの数を指定します。
policy-map	QoS ポリシー マップ コンフィギュレーション モードにアクセスし、QoS ポリシー マップを設定します。
queue-limit	ポリシー マップで設定されているクラス ポリシー用にキューで維持できるパケットの最大数の指定または修正を行います。
random-detect (インターフェイス)	WRED または DWRED を有効にします。
random-detect exponential-weighting-constant	キューの平均キュー サイズ計算用に、WRED および DWRED の指数加重係数を設定します。
random-detect precedence	特定の IP precedence 用に、WRED および DWRED のパラメータを設定します。

■ class (policy-map)

clear cable-diagnostics tdr

Time Domain Reflectometer (TDR; タイム ドメイン リフレクトメータ) をサポートする特定のインターフェイスまたはすべてのインターフェイスをクリアするには、**clear cable-diagnostics tdr** コマンドを使用します。

clear cable-diagnostics tdr [*interface interface interface-number*]

シンタックスの説明	interface interface (任意) インターフェイス タイプを指定します。有効値は fastethernet 、 gigabitethernet 、および tengigabitethernet です。
	interface-number モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。

デフォルト このコマンドにはデフォルト設定がありません。

コマンド モード 特権 EXEC

コマンドの履歴	リリース 変更内容
	12.2(18)ZY このコマンドのサポートが追加されました。

使用上のガイドライン TDR をサポートするモジュールの一覧については、『*Release Notes for Cisco IOS Release 12.2 SX on the Catalyst 6500*』を参照してください。

例 次に、特定のインターフェイスをクリアする例を示します。

```
Router# clear cable-diagnostics tdr interface gigabitethernet 4/1
Router#
```

関連コマンド	コマンド 説明
	show cable-diagnostics tdr TDR ケーブル診断のテスト結果を表示します。
	test cable-diagnostics 48 ポート 10/100/1000 BASE-T モジュール上の 10 ギガビットイーサネット リンクまたは銅ケーブルの状態をテストします。

clear catalyst6000 traffic-meter

トラフィック メーターのカウンタをクリアするには、**clear catalyst6000 traffic-meter** コマンドを使用します。

clear catalyst6000 traffic-meter

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、トラフィック メーターのカウンタをクリアする例を示します。

```
Router# clear catalyst6000 traffic-meter
Router#
```

clear counters

インターフェイス カウンタをクリアするには、**clear counters** コマンドを使用します。

```
clear counters [{interface interface-number} | {null interface-number} | {port-channel
number} | {vlan vlan-id}]
```

シンタックスの説明	
<i>interface</i>	(任意) インターフェイス タイプ。有効値は ethernet 、 fastethernet 、 gigabitethernet 、および tengigabitethernet です。その他の有効値については、「使用上のガイドライン」を参照してください。
<i>interface-number</i>	(任意) モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
null <i>interface-number</i>	(任意) マル インターフェイスを指定します。有効値は 0 です。
port-channel <i>number</i>	(任意) チャンネル インターフェイスを指定します。有効値は 1 ~ 256 の範囲の最大 64 個の値です。
vlan <i>vlan-id</i>	(任意) VLAN ID を指定します。有効値は 1 ~ 4094 です。

デフォルト このコマンドにはデフォルト設定がありません。

コマンド モード 特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン インターフェイスが指定されていない場合、このコマンドはインターフェイスから現在のすべてのインターフェイス カウンタをクリアします。



(注) このコマンドは、Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) で検索されたカウンタはクリアせず、**show queuing interface** コマンドを入力したときに表示されるカウンタだけをクリアします。

interface-number 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

■ clear counters

例

次に、すべてのインターフェイス カウンタをクリアする例を示します。

```
Router# clear counters
Clear "show interface" counters on all interfaces [confirm]y
Router#
```

次に、特定のインターフェイスのカウンタをクリアする例を示します。

```
Router# clear counters vlan 200
Clear "show interface" counters on this interface [confirm]y
Router#
```

関連コマンド

コマンド	説明
show queuing interface	キューイング情報を表示します。

clear fm netflow counters

NetFlow カウンタをクリアするには、**clear fm netflow counters** コマンドを使用します。

clear fm netflow counters

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

デフォルト このコマンドにはデフォルト設定がありません。

コマンドモード 特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、NetFlow カウンタをクリアする例を示します。

```
Router# clear fm netflow counters
Router#
```

clear interface gigabitethernet

ギガビット イーサネット IEEE 802.3z インターフェイスのハードウェア ロジックをクリアするには、**clear interface gigabitethernet** コマンドを使用します。

clear interface gigabitethernet *number*

シンタックスの説明

<i>number</i>	ギガビット イーサネット インターフェイス番号。有効値については、「使用上のガイドライン」を参照してください。
---------------	---

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

number 引数は、モジュールおよびポート番号を指定します。*number* の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロットシャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

例

次に、ギガビット イーサネット IEEE 802.3z インターフェイスのハードウェア ロジックをクリアする例を示します。

```
Router# clear interface gigabitethernet 5
Router#
```

関連コマンド

コマンド	説明
show interfaces status	インターフェイス ステータスを表示したり、LAN ポートで errdisable ステートにあるインターフェイスだけのリストを表示したりします。

clear interface vlan

VLAN のハードウェア ロジックをクリアするには、**clear interface vlan** コマンドを使用します。

clear interface vlan *vlan-id*

シンタックスの説明

vlan-id VLAN ID。有効値は 1 ~ 4094 です。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、特定の VLAN のハードウェア ロジックをクリアする例を示します。

```
Router# clear interface vlan 5
Router#
```

関連コマンド

コマンド	説明
show interfaces status	インターフェイス ステータスを表示したり、LAN ポートで errdisable ステートにあるインターフェイスだけのリストを表示したりします。

clear ip access-template

アクセス リストの統計情報をクリアするには、**clear ip access-template** コマンドを使用します。

clear ip access-template *access-list*

シンタックスの説明

access-list アクセス リスト番号。有効値は IP 拡張アクセス リストについては 100 ~ 199、拡張範囲 IP 拡張アクセス リストについては、2000 ~ 2699 です。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、アクセス リストの統計情報をクリアする例を示します。

```
Router# clear ip access-template 201
Router#
```

関連コマンド

コマンド	説明
show mls netflow	NetFlow ハードウェアに関する設定情報を表示します。

clear ip arp inspection log

ログバッファのステータスをクリアするには、**clear ip arp inspection log** コマンドを使用します。

clear ip arp inspection log

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

デフォルト このコマンドにはデフォルト設定がありません。

コマンドモード 特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、ログバッファのカウンタをクリアする例を示します。

```
Router# clear ip arp inspection log
Router#
```

関連コマンド	コマンド	説明
	arp access-list	ARP インспекションおよび QoS フィルタリング用の ARP ACL を設定し、ARP ACL コンフィギュレーション サブモードを開始します。
	show ip arp inspection log	ログバッファのステータスを表示します。

clear ip arp inspection statistics

Dynamic ARP Inspection (DAI; ダイナミック ARP インスペクション) の統計情報をクリアするには、**clear ip arp inspection statistics** コマンドを使用します。

clear ip arp inspection statistics [vlan *vlan-range*]

シンタックスの説明

vlan *vlan-range* (任意) VLAN 範囲を指定します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、VLAN 1 から DAI 統計情報をクリアする例を示します。

```
Router# clear ip arp inspection statistics vlan 1
Router#
```

関連コマンド

コマンド	説明
arp access-list	ARP インスペクションおよび QoS フィルタリング用の ARP ACL を設定し、ARP ACL コンフィギュレーション サブモードを開始します。
clear ip arp inspection log	ログ バッファのステータスをクリアします。
show ip arp inspection log	ログ バッファのステータスを表示します。

clear ip auth-proxy watch-list

1つのウォッチ リスト エントリまたはすべてのウォッチ リスト エントリを削除するには、**clear ip auth-proxy watch-list** コマンドを使用します。

```
clear ip auth-proxy watch-list {ip-addr | *}
```

シンタックスの説明

<i>ip-addr</i>	ウォッチ リストから削除される IP アドレス
*	ウォッチ リストのすべてのウォッチ リスト エントリ

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ウォッチ リストに有効ではないと考えられるエントリが表示される場合は、ウォッチ リストが期限切れになるのを待機するのではなく、**clear ip auth-proxy watch-list** コマンドを入力して、エントリを手動でクリアできます。

例

次に、1つのウォッチ リスト エントリを削除する例を示します。

```
Router# clear ip auth-proxy watch-list 12.0.0.2
Router#
```

次に、すべてのウォッチ リスト エントリを削除する例を示します。

```
Router# clear ip auth-proxy watch-list *
Router#
```

関連コマンド

コマンド	説明
ip auth-proxy max-login-attempts	ファイアウォール インターフェイスおよび QoS フィルタリングにおけるログイン試行回数を制限し、ARP ACL コンフィギュレーション サブモードを開始します。
ip auth-proxy watch-list	認証プロキシ ウォッチ リストをイネーブルにして設定します。
show ip auth-proxy watch-list	認証プロキシ ウォッチ リストに関する情報を表示します。

clear ip cef epoch full

新しいエポックを開始し、すべてのテーブル（隣接テーブルを含む）のエポック番号を増分するには、**clear ip cef epoch full** コマンドを使用します。

clear ip cef epoch full

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

テーブルを再構築する場合に、**clear ip cef epoch full** コマンドを使用します。このコマンドでは、同一のデータ構造内で以前のテーブル エントリと新しいテーブル エントリを区別することができ、新しいテーブルを構築しても以前の CEF データベースを維持できます。

次の **show** コマンドはエポック情報を表示します。

- **show ip cef summary** : 特定の Forwarding Information Base (FIB; 転送情報ベース) テーブルのテーブル エポックを表示します。
- **show ip cef detail** : 特定の FIB テーブルの各エントリのエポック値を表示します。
- **show adjacency summary** : 隣接テーブルのエポックを表示します。
- **show adjacency detail** : 隣接テーブルの各エントリのエポック値を表示します。

例

次に、エポック テーブルをクリアし、エポック番号を増分する前後の出力例を示します。

```
Router# show ip cef epoch
CEF epoch information:

Table:Default-table
  Table epoch:2 (164 entries at this epoch)

Adjacency table
  Table epoch:1 (33 entries at this epoch)
```

```
Router# clear ip cef epoch full
Router# show ip cef epoch
CEF epoch information:

Table:Default-table
  Table epoch:3 (164 entries at this epoch)

Adjacency table
  Table epoch:2 (33 entries at this epoch)
Router#
```

関連コマンド

コマンド	説明
show adjacency detail	プロトコルの詳細およびタイマーに関する情報を表示します。
show adjacency summary	CEF 隣接情報のサマリーを表示します。
show ip cef detail	詳細 FIB エントリ情報を表示します。
show ip cef epoch	隣接テーブルおよびすべての FIB テーブルのエポック情報を表示します。
show ip cef summary	FIB の概要を表示します。

clear ip cef inconsistency

CEF 一貫性チェッカーの統計情報および記録情報をクリアするには、**clear ip cef inconsistency** コマンドを使用します。

clear ip cef inconsistency

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、**ip cef table consistency-check** コマンドをイネーブルにしたときに集めた統計情報および記録情報をクリアします。

例

次に、CEF 一貫性チェッカーが検出した統計情報および記録情報をクリアする例を示します。

```
Router# clear ip cef inconsistency
Router#
```

関連コマンド

コマンド	説明
ip cef table consistency-check	CEF テーブル一貫性チェッカーのタイプおよびパラメータをイネーブルにします。

clear ip dhcp snooping

DHCP スヌーピングをディセーブルにせずに、DHCP スヌーピング テーブルをクリアするには、**clear ip dhcp snooping** コマンドを使用します。

clear ip dhcp snooping {binding | database | statistics}

シンタックスの説明	binding	DHCP スヌーピングをディセーブルにせずに、DHCP スヌーピング バインディング エントリ テーブルをクリアします。
	database	DHCP スヌーピングをディセーブルにせずに、DHCP スヌーピング データベース テーブルをクリアします。
	statistics	DHCP スヌーピングをディセーブルにせずに、DHCP スヌーピング統計テーブルをクリアします。

デフォルト このコマンドにはデフォルト設定がありません。

コマンドモード 特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、DHCP スヌーピング バインディング エントリ テーブルをクリアする例を示します。

```
Router# clear ip dhcp snooping binding
Router#
```

次に、DHCP スヌーピング データベース テーブルをクリアする例を示します。

```
Router# clear ip dhcp snooping database
Router#
```

次に、DHCP スヌーピング統計をクリアする例を示します。

```
Router# clear ip dhcp snooping statistics
Router#
```

関連コマンド	コマンド	説明
	show ip dhcp snooping	DHCP スヌーピングの設定を表示します。
	show ip dhcp snooping binding	DHCP スヌーピングのバインディング エントリを表示します。
	show ip dhcp snooping database	DHCP スヌーピング データベース エージェントのステータスを表示します。

clear ip flow stats

NetFlow スイッチングの統計情報をクリアするには、**clear ip flow stats** コマンドを使用します。

clear ip flow stats

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

show ip cache flow コマンドは、NetFlow スイッチングの統計情報を表示します。

例

次に、NetFlow スイッチングの統計情報をクリアする例を示します。

```
Router# clear ip flow stats
Router#
```

関連コマンド

コマンド	説明
show ip cache flow	NetFlow キャッシュ フロー エントリのサマリーを表示します。

clear ip igmp group

IGMP グループ キャッシュのエントリを削除するには、**clear ip igmp group** コマンドを使用します。

```
clear ip igmp [vrf vrf-name] group [{interface interface-number} | {group-name |
group-address} {loopback interface-number} | {null interface-number} |
{port-channel number} | {vlan vlan-id}]
```

シンタックスの説明

<i>vrf vrf-name</i>	(任意) マルチキャスト VPN Routing/Forwarding (VRF; VPN ルーティング/転送) インスタンスに割り当てられている名前を指定します。
<i>interface</i>	(任意) インターフェイス タイプ。有効値は ethernet 、 fastethernet 、 gigabitethernet 、および tengigabitethernet です。
<i>interface-number</i>	(任意) モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
<i>group-name</i>	(任意) Domain Name System (DNS; ドメイン ネーム システム) ホスト テーブルまたは ip host コマンドで定義されているグループ名
<i>group-address</i>	(任意) 4 分割ドット表記によるマルチキャスト グループのアドレス
loopback <i>interface-number</i>	(任意) ループバック インターフェイスを指定します。有効値は 0 ~ 2,147,483,647 です。
null <i>interface-number</i>	(任意) ヌル インターフェイスを指定します。有効値は 0 です。
port-channel <i>number</i>	(任意) チャネル インターフェイスを指定します。有効値は 1 ~ 256 の範囲の最大 64 個の値です。
vlan <i>vlan-id</i>	(任意) VLAN ID を指定します。有効値は 1 ~ 4094 です。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

IGMP キャッシュには、直接接続されている LAN 上のホストのリストが含まれます。スイッチがグループに加入すると、このグループもキャッシュに表示されます。

IGMP キャッシュからすべてのエントリを削除する場合は、引数なしで **clear ip igmp group** コマンドを入力します。

interface-number 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

■ clear ip igmp group

例

次に、IGMP キャッシュから特定のグループのエントリをクリアする例を示します。

```
Router# clear ip igmp group 224.0.255.1
Router#
```

次に、IGMP グループ キャッシュの特定のインターフェイスから、IGMP グループ キャッシュ エントリをクリアする例を示します。

```
Router# clear ip igmp group gigabitethernet 2/2
Router#
```

関連コマンド

コマンド	説明
<code>ip host</code>	スタティック ホスト名とアドレスのマッピングをホスト キャッシュで定義します。
<code>show ip igmp groups</code>	ルータに直接接続され、IGMP によって学習されたレシーバーを含むマルチキャスト グループを表示します。
<code>show ip igmp interface</code>	IGMP インターフェイス ステータスおよび設定に関する情報を表示します。

clear ip igmp snooping statistics

IGMP スヌーピングの統計情報をクリアするには、**clear ip igmp snooping statistics** コマンドを使用します。

clear ip igmp snooping statistics [vlan *vlan-id*]

シンタックスの説明	vlan <i>vlan-id</i> (任意) VLAN ID を指定します。有効値は 1 ~ 4094 です。
-----------	--

デフォルト	このコマンドにはデフォルト設定がありません。
-------	------------------------

コマンドモード	特権 EXEC
---------	---------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン	VLAN を指定しない場合、すべての VLAN の IGMP スヌーピング統計情報がクリアされます。
------------	--

例	次に、すべての VLAN の IGMP スヌーピング統計情報をクリアする例を示します。
---	---

```
Router# clear ip igmp snooping statistics
Router#
```

次に、特定の VLAN の IGMP スヌーピング統計情報をクリアする例を示します。

```
Router# clear ip igmp snooping statistics vlan 300
Router#
```

関連コマンド	コマンド	説明
	show ip igmp snooping statistics	IGMPv3 統計に関する情報を表示します。

clear ip mroute

IP マルチキャスト ルーティング テーブルからエントリを削除するには、**clear ip mroute** コマンドを使用します。

```
clear ip mroute [vrf vrf-name] [* | group] [source]
```

シンタックスの説明

vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
*	IP マルチキャスト ルーティング テーブルからすべてのエントリを削除します。
group	マルチキャスト グループの名前または IP アドレス。詳細については、「使用上のガイドライン」を参照してください。
source	(任意) グループに送信するマルチキャスト送信元の名前またはアドレス。詳細については、「使用上のガイドライン」を参照してください。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

group 引数は、次のいずれかを指定します。

- DNS ホスト テーブルまたは **ip host** コマンドで定義されるマルチキャスト グループ名
- 4 分割ドット表記によるマルチキャスト グループの IP アドレス

group の名前またはアドレスを指定する場合、**source** 引数を入力して、グループに送信するマルチキャスト送信元の名前またはアドレスも指定できます。送信元は、グループのメンバーである必要はありません。

例

次に、IP マルチキャスト ルーティング テーブルからすべてのエントリを削除する例を示します。

```
Router# clear ip mroute *
Router#
```

次に、マルチキャスト グループ 224.2.205.42 に送信する 228.3.0.0 サブネット上のすべての送信元を IP マルチキャスト ルーティング テーブルから削除する例を示します。この例では、ネットワーク 228.3 上の個別の送信元ではなく、すべての送信元が削除されます。

```
Router# clear ip mroute 224.2.205.42 228.3.0.0
Router#
```

関連コマンド

コマンド	説明
ip host	スタティック ホスト名とアドレスのマッピングをホスト キャッシュで定義します。
show ip mroute	IP マルチキャスト ルーティング テーブルに関する情報を表示します。

clear ip msdp peer

指定された MSDP ピアへの TCP 接続をクリアするには、**clear ip msdp peer** コマンドを使用します。

```
clear ip msdp [vrf vrf-name] peer {peer-address | peer-name}
```

シンタックスの説明

vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
peer-address peer-name	TCP 接続がクリアされる MSDP ピアの IP アドレスまたは名前

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドによりピアへの TCP 接続はクローズされ、すべての MSDP ピアの統計情報はリセットされ、MSDP ピアでの入力/出力キューはクリアされます。

例

次に、224.15.9.8 の MSDP ピアへの TCP 接続をクリアする例を示します。

```
Router# clear ip msdp peer 224.15.9.8
Router#
```

関連コマンド

コマンド	説明
ip msdp peer	MSDP ピアを設定します。

clear ip msdp sa-cache

MSDP 送信元のアクティブ キャッシュ エントリをクリアするには、**clear ip msdp sa-cache** コマンドを使用します。

```
clear ip msdp [vrf vrf-name] sa-cache [group-address | group-name]
```

シンタックスの説明	パラメータ	説明
	vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
	group-address group-name	(任意) source-active エントリが source-active キャッシュからクリアされるマルチキャスト グループのアドレスまたは名前

デフォルト このコマンドにはデフォルト設定がありません。

コマンド モード 特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン キャッシュ内にクリアする任意の source-active エントリを含めるには、**ip msdp cache-sa-state** コマンドを入力して、source-active キャッシングをイネーブルにする必要があります。

グループのアドレスまたは名前によりマルチキャスト グループが識別されない場合、すべての source-active キャッシュ エントリがクリアされます。

例 次に、キャッシュからマルチキャスト グループ 224.5.6.7 の source-active エントリをクリアする例を示します。

```
Router# clear ip msdp sa-cache 224.5.6.7
Router#
```

関連コマンド	コマンド	説明
	ip msdp peer	MSDP ピアを設定します。
	ip msdp cache-sa-state	ルータに source-active ステートを作成します。
	show ip msdp sa-cache	MSDP ピアから学習した (S,G) 状態を表示します。

clear ip msdp statistics

セッションをリセットせずに、1 つまたはすべての MSDP ピアの統計情報カウンタをクリアするには、**clear ip msdp statistics** コマンドを使用します。

```
clear ip msdp [vrf vrf-name] statistics [peer-address | peer-name]
```

シンタックスの説明

vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
peer-address peer-name	(任意) 統計情報カウンタ、リセットカウント、および入力/出力カウンタがクリアされる MSDP ピアのアドレスまたは名前

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、sanjose という名前のピアのカウンタをクリアする例を示します。

```
Router# clear ip msdp statistics sanjose
Router#
```

関連コマンド

コマンド	説明
show ip msdp sa-cache	MSDP ピアから学習した (S,G) 状態を表示します。

clear ip pim auto-rp

Auto-RP キャッシュからエントリを削除するには、**clear ip pim auto-rp** コマンドを使用します。

clear ip pim [vrf vrf-name] auto-rp rp-address

シンタックスの説明	vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
	rp-address	Rendezvous Point (RP; ランデブー ポイント) アドレス。詳細については、「使用上のガイドライン」を参照してください。

デフォルト このコマンドにはデフォルト設定がありません。

コマンド モード 特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン *rp-address* 引数を入力すると、このアドレスのランデブー ポイントに関連するエントリだけがクリアされます。この引数を省略する場合、Auto-RP キャッシュ全体がクリアされます。

例 次に、Auto-RP キャッシュからすべてのエントリを削除する例を示します。

```
Router# clear ip pim auto-rp 224.5.6.7
Router#
```

関連コマンド	コマンド	説明
	show ip pim rp mapping	PIM グループとアクティブランデブー ポイントのマッピングを表示します。

clear ip pim snooping statistics

IP PIM スヌーピングのグローバルな統計情報を削除するには、**clear ip pim snooping statistics** コマンドを使用します。

clear ip pim snooping statistics

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、IP PIM 統計情報をクリアする例を示します。

```
Router# clear ip pim snooping statistics
Router#
```

関連コマンド

コマンド	説明
ip pim snooping (global configuration mode)	PIM スヌーピングをグローバルにイネーブルにします。
show ip pim snooping statistics	IP PIM スヌーピングに関する統計情報を表示します。

clear ip pim snooping vlan

特定の VLAN 上の IP PIM スヌーピング エントリを削除するには、**clear ip pim snooping vlan** コマンドを使用します。

```
clear ip pim snooping vlan vlan-id mac-address gda-address
```

```
clear ip pim snooping vlan vlan-id mroute {* | {group-addr src-addr}
  {{downstream-neighbor ip-addr} | {upstream-neighbor ip-addr}}
```

```
clear ip pim snooping vlan vlan-id neighbor {* | ip-addr}
```

シンタックスの説明

<i>vlan-id</i>	VLAN ID。有効値は 1 ~ 4094 です。
<i>mac-address</i> <i>gda-address</i>	削除するマルチキャスト グループの MAC アドレスを指定します。
<i>mroute</i> *	すべてのマルチキャスト ルート エントリを削除します。
<i>mroute</i> <i>group-addr</i> <i>src-addr</i>	指定したグループおよび送信元 IP アドレスのマルチキャスト ルート エントリを削除します。
<i>downstream-neighbor</i> <i>ip-addr</i>	join/prune メッセージを発信する特定のダウンストリーム ネイバのエントリを削除します。
<i>upstream-neighbor</i> <i>ip-addr</i>	join/prune メッセージを受信する特定のアップストリーム ネイバのエントリを削除します。
<i>neighbor</i> *	すべてのネイバを削除します。
<i>neighbor</i> <i>ip-addr</i>	特定の IP アドレスのネイバを削除します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、特定の VLAN 上の IP PIM 統計情報をクリアする例を示します。

```
Router# clear ip pim snooping vlan 25 statistics
Router#
```

関連コマンド

コマンド	説明
ip pim snooping (interface configuration mode)	特定のインターフェイスで PIM スヌーピングをイネーブルにします。
show ip pim snooping	IP PIM スヌーピングに関する情報を表示します。

clear lacp counters

特定のチャンネル グループに属するすべてのインターフェイスの統計情報をクリアするには、**clear lacp counters** コマンドを使用します。

clear lacp [*channel-group*] **counters**

シンタックスの説明

channel-group (任意) チャンネル グループ番号。有効値は 1 ~ 256 です。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

channel-group を指定しない場合は、すべてのチャンネル グループがクリアされます。

PAGP モードのメンバーを含むチャンネル グループに対してこのコマンドを入力する場合、このコマンドは無視されます。

例

次に、特定のグループの統計情報をクリアする例を示します。

```
Router# clear lacp 1 counters
Router#
```

関連コマンド

コマンド	説明
show lacp	LACP 情報を表示します。

clear logging ip access-list cache

OAL キャッシュからすべてのエントリをクリアして、Syslog に送信するには、**clear logging ip access-list cache** コマンドを使用します。

clear logging ip access-list cache

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

デフォルト このコマンドにはデフォルト設定がありません。

コマンドモード 特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、OAL キャッシュからすべてのエントリをクリアして、Syslog に送信する例を示します。

```
Router# clear logging ip access-list cache
Router#
```

関連コマンド	コマンド	説明
	logging ip access-list cache (global configuration mode)	OAL パラメータをグローバルに設定します。
	logging ip access-list cache (interface configuration mode)	方向に基づいてインターフェイス上で OAL ロギング キャッシュをイネーブルにします。
	show logging ip access-list	ロギング IP アクセス リストに関する情報を表示します。

clear mac-address-table dynamic

ダイナミック アドレス エントリをレイヤ 2 の MAC アドレス テーブルから削除するには、**clear mac-address-table dynamic** コマンドを使用します。

```
clear mac-address-table dynamic [{address mac-addr} | {interface interface
interface-number} | {protocol {assigned | ip | ipx | other}}] [vlan vlan-id]
```

シンタックスの説明

address mac-addr	(任意) MAC アドレスを指定します。
interface interface	(任意) インターフェイス タイプを指定します。有効値は ethernet 、 fastethernet 、 gigabithernet 、および tengigabithernet です。その他の有効値については、「使用上のガイドライン」を参照してください。
interface-number	(任意) モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
protocol assigned	(任意) DECnet、Banyan VINES、および AppleTalk などの割り当てられたプロトコルのバケット アカウントを指定します。
protocol ip ipx	(任意) クリアするエントリのプロトコル タイプを指定します。
protocol other	(任意) クリアするエントリのプロトコル タイプ (IP または IPX 以外) を指定します。
vlan vlan-id	(任意) VLAN ID を指定します。有効値は 1 ~ 4094 です。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

すべてのダイナミック エントリをテーブルから削除するには、引数なしで **clear mac-address-table dynamic** コマンドを入力します。

interface-number 引数はモジュールおよびポート番号を指定します。**interface-number** の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

例 次に、特定のインターフェイス (e2/1) およびプロトコルタイプ (IPX) のすべてのダイナミック レイヤ 2 エントリをクリアする例を示します。

```
Router# clear mac-address-table dynamic interface e2/1 protocol ipx
Router#
```

関連コマンド

コマンド	説明
mac-address-table aging-time	レイヤ 2 テーブルでエントリのエージング タイムを設定します。
mac-address-table static	スタティック エントリを MAC アドレス テーブルに追加するか、IGMP スヌーピングをアドレスに対してディセーブルにしてスタティック MAC アドレスを設定します。
show mac-address-table	MAC アドレス テーブルに関する情報を表示します。

clear mls acl counters

Multilayer Switching (MLS; マルチレイヤ スwitチング) ACL カウンタをクリアするには、**clear mls acl counters** コマンドを使用します。

```
clear mls acl counters {all | {interface interface interface-number} [{loopback
interface-number} | {null interface-number} | {port-channel number} | {vlan
vlan-id}]}
```

シンタックスの説明

all	すべてのインターフェイスの MLS ACL カウンタをすべてクリアします。
interface interface	指定したインターフェイスに関連付けられたカウンタをクリアします。有効値は ethernet 、 fastethernet 、 gigabitethernet 、および tengigabitethernet です。その他の有効値については、「使用上のガイドライン」を参照してください。
interface-number	モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
loopback interface-number	(任意) ループバック インターフェイスを指定します。有効値は 0 ~ 2,147,483,647 です。
null interface-number	(任意) ヌル インターフェイスを指定します。有効値は 0 です。
port-channel number	(任意) チャネル インターフェイスを指定します。有効値は 1 ~ 256 の範囲の最大 64 個の値です。
vlan vlan-id	(任意) VLAN ID を指定します。有効値は 1 ~ 4094 です。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

clear mls acl counters all を入力すると、すべてのモジュールおよびスーパーバイザ エンジンの全 MLS ACL カウンタがクリアされます。

interface-number 引数はモジュールおよびポート番号を指定します。**interface-number** の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

例

次に、すべてのインターフェイスで MLS ACL カウンタをリセットする例を示します。

```
Router# clear mls acl counters all
```

```
Router#
```

関連コマンド

コマンド	説明
show tcam interface	インターフェイススペースの TCAM に関する情報を表示します。

clear mls cef ip accounting per-prefix

プレフィクス単位の IP アカウンティング統計に関する情報をクリアするには、**clear mls cef ip accounting per-prefix** コマンドを使用します。

clear mls cef ip accounting per-prefix {all | {*prefix mask* [*instance*]}}

シンタックスの説明

all	プレフィクス単位のアカウントリング統計情報をすべてクリアします。
<i>prefix</i>	A.B.C.D のフォーマットでのエントリのプレフィクス
<i>mask</i>	エントリのプレフィクス マスク
<i>instance</i>	(任意) VPN ルーティング/転送インスタンス名

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、プレフィクス単位のアカウントリング統計に関する情報をすべてクリアする例を示します。

```
Router# clear mls cef ip accounting per-prefix all
Router#
```

clear mls cef ipv6 accounting per-prefix

プレフィクス単位の IPv6 アカウンティング統計に関する情報をクリアするには、**clear mls cef ipv6 accounting per-prefix** コマンドを使用します。

```
clear mls cef ipv6 accounting per-prefix {all | {ipv6-address/mask [instance]}}
```

シンタックスの説明

all	プレフィクス単位のアカウント統計情報をすべてクリアします。
<i>ipv6-address</i>	エントリの IPv6 アドレス。フォーマットの詳細については、「使用上のガイドライン」を参照してください。
<i>mask</i>	エントリのプレフィクス マスク
<i>instance</i>	(任意) VPN ルーティング/転送インスタンス名

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ipv6-address/mask 引数を入力する場合、フォーマット *X:X:X:X::X/mask* を使用します。*mask* の有効値は 0 ~ 128 です。

例

次に、プレフィクス単位のアカウント統計に関する情報をすべてクリアする例を示します。

```
Router# clear mls cef ipv6 accounting per-prefix all
Router#
```

clear mls ip multicast bidir-rpcache

Bidirectional (Bidir; 双方向) ランデブー ポイントのキャッシュ エントリをすべてクリアするには、**clear mls ip multicast bidir-rpcache** コマンドを使用します。

clear mls ip multicast bidir-rpcache

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

デフォルト このコマンドにはデフォルト設定がありません。

コマンド モード 特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、Bidir カウンタをリセットする例を示します。

```
Router# clear mls ip multicast bidir-rpcache
Router#
```

関連コマンド	コマンド	説明
	show mls ip multicast bidir	Bidir ハードウェアでスイッチングされるエントリを表示します。

clear mls ip multicast group

IP マルチキャスト グループを削除するには、**clear mls ip multicast group** コマンドを使用します。

```
clear mls ip multicast group {ip-name | group-address}
```

シンタックスの説明

<i>ip-name</i>	ホストの IP 名
<i>group-address</i>	(任意) 4 分割ドット表記によるマルチキャストグループのアドレス

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、IP マルチキャスト グループを削除する例を示します。

```
Router# clear mls ip multicast group 224.0.255.1
Router#
```

関連コマンド

コマンド	説明
show mls ip multicast group	特定のマルチキャストグループアドレスのエントリを表示します。

clear mls ip multicast statistics

IP マルチキャスト統計情報のカウンタをリセットするには、**clear mls ip multicast statistics** コマンドを使用します。

clear mls ip multicast statistics

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、IP マルチキャスト統計情報のカウンタをリセットする例を示します。

```
Router# clear mls ip multicast statistics
Router#
```

関連コマンド

コマンド	説明
show mls ip multicast	MLS IP 情報を表示します。

clear mls nde flow counters

NetFlow Data Export (NDE; NetFlow データ エクスポート) カウンタをクリアするには、**clear mls nde flow counters** コマンドを使用します。

clear mls nde flow counters

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

デフォルト このコマンドにはデフォルト設定がありません。

コマンドモード 特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、NDE カウンタをリセットする例を示します。

```
Router# clear mls nde flow counters
Router#
```

関連コマンド	コマンド	説明
	show mls nde	NDE ハードウェアによってスイッチングされるフローに関する情報を表示します。

clear mls netflow

MLS NetFlow のショートカット エントリをクリアするには、**clear mls netflow** コマンドを使用します。

```
clear mls netflow ip [destination ip-addr [source ip-addr-spec]] [dynamic | {sw-installed
non-static | static}] [module mod]
```

```
clear mls netflow ipv6 [destination ipv6-addr [ipv6-prefix] [source
ipv6-addr [ipv6-prefix]]] [flow {tcp | udp}] [{destination | source} port-num]
[dynamic | {sw-installed [non-static | static}] [module mod]
```

```
clear mls netflow mpls [top-label entry] [dynamic | {sw-installed [non-static | static}]
[module mod]
```

```
clear mls ipx [[module mod] [destination ipx-network [ipx-node]] [source ipx-network]
[macs mac-addr] [macd mac-addr] [interface interface-num] | [all]]
```

シンタックスの説明

ip	IP MLS エントリをクリアします。
destination <i>ip-addr</i>	(任意) 宛先のフル IP アドレスまたはサブネット アドレスを指定します。フォーマットの注意事項については、「使用上のガイドライン」を参照してください。
source <i>ip-addr-spec</i>	(任意) 送信元のフル IP アドレスまたはサブネット アドレスを指定します。フォーマットの注意事項については、「使用上のガイドライン」を参照してください。
dynamic	(任意) ハードウェアで作成された NetFlow 統計情報エントリをクリアします。
sw-installed non-static	(任意) ソフトウェアがインストールされた非スタティック エントリをクリアします。
sw-installed static	(任意) ソフトウェアがインストールされたスタティック エントリをクリアします。
module <i>mod</i>	(任意) モジュール番号を指定します。
ipv6	ソフトウェアがインストールされた IPv6 エントリをクリアします。
destination <i>ipv6-addr</i>	(任意) 宛先のフル IPv6 アドレスまたはサブネット アドレスを指定します。フォーマットの注意事項については、「使用上のガイドライン」を参照してください。
<i>ipv6-prefix</i>	(任意) IPv6 プレフィクス。有効値は 0 ~ 128 です。
source <i>ipv6-addr</i>	(任意) 送信元のフル IPv6 アドレスまたはサブネット アドレスを指定します。フォーマットの注意事項については、「使用上のガイドライン」を参照してください。
flow tcp	(任意) TCP のフロー情報をクリアします。
flow udp	(任意) UDP のフロー情報をクリアします。
destination <i>port-num</i>	(任意) 宛先ポート番号を指定します。
source <i>port-num</i>	(任意) 送信元ポート番号を指定します。
mpls	ソフトウェアがインストールされた MPLS エントリをクリアします。
top-label <i>entry</i>	(任意) top-label エントリをクリアします。有効値は 1 ~ 4,294,967,295 です。
ipx	IPX MLS エントリをクリアします。

destination <i>ipx-network</i>	(任意) 宛先 IPX アドレスを指定します。フォーマットの注意事項については、「使用上のガイドライン」を参照してください。
<i>ipx-node</i>	(任意) IPX ノードアドレス。フォーマットの注意事項については、「使用上のガイドライン」を参照してください。
source <i>ipx-network</i>	(任意) 送信元 IPX アドレスを指定します。フォーマットの注意事項については、「使用上のガイドライン」を参照してください。
macs <i>mac-addr</i>	(任意) 削除するエントリを検索するのに使用する送信元の MAC アドレスを指定します。
macd <i>mac-addr</i>	(任意) 削除するエントリを検索するのに使用する宛先の MAC アドレスを指定します。
interface <i>interface-num</i>	(任意) 指定した VLAN またはインターフェイスに関連付けられるエントリをクリアします。
all	(任意) すべてのエントリをクリアします。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

IPX アドレス構文を入力するときは、次のフォーマットを使用します。

- IPX ネットワーク アドレス : 1 ~ FFFFFFFE
- IPX ノード アドレス : x.x.x (x は 0 ~ FFFF)
- IPX アドレス : ipx_net.ipx_node (たとえば、3.0034.1245.AB45、A43.0000.0000.0001)

入力パラメータの組み合わせを入力することにより、クリアするエントリの検索を絞り込むことができます。**destination** または **source port-num** のキーワードおよび引数には、telnet、File Transfer Protocol (FTP; ファイル転送プロトコル)、WWW、SMTP、X、または DNS のいずれかを指定する必要があります。

16 までのルータを明示的に MLS-RP として組み込むことができます。

IP サブネット アドレスを指定するには、次の構文を使用します。

- *ip-subnet-addr* または *ipv6-subnet-addr* : サブネットアドレスのショートフォーマット。IP または IPv6 アドレス YY.YY.YY.00 の末尾の 10 進数 00 は、IP または IPv6 サブネットアドレスの境界を指定します。たとえば、172.22.36.00 は 24 ビットサブネットアドレス (サブネットマスク 172.22.36.00/255.255.255.0) を示し、173.24.00.00 は 16 ビットサブネットアドレス (サブネットマスク 173.24.00.00/255.255.0.0) を示します。ただし、このフォーマットで識別できるのは、8、16、または 24 ビットのサブネットアドレスだけです。
- *ip-addr/subnet-mask* または *ipv6-addr/subnet-mask* : サブネットアドレスのロングフォーマット。たとえば、172.22.252.00/255.255.252.00 は、22 ビットサブネットアドレスを示します。このフォーマットは、任意のビット数のサブネットアドレスを指定できます。より柔軟に指定するには、*ip-addr* または *ipv6-addr* に 172.22.253.1/255.255.252.00 のようなフルホストアドレスを指定します。

clear mls netflow

- *ip-addr/maskbits* または *ipv6-addr/maskbits* : サブネット アドレスの簡易ロング フォーマット。マスク ビットは、ネットワーク マスクのビット数を指定します。たとえば、172.22.252.00/22 は、22 ビット サブネット アドレスを示します。*ip-addr* または *ipv6-addr* は 193.22.253.1/22 のようなフル ホスト アドレスであり、*ip-subnet-addr* または *ipv6-subnet-addr* と同じサブネット アドレスを含みます。

all キーワードを使用しない場合、少なくとも他の 4 つのキーワード (**source**、**destination**、**flow**、または **interface**) の中の 1 つとその引数を指定する必要があります。

destination または **source port-num** のキーワードおよび引数の値を 0 にすると、すべてのエントリがクリアされます。指定されていないオプションはワイルドカードとして扱われ、エントリがすべてクリアされます。

例

次に、特定のモジュール (2) に関連付けられ、特定の宛先 IP アドレス (173.11.50.89) を持つすべてのエントリをクリアする例を示します。

```
Router# clear mls netflow ip destination 173.11.50.89 module 2
Router#
```

次に、ソフトウェアがインストールされた IPv6 エントリをクリアする例を示します。

```
Router# clear mls netflow ipv6
Router#
```

次に、統計情報をクリアする例を示します。

```
Router# clear mls netflow dynamic
Router#
```

関連コマンド

コマンド	説明
show mls netflow ip	ハードウェア NetFlow IP に関する情報を表示します。
show mls netflow ipv6	ハードウェア NetFlow IPv6 設定に関する情報を表示します。

clear mls qos

MLS の集約 QoS 統計情報をクリアするには、**clear mls qos** コマンドを使用します。

```
clear mls qos [{ip | ipx | mac | mpls | ipv6 | arp}] [{interface interface-number} |
{null interface-number} | {port-channel number} | {vlan vlan-id}]]
```

シンタックスの説明

ip	(任意) MLS の IP 集約 QoS 統計情報をクリアします。
ipx	(任意) MLS の IPX 集約 QoS 統計情報をクリアします。
mac	(任意) MLS の MAC 集約 QoS 統計情報をクリアします。
mpls	(任意) MLS の MPLS 集約 QoS 統計情報をクリアします。
ipv6	(任意) MLS の IPv6 集約 QoS 統計情報をクリアします。
arp	(任意) MLS の ARP 集約 QoS 統計情報をクリアします。
<i>interface</i>	(任意) インターフェイス タイプ。有効値は ethernet 、 fastethernet 、 gigabitethernet 、および tengigabitethernet です。その他の有効値については、「使用上のガイドライン」を参照してください。
<i>interface-number</i>	(任意) モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
null <i>interface-number</i>	(任意) nul インターフェイスを指定します。有効値は 0 です。
port-channel <i>number</i>	(任意) チャンネル インターフェイスを指定します。有効値は 1 ~ 256 の範囲の最大 64 個の値です。
vlan <i>vlan-id</i>	(任意) VLAN ID を指定します。有効値は 1 ~ 4094 です。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



(注)

clear mls qos コマンドを入力した場合、ポリシングのトークン バケット カウンタが影響を受け、ポリシングされるはずのトラフィックが転送される可能性があります。

interface-number 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

■ clear mls qos

引数なしで **clear mls qos** コマンドを入力すると、すべてのプロトコルでグローバルおよびインターフェイス単位の集約 QoS カウンタがクリアされます。

インターフェイス タイプを入力しない場合、すべてのインターフェイスのプロトコル集約 QoS カウンタがクリアされます。

例

次に、すべてのプロトコルでグローバルおよびインターフェイス単位の集約 QoS カウンタをクリアする例を示します。

```
Router# clear mls qos
Router#
```

次に、すべてのインターフェイスで特定プロトコルの集約 QoS カウンタをクリアする例を示します。

```
Router# clear mls qos ip
Router#
```

関連コマンド

コマンド	説明
show mls qos	MLS QoS 情報を表示します。

clear mls statistics

MLS 統計情報のカウンタをリセットするには、**clear mls statistics** コマンドを使用します。

clear mls statistics [module num]

シンタックスの説明

module num (任意) モジュール番号を指定します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

clear mls stats コマンドが、このコマンドに置き換えられました。

例

次に、すべてのモジュールの MLS 統計情報カウンタをリセットする例を示します。

```
Router# clear mls statistics
Router#
```

次に、特定のモジュールの MLS 統計情報カウンタをリセットする例を示します。

```
Router# clear mls statistics module 5
Router#
```

関連コマンド

コマンド	説明
show mls statistics	IP、IPX、マルチキャスト、レイヤ 2 プロトコル、および QoS の MLS 統計情報を表示します。

clear mls stats

MLS の統計情報をクリアするには、**clear mls stats** コマンドを使用します。

clear mls stats

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、すべてのモジュールの MLS 統計情報をクリアする例を示します。

```
Router# clear mls stats
Router#
```

関連コマンド

コマンド	説明
clear mls statistics	MLS 統計カウンタをリセットします。

clear pagp

ポート チャネル情報をクリアするには、**clear pagp** コマンドを使用します。

```
clear pagp {group-number | counters}
```

シンタックスの説明

<i>group-number</i>	チャンネル グループ番号。有効値は 1 ～ 256 の範囲の最大 64 個の値です。
counters	トラフィック フィルタをクリアします。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、特定グループのポート チャネル情報をクリアする例を示します。

```
Router# clear pagp 324  
Router#
```

次に、ポート チャネル トラフィック フィルタをクリアする例を示します。

```
Router# clear pagp counters  
Router#
```

関連コマンド

コマンド	説明
show pagp	ポート チャネル情報を表示します。

clear platform netint

プラットフォームの割り込みスロットリング カウンタをクリアするには、**clear platform netint** コマンドを使用します。

clear platform netint

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、プラットフォームの割り込みスロットリング カウンタをクリアする例を示します。

```
Router# clear platform netint
Router#
```

関連コマンド

コマンド	説明
show platform netint	プラットフォームのネットワーク割り込み情報を表示します。

clear platform pisa ixp counters

Supervisor Engine 32 PISA 固有カウンタをクリアするには、**clear platform pisa ixp** コマンドを使用します。

clear platform pisa ixp counters *counter*

シンタックスの説明	<i>counter</i>	カウンタ情報。有効値については、「使用上のガイドライン」を参照してください。
-----------	----------------	--

デフォルト このコマンドにはデフォルト設定がありません。

コマンドモード 特権 EXEC (#)

コマンドの履歴	リリース	変更内容
	12.2(18)ZYA	このコマンドのサポートが追加されました。
	12.2(18)ZYA1	このコマンドのサポートは、 clear platform pisa np counters コマンドの使用が推奨されるため廃止されました。

使用上のガイドライン *counter* 引数の有効値は次のとおりです。

- **all counters** : Supervisor Engine 32 PISA 固有カウンタをすべてクリアします。
- **fpm counters** : Flexible Packet Matching (FPM; フレキシブル パケット マッチング) カウンタをクリアします。
- **me num counters** : マイクロエンジン情報をクリアします。有効値は 0 ~ 15 です。
- **mqc counters** : モジュラ サービス品質 (QoS) CLI カウンタをクリアします。
- **mtacl counters** : MTrie ACL カウンタをクリアします。
- **nbar counters** : Network-Based Application Recognition (NBAR) カウンタをクリアします。
- **rx counters** : 受信エンジン カウンタをクリアします。
- **tx counters** : 送信エンジン カウンタをクリアします。
- **urlf counters** : URL フィルタリング カウンタをクリアします。
- **vfr counters** : Virtual Fragmentation and Reassembly (VFR) カウンタをクリアします。

例 次に、プラットフォームのフレキシブルパケットマッチング (FPM) カウンタをクリアする例を示します。

```
Router# clear platform pisa ixp counters fpm
FPM Statistics cleared
```

```
Router#
```

■ clear platform pisa ixp counters

関連コマンド

コマンド	説明
show platform pisa np	Supervisor Engine 32 PISA 固有情報を表示します。

clear platform pisa np counters

プラットフォームの Supervisor Engine 32 PISA 固有カウンタをクリアするには、**clear platform pisa np counters** コマンドを使用します。

clear platform pisa np counter counters

シンタックスの説明	<i>counter</i>	カウンタ情報。有効値については、「使用上のガイドライン」を参照してください。
-----------	----------------	--

デフォルト このコマンドにはデフォルト設定がありません。

コマンドモード 特権 EXEC (#)

コマンドの履歴	リリース	変更内容
	12.2(18)ZYA1	このコマンドのサポートが、 clear platform pisa ixp counters コマンドを入れ替えるために導入されました。

使用上のガイドライン counter 引数の有効値は次のとおりです。

- **all** : すべての Supervisor Engine 32 PISA 固有カウンタをクリアします。
- **fpm** : フレキシブル パケット マッチング (FPM) カウンタをクリアします。
- **me num** : マイクロエンジン情報をクリアします。有効値は 0 ~ 15 です。
- **mqc** : サービス品質 (QoS) CLI カウンタをクリアします。
- **mtacl** : MTrie ACL カウンタをクリアします。
- **nbar** : Network-Based Application Recognition (NBAR) カウンタをクリアします。
- **rx** : 受信エンジン カウンタをクリアします。
- **tagging** : プロトコル タギング カウンタをクリアします。
- **tx** : 送信エンジンカウンタ をクリアします。
- **urlf** : URL フィルタリング カウンタをクリアします。
- **vfr** : Virtual Fragmentation and Reassembly (VFR) カウンタをクリアします。

例 次に、プラットフォームのすべての Supervisor Engine 32 PISA 固有カウンタをクリアする例を示します。

```
Router# clear platform pisa np all counters
RX Statistics cleared for ME: 0
TX Statistics cleared for ME: 1
NBAR Statistics cleared
URLF Statistics cleared
MQC Statistics cleared
```

■ clear platform pisa np counters

```
ACL Statistics cleared
FPM Statistics cleared
VFR Statistics cleared
Protocol Tagging Statistics cleared
Stubs Statistics cleared for ME: 2 to 15
```

Router#

関連コマンド

コマンド	説明
show platform pisa np	Supervisor Engine 32 PISA 固有情報を表示します。

clear port-security

MAC アドレス テーブルからセキュア MAC アドレスおよびスティッキ MAC アドレスを削除するには、**clear port-security** コマンドを使用します。

```
clear port-security dynamic [{address mac-addr} | {interface interface-id}] [vlan vlan-id]
```

シンタックスの説明

address mac-addr	(任意) 指定されたセキュア MAC アドレスまたはスティッキ MAC アドレスを削除します。
interface interface-id	(任意) 指定された物理ポートまたはポート チャネル上のすべてのセキュア MAC アドレスおよびスティッキ MAC アドレスを削除します。
vlan vlan-id	(任意) 指定された VLAN から特定のセキュア MAC アドレスまたはスティッキ MAC アドレスを削除します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドをサポートするのは、ネゴシエートされたトランクだけです。

キーワードまたは引数を指定せずに **clear port-security** コマンドを入力した場合、MAC アドレス テーブルからすべてのセキュア MAC アドレスおよびスティッキ MAC アドレスが削除されます。

clear port-security dynamic interface interface-id コマンドを入力すると、インターフェイス上のすべてのセキュア MAC アドレスおよびスティッキ MAC アドレスが MAC アドレス テーブルから削除されます。

この情報が削除されたことを確認する場合は、**show port-security** コマンドを入力します。

例

次に、MAC アドレス テーブルから特定のセキュア MAC アドレスを削除する例を示します。

```
Router# clear port-security dynamic address 0008.0070.0007
Router#
```

次に、特定のインターフェイスで学習されたすべてのセキュア MAC アドレスおよびスティッキ MAC アドレスを削除する例を示します。

```
Router# clear port-security dynamic interface gigabitethernet0/1
Router#
```

■ clear port-security

関連コマンド

コマンド	説明
show port-security	ポート セキュリティ設定に関する情報を表示します。
switchport port-security mac-address	セキュア MAC アドレスのリストに MAC アドレスを追加します。

clear spanning-tree detected-protocol

プロトコル マイグレーションを再開するには、**clear spanning-tree detected-protocol** コマンドを使用します。

clear spanning-tree detected-protocol [*interface interface interface-num*]

シンタックスの説明	interface interface
	(任意) インターフェイスのタイプと番号を指定します。タイプの有効値は ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 port-channel 、および vlan です。その他の有効値については、「使用上のガイドライン」を参照してください。
	<i>interface-num</i> モジュールおよびポート番号。 port-channel および vlan の有効値については、「使用上のガイドライン」を参照してください。

デフォルト このコマンドにはデフォルト設定がありません。

コマンド モード EXEC

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン RSTP および MST には他のリージョンまたは別のバージョンの IEEE スパニング ツリーと正しく対話するための互換メカニズムが組み込まれています。たとえば、レガシーブリッジに接続した RSTP ブリッジは、ポートのいずれかで 802.1D BPDU を送信できます。MST ブリッジがレガシー BPDU または別のリージョンに関連付けられた MST BPDU を受信すると、ポートがリージョンの境界にあることを検出します。このようなメカニズムは必ずしも最も効率的なモードへ復帰できるとはかぎりません。たとえば、レガシー 802.1D に指定された RSTP ブリッジは、レガシーブリッジがリンクから取り外されたあとも 802.1D モードのままです。同様に、MST ポートは接続しているブリッジが同じリージョンに加入したあとも、自身を境界ポートと見なします。強制的にネイバと再ネゴシエーションさせる場合は、**clear spanning-tree detected-protocol** コマンドを入力します。

interface-number の有効値は、指定したインターフェイス タイプおよび使用されているシャーシおよびモジュールによって決まります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 2 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

port-channel number の有効値は、1 ~ 256 の範囲の最大 64 個の値です。

引数なしで **clear spanning-tree detected-protocol** コマンドを入力する場合、コマンドは Catalyst 6500 シリーズ スイッチのすべてのポートに適用されます。

■ clear spanning-tree detected-protocol

例

次に、特定のインターフェイスでプロトコルマイグレーションを再開させる例を示します。

```
Router# clear spanning-tree detected-protocol fa1/1
Router#
```

関連コマンド

コマンド	説明
show spanning-tree mst	MST プロトコルに関する情報を表示します。

clear top counters interface report

TopN レポートをクリアするには、**clear top counters interface report** コマンドを使用します。

clear top counters interface report *number*

シンタックスの説明	<i>number</i> (任意) 表示されるポートの数。有効値は、1 ~ 5000 の物理ポートです。
-----------	---

デフォルト	このコマンドにはデフォルト設定がありません。
-------	------------------------

コマンドモード	EXEC
---------	------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドは、イーサネット、ファストイーサネット、ギガビットイーサネット、および10ギガビットイーサネットのポートだけでサポートされます。OSM 上の LAN ポートもサポートされます。

clear top interface report コマンドにより、完了したすべてのレポートがクリアされます。保留中の TopN レポートは削除されません。レポート番号が指定された場合、TopN タスクはステータスに関係なくクリアされます。

例 次に、すべての TopN タスクをクリアする例を示します。

```
Router# clear top counters interface report
04:00:06: %TOPN_COUNTERS-5-DELETED: TopN report 1 deleted by the console
04:00:06: %TOPN_COUNTERS-5-DELETED: TopN report 2 deleted by the console
04:00:06: %TOPN_COUNTERS-5-DELETED: TopN report 3 deleted by the console
04:00:06: %TOPN_COUNTERS-5-DELETED: TopN report 4 deleted by the console1/24/
Router#
```

次に、保留中の TopN タスクをクリアしようとした場合の出力例を示します。

```
Router# clear top counters interface report 4
04:52:12: %TOPN_COUNTERS-5-KILLED: TopN report 4 killed by the sattili onvty0 (9.10.69.9)
Router#
```

関連コマンド	コマンド	説明
	collect top counters interface	TopN プロセスおよび特定の TopN レポートを表示します。
	show top counters interface report	TopN レポートおよび情報を表示します。

clear vlan counters

ソフトウェア キャッシュ カウンタの値をクリアし、指定された VLAN または既存のすべての VLAN で再び 0 から開始するには、**clear vlan counters** コマンドを使用します。

clear vlan [vlan-id] counters

シンタックスの説明

vlan-id (任意) VLAN ID。有効値については、「使用上のガイドライン」を参照してください。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

vlan-id を指定しない場合、既存のすべての VLAN に対するソフトウェア キャッシュ カウンタの値がクリアされます。

例

次に、指定した VLAN に対するソフトウェア キャッシュ カウンタの値をクリアする例を示します。

```
Router# clear vlan 10 counters
Clear "show vlan" counters on this vlan [confirm]y
Router#
```

関連コマンド

コマンド	説明
show vlan counters	ソフトウェア キャッシュ カウンタの値を表示します。

clock

1000BASE-T トランシーバにポート クロッキング モードを設定するには、**clock** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

clock {**auto** | **active** [**prefer**] | **passive** [**prefer**]}

no clock

シンタックスの説明

auto	自動クロック コンフィギュレーションをイネーブルにします。
active	アクティブ動作をイネーブルにします。
prefer	(任意) 指定されたモードをリンクの遠端とネゴシエートします。
passive	パッシブ動作をイネーブルにします。

デフォルト

auto

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、1000BASE-T トランシーバだけでサポートされています。

リンクの近端のクロック モードが遠端のクロック モードと一致しない場合、ライン プロトコルは動作しません。

自動ネゴシエーション中に、アクティブおよびパッシブ クロック ステータスが決定されてから、伝送リンクが確立されます。

clock コマンドは、次のコンフィギュレーションをサポートしています。

- **auto** : リンクの遠端と自動ネゴシエートしますが、アクティブクロック スイッチが優先されます。
- **active** : ローカル クロックを使用して、トランスミッタ動作のタイミングを決定します。
- **passive** : クロックを受信信号から回復し、回復済みクロックを使用して、トランスミッタ動作のタイミングを決定します。
- **active prefer** : リンクの遠端と自動ネゴシエートしますが、アクティブクロック スイッチが優先されます。
- **passive prefer** : リンクの遠端と自動ネゴシエートしますが、パッシブクロック スイッチが優先されます。

現在のクロック モードを表示するには、**show running-config interface** コマンドを使用します。

ファームウェアによりネゴシエートされたクロック モードを表示するには、**show interfaces** コマンドを入力します。

■ clock

例 次に、アクティブクロックの動作をイネーブルにする例を示します。

```
Router(config-if)# clock active  
Router(config-if)#
```

関連コマンド

コマンド	説明
show interfaces	特定のインターフェイスが認識するトラフィックを表示します。
show running-config interface	モジュールまたはレイヤ 2 VLAN のステータスおよび設定を表示します。

collect top counters interface

TopN プロセスおよび特定の TopN レポートを表示するには、**collect top counters interface** コマンドを使用します。

```
collect top [number] counters interface interface-type [interval seconds] [sort-by
sort-by-value]
```

シンタックスの説明

<i>number</i>	(任意) 表示されるポートの数。有効値は、1 ~ 5000 の物理ポートです。
<i>interface-type</i>	TopN 要求で使用されるポート タイプ。有効値は、 all 、 ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 layer-2 vlan-num 、および layer-3 です。
<i>interval seconds</i>	(任意) 統計情報を収集するインターバルを指定します。有効値は、0 ~ 999 秒です。
<i>sort-by sort-by-value</i>	(任意) レポートを生成するポート統計情報を指定します。有効値は、次のとおりです。 <ul style="list-style-type: none"> • broadcast : 送受信ブロードキャスト パケットに基づいて、レポートをソートします。 • bytes : 送受信バイトに基づいて、レポートをソートします。 • errors : 受信エラーに基づいて、レポートをソートします。 • multicast : 送受信マルチキャスト パケットに基づいて、レポートをソートします。 • overflow : 送信オーバーフロー エラーに基づいて、レポートをソートします。 • packets : 送受信パケットに基づいて、レポートをソートします。 • utilization : ポートの利用率に基づいて、レポートをソートします。

デフォルト

デフォルト設定は次のとおりです。

- *number* は、**20** の物理ポートです。
- *sort-by-value* は、**util** です。
- *seconds* は、**30** 秒です。
- *interface-type* は、**all** です。

コマンドモード

EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、イーサネット、ファストイーサネット、ギガビットイーサネットおよび 10 ギガビットイーサネットポートだけでサポートされます。OSM 上の LAN ポートもサポートされます。

0 秒のインターバルを指定すると、TopN レポートは絶対カウンタ値に基づいて生成されます。特定のインターバルで計算されるのは利用率だけであるため、ソート基準が **utilization** の場合は、**interval seconds** キーワードおよび引数は指定できません。

layer-2 vlan-num を指定した場合、有効値は 1 ~ 4094 で、レイヤ 2 インターフェイス数を示します。レポートを表示できるのは、完了済みステータスを伴う TopN タスクだけです。不完全（保留中）であるレポートを表示しようとすると、該当するメッセージが表示されます。

TopN ユーティリティは、*seconds* インターバルで次の物理ポート単位のポート利用率データを収集します。

- 送受信バイトの総数
- 送受信パケットの総数
- 送受信ブロードキャストパケットの総数
- 送受信マルチキャストパケットの総数
- エラーの総数（Cyclic Redundancy Check（CRC; 巡回冗長検査）などのイーサネットポート、サイズ不足パケット（+Runt）、サイズ超過パケット、フラグメンテーション、およびジャバー）
- アウトロストパケットを含むバッファオーバーフローエラーの総数（バッファが満杯であることが原因の送信エラーおよび dmaTxOverflow、dmaTxFull のイーサネットポートなど）

情報が収集されると、ポートは *sort-by-value* 引数に従ってソートされ、上から *number* 個のポートが表示されます。

TopN レポートの準備ができると、TopN レポートが使用できるという Syslog メッセージが表示されます。レポートを表示する場合は、**show top interface report** コマンドを使用します。**clear top interface report** コマンドを入力してレポートをクリアするまで、何度でも TopN レポートを表示できます。

レポートをクリアするには、**clear top interface report** コマンドを使用します。

例

次に、送受信ブロードキャストパケットに基づいて TopN レポートをソートする例を示します。

```
Router# collect top 40 counters interface all sort-by broadcast
Router#
```

次に、送受信ブロードキャストパケットに基づいて TopN レポートをソートして、TopN サンプリングインターバルを指定する例を示します。

```
Router# collect top 40 counters interface all sort-by broadcast interval 500
Router#
```

関連コマンド

コマンド	説明
clear top counters interface report	TopN レポートをクリアします。
show top counters interface report	TopN レポートおよび情報を表示します。

control-plane

ユーザが、装置のコントロールプレーンに関連付けられた引数またはパラメータ（サービス ポリシー など）の関連付けおよび変更が許可されるコントロールプレーン コンフィギュレーション モードを開始するには、**control-plane** コマンドを使用します。

control-plane

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

デフォルト

コントロールプレーンのサービス ポリシーは、定義されていません。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



(注)

すべてのクラスにポリシー アクションを設定する必要があります。すべてのクラスにポリシー アクションを設定しなかった場合、トラフィックはポリシー アクションがないクラスをスキップし、後続クラスとマッチングします。

control-plane コマンドを入力すると、ルート プロセッサの集約コントロールプレーン サービスを定義できます。たとえば、コントロールプレーンとサービス ポリシーを関連付けて、コントロールプレーン宛のすべてのトラフィックをポリシングできます。

例

次に、信頼できるホストを送信元アドレス 10.1.1.1 および 10.1.1.2 に設定して、Telnet パケットをコントロールプレーンに制限なく転送し、残りのすべての Telnet パケットには指定速度でのポリシングを許可する例を示します。

```
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
! Allow 10.1.1.2 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
! Rate limit all other Telnet traffic.
Router(config)# access-list 140 permit tcp any any eq telnet
! Define class-map "telnet-class."
Router(config)# class-map telnet-class
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map control-plane
Router(config-pmap)# class telnet-class
```

control-plane

```

Router(config-pmap-c)# police 80000 conform transmit exceed drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
! Define aggregate control plane service for the active Route Processor.
Router(config)# control-plane
Router(config-cp)# service-policy input control-plane-policy
Router(config-cp)# exit

```

関連コマンド

コマンド	説明
class (policy-map)	作成または変更を行うポリシーがあるクラスの名前を指定するか、ポリシーを設定する前にデフォルトクラス（一般には <code>class-default</code> クラス）を指定します。
class-map	QoS クラス マップを設定するための QoS クラス マップ コンフィギュレーションモードにアクセスします。
drop	特定のクラスに属すパケットを破棄するようにトラフィック クラスを設定します。
match access-group	指定された ACL を基に、クラス マップの一致基準を設定します。
policy-map	QoS ポリシー マップを設定するための QoS ポリシー マップ コンフィギュレーションモードにアクセスします。
service-policy (control-plane)	集約コントロールプレーン サービスのコントロールプレーンにポリシー マップを付加します。
show policy-map control-plane	コントロールプレーンのポリシー マップの 1 つのクラスまたはすべてのクラスの設定を表示します。

copy /noverify

現在のコピー操作の自動イメージ確認をディセーブルにするには、**copy /noverify** コマンドを使用します。

copy /noverify source-url destination-url

シンタックスの説明

<i>source-url</i>	コピー元のファイルまたはディレクトリの場所を示す URL またはエイリアス。詳細については「使用上のガイドライン」を参照してください。
<i>destination-url</i>	ファイルまたはディレクトリのコピー先を示す URL またはエイリアス。詳細については「使用上のガイドライン」を参照してください。

デフォルト

コピー操作が完了すると自動的に確認が行われます。

コマンド モード

EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

コピー元およびコピー先の URL の形式は、ファイルまたはディレクトリの場所によって変わります。特定のファイルのエイリアス キーワードまたはファイル システム タイプのエイリアス キーワード（特定のタイプ内のファイルではない）のどちらを使用してもかまいません。



ワンポイントアドバイス

エイリアスは入力量を少なくするために使用します。たとえば、**copy system:r nvram:s**（**copy system:running-config nvram:startup-config** コマンドの省略形）と入力するよりも **copy run start**（**copy running-config startup-config** コマンドの省略形）の方が簡単です。エイリアスを使用すると、以前のバージョンの Cisco IOS ソフトウェアで使用されていた共通コマンドの一部を引き続き使用できます。

表 2-3 に、URL のキーワード ショートカットを 2 つ示します。

表 2-3 URL の共通キーワード エイリアス

キーワード	コピー元またはコピー先
running-config	(任意) system:running-config の URL のエイリアスを指定します。このキーワードは、 more および show file コマンド構文では動作しません。
startup-config	(任意) nvram:startup-config の URL のエイリアスを指定します。 nvram:startup-config キーワードは、初期化（起動）中に使用されるコンフィギュレーション ファイルを示します。このファイルは NVRAM に保存されます。このキーワードは、 more および show file EXEC コマンド構文では動作しません。

表 2-4 から表 2-6 に、ファイル システム タイプ別のエイリアスを紹介します。エイリアスを指定しない場合、システムは現在のディレクトリ内のファイルを検索します。

表 2-4 に、特別な (opaque) ファイル システムの URL プレフィクス エイリアスを、表 2-5 にネットワーク ファイル システムの URL プレフィクス エイリアスを、表 2-6 にローカルで書き込み可能なストレージ ファイル システムの URL プレフィクス エイリアスを示します。

表 2-4 特別なファイル システムの URL プレフィクス エイリアス

エイリアス	コピー元またはコピー先
flh:	フラッシュのロード ヘルパー ログ ファイルのコピー元 URL
nvr:	ルータの NVRAM。NVRAM から、または NVRAM ヘスタートアップ コンフィギュレーションをコピーできます。また、プライベート コンフィギュレーション ファイルのサイズの表示もできます。
null:	ヌルのコピー先またはファイル。リモート ファイルをヌルへコピーして、サイズを判別できます。
system:	システム メモリのコピー元またはコピー先 URL (実行コンフィギュレーションを含む)
xmodem:	Xmodem プロトコルを使用するネットワーク装置からのファイルのコピー元またはコピー先
ymodem:	Ymodem プロトコルを使用するネットワーク装置からのファイルのコピー元またはコピー先

表 2-5 ネットワーク ファイル システムの URL プレフィクス エイリアス

エイリアス	コピー元またはコピー先
ftp:	FTP ネットワーク サーバのコピー元またはコピー先 URL。このエイリアスの構文は次のとおりです。 ftp: [[[//username [:password]@]location]/directory]/filename
rcp:	rcp ネットワーク サーバのコピー元またはコピー先 URL。このエイリアスの構文は次のとおりです。 rcp: [[[//username@]location]/directory]/filename
tftp:	TFTP ネットワーク サーバのコピー元またはコピー先 URL。このエイリアスの構文は次のとおりです。 tftp: [[[//location]/directory]/filename

表 2-6 ローカルで書き込み可能なストレージ ファイル システムの URL プレフィクス エイリアス

エイリアス	コピー元またはコピー先
bootflash:	ブート フラッシュ メモリのコピー元またはコピー先 URL
disk0: および disk1:	回転メディアのコピー元またはコピー先 URL
flash:	フラッシュ メモリのコピー元またはコピー先 URL。このエイリアスはすべてのプラットフォームで使用できます。 フラッシュ装置のないプラットフォームの場合、 flash: のエイリアスは slot0: に設定されるため、すべてのプラットフォームのメイン フラッシュ メモリのストレージ エリアを指定できます。

表 2-6 ローカルで書き込み可能なストレージ ファイル システムの URL プレフィクス エイリアス (続)

エイリアス	コピー元またはコピー先
slavebootflash:	High System Availability (HSA; ハイ システム アベイラビリティ) に設定された装置のスレーブ RSP カード上にある内部フラッシュ メモリのコピー元またはコピー先 URL
slaveram:	HSA に設定された装置のスレーブ RSP カード上の NVRAM
slavedisk0:	HSA に設定された装置のスレーブ RSP カード上にある最初の PCMCIA カードのコピー元またはコピー先 URL
slavedisk1:	HSA に設定された装置のスレーブ RSP カード上にある 2 番目の PCMCIA スロットのコピー元またはコピー先 URL
slaveslot0:	HSA に設定されたルータのスレーブ RSP カード上にある最初の PCMCIA カードのコピー元またはコピー先 URL (サポート対象外)
slaveslot1:	HSA に設定されたルータのスレーブ RSP カード上にある 2 番目の PCMCIA カードのコピー元またはコピー先 URL (サポート対象外)
slot0:	最初の PCMCIA フラッシュ メモリ カードのコピー元またはコピー先 URL (サポート対象外)
slot1:	2 番目の PCMCIA フラッシュ メモリ カードのコピー元またはコピー先 URL (サポート対象外)

コマンドライン上で必要なすべてのコピー元およびコピー先 URL 情報、および使用するユーザ名とパスワードを入力できます。または、**copy** コマンドを入力して、不足している情報の入力をスイッチに指示させることができます。

情報を入力する場合は、3 つのオプション (**running-config**、**startup-config**、またはファイル システム エイリアス) のいずれか 1 つを選択します (表 2-3 ~ 表 2-6 を参照してください)。コピー元またはコピー先 URL の形式は、ファイル システムの場所によって決まります。

エイリアスの後ろにはコロンが必要です。コロンを必要としない以前のコマンドも引き続きサポートされていますが、コンテキスト ヘルプでは使用できません。

コピー処理は全体で数分かかる場合がありますが、プロトコルやネットワークによって異なります。

ftp:、**rep:**、および **tftp:** のエイリアス構文では、ロケーションは IP アドレスまたはホスト名です。ファイル名は、ファイル転送で使用するディレクトリに対して指定します。

確認をグローバルに設定するには、**file verify auto** コマンドを使用します。

例

次に、現在のコピー操作の自動イメージ確認をディセーブルにする例を示します。

```
Router# copy /noverify tftp: sup-bootflash:
.....
[OK - 24301348 bytes]
24301348 bytes copied in 157.328 secs (154463 bytes/sec)
Router#
```

関連コマンド

コマンド	説明
file verify auto	圧縮 Cisco IOS イメージチェックサムを確認します。
verify	フラッシュ メモリ ファイル システムのファイルのチェックサムを確認するか、ファイルの MD5 シグニチャを計算します。

■ copy /noverify

define interface-range

インターフェイス レンジ マクロを作成するには、**define interface-range** コマンドを使用します。

define interface-range *macro-name interface-range*

シンタックスの説明

<i>macro-name</i>	インターフェイス レンジ マクロ名。32 文字まで指定できます。
<i>interface-range</i>	インターフェイス範囲を指定します。インターフェイス範囲の有効値の一覧については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

マクロ名は 32 文字までの文字ストリングです。

マクロには最大 5 つまでの範囲を含むことができます。インターフェイス範囲はスロットをまたがることはできません。*interface-range* を入力する場合、次のフォーマットを使用できます。

- *card-type* {*slot*}/*{first-interface}* - *{last-interface}*
- *card-type* {*slot*}/*{first-interface}* - *{last-interface}*

card-type の有効値は次のとおりです。

- **ethernet**
- **fastethernet**
- **gigabitethernet**
- **loopback**
- **tengigabitethernet**
- **tunnel**
- **vlan** *vlan-id* (有効値は 1 ~ 4094)
- **port-channel** *interface-number* (有効値は 1 ~ 256)

■ **define interface-range**

例 次に、複数のインターフェイスのマクロを作成する例を示します。

```
Router(config)# define interface-range macro1 ethernet 1/2 - 5, fastethernet 5/5 - 10  
Router(config)#
```

関連コマンド

コマンド	説明
interface range	複数のポートに同時にコマンドを実行します。

diagnostic bootup level

ブートアップ診断レベルを設定するには **diagnostic bootup level** コマンドを使用します。診断テストをすべて省略するには、このコマンドの **no** 形式を使用します。

diagnostic bootup level {minimal | complete}

default diagnostic bootup level

no diagnostic bootup level

シンタックスの説明

minimal	最小限の診断を指定します。詳細については、「使用上のガイドライン」を参照してください。
complete	すべての診断を指定します。詳細については、「使用上のガイドライン」を参照してください。
default	デフォルト設定に戻します。

コマンドのデフォルト

minimal

コマンドモード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

診断レベルの設定により、システムまたはモジュールがリセットされるときに行われるテストのレベルが決定します。次の 2 つのレベルがあります。

- **complete** : すべてのテストを実行します。
- **minimal** : スーパーバイザ エンジンには Enhanced Address Recognition Logic (EARL) テストだけを実行し、システムのすべてのポートにはループバック テストを行います。



(注) デフォルトは **minimal** ですが、ハードウェアの問題をトラブルシューティングするために診断レベルを **complete** に設定できます。

特定の状況においては、ブートアップ オンライン診断をすべて省略する必要がある場合もあります。たとえば、オンライン診断で不良と診断されたポートが本当に不良かを確認するのに、ブートアップ オンライン診断を省略する場合などです。完全に診断テストを省略するには、**no diagnostic bootup level** コマンドを入力します。

診断テスト タイプの詳細については、[show diagnostic](#) コマンドを参照してください。

新しいレベルは、次回のリロード時または、次に Online Insertion and Removal (OIR; ホットスワップ) が行われたときに実施されます。

例

次に、ブートアップ診断レベルを設定する例を示します。

```
Router(config)# diagnostic bootup level complete  
Router(config)#
```

関連コマンド

コマンド	説明
show diagnostic bootup level	設定されたブートアップ診断のカバレッジ レベルを表示します。

diagnostic cns

Cisco Networking Services (CNS) 診断を設定するには、**diagnostic cns** コマンドを使用します。CNS イベントバスへの診断結果の送信をディセーブルにするには、このコマンドの **no** 形式を使用します。

diagnostic cns {**publish** | **subscribe**} [*subject*]

default diagnostic cns {**publish** | **subscribe**}

no diagnostic cns {**publish** | **subscribe**} [*subject*]

シンタックスの説明

publish	診断結果をリモート ネットワーク アプリケーションに送信し、診断結果に基づく決定および修正処置を行います。
subscribe	リモート ネットワーク アプリケーションからメッセージを受信し、診断テストの実行または診断結果の検索を行います。
<i>subject</i>	(任意) イベント サブジェクト名
default	デフォルト値に設定します。

コマンド モード

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

オンライン診断は、イベントの *subject* 名を **subscribe** (予約) することにより、イベントを受信します。*subject* は、CNS バスを通じて **subscribe** (受信) または **publish** (生成) するイベントです。

diagnostic cns publish コマンドは、診断結果をリモート ネットワーク アプリケーションに送信し、診断結果に基づく決定および修正処置を行います。

diagnostic cns subscribe コマンドは、リモート ネットワーク アプリケーションからメッセージを受信し、診断テストまたは診断結果の検索を行います。

例

次に、診断結果の生成をイネーブルにする例を示します。

```
Router(config)# diagnostic cns publish
Router(config)#
```

■ diagnostic cns

次に、リモート ネットワーク アプリケーションからメッセージを受信し、診断テストの実行または診断結果の検索を行う例を示します。

```
Router(config)# diagnostic cns subscribe
Router(config)#
```

次に、デフォルトを **publish** に設定する例を示します。

```
Router(config)# default diagnostic cns publish
Router(config)#
```

コマンドのデフォルト

コマンド	説明
<code>show diagnostic cns</code>	CNS サブジェクトに関する情報を表示します。

diagnostic event-log size

診断イベントログのサイズを動的に変更するには、**diagnostic event-log size** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

diagnostic event-log size *size*

default diagnostic event-log size

no diagnostic event-log size

シンタックスの説明

<i>size</i>	診断イベントログのサイズ。有効値は 1 ~ 10,000 エントリです。
default	デフォルト設定に戻します。

コマンドのデフォルト

size は 500 エントリです。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

イベントは動的に割り当てられ、循環キューに保存されます。

デフォルト設定に戻すには、**default diagnostic event-log size** コマンド、または **no diagnostic event-log size** コマンドを使用します。

例

次に、診断イベントログのサイズを設定する例を示します。

```
Router(config)# diagnostic event-log size 600
Router(config)#
```

関連コマンド

コマンド	説明
show diagnostic events	診断イベントのイベント ログを表示します。

diagnostic monitor

ヘルス モニタリング診断テストを設定するには、**diagnostic monitor** コマンドを使用します。診断テストをディセーブルにするには、このコマンドの **no** 形式を使用します。

diagnostic monitor interval {*module num*} **test** {*test-id* | *test-id-range* | **all**} [*hour hh*]
 [*min mm*] [*second ss*] [*millisec ms*] [*day day*]

diagnostic monitor syslog

diagnostic monitor {*module num*} **test** {*test-id* | *test-id-range* | **all**}

no diagnostic monitor {*interval* | *syslog*}

シンタックスの説明

interval	テストを行う間隔を設定します。
module num	モジュール番号を指定します。
test	テストの実行を指定します。
<i>test-id</i>	実行するテストの ID 番号。詳細については、「使用上のガイドライン」を参照してください。
<i>test-id-range</i>	実行するテストの ID 番号の範囲。詳細については、「使用上のガイドライン」を参照してください。
all	すべての診断テストを実行します。
hour hh	(任意) テスト間隔 (時間) を指定します。フォーマットの注意事項については、「使用上のガイドライン」を参照してください。
min mm	(任意) テスト間隔 (分) を指定します。フォーマットの注意事項については、「使用上のガイドライン」を参照してください。
second ss	(任意) テスト間隔 (秒) を指定します。フォーマットの注意事項については、「使用上のガイドライン」を参照してください。
millisec ms	(任意) テスト間隔 (ミリ秒) を指定します。フォーマットの注意事項については、「使用上のガイドライン」を参照してください。
day day	(任意) テスト間隔 (日数) を指定します。フォーマットの注意事項については、「使用上のガイドライン」を参照してください。
syslog	ヘルス モニタリング テストが失敗した場合に、Syslog メッセージの生成をイネーブルにします。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- 実行するテストに応じて、モニタリングはイネーブルまたはディセーブルになります。
- 実行するテストに応じて、デフォルト モニタリング間隔は変わります。
- **syslog** はイネーブルです。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

テストのスケジューリングを行う際には、次の注意事項に従ってください。

- *test-id* : テスト ID の一覧を表示するには、**show diagnostic content** コマンドを使用します。
- *test-id-range* : テスト ID の一覧を表示するには、**show diagnostic content** コマンドを使用します。カンマおよびハイフンで区切られた整数でテスト ID の範囲を指定します (たとえば、1,3-6 は、1、3、4、5、および 6 のテスト ID を示します)。
- *hh* : 時間を指定します (1 ~ 24)。
- *mm* : 分を指定します (1 ~ 60)。
- *day* : 曜日を 1 ~ 7 の番号で指定します (1 は日曜日)。
- *ss* : 秒を指定します (1 ~ 60)。
- *ms* : ミリ秒を指定します (1 ~ 1000)。

指定したヘルス モニタリング テストをイネーブルまたはディセーブルにするには、**[no] diagnostic monitor test {test-id | test-id-range | all}** コマンドを使用します。

diagnostic monitor {module num} test {test-id | test-id-range | all} コマンドを入力する際、以下について留意してください。

- 必須
 - すべての接続ポートをディセーブルにしてネットワーク トラフィックを分離し、テスト中にテスト パケットを吸い上げないようにします。
 - スーパーバイザ エンジンの PFC にある FIB TCAM および SSRAM メモリをテストする場合、すべてのモジュールを取り外します。
 - テスト モジュールまたはシステムをリセットしてから、システムを通常の動作モードに戻してください。
- 推奨
 - **no diagnostic monitor {module num} test {test-id | test-id-range | all}** コマンドを使用して、スーパーバイザ エンジンおよびモジュールのバックグラウンドヘルス モニタリング テストをすべてオフにします。

中央 PFC3B (スーパーバイザ エンジン上) の FIB TCAM テストには、約 4 時間 30 分かかります。

FIB TCAM テストには、約 16 時間かかります。

例

次に、指定したテストを 3 日、10 時間、および 2 分ごとに実行する例を示します。

```
Router(config)# diagnostic monitor interval module 1 test 1 day 3 hours 10 min 2
Router(config)#
```

次に、ヘルス モニタリング テストが失敗した場合に、Syslog メッセージの生成をイネーブルにする例を示します。

```
Router(config)# diagnostic monitor syslog
Router(config)#
```

関連コマンド

コマンド	説明
<code>show diagnostic content</code>	各テストおよびすべてのモジュールについて、テスト ID、テスト属性、およびサポートされているカバレッジ テスト レベルなどのテスト情報を表示します。

diagnostic ondemand

オンデマンド診断を設定するには、**diagnostic ondemand** コマンドを使用します。

```
diagnostic ondemand {iteration iteration-count} | {action-on-error {continue | stop}
[error-count]}
```

シンタックスの説明

iteration <i>iteration-count</i>	コマンドの入力時に同じテストを繰り返し実行する回数を設定します。
action-on-error	エラー検出時に実行するアクションを設定します。
continue	テスト失敗の検出時にテストを継続します。
stop	テスト失敗の検出時にテストを停止します。
error-count	(任意) 停止するまでに許容するエラー数 (continue オプションを使用する場合)

コマンドのデフォルト

デフォルト設定は次のとおりです。

- *iteration-count* は **1** です。
- **action-on-error** は **continue** です。
- *error-count* は **0** です。

コマンドモード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

error-count に **0** を指定すると、許容されるエラー数が無制限に設定されます。

例

次に、オンデマンドテストの反復回数を設定する例を示します。

```
Router# diagnostic ondemand iteration 4
Router#
```

次に、エラー検出時のアクションを設定する例を示します。

```
Router# diagnostic ondemand action-on-error continue 2
Router#
```

関連コマンド

コマンド	説明
show diagnostic ondemand	オンデマンド診断の設定を表示します。

diagnostic schedule test

特定のモジュールに対するテストベース診断テストのスケジュールを設定したり、スーパーバイザエンジンのスイッチオーバーをスケジューリングしたりするには、**diagnostic schedule test** コマンドを使用します。スケジュールを解除するには、このコマンドの **no** 形式を使用します。

```
diagnostic schedule {module {num | active-sup-slot}} test {test-id | test-id-range | all}
  [port {num | num-range | all}] {on mm dd yyyy hh:mm} | {daily hh:mm} | {weekly
  day-of-week hh:mm}
```

```
no diagnostic schedule test
```

シンタックスの説明

module <i>num</i>	モジュール番号を指定します。
module <i>active-sup-slot</i>	アクティブスーパーバイザエンジンのスロット番号を指定します。
<i>test-id</i>	実行するテストの ID 番号。詳細については、「使用上のガイドライン」を参照してください。
<i>test-id-range</i>	実行するテストの ID 番号の範囲。詳細については、「使用上のガイドライン」を参照してください。
all	すべての診断テストを実行します。
port	(任意) テストのスケジュールを設定するポートを指定します。
<i>num</i>	ポート番号
<i>num-range</i>	ポート番号の範囲 (ハイフンで区切ります)
all	すべてのポートを指定します。
on <i>mm dd yyyy</i> <i>hh:mm</i>	テストごとの診断作業のスケジュールを指定します。フォーマットの注意事項については、「使用上のガイドライン」を参照してください。
daily <i>hh:mm</i>	テストごとの診断作業の日次スケジュールを指定します。フォーマットの注意事項については、「使用上のガイドライン」を参照してください。
weekly <i>day-of-week</i> <i>hh:mm</i>	テストごとの診断作業の週間スケジュールを指定します。フォーマットの注意事項については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

テストのスケジューリングを行う際には、次の注意事項に従ってください。

- *test-id* : テスト ID の一覧を表示するには、**show diagnostic content** コマンドを使用します。
- *test-id-range* : テスト ID の一覧を表示するには、**show diagnostic content** コマンドを使用します。カンマおよびハイフンで区切られた整数でテスト ID の範囲を指定します (たとえば、1,3-6 は、1、3、4、5、および 6 のテスト ID を示します)。
- *num-range* : カンマおよびハイフンで区切られた整数でポートの範囲を指定します (たとえば、1,3-6 は、1、3、4、5、および 6 のポートを示します)。
- *mm* : 月を明記します (January、February ... December など)。大文字と小文字のいずれでも構いません。
- *dd* : 日を 2 桁の数字で指定します。
- *yyyy* : 年を 4 桁の数字で指定します。
- *hh:mm* : 時間と分を 2 桁の数字 (24 時間制) で指定します。コロン (:) は必須です。
- *day-of-week* : 曜日を明記します (Monday、Tuesday... Sunday など)。大文字と小文字のどちらでも構いません。
- **port {num | num-range | all}** : スケジューリングされたスイッチオーバーを指定する場合は、サポートされません。

テスト ID の一覧を表示するには、**show diagnostic content** コマンドを使用します。

diagnostic schedule module active-sup-slot test test-id コマンドを使用すると、アクティブ スーパーバイザ エンジンからスタンバイ スーパーバイザ エンジンにスイッチオーバーをスケジューリングできます。

テスト ID 一覧を表示して、ScheduleSwitchover フィールドのテスト ID を検索するには、**show diagnostic content active-sup-slot** コマンドを入力します。

次のコマンドを使用すると、定期的なスイッチオーバー (毎日または毎週) または指定した時点での 1 回のスイッチオーバーを指定できます。

- **diagnostic schedule module active-sup-slot test test-id on mm dd yyyy hh:mm**
- **diagnostic schedule module active-sup-slot test test-id daily hh:mm**
- **diagnostic schedule module active-sup-slot test test-id weekly day-of-week hh:mm**



(注)

スタンバイ スーパーバイザ エンジンがシステムをスイッチオーバーできない場合のシステムのダウンタイムを回避するため、スタンバイ スーパーバイザ エンジンからアクティブ スーパーバイザ エンジンへのスイッチオーバーをスイッチオーバーが発生してから 10 分後にスケジューリングすることを推奨します。詳細については、「例」を参照してください。

例

次に、特定のモジュールとポートに対して特定の日に診断テストを行うように、スケジュール設定する例を示します。

```
Router(config)# diagnostic schedule module 1 test 1,2,5-9 port 3 on january 3 2003 23:32
Router(config)#
```

次に、特定のポートとモジュールに対して特定の時間に毎日診断テストを行うように、スケジュール設定する例を示します。

```
Router(config)# diagnostic schedule module 1 test 1,2,5-9 port 3 daily 12:34
Router(config)#
```

次に、特定のポートとモジュールに対して特定の曜日に毎週診断テストを行うように、スケジュール設定する例を示します。

```
Router(config)# diagnostic schedule module 1 test 1,2,5-9 port 3 weekly friday 09:23
Router(config)#
```

次に、毎週金曜の 10:00 pm にアクティブ スーパーバイザ エンジンのスイッチオーバーをスケジュールリングし、スイッチオーバーが発生してから 10 分後に、スタンバイ スーパーバイザ エンジンをアクティブ スーパーバイザ エンジンに戻す例を示します。この例では、次の条件が適用されます。

- *test-id* は 32 です。
- アクティブ スーパーバイザ エンジンには、スロット 5 に装着されています。
- スタンバイ スーパーバイザ エンジンには、スロット 6 に装着されています。

関連コマンド

コマンド	説明
show diagnostic content	各テストおよびすべてのモジュールについて、テスト ID、テスト属性、およびサポートされているカバレッジテスト レベルなどのテスト情報を表示します。
show diagnostic schedule	現在スケジュールリング済みの診断タスクを表示します。

diagnostic start

指定した診断テストを実行するには、**diagnostic start** コマンドを使用します。

```
diagnostic start {module num} test {test-id | test-id-range | minimal | complete | basic |
per-port | non-disruptive | all} [port {num | port#-range | all}]
```

シンタックスの説明

module num	モジュール番号を指定します。
test	テストの実行を指定します。
<i>test-id</i>	実行するテストの ID 番号。詳細については、「使用上のガイドライン」を参照してください。
<i>test-id-range</i>	実行するテストの ID 番号の範囲。詳細については、「使用上のガイドライン」を参照してください。
minimal	最小限のブートアップ診断テストを実行します。
complete	すべてのブートアップ診断テストを実行します。
basic	基本的なオンデマンド診断テストを実行します。
per-port	ポート単位のレベル テストを実行します。
non-disruptive	中断を伴わないヘルス モニタリング テストを実行します。
all	すべての診断テストを実行します。
port num	(任意) インターフェイス ポート番号を指定します。
port port#-range	インターフェイス ポート番号の範囲を指定します。詳細については、「使用上のガイドライン」を参照してください。
port all	すべてのポートを指定します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



(注) オンライン診断テストをイネーブルにする前に、ロギング コンソール/モニタをイネーブルにして、すべての警告メッセージを参照することを推奨します。



(注) 中断を伴うテストを実行する場合、コンソール接続だけでテストを実行することを推奨します。中断を伴うテストが完了すると、システムをリロードして通常の動作に戻すことを推奨する警告メッセージがコンソール上に表示されます。注：この警告に必ず従ってください。

diagnostic start



(注) このテストの実行中、すべてのポートはシャットダウンされ、内部でポートをループさせた状態でストレステストが実行されます。外部トラフィックによって、テスト結果にずれが生じる場合があります。スイッチを通常の動作に戻すには、スイッチ全体を再起動する必要があります。スイッチをリロードするコマンドを入力すると、コンフィギュレーションを保存するかどうかを聞かれます。(注) コンフィギュレーションを保存しないでください。



(注) スーパーバイザエンジンではないモジュールでテストを実行している場合、テストを開始して完了したら、モジュールをリセットする必要があります。



(注) DFC3A が搭載されたシステムでは、**diagnostic start module x test all** コマンドを入力しないでください。このコマンドは、TCAM テストが失敗する原因になります。

テスト ID の一覧を表示するには、**show diagnostic content** コマンドを使用します。

カンマおよびハイフンで区切られた整数で *test-id-range* または *port#-range* を指定します (たとえば、1,3-6 は、1、3、4、5、および 6 のテスト ID を示します)。

テストを停止する場合は、**diagnostic stop** コマンドを使用します。

例

次に、指定したスロットで指定した診断テストを実行する例を示します。

```
Router# diagnostic start module 1 test 5
Module 1:Running test(s) 5 may disrupt normal system operation
Do you want to run disruptive tests? [no]yes
00:48:14:Running OnDemand Diagnostics [Iteration #1] ...
00:48:14:%DIAG-SP-6-TEST_RUNNING:Module 1:Running TestNewLearn{ID=5} ...
00:48:14:%DIAG-SP-6-TEST_OK:Module 1:TestNewLearn{ID=5} has completed successfully
00:48:14:Running OnDemand Diagnostics [Iteration #2] ...
00:48:14:%DIAG-SP-6-TEST_RUNNING:Module 1:Running TestNewLearn{ID=5} ...
00:48:14:%DIAG-SP-6-TEST_OK:Module 1:TestNewLearn{ID=5} has completed successfully
Router#
```

関連コマンド

コマンド	説明
diagnostic stop	テストを停止します。
show diagnostic	オンライン診断のテスト結果を表示し、サポートされているテストを一覧表示します。

diagnostic stop

テストを停止するには、**diagnostic stop** コマンドを使用します。

diagnostic stop {*module num*}

シンタックスの説明

module num	モジュール番号
-------------------	---------

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

テストを開始する場合は、**diagnostic start** コマンドを使用します。

例

次に、診断テストを停止する例を示します。

```
Router# diagnostic stop module 3
Router#
```

関連コマンド

コマンド	説明
diagnostic start	テスト プロセスを実行します。
show diagnostic	オンライン診断のテスト結果を表示し、サポートされているテストを一覧表示します。

disconnect qdm

QoS device manager (QDM) セッションを切断するには、**disconnect qdm** コマンドを使用します。

disconnect qdm [**{client client-id}**]

シンタックスの説明

client client-id (任意) 切断するクライアントを指定します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

QDM は OSM インターフェイスではサポートされていません。

引数なしで **disconnect qdm** を入力する場合、すべての QDM セッションが切断されます。*client-id* を取得する場合は、**show qdm status** コマンドを使用します。

例

次に、QDM セッションを切断する例を示します。

```
Router# disconnect qdm client 1
Router#
```

関連コマンド

コマンド	説明
show qdm status	Catalyst 6500 シリーズ スイッチに接続している、現在アクティブな QDM クライアントのステータス情報を表示します。

do

グローバル コンフィギュレーション モードまたは他のコンフィギュレーション モード/サブモードで EXEC レベルのコマンドを実行するには、**do** コマンドを使用します。

do command

シンタックスの説明

<i>command</i>	実行する EXEC レベルのコマンド
----------------	--------------------

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC レベルのコマンドを実行するグローバル コンフィギュレーション (**config**) モードまたは他のコンフィギュレーション モードまたはサブモード

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



注意

EXEC モードで **do** コマンドを入力しないでください。サービスが遮断される可能性があります。

do コマンドを使用して、**configure terminal** コマンドを実できません。**configure terminal** コマンドを入力すると、コンフィギュレーション モードにモード変更されるからです。

グローバル コンフィギュレーションまたは他のコンフィギュレーション モードまたはサブモードで、**do** コマンドを使用して **copy** または **write** コマンドを実行することはできません。

例

次に、グローバル コンフィギュレーション モードで EXEC レベルの **show interfaces** コマンドを実行する例を示します。

```
Router(config)# do show interfaces serial 3/0

Serial3/0 is up, line protocol is up
  Hardware is M8T-RS232
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output 1d17h, output hang never
  Last clearing of "show interface" counters never
  .
  .
  .
Router(config)#
```

dot1x default

設定可能な 802.1X (dot1x) パラメータをデフォルトの設定にリセットするには、**dot1x default** コマンドを使用します。

dot1x default

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

デフォルト値は次のとおりです。

- インターフェイス単位の 802.1X プロトコル イネーブル ステートは、ディセーブルです (強制的に許可)。
- 再認証試行間隔の秒数は、3600 秒です。
- 待機時間は 60 秒です。
- 再送信時間は 30 秒です。
- 最大再送信回数は 2 回です。
- 複数ホストのサポートは、ディセーブルです。
- クライアント タイムアウト時間は、30 秒です。
- 認証サーバのタイムアウト時間は、30 秒です。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、設定可能な 802.1X パラメータをデフォルト値にリセットする例を示します。

```
Router(config-if)# dot1x default
Setting the Default Configuration for Dot1x on this interface

Router(config-if)#
```

関連コマンド

コマンド	説明
show dot1x	802.1X 情報を表示します。

dot1x max-req

認証プロセスを再開するまでにスイッチが Extensible Authentication Protocol (EAP) 要求/ID フレームをクライアントに送信する回数を設定するには、**dot1x max-req** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x max-req count

no dot1x max-req

シンタックスの説明	<i>count</i> 認証プロセスを再開するまでにスイッチがクライアントに EAP 要求/ID フレームを送信する回数。有効値は 1 ~ 10 です。
------------------	---

コマンドのデフォルト	<i>count</i> は、2 です。
-------------------	----------------------

コマンド モード	インターフェイス コンフィギュレーション (config-if)
-----------------	----------------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン	デフォルト値の変更は、信頼性のないリンクや、特定のクライアントおよび認証サーバに関する動作問題など、異常な状況に対して調整する場合にだけ行ってください。
-------------------	--

例	次に、認証プロセスを再開するまでに、スイッチが EAP 要求/ID フレームを送信する回数を 5 に設定する例を示します。
----------	---

```
Router(config-if)# dot1x max-req 5
Router(config-if)#
```

関連コマンド	コマンド	説明
	show dot1x	802.1X 情報を表示します。

dot1x multi-hosts

802.1X 許可済みのポート上で複数のホスト（クライアント）を許可するには、**dot1x multi-hosts** コマンドを使用します。複数のホストを許可しないようにするには、このコマンドの **no** 形式を使用します。

dot1x multi-hosts

no dot1x multi-hosts

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドを入力する前に、**dot1x port-control** コマンドが、指定したインターフェイスで **auto** に設定されていることを必ず確認してください。

例

次に、複数のホストを許可する例を示します。

```
Router(config-if)# dot1x multi-hosts  
Router(config-if)#
```

次に、複数のホストを許可しないようにする例を示します。

```
Router(config-if)# no dot1x multi-hosts  
Router(config-if)#
```

関連コマンド

コマンド	説明
dot1x port-control	ポート制御値を設定します。
show dot1x	802.1X 情報を表示します。

dot1x port-control

ポート制御値を設定するには、**dot1x port-control** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x port-control value

no dot1x port-control

シンタックスの説明	<i>value</i>	ポート制御値。指定できる値は、 auto 、 force-authorized 、および force-unauthorized です。詳細については、「使用上のガイドライン」を参照してください。
------------------	--------------	--

コマンドのデフォルト	force-authorized
-------------------	-------------------------

コマンド モード	インターフェイス コンフィギュレーション (config-if)
-----------------	----------------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン ポート制御 *value* の定義は次のとおりです。

- **force-authorized** : 802.1X ポートベース認証をディセーブルにし、認証交換を必要とせずポートを許可ステートに移行させます。ポートは、クライアントの 802.1X ベース認証なしで通常のトラフィックを送受信します。
- **force-unauthorized** : クライアントからの認証の試みをすべて無視し、ポートを無許可ステートのままにします。インターフェイスを介してクライアントに認証サービスは提供されません。
- **auto** : 802.1X ポートベースの認証をイネーブルにします。ポートは最初、無許可ステートであり、ポート経由で送受信できるのは EAPOL フレームだけです。ポートのリンク ステートがダウンからアップに移行したとき、または EAPOL-start フレームを受信したときに、認証プロセスが開始されます。システムはクライアントの識別情報を要求し、クライアントと認証サーバの間で認証メッセージのリレーを開始します。クライアントの MAC アドレスを使用して、ネットワーク アクセスを試みる各クライアントを一意に識別します。

ポート制御コンフィギュレーションをチェックするには、**show dot1x** コマンドを入力し、802.1X Port Summary セクションの Status カラムを参照します。*enabled* ステータスとは、ポート制御値が **auto** または **force-unauthorized** に設定されていることです。

例 次に、ポート制御を **auto** に設定する例を示します。

```
Router(config-if)# dot1x port-control auto
Router(config-if)#
```

■ dot1x port-control

関連コマンド

コマンド	説明
show dot1x	802.1X 情報を表示します。

dot1x reauthentication

クライアントの定期的な再認証をイネーブルにするには、**dot1x reauthentication** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x reauthentication

no dot1x reauthentication

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト デイセーブル

コマンド モード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン 再認証は、すでに許可されたポートのステートに干渉しません。

例 次に、クライアントの定期的な再認証をイネーブルにする例を示します。

```
Router(config-if)# dot1x reauthentication
Router(config-if)#
```

次に、クライアントの定期的な再認証をデイセーブルにする例を示します。

```
Router(config-if)# no dot1x reauthentication
Router(config-if)#
```

関連コマンド	コマンド	説明
	dot1x timeout	再認証タイマーを設定します。
	show dot1x	802.1X 情報を表示します。

dot1x system-auth-control

802.1X をグローバルにイネーブルにするには、**dot1x system-auth-control** コマンドを使用します。
802.1X をグローバルにディセーブルにするには、このコマンドの **no** 形式を使用します。

dot1x system-auth-control

no dot1x system-auth-control

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

802.1X をイネーブルにする前に、AAA (認証、許可、アカウントिंग) をイネーブルにし、認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためのクエリー送信を行う手順と認証方式を記述したものです。

例

次に、802.1X をグローバルにイネーブルにする例を示します。

```
Router(config)# dot1x system-auth-control
Router(config)#
```

次に、802.1X をグローバルにディセーブルにする例を示します。

```
Router(config)# no dot1x system-auth-control
Router(config)#
```

関連コマンド

コマンド	説明
aaa authentication dot1x	IEEE 802.1X を実行しているインターフェイスで使用する、1 つまたは複数の AAA 方式を指定します。
aaa new-model	AAA アクセス制御モデルをイネーブルにします。
show dot1x	802.1X 情報を表示します。

dot1x timeout

再認証タイマーを設定するには、**dot1x timeout** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
dot1x timeout {{reauth-period seconds} | {quiet-period seconds} | {tx-period seconds} |
               {supp-timeout seconds} | {server-timeout seconds}}
```

```
no dot1x timeout {reauth-period | quiet-period | tx-period | supp-timeout |
                  server-timeout}
```

シンタックスの説明	
reauth-period seconds	再認証試行間の秒数を指定します。有効値は、1 ~ 65,535 です。詳細については、「使用上のガイドライン」を参照してください。
quiet-period seconds	クライアントとの認証交換が失敗したあと、システムが待機状態にある秒数を指定します。有効値は 0 ~ 65,535 秒です。
tx-period seconds	要求を再送信するまでに、システムがクライアントからの EAP 要求 /ID フレームに対する応答を待機する秒数を指定します。有効値は 30 ~ 65,535 秒です。
supp-timeout seconds	EAP 要求パケットの再送信を待機する秒数を指定します。指定できる範囲は 30 ~ 65,535 秒です。
server-timeout seconds	システムがバックエンド認証者による認証サーバへのパケットの再送信を待機する秒数を指定します。有効値は 30 ~ 65,535 秒です。

コマンドのデフォルト デフォルト設定は次のとおりです。

- **reauth-period** は 3600 秒です。
- **quiet-period** は 60 秒です。
- **tx-period** は 30 秒です。
- **supp-timeout** は 30 秒です。
- **server-timeout** は 30 秒です。

コマンドモード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン **dot1x timeout reauth-period** コマンドを入力する前に、定期的な再認証をイネーブルにしておく必要があります。定期的な再認証をイネーブルにするには、**dot1x reauthentication** コマンドを入力します。定期的な再認証がイネーブルに設定されている場合にだけ、**dot1x timeout reauth-period** コマンドはシステムの動作を有効にします。

例 次に、再認証を試行する間隔を 4000 秒に設定する例を示します。

```
Router(config-if)# dot1x timeout reauth-period 4000
Router(config-if)#
```

次に、システムの待機時間を 30 秒に設定する例を示します。

```
Router(config-if)# dot1x timeout quiet-period 30
Router(config-if)#
```

次に、要求を再送信するまでに、クライアントからの EAP 要求/ID フレームに対する応答を待機する秒数を 60 に設定する例を示します。

```
Router(config-if)# dot1x timeout tx-period 60
Router(config-if)#
```

次に、EAP 要求フレームに対するシステム/クライアント間の再送信時間を 25 秒に設定する例を示します。

```
Router(config-if)# dot1x timeout supp-timeout 25
Router(config-if)#
```

次に、トランスポート レイヤ パケットに対するシステム/認証サーバ間の再送信時間を 25 秒に設定する例を示します。

```
Router(config-if)# dot1x timeout server-timeout 25
Router(config-if)#
```

次に、デフォルトの再認証時間に戻す例を示します。

```
Router(config-if)# no dot1x timeout reauth-period
Router(config-if)#
```

関連コマンド

コマンド	説明
dot1x reauthentication	クライアントの定期的な再認証をイネーブルにします。
show dot1x	802.1X 情報を表示します。

duplex

インターフェイス上でデュプレックス動作を設定するには、**duplex** コマンドを使用します。システムを半二重モードに戻すには、このコマンドの **no** 形式を使用します。

duplex {full | half}

no duplex

シンタックスの説明	full	half
	全二重動作を指定します。	半二重動作を指定します。

コマンドのデフォルト **half**

コマンドモード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン 表 2-7 に、サポートされているコマンド オプションをインターフェイス別に示します。

表 2-7 サポートされている duplex コマンド オプション

インターフェイス タイプ	サポートされている構文	デフォルト設定	使用上のガイドライン
10/100 Mbps モジュール	duplex [half full]	「使用上のガイドライン」を参照してください。	速度が auto に設定されている場合は、 duplex を設定できません。 速度が 10 または 100 に設定されている場合に、デュプレックスを設定しないと、デュプレックスは half に設定されます。
100 Mbps ファイバ モジュール	duplex [half full]	half	—
ギガビットイーサネット インターフェイス	duplex full	full	—
10 Mbps ポート	duplex [half full]	half	—

16 ポート RJ-45 ギガビット イーサネット ポート上での伝送速度が 1000 に設定されている場合、デュプレックス モードは全二重に設定されます。伝送速度が 10 または 100 に変化した場合、デュプレックス モードは半二重のままです。伝送速度が 1000 Mbps から 10 または 100 に変化した場合、正しいデュプレックス モードを設定する必要があります。

ギガビット イーサネットは、全二重だけです。ギガビット イーサネット ポートまたはギガビット イーサネットに設定された 10/100/1000 Mbps ポートのデュプレックス モードは変更できません。

インターフェイス速度を手動で 10 または 100 Mbps に設定した場合は、インターフェイスのデュプレックス モードも設定する必要があります。



(注) Catalyst 6500 シリーズ スイッチは、いずれかの接続先インターフェイスが **auto** 以外の値に設定されている場合、インターフェイス速度およびデュプレックス モードを自動ネゴシエーションできません。



注意

インターフェイス速度およびデュプレックス モードの設定を変更すると、インターフェイスがシャットダウンされ再びイネーブルになる場合があります。

表 2-8 に、**duplex** および **speed** コマンドの関係とさまざまな組み合わせによる結果を示します。

表 2-8 duplex コマンドと speed コマンドの関係

duplex コマンド	speed コマンド	システム アクション
duplex half または duplex full	speed auto	速度とデュプレックス モードの両方を自動ネゴシエーションします。
duplex half	speed 10	強制的に 10 Mbps および半二重になります。
duplex full	speed 10	強制的に 10 Mbps および全二重になります。
duplex half	speed 100	強制的に 100 Mbps および半二重になります。
duplex full	speed 100	強制的に 100 Mbps および全二重になります。

例 次に、全二重動作のインターフェイスを設定する例を示します。

```
Router(config-if)# duplex full
Router(config-if)#
```

関連コマンド

コマンド	説明
interface	設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
show controllers	モジュールのハードウェアに固有な情報を表示します。
show interfaces	特定のインターフェイスが認識するトラフィックを表示します。
speed	イーサネット インターフェイスのポート速度を設定します。

eigrp event-log-size

IP-EIGRP イベント ログのサイズを設定するには、**eigrp event-log-size** コマンドを使用します。

eigrp event-log-size *size*

シンタックスの説明	<i>size</i> IP-EIGRP イベント ログ サイズ。有効値は、0 ~ 4,294,967,295 です。
-----------	---

コマンドのデフォルト	このコマンドにはデフォルト設定がありません。
------------	------------------------

コマンドモード	ルータ コンフィギュレーション (config-router)
---------	---------------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン	設定されたイベント ログ サイズの値が超過すると、最後に設定された (event-log-size) のログ行数が保持されます。
------------	--

例	次に、IP-EIGRP イベント ログのサイズを設定する例を示します。
---	-------------------------------------

```
Router (config-router)# eigrp event-log-size 5000010
Router (config-router)#
```

関連コマンド	コマンド	説明
	clear ip eigrp event	IP-EIGRP イベント ログをクリアします。

encapsulation dot1q

VLAN 内の指定のサブインターフェイス上でトラフィックの IEEE802.1Q (dot1q) カプセル化をイネーブルにするには、**encapsulation dot1q** コマンドを使用します。

encapsulation dot1q *vlan-id* [native]

シンタックスの説明

<i>vlan-id</i>	仮想 LAN 識別番号。有効値は 1 ~ 4094 です。
native	(任意) ポートの PVID (ポート VLAN ID) を <i>vlan-id</i> の値に設定します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

サブインターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

vlan-id が 802.1Q ネイティブ VLAN の ID の場合には、必ず **native** キーワードを使用します。**native** キーワードを指定せずに、802.1Q トランクのネイティブ VLAN 上でカプセル化の設定を行わないでください。

サブインターフェイス コンフィギュレーション モードを開始するには、まずインターフェイス コンフィギュレーション モードを開始して、次にサブインターフェイスを指定する **interface** コマンドを入力します。

例

次に、802.1Q プロトコルを使用して VLAN 100 に VLAN トラフィックのカプセル化を設定する例を示します。

```
Router(config-subif)# encapsulation dot1q 100
Router(config-subif)#
```

関連コマンド

コマンド	説明
encapsulation isl	Inter-Switch Link (ISL; スイッチ間リンク) をイネーブルにします。

encapsulation isl

ISL をイネーブルにするには、**encapsulation isl** コマンドを使用します。

encapsulation isl *vlan-identifier*

シンタックスの説明	<i>vlan-identifier</i>	VLAN ID。有効値は 1 ~ 4094 です。
-----------	------------------------	---------------------------

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード サブインターフェイス コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン ISL は複数のスイッチやルータの相互接続、および VLAN トポロジーの定義に使用するシスコのプロトコルです。

ISL カプセル化を使用すると、イーサネット フレームの最初に 26 バイトのヘッダーが追加されます。ヘッダーには、スイッチ間で VLAN メンバーシップ ID を伝達する 10 ビットの VLAN ID が含まれます。

サブインターフェイス コンフィギュレーション モードを開始するには、まずインターフェイス コンフィギュレーション モードを開始して、次にサブインターフェイスを指定する **interface** コマンドを入力します。

例 次に、ファストイーサネット サブインターフェイス 2/1.20 で ISL をイネーブルにする例を示します。

```
Router(config-subif)# encapsulation isl 400
Router(config-subif)#
```

関連コマンド	コマンド	説明
	bridge-group	それぞれのネットワーク インターフェイスをブリッジ グループに割り当てます。
	show bridge vlan	仮想 LAN サブインターフェイスを表示します。
	show interfaces	特定のインターフェイスが認識するトラフィックを表示します。
	show vlans	Cisco IOS VLAN サブインターフェイスに関する情報を表示します。

erase

ファイル システムを消去するには、**erase** コマンドを使用します。

erase {const_nvram: | nvram: | startup-config:}

シンタックスの説明

const_nvram:	const_nvram: パーティション下のすべてのファイルを消去します。
nvram:	NVRAM を消去します。
startup-config:	コンフィギュレーション メモリの内容を消去します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



注意

erase コマンドを使用してファイル システムを消去した場合、ファイル システムのファイルを復元できません。

erase nvram: コマンドは、**write erase** コマンドおよび **erase startup-config** コマンドに置き換えられます。

クラス B フラッシュ ファイル システムとクラス C フラッシュ ファイル システム上だけで **erase** コマンドを使用できます。**delete** コマンドでファイルを削除してからフラッシュ ファイル システムのスペースを再生するには、**erase** コマンドを使用します。**erase** コマンドは、フラッシュ ファイル システムのすべてのファイルを消去します。

クラス A フラッシュ システムを消去できません。**delete** コマンドを使用して個々のファイルを削除したあとに、**squeeze** コマンドを使用してスペースを再生できます。**format** コマンドを使用して、フラッシュ ファイル システムをフォーマットすることもできます。

クラス C フラッシュ ファイル システムでは、**delete** コマンドを使用するとスペースが動的に再生されます。また、**format** または **erase** コマンドのいずれかを使用して、クラス C フラッシュ ファイル システムを再初期化することもできます。

erase nvram: コマンドは NVRAM を消去します。クラス A ファイル システムのプラットフォームの場合、CONFIG_FILE 変数によってフラッシュ メモリ内のファイルが指定されると、指定されたファイルが [delete] とマークされます。

erase const_nvram コマンドを入力して、VLAN データベースのコンフィギュレーション ファイルを消去できます。

例 次に、NVRAM および NVRAM 内のスタートアップ コンフィギュレーションを消去する例を示します。

```
Router# erase nvram:  
Router#
```

関連コマンド

コマンド	説明
boot config	システムが初期化時（起動時）に自身を設定するコンフィギュレーションファイルのデバイスおよびファイル名を指定します。
delete	フラッシュ メモリ デバイスまたは NVRAM からファイルを削除します。
more nvram:startup-config:	NVRAM に含まれる、または CONFIG-FILE 環境変数によって指定されるスタートアップ コンフィギュレーション ファイルを表示します。
show bootvar	BOOT 環境変数に関する情報を表示します。
undelete	フラッシュ ファイル システムで [delete] マークが付いたファイルを回復します。

errdisable detect cause

errdisable 検出をイネーブルにするには、**errdisable detect cause** コマンドを使用します。errdisable 検出をディセーブルにするには、このコマンドの **no** 形式を使用します。

errdisable detect cause {all | dtp-flap | l2ptguard | link-flap | packet-buffer-error | pagp-flap | udld}

no errdisable detect cause {all | dtp-flap | l2ptguard | link-flap | pagp-flap | udld}

シンタックスの説明

all	すべての errdisable 原因に対する errdisable 検出を指定します。
dtp-flap	Dynamic Trunking Protocol (DTP; ダイナミック トランキング プロトコル) フラップが errdisable 原因の検出を指定します。
l2ptguard	レイヤ 2 プロトコル トンネリングが errdisable 原因の検出を指定します。
link-flap	リンク フラップが errdisable 原因の検出を指定します。
packet-buffer-error	パケット バッファ エラーにより影響のあるポートが errdisable ステートになります。
pagp-flap	PAgP フラップが errdisable 原因の検出を指定します。
udld	UniDirectional Link Detection Protocol (UDLD; 単一方向リンク検出) が errdisable 原因の検出を指定します。

コマンドのデフォルト

すべての原因に対してイネーブル

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



(注)

no errdisable detect cause packet-buffer-error コマンドを入力すると、影響のあるモジュールでオフ/オンが発生するような障害を検出できます。

原因 (bpduguard、dtp-flap、link-flap、pagp-flap、root-guard、udld) は、errdisable ステートが発生した理由として定義されます。原因がインターフェイス上で検出される場合は、インターフェイスは errdisable ステート (リンク ダウン ステートに似た操作ステート) となります。

インターフェイスを errdisable ステートから手動で回復するには、**shutdown** コマンドを入力し、次に **no shutdown** コマンドを入力する必要があります。

例 次に、レイヤ 2 プロトコル トンネリング ガードの errdisable 原因に対して errdisable 検出をイネーブルにする例を示します。

```
Router(config)# errdisable detect cause l2ptguard  
Router(config)#
```

関連コマンド

コマンド	説明
show errdisable detect	errdisable 検出ステータスを表示します。
show interfaces status	インターフェイス ステータスを表示したり、LAN ポートで errdisable ステータスにあるインターフェイスだけのリストを表示したりします。

errdisable recovery

回復メカニズム変数を設定するには、**errdisable recovery** コマンドを使用します。デフォルト ステータスに戻すには、このコマンドの **no** 形式を使用します。

```
errdisable recovery cause {all | arp-inspection | bpduguard | channel-misconfig |
dhcp-rate-limit | dtp-flap | gbic-invalid | l2ptguard | link-flap | pagp-flap |
psecure-violation | security-violation | udld | unicast-flood}
```

```
errdisable recovery {interval interval}
```

```
no errdisable recovery cause {all | {arp-inspection | bpduguard | channel-misconfig |
dhcp-rate-limit | dtp-flap | gbic-invalid | l2ptguard | link-flap | pagp-flap |
psecure-violation | security-violation | udld | unicast-flood}}
```

```
no errdisable recovery {interval interval}
```

シンタックスの説明

cause	特定の原因から回復するための errdisable 回復をイネーブルにします。
all	すべての errdisable 原因の回復タイマーをイネーブルにします。
arp-inspection	ARP インスペクションによる原因から回復するための errdisable 回復をイネーブルにします。
bpduguard	BPDU ガードが errdisable 原因の回復タイマーをイネーブルにします。
channel-misconfig	チャンネル誤設定が errdisable 原因の回復タイマーをイネーブルにします。
dhcp-rate-limit	DHCP レート制限が errdisable 原因の回復タイマーをイネーブルにします。
dtp-flap	DTP フラップが errdisable 原因の回復タイマーをイネーブルにします。
gbic-invalid	Gigabit Interface Converter (GBIC; ギガビット インターフェイス コンバータ) 無効が errdisable 原因の回復タイマーをイネーブルにします。
l2ptguard	レイヤ 2 プロトコル トンネリングが errdisable 原因の回復タイマーをイネーブルにします。
link-flap	リンク フラップが errdisable 原因の回復タイマーをイネーブルにします。
pagp-flap	PAgP フラップが errdisable 原因の回復タイマーをイネーブルにします。
psecure-violation	psecure 違反が errdisable 原因の回復タイマーをイネーブルにします。
security-violation	802.1X セキュリティ違反によりディセーブルになったポートの自動回復をイネーブルにします。
udld	UDLD が errdisable 原因の回復タイマーをイネーブルにします。
unicast-flood	ユニキャスト フラッドが errdisable 原因の回復タイマーをイネーブルにします。
interval interval	指定された errdisable 原因から回復する時間を指定します。指定できる値は 30 ~ 86,400 秒です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- すべての原因に対してディセーブル
- イネーブルの場合、*interval* は 300 秒です。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

secure-violation オプションはサポートされていません。

原因 (bpduguard、dhcp-rate-limit、dtp-flap、l2ptguard、link-flap、pagp-flap、security-violation、channel-misconfig、psecure-violation、udld、または unicast-flood) は、errdisable ステートが発生した理由として定義されます。原因がインターフェイス上で検出される場合は、インターフェイスは errdisable ステート (リンク ダウン ステートに似た操作ステート) となります。その原因の errdisable 回復をイネーブルにしない場合、shutdown および no shutdown が実行されるまでインターフェイスは errdisable ステートのままです。原因の回復をイネーブルにした場合、インターフェイスは errdisable ステートから抜け出し、すべての原因がタイムアウトになったときに動作を再試行できるようになります。

インターフェイスを errdisable ステートから手動で回復するには、**shutdown** コマンドを入力し、次に **no shutdown** コマンドを入力する必要があります。

例

次に、BPDU ガードが errdisable 原因の回復タイマーをイネーブルにする例を示します。

```
Router (config) # errdisable recovery cause bpduguard
Router (config) #
```

次に、タイマーを 300 秒に設定する例を示します。

```
Router (config) # errdisable recovery interval 300
Router (config) #
```

関連コマンド

コマンド	説明
show errdisable recovery	errdisable 回復タイマーに関する情報を表示します。
show interfaces status	インターフェイス ステータスを表示したり、LAN ポートで errdisable ステートにあるインターフェイスだけのリストを表示したりします。

error-detection packet-buffer action

パケットバッファメモリ障害の発生後にモジュールが実行するアクションを指定するには、**error-detection packet-buffer action** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

error-detection packet-buffer action {module num} {error-disable | power-down | reset}

シンタックスの説明

module num	モジュール番号を指定します。
error-disable	モジュールをエラー ディセーブルにします。
power-down	モジュールの電源を切断します。
reset	モジュールをリセットします。

コマンドのデフォルト

ポート グループをエラー ディセーブルにします。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、次のモジュールだけでサポートされています。

- WS-X6348-RJ-45
- WS-X6348-RJ-21V
- WS-X6248-RJ-45
- WS-X6248-TEL
- WS-X6148-RJ-45
- WS-X6148-RJ-21

reset キーワードを指定すると、通常のリブート (約 45 ~ 50 秒) ではなく、高速リブート (約 10 秒) が実行されます。このリリース以前では、モジュールのリブートは、高速ではありませんでした。

例 次に、パケット バッファ メモリ 障害の発生後にモジュールをエラー ディセーブルにするように設定する例を示します。

```
Router(config)# error-detection packet-buffer action module 2 error-disable  
Router(config)#
```

次に、パケット バッファ メモリ 障害の発生後にモジュールの電源を切断するように設定する例を示します。

```
Router(config)# error-detection packet-buffer action module 2 power-down  
Router(config)#
```

次に、パケット バッファ メモリ 障害の発生後にモジュールをリセットするように設定する例を示します。

```
Router(config)# error-detection packet-buffer action module 2 reset  
Router(config)#
```

file verify auto

圧縮された Cisco IOS イメージのチェックサムを確認するには、**file verify auto** コマンドを使用します。コピーの操作を行ったあとで自動確認をオフに切り替えるには、このコマンドの **no** 形式を使用します。

file verify auto

no file verify auto

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト コピー操作が完了すると自動的に確認が行われます。

コマンド モード グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン 個別のコピー操作のデフォルト設定を上書きするには、**copy /noverify** コマンドを使用します。

例 次に、圧縮された Cisco IOS イメージのチェックサムを確認する例を示します。

```
Router(config)# file verify auto
Router(config)#
```

関連コマンド	コマンド	説明
	copy /noverify	現在のコピー操作の自動イメージ確認をディセーブルにします。
	verify	フラッシュメモリ ファイル システムのファイルのチェックサムを確認するか、ファイルの MD5 シグニチャを計算します。

flowcontrol

ポートがポーズ フレームを送信または受信するよう設定するには、**flowcontrol** コマンドを使用します。

flowcontrol {send | receive} {desired | off | on}

シンタックスの説明

send	ポートがポーズ フレームを送信するよう指定します。
receive	ポートがポーズ フレームを処理するよう指定します。
desired	リモート ポートが、 on 、 off 、または desired のいずれかに設定されていても、予測できる結果を得ます。
off	ローカル ポートがリモート ポートからのポーズ フレームを受信して処理したり、リモート ポートへポーズ フレームを送信したりするのを禁止します。
on	ローカル ポートがリモート ポートからのポーズ フレームを受信して処理したり、リモート ポートへポーズ フレームを送信したりする機能をイネーブルにします。

コマンドのデフォルト

フロー制御のデフォルト値は、ポートの速度によって異なります。デフォルト設定は次のとおりです。

- ギガビット イーサネット ポートのデフォルトは、受信については **off** で、送信については **desired** です。
- ファスト イーサネット ポートのデフォルトは、受信については **off** で、送信については **on** です。
- 24 ポート 100BASE-FX モジュールおよび 48 ポート 10/100 BASE-TX RJ-45 モジュールのデフォルトは、受信も送信も **off** になっています。
- 10 ギガビット イーサネット ポートは、常にポーズ フレームに応答するように設定されています。送信についてのデフォルトは、**off** です。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

send および **desired** のキーワードをサポートするのはギガビット イーサネット ポートだけです。

ポーズ フレームは、バッファが満杯であるために特定の期間フレームの送信を停止する信号を送信元に送る特殊なパケットです。

Catalyst 6500 シリーズ スイッチのギガビット イーサネット ポートはフロー制御を使用して、一定時間、ポートへのパケットの伝送を禁止します。その他のイーサネット ポートは、フロー制御を使用してフロー制御要求に応答します。

ギガビット イーサネット ポートの受信バッファが満杯になると、指定された時間中、パケットの送信を遅らせるようにリモート ポートに要求する「ポーズ」パケットが送信されます。すべてのイーサネット ポート (1000Mbps、100 Mbps、および 10 Mbps) は、他の装置から「ポーズ」パケットを受信し、これに応答できます。

ギガビット イーサネット以外のポートを設定して、受信済みポーズ フレームを無視することも (**disable**)、対応することも (**enable**) 可能です。

receive を使用すると、**on** および **desired** のキーワードの結果は同一になります。

すべての Catalyst 6500 シリーズ スイッチ ギガビット イーサネット ポートは、リモート装置からポーズ フレームを受信し、処理できます。

予測できる結果を得るには、次の注意事項に従います。

- **send on** は、リモート ポートが **receive on** または **receive desired** に設定されている場合にだけ使用します。
- **send off** は、リモート ポートが **receive off** または **receive desired** に設定されている場合にだけ使用します。
- **receive on** は、リモート ポートが **send on** または **send desired** に設定されている場合にだけ使用します。
- **send off** は、リモート ポートが **receive off** または **receive desired** に設定されている場合にだけ使用します。

例

次に、ローカル ポートがリモート ポートによるいかなるレベルのフロー制御もサポートしないよう設定する例を示します。

```
Router(config-if)# flowcontrol receive off
Router(config-if)#
```

```
Router(config-if)# flowcontrol send off
Router(config-if)#
```

関連コマンド

コマンド	説明
show interfaces flowcontrol	フロー制御情報を表示します。

format

クラス A またはクラス C のフラッシュ ファイル システムをフォーマットするには、**format** コマンドを使用します。

クラス A フラッシュ ファイル システムの場合

```
format bootflash: [spare spare-number] filesystem1: [[filesystem2:][monlib-filename]]
```

クラス C フラッシュ ファイル システムの場合

```
format filesystem1:
```



注意

予備として一定数のメモリ セクタを確保しておいてください。セクタの一部に障害が発生した場合でも、フラッシュ PC カードの大部分をそのまま使用できます。予備セクタを確保していないと、セクタの一部に障害が発生した場合に、フラッシュ PC カードを再フォーマットする必要があります。

シンタックスの説明

spare spare-number	(任意) フォーマットされたフラッシュ メモリに確保する予備セクタ数を指定します。指定できる値は、0 ~ 16 です。
<i>filesystem1</i> :	フォーマットするファイル システム。有効値は、 disk0: 、 bootdisk: 、および sup-bootdisk: です。詳細については、「使用上のガイドライン」を参照してください。
<i>filesystem2</i> :	(任意) あとにコロンが付く <i>filesystem1</i> のフォーマットに使用する、 monlib ファイルを含むファイル システム
<i>monlib-filename</i>	(任意) <i>filesystem1</i> 引数のフォーマットに使用される ROM モニタ ライブラリ ファイル (monlib ファイル) 名

コマンドのデフォルト

デフォルト設定は次のとおりです。

- *monlib-filename* はシステム ソフトウェアに組み込まれています。
- *spare-number* はゼロ (0) です。

コマンドモード

EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドを使用して、クラス A またはクラス C フラッシュ ファイル システムをフォーマットします。

Supervisor Engine 32 PISA には、次のフラッシュ メモリ デバイスが搭載されています。

- **disk0:**
 - 外部 CompactFlash Type II スロット×1
 - CompactFlash Type II フラッシュ PC カードをサポート
- **sup-bootdisk:**
 - Supervisor Engine 32 PISA 256-MB 内部 CompactFlash フラッシュ メモリ
 - Supervisor Engine 32 PISA ROMMON からの場合は、bootdisk:
- **bootdisk:**
 - PISA 256-MB 内部 CompactFlash フラッシュ メモリ
 - Supervisor Engine 32 ROMMON PISA からアクセス不能

新しいフラッシュ PC カードを挿入してイメージをロードしたり、コンフィギュレーション ファイルを新しいフラッシュ PC カードにバックアップしたりする必要がある場合には、新しいフラッシュ PC カードを使用する前に、フラッシュ PC カードを必ずフォーマットしてください。

フラッシュ PC カードのセクタに障害が発生する可能性があります。**format** コマンドの任意の *spare* 引数を使用して 0 ~ 16 の予備セクタを指定し、一部のフラッシュ PC カードセクタを「予備」として確保します。緊急用としての予備セクタを少数しか確保していなくても、フラッシュ PC カードの大部分を使用できます。予備セクタを 0 に指定していて、セクタの一部に障害が発生した場合は、フラッシュ PC カードを再フォーマットする必要があるため、すべての既存データは消去されます。

monlib ファイルは、ROM モニタ ライブラリです。ROM モニタは、このファイルを使用して、フラッシュ ファイル システムのファイルにアクセスします。Cisco IOS システム ソフトウェアには、**monlib** ファイルが組み込まれています。

HAS (ハイ システム アベイラビリティ) を使用している場合、*monlib-filename* 引数を指定しないと、システムは ROM モニタ ライブラリ ファイルをスレーブ イメージ バンドルから取得します。*monlib-filename* 引数を指定した場合、システムはファイルがスレーブ装置にあると見なします。

コマンドの構文では、*filesystem1:* は、フォーマットするデバイスを指定し、*filesystem2:* は、*filesystem1:* のフォーマットに使用する、**monlib file** を含む任意の装置を指定します。任意の *filesystem2:* 引数および *monlib-filename* 引数を省略した場合、システムはシステム ソフトウェアにすでに組み込まれた **monlib** ファイルを使用して、*filesystem1:* をフォーマットします。任意の *filesystem2:* 引数だけを省略した場合、システムは **cd** コマンドで指定した装置から **monlib** ファイルを使用して、*filesystem1:* をフォーマットします。任意の *monlib-filename* 引数だけを省略した場合、システムは *filesystem2:* の **monlib** ファイルを使用して、*filesystem1:* をフォーマットします。*filesystem2:* 引数および *monlib-filename* 引数の両方を指定した場合、システムは指定した装置から **monlib** ファイルを使用して *filesystem1:* をフォーマットします。*filesystem1:* 独自の **monlib** ファイルをこの引数で指定できます。**monlib** ファイルが見つからない場合、フォーマットが打ち切られます。

例

次に、スロット 0 に挿入されたコンパクトフラッシュ PC カードをフォーマットする例を示します。

```
Router# format disk0:
Running config file on this device, proceed? [confirm]y
All sectors will be erased, proceed? [confirm]y
Enter volume id (up to 31 characters): <Return>
Formatting sector 1 (erasing)
Format device disk0 completed
```

コンソールが EXEC プロンプトに戻ると、新しいコンパクトフラッシュ PC カードのフォーマットが成功し、使用が可能になります。

関連コマンド

コマンド	説明
cd	デフォルトのディレクトリまたはファイルシステムを変更します。
copy	コピー元からコピー先に任意のファイルをコピーします。
delete	フラッシュ メモリ デバイスまたは NVRAM からファイルを削除します。
show file systems	使用可能なファイル システムを表示します。
undelete	フラッシュ ファイル システムで [delete] マークが付いたファイルを回復します。

fsck

フラッシュ ファイル システムに損傷がないかどうかをチェックし、問題を修復するには、**fsck** コマンドを使用します。

fsck [/automatic | disk0:]

シンタックスの説明

/automatic	(任意) 自動モードを指定します。詳細については、「使用上のガイドライン」を参照してください。
disk0:	(任意) チェックするファイル システムを指定します。

コマンドのデフォルト

disk0: を指定しない場合、現在のファイル システムがチェックされます。

コマンド モード

EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

クラス C フラッシュ システムと、PCMCIA Advanced Technology Attachment (ATA) のフラッシュ ディスクおよびコンパクトフラッシュ ディスク上だけで、このコマンドは有効です。

引数を入力しない場合、現在のファイル システムが使用されます。現在のファイル システムを表示するには、**pwd** コマンドを使用します。

disk0: キーワードを入力した場合、**file system consistency check (fsck)** ユーティリティは、選択されたファイル システムに問題がないかどうかをチェックします。問題が検出された場合、問題を修復するかを尋ねるプロンプトが表示されます。

/automatic キーワードを入力した場合、自動モードにするかどうか確認するプロンプトが表示されます。自動モードでは、問題が自動的に修復され、確認のプロンプトが表示されません。

表 2-9 に、fsck ユーティリティが実行するチェック内容とアクション内容を示します。

表 2-9 fsck ユーティリティのチェック内容およびアクション内容

チェック内容	アクション内容
ブート セクタおよびパーティション テーブルをチェックし、エラーをレポートします。	アクションはありません。
最初のセクタの最終 2 バイト (それぞれ、0x55 および 0xaa) にシグニチャをつけてメディアを検証します。	アクションはありません。
os_id をチェックして、File Allocation Table (FAT) -12 または FAT-16 のファイル システム (有効値は、0、1、4、および 6) かどうか検出します。	アクションはありません。
FAT のフィールド番号 (正しい値は、1 および 2) をチェックします。	アクションはありません。

表 2-9 fsck ユーティリティのチェック内容およびアクション内容 (続き)

チェック内容	アクション内容
次の値をチェックします。 <ul style="list-style-type: none"> • n_fat_sectors が 1 以上であるか。 • n_root_entries が 16 以上であるか。 • n_root_sectors が 2 以上であるか。 • base_fat_sector、n_sectors_per_cluster、n_heads、n_sectors_per_track が 0 でないか。 	アクションはありません。
次のエラーについてファイルおよび FAT をチェックします。	
FAT に無効なクラスタ番号がないかを確認します。	クラスタがファイルチェーンに含まれている場合、クラスタが End of File (EOF) に変更されます。クラスタがファイルチェーンに含まれていない場合、クラスタは空リストおよび未使用のクラスタチェーンに追加されます。表 2-10 に、有効なクラスタ番号を示します。表 2-10 に表示されていない番号は、無効の番号となります。
ファイルのクラスタチェーンのループを確認します。	ループが壊れている場合、ループが発生したクラスタでファイルが切り捨てられます。
ディレクトリにゼロ以外のサイズフィールドがないかを確認します。	ゼロ以外のサイズフィールドを持つディレクトリが検出されると、サイズが 0 にリセットされます。
無効な開始クラスタファイル番号がないかを確認します。	ファイルの開始クラスタ番号が無効である場合、ファイルが削除されます。
不良または空クラスタのファイルがないかを確認します。	ファイルが不良または空クラスタを持つ場合、ファイルは最後の正常なクラスタで切り捨てられます (たとえば、この不良/空クラスタをポイントするクラスタ)。
ファイルのクラスタチェーンがサイズフィールドに指定されたものより長くないかを確認します。	ファイルのクラスタチェーンがサイズフィールドで指定されたものより長い場合、ファイルサイズが再計算され、ディレクトリエントリが更新されます。
複数のファイルが同じクラスタを共有していないか (クロスリンクされていないか) を確認します。	複数のファイルがクロスリンクされている場合、修復を許可するようにプロンプトが表示され、ファイルの 1 つが切り捨てられます。
ファイルのクラスタチェーンがサイズフィールドに指定されたものより短くないかを確認します。	ファイルのクラスタチェーンがサイズフィールドで指定されたものより短い場合、ファイルサイズが再計算され、ディレクトリエントリが更新されます。
未使用のクラスタチェーンがないかを確認します。	未使用のクラスタチェーンが検出された場合、新しいファイルが作成され、fsck-start cluster という名前でそのファイルにリンクされます。

表 2-10 有効なクラスタ番号

クラスタ	FAT-12	FAT-16
チェーンの次のエントリ	2-FEF	2-FFE
チェーンの最終エントリ	FF8-FFF	FFF8-FFFF
有効なクラスタ	0	0
不良クラスタ	FF7	FFF7

例

次に、現在のファイルシステムに対してチェックを実行する例を示します。

```
Router# fsck
Checking the boot sector and partition table...
Checking FAT, Files and Directories...
Files
1) disk0:/FILE3 and
2) disk0:/FILE2
have a common cluster.
Press 1/2 to truncate or any other character to ignore[confirm] q
Ignoring this error and continuing with the rest of the check...
Files
1) disk0:/FILE5 and
2) disk0:/FILE4
have a common cluster.
Press 1/2 to truncate or any other character to ignore[confirm] 1
File disk0:/FILE5 truncated.
Files
1) disk0:/FILE7 and
2) disk0:/FILE6
have a common cluster.
.
.
.
1) disk0:/FILE15 and
2) disk0:/FILE13
have a common cluster.
Press 1/2 to truncate or any other character to ignore[confirm] i
Ignoring this error and continuing with the rest of the check...
Reclaiming unused space...
Created file disk0:/fsck-11 for an unused cluster chain
Created file disk0:/fsck-20 for an unused cluster chain
Created file disk0:/fsck-30 for an unused cluster chain
Created file disk0:/fsck-35 for an unused cluster chain
Created file disk0:/fsck-40 for an unused cluster chain
Created file disk0:/fsck-46 for an unused cluster chain
Created file disk0:/fsck-55 for an unused cluster chain
Created file disk0:/fsck-62 for an unused cluster chain
Created file disk0:/fsck-90 for an unused cluster chain
Updating FAT...
fsck of disk0: complete
Router#
```

hold-queue

インターフェイス上の IP 出力キューのサイズを制限するには、**hold-queue** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

hold-queue *length* {**in** | **out**}

no hold-queue {**in** | **out**}

シンタックスの説明

<i>length</i>	キュー内の最大パケット数。有効値は 0 ～ 65,535 です。
in	入力キューを指定します。
out	出力キューを指定します。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- 入力の **hold-queue** 制限は 75 パケットです。
- 出力の **hold-queue** 制限は 40 パケットです。
- 非同期インターフェイスのデフォルトは 10 パケットです。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、OSM ではサポートされません。

デフォルトの制限を使用すると、故障したインターフェイスが過剰にメモリを消費するのを防止できます。キューのサイズの上限は決まっていません。

デフォルトの 10 パケットを設定すると、CiscoIOS ソフトウェアは多くのバックツープックのルーティング アップデートをキューイングできます。デフォルト値は、非同期インターフェイスの場合です。他のメディア タイプのデフォルト値は異なります。

ホールド キューおよび優先キューイングの注意事項は、次のとおりです。

- ホールド キューはネットワークから受信して、クライアントに送信されるのを待機しているパケットを保管します。非同期インターフェイスでは、キュー サイズが 10 パケットを超えないように設定してください。他のほとんどのインターフェイスの場合、キュー サイズを 100 パケット以下に設定する必要があります。
- 入力ホールド キューを設定すると、単一のインターフェイスが過剰な入力パケットでネットワーク サーバをフラグディングするのを回避できます。そのインターフェイスにシステム内で未処理の入力パケットが大量にある場合、以降の入力パケットは廃棄されます。
- 優先出力キューイングを使用する場合、**priority-list** グローバル コンフィギュレーション コマンドを使用して 4 つの出力キューのサイズを設定できます。この状況で、**hold-queue** コマンドを使用して出力ホールド キューのサイズを設定することはできません。

- 低速リンクの場合、出力ホールド キューの制限を小さくして、リンクの伝送能力を超える速度でパケットが保存されないようにします。
- 高速リンクの場合、出力ホールド キューの制限を大きくします。高速リンクは短時間でビジーになる（ホールド キューが必要） こともあります。容量が回復すると出力ホールド キューを速やかに空にします。
- 現在のホールド キュー設定およびホールド キューのオーバーフローにより廃棄されるパケット数を表示するには、EXEC モードで **show interfaces** コマンドを使用します。

**注意**

ホールド キューを大きくすると、ネットワークのルーティングや応答時間に悪影響を与える場合があります。sequence/acknowledge パケットでラウンドトリップ時間を判断するプロトコルを使用する場合、出力キューを大きくしないでください。代わりに、Catalyst 6500 シリーズ スイッチを設定して、パケットを廃棄し、使用可能な帯域幅に合わせて送信速度を遅くするようホストに通知することを推奨します。また、ネットワーク内で同じパケットの複製を作らないようにしてください。

例

次に、低速シリアル回線で小さな入力キューを設定する例を示します。

```
Router(config)# interface serial 0
Router(config-if)# hold-queue 30 i
```

関連コマンド

コマンド	説明
priority-list	プロトコルタイプに基づいて、キューイングプライオリティを確立します。
show interfaces	特定のインターフェイスが認識するトラフィックを表示します。

hw-module boot

電源管理バス制御レジスタでモジュールのブート オプションを指定するには、**hw-module boot** コマンドを使用します。

```
hw-module {module num} {boot [value] {config-register | eobc | {flash image} | rom-monitor}}
```

シンタックスの説明	
module num	コマンドを適用するモジュールの番号を指定します。
value	(任意) モジュールのブート オプションのリテラル値。有効値は 0 ~ 15 です。詳細については、「使用上のガイドライン」を参照してください。
config-register	モジュールの設定レジスタ値を使用してブートします。
eobc	Ethernet out-of-band channel (EOBC) でダウンロードしたイメージを使用してブートします。
flash image	モジュールの内部フラッシュ メモリにある、モジュールのブート オプションのイメージ番号を指定します。有効値は 1 および 2 です。
rom-monitor	モジュールのリセット後、ROM モニタ モードに留まります。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード 特権 EXEC (#)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドをサポートするのは、Communication Media Module (CMM) だけです。

boot value 引数の有効値は次のとおりです。

- 0 : モジュールの設定レジスタ値を指定します。
- 1 : フラッシュ メモリの最初のイメージを指定します。
- 2 : フラッシュ メモリの 2 番目のイメージを指定します。
- 3 : モジュールのリセット後、ROM モニタ モードに留まります。
- 4 : EOBC でダウンロードしたイメージを指定します。

例

次に、モジュールの設定レジスタ値を使用してスロット 6 のモジュールをリロードする例を示します。

```
Router# hw-module slot 1/6 boot config-register  
Router#
```

次に、EOBC でダウンロードしたイメージを使用してスロット 3 のモジュールをリロードする例を示します。

```
Router# hw-module slot 1/3 boot eobc  
Router#
```

hw-module fan-tray version

ファンタイプ（高出力または低出力）を設定するには、**hw-module fan-tray version** コマンドを使用します。

hw-module fan-tray version [1 | 2]

シンタックスの説明

1 | 2 (任意) バージョン番号を指定します。詳細については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

高機能ファントレイを設置する前に **hw-module fan-tray version 2** コマンドを入力し、電源装置の互換性や電源容量などの設定の問題を確認してください。問題がない場合は、バージョン 1 からバージョン 2 にファントレイを変更するようメッセージが表示されます。この時点で古いファントレイを取り外し、すぐに新しい高機能ファントレイを装着します。

このコマンドは、次のシャーシでサポートされています。

- WS-C6506
- WS-C6509
- WS-C6509-NEB/OSR7609

高出力のファントレイを取り付ける前に、バージョンを **2** に設定してください。低出力のファントレイを取り付ける前に、バージョンを **1** に設定してください。

コマンドを入力しても、ファンの電力消費または冷却能力は変わりません。コマンドによって、バックプレーンの IDPROM が更新されます。更新された値は、次にファンを取り付けたときに有効になります。

このコマンドを実行すると、ソフトウェアはコンフィギュレーションをチェックし、確認が求められます。誤ったコンフィギュレーション（電源との不適合など）があると、警告が表示され、コマンドは有効になりません。

例

次に、ファンタイプを低出力ファントレイに設定する例を示します。

```
Router # hw-module fan-tray version 1
Router #
```

関連コマンド

コマンド	説明
show environment cooling	冷却パラメータに関する情報を表示します。

hw-module oversubscription

モジュール上でオーバーサブスクリプトしたポート (3、4、7、および 8) を管理上のディセーブルにするには、**hw-module oversubscription** コマンドを使用します。オーバーサブスクリプトしたポートをイネーブルにするには、このコマンドの **no** 形式を使用します。

hw-module {module num} oversubscription

no hw-module {module num} oversubscription

シンタックスの説明

module num 特定のモジュールにコマンドを適用します。

コマンドのデフォルト

イネーブル

コマンドモード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、WS-X6708-10G-3C モジュールおよび WS-X6708-10G-3CXL モジュールだけでサポートされています。

オーバーサブスクリプトしたポートをディセーブルにすると、ポートがシャットダウンモードになります。このモードでは、ディセーブルになっているポートに **no shut** コマンドを入力できません。ディセーブルになっているポートに **no shut** コマンドを入力しようとすると、次のメッセージが表示されます。

```
The current module is operating in non-oversubscription mode. To utilise this interface,
enable oversubscription mode for the module.
```

num 引数は、モジュール番号を指定します。有効値は、使用するシャーシによって異なります。たとえば、13 スロットシャーシを使用している場合、モジュール番号の有効値は 1 ~ 13 です。

ディセーブルになっているポートに **show interfaces** コマンドを入力すると、出力に [disabled for performance] と表示されて、通常のポートのシャットダウンとパフォーマンス用のシャットダウンが区別されます。

例

次に、モジュール上のオーバーサブスクリプトしたポートを管理上のディセーブルにする例を示します。

```
Router # hw-module module 3 oversubscription
Router #
```

次に、モジュール上でオーバーサブスクリプトしたポートを管理上のイネーブルにする例を示します。

```
Router # no hw-module module 3 oversubscription
Router #
```

関連コマンド

コマンド	説明
show interfaces	特定のインターフェイスで認識されるトラフィックを表示します。

hw-module reset

電源をいったんオフにしてから再びオンにしてモジュールをリセットするには、**hw-module reset** コマンドを使用します。

hw-module {module num} reset

シンタックスの説明	module num	特定のモジュールにコマンドを適用します。有効値については、「使用上のガイドライン」を参照してください。
------------------	-------------------	---

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード 特権 EXEC (#)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン *num* 引数は、モジュール番号を指定します。有効値は、使用するシャーシによって異なります。たとえば、13 スロットシャーシを使用している場合、モジュール番号の有効値は 1 ~ 13 です。

例 次に、特定のモジュールをリロードする例を示します。

```
Router # hw-module module 3 reset  
Router #
```

hw-module shutdown

モジュールをシャットダウンするには、**hw-module shutdown** コマンドを使用します。

hw-module {module num} shutdown

シンタックスの説明

module num	特定のモジュールにコマンドを適用します。有効値については、「使用上のガイドライン」を参照してください。
-------------------	---

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、Secure Sockets Layer (SSL) サービス モジュールおよび Network Analysis Module (NAM; ネットワーク解析モジュール) でサポートされています。

hw-module shutdown コマンドを使用してモジュールをシャットダウンする場合、**no power enable module** コマンドを入力し、**power enable module** コマンドを入力してモジュールを再起動（電源のオフ/オン）する必要があります。

例

次に、モジュールをシャットダウンして再起動する例を示します。

```
Router# hw-module module 3 shutdown
Router# no power enable module 3
Router# power enable module 3
```

hw-module simulate link-up

指定されたモジュールでソフトウェア リンクをイネーブルにするには、**hw-module simulate link-up** コマンドを使用します。ソフトウェア リンクのディセーブル化の詳細については、「使用上のガイドライン」を参照してください。

hw-module {module num} simulate link-up

シンタックスの説明	module num 特定のモジュールにコマンドを適用します。有効値については、「使用上のガイドライン」を参照してください。
------------------	---

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード 特権 EXEC (#)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドをサポートするのは、イーサネット モジュールだけです。モジュールのソフトウェア リンクをディセーブルにするには、次のいずれかの手順を実行します。

- モジュールのすべてのポートで、**shutdown** コマンド、続いて **no shutdown** コマンドを入力します。
- hw-module reset** コマンドを入力します。

このコマンドをモジュールに適用すると、モジュールのポート LED がグリーンに点灯し、リンクアップ条件をシミュレートします。このコマンドを使用すると、インターフェイスにケーブル接続せずにインターフェイス コンフィギュレーションをテストできます。

num 引数は、モジュール番号を指定します。有効値は、使用するシャーシによって異なります。たとえば、13 スロット シャーシを使用している場合、モジュール番号の有効値は 1 ~ 13 です。

例 次に、モジュールのソフトリンクをイネーブルにする例を示します。

```
Router# hw-module module 3 simulate link-up
Router#
```

関連コマンド	コマンド	説明
	hw-module reset	電源をオフにしてからオンに切り替え、モジュールをリセットします。

instance

1 つまたは一連の VLAN を MST インスタンスにマッピングするには、**instance** コマンドを使用します。デフォルトインスタンス (Common and Internal Spanning Tree (CIST)) に VLAN を返すには、このコマンドの **no** 形式を使用します。

```
instance instance-id {vlans vlan-range}
```

```
no instance instance-id
```

シンタックスの説明

<i>instance-id</i>	指定された VLAN がマッピングされるインスタンス。有効値は 0 ~ 4094 です。
vlan s <i>vlan-range</i>	指定されたインスタンスにマッピングする VLAN の番号。有効値は 1 ~ 4094 です。

コマンドのデフォルト

VLAN はどの MST インスタンスにもマッピングされません (すべての VLAN は CIST インスタンスにマッピングされます)。

コマンドモード

MST コンフィギュレーション サブモード

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

vlans *vlan-range* は、単一値または範囲として入力します。

マッピングは増分であり、絶対値ではありません。VLAN の範囲を入力した場合には、この範囲が既存のインスタンスに追加されるか、既存のインスタンスから削除されます。

マッピングされていない VLAN は、CIST インスタンスにマッピングされます。

最大 65 のインターフェイスを設定できるようになりました。

例

次に、VLAN の範囲を **instance 2** にマッピングする例を示します。

```
Router(config-mst)# instance 2 vlans 1-100  
Router(config-mst)#
```

次に、単一の VLAN を **instance 5** にマッピングする例を示します。

```
Router(config-mst)# instance 5 vlans 1100  
Router(config-mst)#
```

次に、VLAN の範囲を instance 2 から CIST インスタンスに移動する例を示します。

```
Router(config-mst)# no instance 2 vlans 40-60
Router(config-mst)#
```

次に、instance 2 にマッピングされているすべての VLAN を再び CIST インスタンスに移動する例を示します。

```
Router(config-mst)# no instance 2
Router(config-mst)#
```

関連コマンド

コマンド	説明
name (MST configuration submode)	MST リージョン名を設定します。
revision	MST コンフィギュレーションのリビジョン番号を設定します。
show	MST の設定を確認します。
show spanning-tree mst	MST プロトコルに関する情報を表示します。
spanning-tree mst configuration	MST コンフィギュレーション サブモードを開始します。

interface

設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始するには、**interface** コマンドを使用します。

```
interface {type module} [.subinterface]
```

シンタックスの説明

<i>type</i>	設定するインターフェイスのタイプ。有効値については、表 2-11 を参照してください。
<i>module</i>	モジュールおよびポート番号またはポートサブインターフェイス番号。詳細については、「使用上のガイドライン」を参照してください。
<i>.subinterface</i>	(任意) 設定するサブインターフェイス番号。有効値は 0 ~ 4,294,967,295 です。

コマンドのデフォルト

インターフェイスのタイプは設定されていません。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

表 2-11 に、*type* の有効値の一覧を示します。

表 2-11 有効な *type* 値

キーワード	定義
fastethernet	100 Mbps イーサネット インターフェイス
gigabitethernet	ギガビット イーサネット IEEE 802.3z インターフェイス
tengigabitethernet	10 ギガビット イーサネット IEEE 802.3ae インターフェイス
ge-wan	ギガビット イーサネット WAN IEEE 802.3z インターフェイス
pos	Packet over SONET (PoS) インターフェイス プロセッサ上のパケット OC-3 インターフェイス
atm	ATM インターフェイス
vlan	VLAN インターフェイス。 interface vlan コマンドを参照してください。
port-channel	ポート チャネル インターフェイス。 interface port-channel コマンドを参照してください。
null	ヌル インターフェイス。有効値は 0 です。
tunnel	トンネル インターフェイス

デフォルトでは、Supervisor Engine 32 PISA EtherChannel (ポート チャネル インターフェイス 256。 **pisa-channel** コマンドを使用して自動的に設定) は、1 Gps EtherChannel です。



(注) **pisa-channel** コマンドはコンフィギュレーションファイルには表示されますが、ユーザは設定できません。

次のフォーマットで、ポート サブインターフェイスの数を入力できます。

```
interface {{type module/port.subinterface}}
```

Supervisor Engine 32 PISA ポートは、次のとおりです。

- Supervisor Engine 32 PISA 管理ポート : Supervisor Engine 32 PISA ポートのコンソール ポートは、EIA/TIA-232 (RS-232) ポートです。 Supervisor Engine 32 PISA には、現在イネーブルにされていない 2 つの Universal Serial Bus (USB) 2.0 ポートがあります。
- WS-S32-10GE-PISA の Supervisor Engine 32 PISA データ ポートには、次のポートがあります。
 - ポート 1 および 2 : XENPAK 10 ギガビット イーサネット
 - ポート 3 : 10/100/1000 Mbps RJ-45
 -



(注) ポート 3 をディセーブルにして、PISA EtherChannel にポート Application-Specific Integrated Circuit (ASIC; 特定用途向け IC) の容量を再度割り当てることができます (『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*』の「Configuring Full PISA EtherChannel Bandwidth」を参照)。

- WS-S32-GE-PISA の Supervisor Engine 32 PISA データ ポートには、次のポートがあります。
 - ポート 1 ~ 8 : Small Form-factor Pluggable (SFP; 着脱可能小型フォーム ファクタ) ギガビット イーサネット
 - ポート 9 : 10/100/1000 Mbps RJ-45 ポート



(注) ポート 9 をディセーブルにして、PISA EtherChannel にポート ASIC の容量を再度割り当てることができます (『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*』の「Configuring Full PISA EtherChannel Bandwidth」を参照)。



(注) ポートが PISA EtherChannel のメンバーになった場合、メンバーである間は **no channel-group 256 mode on** コマンドだけがポートに影響します。ポートが PISA EtherChannel のメンバーである間、**no channel-group 256 mode on** コマンド以外のすべてのポートのコンフィギュレーション コマンドが無視されます。

WS-S32-GE-PISA の場合、ポート 8 と 9 の両方を PISA EtherChannel に割り当てることができます。ポート チャネル インターフェイス 256 では、どのコンフィギュレーションも開始できません。PISA EtherChannel MTU のサイズは、4096 バイトです。

interface

例

次に、スロット 5 に装着された WS-S32-10GE-PISA の PISA EtherChannel にポート 3 のポート ASIC の容量を割り当てる例を示します。

```
Router(config)# interface gigabitethernet 5/3
Router(config-if)# channel-group 256 mode on
Router(config-if)#
```

次に、スロット 5 に装着された WS-S32-GE-PISA の PISA EtherChannel にポート 9 のポート ASIC の容量を割り当てる例を示します。

```
Router(config)# interface gigabitethernet 5/9
Router(config-if)# channel-group 256 mode on
Router(config-if)#
```

次に、デフォルトのポート ASIC 容量の割り当てに戻す例を示します。

```
Router(config)# interface gigabitethernet 5/9
Router(config-if)# no channel-group 256 mode on
Router(config-if)#
```

関連コマンド

コマンド	説明
show interfaces	特定のインターフェイスが認識するトラフィックを表示します。

interface port-channel

ポートチャンネル仮想インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始するには、**interface port-channel** コマンドを使用します。仮想インターフェイスまたはサブインターフェイスを削除するには、このコマンドの **no** 形式を使用します。

```
interface port-channel channel-number[.subinterface]
```

```
no interface port-channel channel-number[.subinterface]
```

シンタックスの説明

<i>channel-number</i>	このポートチャンネル インターフェイスに割り当てられたチャンネル番号。有効値は 1 ~ 256 です。
<i>.subinterface</i>	(任意) 設定するサブインターフェイス番号。有効値は 0 ~ 4,294,967,295 です。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、Intrusion Detection System Module (IDSM) および NAM ではサポートされていません。

このコマンドは、EtherChannel、Fast EtherChannel、Gigabit EtherChannel、10- Gigabit EtherChannel のインターフェイスでサポートされます。

channel-number 引数の有効値は 1 ~ 256 で、最大 128 のポート チャンネル インターフェイスを指定できます。

レイヤ 2 ポート チャンネルはダイナミックに、または **interface port-channel** コマンドを使用することによって作成できます。レイヤ 3 ポート チャンネルは、**interface port-channel** コマンドを使用することによってだけ作成できます。レイヤ 3 ポート チャンネルをダイナミックに作成することはできません。

1 つのチャンネル グループには、ポート チャンネルは 1 つだけです。

ポートは任意のモジュール間でバンドルできます。



注意

レイヤ 3 ポート チャンネル インターフェイスは、ルーテッド インターフェイスです。物理ファストイーサネット インターフェイスでレイヤ 3 アドレスをイネーブルにしないでください。

interface port-channel

interface port-channel コマンドを使用する場合、次の注意事項に従ってください。

- ISL を設定する場合、switched virtual interface (SVI; スイッチ仮想インターフェイス) に IP アドレスを割り当てる必要があります。
- Cisco Discovery Protocol (CDP) を使用する場合は、物理ファストイーサネットインターフェイス上だけで設定する必要があります。ポートチャネルインターフェイス上で設定することはできません。
- スタティック MAC アドレスをポートチャネルインターフェイスに割り当てない場合、MAC アドレスが自動的に割り当てられます。スタティック MAC アドレスを割り当てたあとに、そのアドレスを削除した場合、MAC アドレスが自動的に割り当てられます。

例

次に、チャンネルグループ番号 256 でポートチャネルインターフェイスを作成する例を示します。

```
Router(config)# interface port-channel 256
Creating a switch port Po256. channel-group 256 is L2
Router(config-if)#
```



(注)

show counters interface port-channel コマンドおよび **show interface port-channel counters** コマンドにより表示されるポートチャネルインターフェイスカウンタは、IEEE 802.1Q in 802.1Q (QinQ) リンクバンドルに GE-WAN インターフェイスを使用するチャンネルグループではサポートされません。ただし、**show interface port-channel {number | number.subif}** コマンド (**counters** キーワードなし) は、サポートされます。

関連コマンド

コマンド	説明
channel-group	EtherChannel インターフェイスの EtherChannel グループへの割り当ておよび設定を行います。
show etherchannel	チャンネルの EtherChannel 情報を表示します。

interface range

コマンドを複数のポートで同時に実行するには、**interface range** コマンドを使用します。

```
interface range {port-range | {macro name}}
```

シンタックスの説明

<i>port-range</i>	ポート範囲。 <i>port-range</i> の指定できる値のリストについては、「使用上のガイドライン」を参照してください。
<i>macro name</i>	マクロ名を指定します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバルまたはインターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

interface range vlan コマンドで入力した値がすべての既存 VLAN SVI に適用されます。

マクロを使用する前に、**define interface-range** コマンドで範囲を定義する必要があります。

ポート範囲に対して行われるすべての設定変更は NVRAM に保存されますが、**interface range** コマンドで作成されたポート範囲は NVRAM には保存されません。

ポート範囲は次の 2 つの方法で入力できます。

- 最大 5 つのポート範囲を指定
- 以前定義したマクロを指定

ポートまたはポート範囲マクロ名のいずれかを指定できます。ポート範囲は、同じポート タイプで構成される必要があり、範囲内のポートはスロットをまたがることはできません。

1 つのコマンドで最大 5 つのポート範囲を定義できます。それぞれの範囲はカンマで区切ってください。

スペースが存在するかどうかに関係なく範囲を入力できます。たとえば、**gigabitethernet 7/1 -7** または **gigabitethernet 7/1-7** として範囲を入力できます。

VLAN の範囲を指定すると、その範囲に存在しない SVI が作成されます。

port-range を入力する場合、次のフォーマットを使用します。 *card-type* {slot}/{first-port} - {last-port}

card-type の有効値は次のとおりです。

- ethernet
- fastethernet
- gigabitethernet
- loopback
- tengigabitethernet

interface range

- **tunnel**
- **ge-wan**
- **pos**
- **atm**
- **vlan *vlan-id*** (有効値は 1 ~ 4094)
- **port-channel *interface-number*** (有効値は 1 ~ 256)

同じコマンドでマクロとインターフェイス範囲の両方を指定することはできません。マクロを作成したあと、CLI でさらに範囲を入力することはできません。すでにインターフェイス範囲を入力している場合は、CLI でマクロを入力できません。

また、*port-range* に 1 つのインターフェイスを指定することもできます。

例

次に、2 つのポート範囲でコマンドを実行する例を示します。

```
Router(config)# interface range fastethernet 5/18 -20, ethernet 3/1 -24
Router(config-if-range)#
```

次に、ポート範囲マクロを実行する例を示します。

```
Router(config)# interface range macro macrol
Router(config-if-range)#
```

関連コマンド

コマンド	説明
define interface-range	インターフェイス レンジ マクロを作成します。
show running-config	モジュールまたはレイヤ 2 VLAN のステータスおよび設定を表示します。

interface vlan

ダイナミック SVI の作成またはアクセスを行うには、**interface vlan** コマンドを使用します。SVI を削除するには、このコマンドの **no** 形式を使用します。

```
interface vlan vlan-id
```

```
no interface vlan vlan-id
```

シンタックスの説明

<i>vlan-id</i>	VLAN の番号。有効値は 1 ~ 4094 です。
----------------	----------------------------

コマンドのデフォルト

Fast EtherChannel は指定されていません。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

SVI は、特定の VLAN に最初に **interface vlan *vlan-id*** コマンドを入力したときに作成されます。*vlan-id* 値は、ISL 上のデータ フレームに関連付けられた VLAN タグ、802.1Q カプセル化トランク、またはアクセス ポートに設定された VLAN ID に対応します。新規 VLAN インターフェイスを作成するたびにメッセージが表示され、入力した VLAN 番号が正しいかどうか確認できます。

no interface vlan *vlan-id* コマンドを入力して SVI を削除した場合、関連付けられた **interface descriptor block** (IDB; インターフェイス記述ブロック) ペアは強制的に管理上のダウン ステートになり、削除とマークされます。削除されたインターフェイスは、**show interface** コマンドで確認できなくなります。

削除されたインターフェイスに **interface vlan *vlan-id*** コマンドを入力すると、削除された SVI を元に戻すことができます。インターフェイスは戻りますが、以前の設定の多くは消えてしまいます。

1006 ~ 1014 の VLAN は、Catalyst 6500 シリーズ スイッチ上の内部 VLAN であり、新規 VLAN の作成に使用することはできません。

例

次に、新規の VLAN 番号に **interface vlan *vlan-id*** コマンドを入力したときの出力例を示します。

```
Router(config)# interface vlan 23
% Creating new VLAN interface.
Router(config)#
```

inter-packet gap 6502-mode

inter packet gap (IPG) 値を設定するには、**inter-packet gap 6502-mode** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

inter-packet gap 6502-mode

no inter-packet gap 6502-mode

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

レイヤ 4 ポート情報および許可アクションを含む ACE から受信するフローのフラグメントはすべて許可されます。その他のフラグメントは、すべてハードウェアで廃棄されます。これはこのコマンド設定に関係なく、ソフトウェアで処理されたフローに対しても適用されます。

コマンドモード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、WS-X6704-10GE が WS-X6502-10GE だけに接続されている状況でサポートされます。WS-X6704-10GE の IPG 値を変更して WS-X6502-10GE と一致させるには、このコマンドを入力します。

デフォルトの 6704 モードでは、IPG 値が平均 12 に設定されます。パケット サイズに基づいて、連続するパケット間の IPG の範囲は 9 ~ 15 です。

6502 モードでは、IPG 値が平均 16 に設定されます。パケット サイズに基づいて、連続するパケット間の IPG の範囲は 13 ~ 19 です。

例

次に、IPG を 6502 モードに設定する例を示します。

```
Router(config-if)# inter-packet gap 6502-mode  
Router(config-if)#
```

次に、IPG をデフォルト モードに設定する例を示します。

```
Router(config-if)# no inter-packet gap 6502-mode  
Router(config-if)#
```

ip access-list hardware permit fragments

ハードウェアですべての非初期フラグメントを許可するには、**ip access-list hardware permit fragments** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip access-list hardware permit fragments

no ip access-list hardware permit fragments

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト レイヤ 4 ポート情報および許可アクションを含む ACE から受信するフローのフラグメントはすべて許可されます。その他のフラグメントは、すべてハードウェアで廃棄されます。これはこのコマンド設定に関係なく、ソフトウェアで処理されたフローに対しても適用されます。

コマンドモード グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン レイヤ 4 ポート情報および許可結果を含む ACE に一致するフロー フラグメントはハードウェアで許可され、その他のフラグメントはすべて廃棄されます。レイヤ 4 ポート情報および許可アクションを含む各 ACE に対して、エントリが TCAM に追加されます。これによって、ACL が大きくなり、TCAM に適合しなくなる場合があります。このような状況が発生した場合は、**ip access-list hardware permit fragments** コマンドを使用して、ハードウェアですべての非初期フラグメントを許可します。

このコマンドは、新しく適用された ACL だけでなく、インターフェイスに現在適用されているすべての ACL に影響します。

レイヤ 4 ポート情報および許可結果を含む ACE に一致するフローの初期フラグメントは、ハードウェアで許可されます。その他の初期フラグメントは、すべてハードウェアで廃棄されます。

例 次に、すべての非初期フラグメントをハードウェアで許可する例を示します。

```
Router(config)# ip access-list hardware permit fragments
Router(config)#
```

次に、デフォルト設定に戻す例を示します。

```
Router(config)# no ip access-list hardware permit fragments
Router(config)#
```

関連コマンド	コマンド	説明
	show ip interface	IP 用に設定したインターフェイスのユーザビリティ ステータスを表示します。

ip arp inspection filter vlan

DAI がイネーブルの場合に、スタティック IP に設定されたホストからの ARP を許可し、ARP アクセス リストを定義して、これを VLAN に適用するには、**ip arp inspection filter vlan** コマンドを使用します。適用をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ip arp inspection filter arp-acl-name {vlan vlan-range} [static]
```

```
no ip arp inspection filter arp-acl-name {vlan vlan-range} [static]
```

シンタックスの説明

<i>arp-acl-name</i>	アクセス制御リスト名
<i>vlan-range</i>	VLAN 番号または VLAN 範囲。有効値は 1 ~ 4094 です。
static	(任意) ARP ACL の暗黙的な拒否を明示的な拒否として処理し、ACL 内の以前の句と一致しないパケットを廃棄します。

コマンドのデフォルト

定義済みの ARP ACL は、VLAN に適用されません。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

vlan-range には、スイッチおよびホストが属する VLAN を指定できます。VLAN ID 番号により識別される単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。

ダイナミック ARP インスペクション用に ARP ACL が VLAN に適用される場合、IP と Ethernet 間の MAC バインディングだけを含む ARP パケットが、ACL と比較されます。他のすべてのタイプのパケットは、確認されずに着信 VLAN でブリッジされます。

このコマンドは、着信 ARP パケットが ARP ACL と比較され、ACL が許可した場合にだけパケットが許可されることを指定します。

ACL が明示的な拒否によりパケットを拒否した場合、これらのパケットは廃棄されます。パケットが暗黙的な拒否により拒否された場合、ACL がスタティックに適用されていない場合は DHCP バインディングのリストと照合されます。

static キーワードを指定しない場合、ACL にパケットを拒否する明示的な拒否がないことを意味し、パケットが ACL のどの句にも一致しなければ、DHCP バインディングがパケットを許可するか拒否するかを決定します。

例 次に、DAI 用に ARP ACL のスタティックなホストを VLAN 1 に適用する例を示します。

```
Switch# config terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)# ip arp inspection filter static-hosts vlan 1  
Router(config)#
```

関連コマンド

コマンド	説明
arp access-list	ARP インспекションおよび QoS フィルタリング用の ARP ACL を設定し、ARP ACL コンフィギュレーションサブモードを開始します。
show ip arp inspection	特定の範囲の VLAN について DAI のステータスを表示します。

ip arp inspection limit

インターフェイス上で着信 ARP 要求および応答のレートを制限し、denial of service (DoS) 攻撃の場合に DAI によりすべてのシステム リソースが消費されないようにするには、**ip arp inspection limit** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip arp inspection limit {rate pps [*burst interval seconds*]} | none

no ip arp inspection limit

シンタックスの説明

rate pps	秒単位で処理される着信パケット数の上限を指定します。有効値は、1 ~ 2048 pps です。
burst interval seconds	(任意) インターフェイスが高レート of ARP パケットに関してモニタされる連続的インターバル (秒) を指定します。有効値は 1 ~ 15 秒です。
none	処理できる着信 ARP パケットのレートに上限がないことを指定します。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- 信頼できないインターフェイスでは、**rate pps** は **15 packets per second** (ppsec; パケット/秒) に設定されています。このネットワークが毎秒 15 の新しいホストに接続される 1 つのホストを持つスイッチドネットワークであると想定しています。
- 信頼できるすべてのインターフェイス上では、レートは無制限になります。
- burst interval seconds** は、**1** 秒に設定されています。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

トランク ポートでは集約を反映するため、より高いレートを設定する必要があります。着信パケットのレートがユーザ設定のレートを超過すると、インターフェイスは **errdisable** ステートになります。**errdisable** タイムアウト機能を使用すると、**errdisable** ステートからポートを削除できます。このレートは、信頼できるインターフェイスおよび信頼できないインターフェイスの両方に適用されます。トランクに適切なレートを設定して複数の DAI 対応 VLAN 間のパケットを処理するか、または **none** キーワードを使用してレートを無制限にします。

チャンネル ポートの着信 ARP パケットのレートは、すべてのチャンネル メンバーからの着信パケットのレートの合計と同じです。チャンネルメンバーの着信 ARP パケットのレートを検討してから、チャンネルポートのレート制限を設定してください。

バースト時にスイッチが受信するパケット レートが、設定されたパケット レートを毎秒連続して超過すると、インターフェイスは **errdisable** ステートになります。

例

次に、着信 ARP 要求のレートを 25 パケット/秒に制限する例を示します。

```
Router# config terminal
Router(config)# interface fa6/3
Router(config-if)# ip arp inspection limit rate 25
Router(config-if)#
```

次に、着信 ARP 要求のレートを 20 パケット/秒に制限し、インターフェイスのモニタリング インターバルを連続した 5 秒に設定する例を示します。

```
Router# config terminal
Router(config)# interface fa6/1
Router(config-if)# ip arp inspection limit rate 20 burst interval 5
Router(config-if)#
```

関連コマンド

コマンド	説明
show ip arp inspection	特定の範囲の VLAN について DAI のステータスを表示します。

ip arp inspection log-buffer

ロギングバッファに関連付けられるパラメータを設定するには、**ip arp inspection log-buffer** コマンドを使用します。パラメータをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip arp inspection log-buffer *{{entries number} | {logs number} {interval seconds}}*

no ip arp inspection log-buffer *{entries | logs}*

シンタックスの説明

entries number	ロギングバッファからのエントリ数を指定します。有効値は 0 ~ 1024 です。
logs number	一定のインターバルでロギングされるエントリ数を指定します。有効値は 0 ~ 1024 です。
interval seconds	ロギングレートを指定します。有効値は 0 ~ 86,400 (1 日) です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- ダイナミック ARP インспекションがイネーブルであるか、拒否または廃棄されると、ARP パケットはロギングされます。
- **entries number** は、**32** です。
- **logs number** は、**5/秒**です。
- **interval seconds** は、**1 秒**です。

コマンドモード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

logs number が **0** の場合は、このバッファからエントリがロギングされないことを意味します。

interval seconds キーワードと引数が **0** の場合は、即時ログを意味します。

logs number および **interval seconds** キーワードおよび引数の両方に **0** を入力することはできません。

所定のフローの最初の廃棄パケットは、ただちにロギングされます。同じフローのそれ以降のパケットは登録されますが、ただちにロギングされません。これらパケットは、すべての VLAN で共有されるログバッファで登録されます。このバッファからのエントリは、レート制限単位でロギングされます。

例

次に、ロギングバッファで最大 45 エントリを維持するよう設定する例を示します。

```
Router# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip arp inspection log-buffer entries 45
Router(config)#
```

次に、ロギング レートを 10 ログ/3 秒に設定する例を示します。

```
Router(config)# ip arp inspection log-buffer logs 10 interval 3
Router(config)#
```

関連コマンド

コマンド	説明
arp access-list	ARP インспекションおよび QoS フィルタリング用の ARP ACL を設定し、ARP ACL コンフィギュレーション サブモードを開始します。
clear ip arp inspection log	ログ バッファのステータスをクリアします。
show ip arp inspection log	ログ バッファのステータスを表示します。

ip arp inspection trust

ポート単位で設定可能な信頼状態を設定して、着信 ARP パケットが検査される一連のインターフェイスを決定するには、**ip arp inspection trust** コマンドを使用します。インターフェイスを信頼できないようにするには、このコマンドの **no** 形式を使用します。

ip arp inspection trust

no ip arp inspection trust

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、インターフェイスを信頼できる状態に設定する例を示します。

```
Router# config terminal
Router(config)# interface fastEthernet 6/3
Router(config-if)# ip arp inspection trust
Router(config-if)#
```

関連コマンド

コマンド	説明
show ip arp inspection	特定の範囲の VLAN について DAI のステータスを表示します。

ip arp inspection validate

ARP インспекションに関して特定の確認を行うには、**ip arp inspection validate** コマンドを使用します。ARP インспекションの確認をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip arp inspection validate [src-mac] [dst-mac] [ip]

no ip arp inspection validate [src-mac] [dst-mac] [ip]

シンタックスの説明

src-mac	(任意) イーサネットヘッダーの送信元 MAC アドレスを、ARP 本体の送信側の MAC アドレスと比較します。
dst-mac	(任意) イーサネットヘッダーの宛先 MAC アドレスを、ARP 本体のターゲット MAC アドレスと比較します。
ip	(任意) 無効および想定外の IP アドレスがないか ARP 本体を確認します。

コマンドのデフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

送信側の IP アドレスはすべての ARP 要求および応答で確認され、ターゲット IP アドレスは ARP 応答だけで確認されます。アドレスには、0.0.0.0、255.255.255.255、およびすべての IP マルチキャストアドレスが含まれます。

src-mac 確認は、ARP 要求および応答の両方に対して行われます。**dst-mac** 確認は、ARP 応答に対して行われます。



(注)

イネーブルの場合、異なる MAC アドレスを持つパケットは無効として分類され、廃棄されます。

確認をイネーブルにする場合、コマンドラインで少なくとも 1 つのキーワード (**src-mac**、**dst-mac**、および **ip**) を指定します。各コマンドでは、以前のコマンドの設定は上書きされます。あるコマンドで **src** および **dst mac** 確認をイネーブルにし、2 番目のコマンドでは IP 確認だけをイネーブルにした場合、**src** および **dst mac** 確認は 2 番目のコマンドの結果としてディセーブルになります。

このコマンドの **no** 形式により、指定された確認だけがディセーブルになります。確認オプションがディセーブルの場合、すべての確認がディセーブルとなります。

例

次に、送信元 MAC 確認をイネーブルにする例を示します。

```
Router(config)# ip arp inspection validate src-mac
Router(config)#
```

関連コマンド

コマンド	説明
arp access-list	ARP インспекションおよび QoS フィルタリング用の ARP ACL を設定し、ARP ACL コンフィギュレーションサブモードを開始します。
show ip arp inspection	特定の範囲の VLAN について DAI のステータスを表示します。

ip arp inspection vlan

VLAN 単位で DAI をイネーブルにするには、**ip arp inspection vlan** コマンドを使用します。DAI をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip arp inspection vlan *vlan-range*

no ip arp inspection vlan *vlan-range*

シンタックスの説明

vlan-range VLAN 番号または VLAN 範囲。有効値は 1 ~ 4094 です。

コマンドのデフォルト

ARP インスペクションは、すべての VLAN でディセーブルです。

コマンドモード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

vlan-range では、VLAN ID 番号により識別される単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。

DAI をイネーブルにする VLAN を指定する必要があります。VLAN が作成されていないか、または Private VLAN (PVLAN; プライベート VLAN) である場合は、DAI は設定済み VLAN 上で機能しない可能性があります。

例

次に、VLAN 1 で DAI をイネーブルにする例を示します。

```
Router(config)# ip arp inspection vlan 1
Router(config)#
```

関連コマンド

コマンド	説明
arp access-list	ARP インスペクションおよび QoS フィルタリング用の ARP ACL を設定し、ARP ACL コンフィギュレーション サブモードを開始します。
show ip arp inspection	特定の範囲の VLAN について DAI のステータスを表示します。

ip arp inspection vlan logging

ロギングされるパケットタイプを制御するには、**ip arp inspection vlan logging** コマンドを使用します。このロギング制御をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ip arp inspection vlan vlan-range logging {acl-match {matchlog | none} | dhcp-bindings
{permit | all | none}}
```

```
no ip arp inspection vlan vlan-range logging {acl-match | dhcp-bindings}
```

シンタックスの説明

vlan-range	指定されたインスタンスにマッピングされる VLAN の番号。番号は、1 つの値または範囲として入力できます。設定できる値は 1 ~ 4094 です。
acl-match	ACL との照合に基づいて廃棄または許可されるパケットのロギング基準を指定します。
matchlog	ACL に照合されるパケットのロギングは、ACL の許可および拒否アクセス制御エントリの matchlog キーワードにより制御されることを指定します。
none	ACL に一致するパケットはロギングされないことを指定します。
dhcp-bindings	DHCP バインディングとの照合に基づいて廃棄または許可されるパケットのロギング基準を指定します。
permit	DHCP バインディングにより許可される場合のロギングを指定します。
all	DHCP バインディングにより許可または拒否される場合のロギングを指定します。
none	DHCP バインディングにより許可または拒否されるすべてのパケットをロギングしません。

コマンドのデフォルト

拒否または廃棄されたパケットのすべてが、ロギングされます。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

デフォルトでは、**matchlog** キーワードは ACE で使用できません。**matchlog** キーワードを入力すると、拒否されたパケットはロギングされません。パケットは、**matchlog** キーワードを持つ ACE に照合される場合にだけロギングされます。

acl-match および **dhcp-bindings** キーワードは、相互に統合します。ACL 一致コンフィギュレーションを設定すると、DHCP バインディング コンフィギュレーションはイネーブルになります。一部のロギング基準をデフォルトにリセットする場合は、このコマンドの **no** 形式を使用できます。オプションを指定しない場合、ARP パケットが拒否された際にすべてのロギングタイプがログオンにリセットされます。次の 2 つのオプションを使用できます。

- **acl-match** : ACL 一致に基づくログオンは、ログオン拒否にリセットされます。
- **dhcp-bindings** : DHCP バインディングに基づくログオンは、ログオン拒否にリセットされます。

例 次に、VLAN 1 上で ARP インспекションを設定して、ACL に一致するログにパケットを追加する例を示します。

```
Router# config terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)# ip arp inspection vlan 1 logging acl-match matchlog  
Router(config)#
```

関連コマンド

コマンド	説明
arp access-list	ARP インспекションおよび QoS フィルタリング用の ARP ACL を設定し、ARP ACL コンフィギュレーションサブモードを開始します。
show ip arp inspection	特定の範囲の VLAN について DAI のステータスを表示します。

ip auth-proxy max-login-attempts

ファイアウォール インターフェイスでログインの試行回数を制限するには、**ip auth-proxy max-login-attempts** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip auth-proxy max-login-attempts *l-maxint*

no ip auth-proxy max-login-attempts

シンタックスの説明

l-maxint 最大ログイン試行回数。有効値は 1 ～ 2147483647 です。

コマンドのデフォルト

l-maxint は 5 です。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、ファイアウォール インターフェイスだけでサポートされています。

最大ログイン試行回数の機能は、ウォッチ リスト機能には無関係です。(**ip access-list hardware permit fragments** コマンドを使用して) ウォッチ リストを設定せずに、最大ログイン試行回数を設定すると、既存の認証プロキシ動作が行われますが、再試行回数には新しい数値が表示されます。ウォッチ リストを設定すると、設定された試行回数に達したときに、ウォッチ リストに IP アドレスが追加されます。

例

次に、ファイアウォール インターフェイスでログイン試行回数に制限を設定する例を示します。

```
Router(config-if)# ip auth-proxy max-login-attempts 4
Router(config-if)#
```

関連コマンド

コマンド	説明
clear ip auth-proxy watch-list	1 つのウォッチ リスト エントリまたはすべてのウォッチ リスト エントリを削除します。
ip auth-proxy watch-list	認証プロキシ ウォッチ リストをイネーブルにして設定します。
show ip auth-proxy watch-list	認証プロキシ ウォッチ リストに関する情報を表示します。

ip auth-proxy watch-list

認証プロキシ ウォッチ リストをイネーブルにして設定するには、**ip auth-proxy watch-list** コマンドを使用します。このコマンドの **no** 形式の使用法については、「使用上のガイドライン」を参照してください。

```
ip auth-proxy watch-list {{add-item ip-addr} | enable | {expiry-time minutes}}
```

```
no ip auth-proxy watch-list [{add-item ip-addr} | expiry-time]
```

シンタックスの説明

add-item ip-addr	ウォッチ リストに IP アドレスを追加します。
enable	ウォッチ リストをイネーブルにします。
expiry-time minutes	エントリがウォッチ リスト内に保持される期間を指定します。有効値については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- *minutes* は 30 分です。
- ウォッチ リスト機能はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

minutes の有効値は、0 から最大 32 ビットの正数 (0x7FFFFFFF または 10 進数 2147483647) です。*minutes* を 0 (ゼロ) に設定すると、リストのエントリは永続的になります。

このコマンドは、ファイアウォール インターフェイスだけでサポートされています。

このコマンドの **no** 形式は、次の場合に使用します。

- **no ip auth-proxy watch-list** : ウォッチ リスト機能をディセーブルにします。
- **no ip auth-proxy watch-list add-item ip-addr** : ウォッチ リストから IP アドレスを削除します。
- **no ip auth-proxy watch-list expiry-time** : デフォルト設定に戻します。

ウォッチ リストは、ポート 80 への TCP 接続を開き、データをまだ送信していない IP アドレスで構成されます。このタイプの IP アドレスから (ポート 80 への) 新しい接続は受け入れられず、パケットは廃棄されます。

エントリは、**expiry-time minutes** で指定された期間ウォッチ リストに保持されます。

ウォッチ リストをディセーブルにすると、新しいエントリはウォッチ リストに追加されませんが、セッションは SERVICE_DENIED ステートになります。タイマーは、2 分後にセッションを削除します。

例

次に、認証プロキシ ウォッチ リストをイネーブルにする例を示します。

```
Router(config-if)# ip auth-proxy watch-list enable
Router(config-if)#
```

次に、認証プロキシ ウォッチ リストをディセーブルにする例を示します。

```
Router(config-if)# no ip auth-proxy watch-list
Router(config-if)#
```

次に、ウォッチ リストに IP アドレスを追加する例を示します。

```
Router(config-if)# ip auth-proxy watch-list add-item 12.0.0.2
Router(config-if)#
```

次に、エントリがウォッチ リスト内に保持される期間を設定する例を示します。

```
Router(config-if)# ip auth-proxy watch-list expiry-time 29
Router(config-if)#
```

関連コマンド

コマンド	説明
clear ip auth-proxy watch-list	1 つのウォッチ リスト エントリまたはすべてのウォッチ リスト エントリを削除します。
ip auth-proxy max-login-attempts	ファイアウォール インターフェイスでログインの試行回数を制限します。
show ip auth-proxy watch-list	認証プロキシ ウォッチ リストに関する情報を表示します。

ip casa

フォワーディング エージェントとして機能するようにルータを設定するには、**ip casa** コマンドを使用します。フォワーディング エージェントをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip casa [*control-address igmp-address* [*udp-limit*]]

no ip casa

シンタックスの説明	
<i>control-address</i>	(任意) サービス マネージャのフォワーディング エージェント側および信号の送信用に使用されるフォワーディング エージェント トンネルの IP アドレス。
<i>igmp-address</i>	フォワーディング エージェントがワイルドカードおよび固定のアフィニティを待ち受ける IGMP アドレス。
<i>udp-limit</i>	(任意) UDP キューの最大の長さ。有効値は 50 ~ 65,535 です。

コマンドのデフォルト デフォルトの *udp-limit* 値は、256 です。

コマンド モード グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン *udp-limit* の最大値を超える値がバースト状態で到着すると、サービス マネージャからの Cisco Appliance Services Architecture (CASA) ワイルドカードのアップデートがドロップされる可能性があります。

control-address の値は、各フォワーディング エージェントで一意です。

例 次に、フォワーディング エージェントに IP アドレス (10.10.4.1) と IGMP アドレス (224.0.1.2) を指定して、UDP キューの長さを 300 に設定する例を示します。

```
Router(config)# ip-casa 10.10.4.1 224.0.1.2 300
Router(config)#
```

関連コマンド	コマンド	説明
	forwarding-agent	フォワーディング エージェントがワイルドカードおよび固定のアフィニティを待ち受けるポートを指定します。

ip cef load-sharing algorithm

CEF ロードバランス アルゴリズムを選択するには、**ip cef load-sharing algorithm** コマンドを使用します。デフォルトのユニバーサル ロードバランス アルゴリズムに戻るには、このコマンドの **no** 形式を使用します。

ip cef load-sharing algorithm {original | tunnel [*id*] | universal [*id*]}

no ip cef load-sharing algorithm {original | tunnel [*id*] | universal [*id*]}

シンタックスの説明

original	送信元および宛先のハッシュに基づいて、ロードバランス アルゴリズムをオリジナルに設定します。
tunnel	トンネル環境、または IP 送信元アドレスと宛先アドレスのペアが少ない環境で使用するロードバランス アルゴリズムを設定します。
universal	送信元ハッシュ、宛先ハッシュ、ID ハッシュを使用するユニバーサル アルゴリズムに、ロードバランス アルゴリズムを設定します。
<i>id</i>	(任意) 固定 ID

コマンドのデフォルト

ユニバーサル ロードバランスが選択されています。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

オリジナルの CEF ロードシェアリング アルゴリズムでは、すべてのルータで同じアルゴリズムを使用するため、複数のルータ間でロードバランスのゆがみが発生します。ロードバランス アルゴリズムをユニバーサル モードに設定すると、ネットワークのそれぞれのルータは、送信元アドレスと宛先アドレスのペアごとに別々のロードバランス決定を下すことができるようになり、ロードバランスのゆがみが解消します。

関連する送信元アドレスと宛先アドレスのペアが少ない場合は、より公平に負荷を共有するため、トンネル アルゴリズムを使用します。

例

次に、ユニバーサル環境用に CEF ロードバランス アルゴリズムをイネーブルにする例を示します。

```
Router(config)# ip cef load-sharing algorithm universal 1
Router(config)#
```

関連コマンド

コマンド	説明
ip load-sharing	ロード バランスをイネーブルにします。

ip cef table consistency-check

CEF テーブル一貫性チェッカーのタイプおよびパラメータをイネーブルにするには、**ip cef table consistency-check** コマンドを使用します。一貫性チェッカーをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ip cef table consistency-check [type {lc-detect | scan-lc | scan-rib | scan-rp}] [count
count-number] [period seconds]
```

```
ip cef table consistency-check [settle-time seconds]
```

```
no ip cef table consistency-check [type {lc-detect | scan-lc | scan-rib | scan-rp}] [count
count-number] [period seconds]
```

```
no ip cef table consistency-check [settle-time seconds]
```

シンタックスの説明

type	(任意) 設定する一貫性チェックのタイプを指定します。
lc-detect	(任意) モジュールが不明のプレフィクスを検出するように指定します。
scan-lc	(任意) モジュールにテーブルのパッシブ スキャン チェックを指定します。
scan-rib	(任意) ランデブー ポイントに、routing information base (RIB) を対象にしたテーブルのパッシブ スキャン チェックを指定します。
scan-rp	(任意) ランデブー ポイントにテーブルのパッシブ スキャン チェックを指定します。
count count-number	(任意) 各スキャンでチェックする最大プレフィクス数を指定します。有効値は 1 ~ 225 です。
period seconds	(任意) スキャン間隔を指定します。有効値は 30 ~ 3600 秒です。
settle-time seconds	(任意) 候補のプレフィクスの更新が不一致として無視される経過時間を指定します。有効値は、1 ~ 3600 秒です。

コマンドのデフォルト

イネーブル

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、CEF テーブル一貫性チェッカーおよびパラメータを表 2-12 に一覧表示される検出メカニズム タイプに設定します。

表 2-12 検出メカニズム タイプ

メカニズム	動作環境	説明
Lc-detect	モジュール	モジュール上で動作し、FIB テーブルで不明であると検出された IP プレフィックスを検索します。IP プレフィックスが不明の場合、モジュールはこのアドレスの packets を転送できません。Lc-detect は、確認のためランデブー ポイントに IP プレフィックスを送信します。ランデブー ポイントで関連するエントリが検出されると、不一致が検出され、システム メッセージが表示されます。また、IP プレフィックスが不一致であることを確認するためにランデブー ポイントはモジュールに信号を戻します。
Scan-lc	モジュール	モジュール上で動作し、FIB テーブルを設定可能な時間内で検索してランデブー ポイントに次の n 個のプレフィックスを送信します。ランデブー ポイントは、完全一致検索を実行します。ランデブー ポイントがプレフィックスを不明と判断した場合、ランデブー ポイントは不一致をレポートします。最後に、ランデブー ポイントが確認のためにモジュールに信号を戻します。
Scan-rp	ルート プロセッサ	ランデブー ポイント上で動作し (scan-lc の逆)、FIB テーブルを設定可能な時間内で検索して次の n 個のプレフィックスをモジュールに送信します。モジュールは、完全一致検索を実行します。モジュールがプレフィックスを不明と判断した場合、モジュールは不一致をレポートし、最終的に確認のためランデブー ポイントに信号を戻します。
Scan-rib	ルート プロセッサ	すべての RP 上で動作し (割り当てられていない場合でも)、RIB をスキャンしてプレフィックス エントリがランデブー ポイント FIB テーブルに存在することを確認します。

例

次に、CEF テーブル一貫性チェッカーをイネーブルにする例を示します。

```
Router(config)# ip cef table consistency-check
Router(config)#
```

関連コマンド

コマンド	説明
<code>clear ip cef inconsistency</code>	CEF 一貫性チェッカーの統計情報および記録情報をクリアします。
<code>show ip cef inconsistency</code>	IP CEF の不一致を表示します。

ip dhcp relay information option trust-all

DHCP のリレー エージェント情報オプションの信頼できる送信元としてすべてのインターフェイスをイネーブルにするには、**ip dhcp relay information option trust-all** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip dhcp relay information option trust-all

no ip dhcp relay information option trust-all

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト DHCP サーバはリレー情報を書き込みません。

コマンド モード グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドは、ケーブル アクセス ルータの終端システムで使用されます。この機能を使用すると、DHCP サーバは要求を送信するユーザ（ケーブル アクセス ルータ）を識別し、この要求に基づいて適切な処理を行うことができます。

例 次に、ルータ上のすべてのインターフェイスを信頼するよう指定する例を示します。

```
Router(config)# ip dhcp relay information option trust-all
Router(config)#
```

関連コマンド	コマンド	説明
	show ip dhcp relay information trusted-sources	設定済みの信頼されるインターフェイスをすべて一覧表示します。

ip dhcp relay information trust

DHCP のリレー エージェント情報の信頼できる送信元として単一のインターフェイスをイネーブルにするには、**ip dhcp relay information trust** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip dhcp relay information trust

no ip dhcp relay information trust

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

ルータ上のインターフェイスはすべて信頼されていません。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

リレー エージェント情報の信頼できる送信元としてインターフェイスを設定すると、インターフェイスは DHCP 検出パケットまたは要求パケットを受信できます。DHCP 検出パケットまたは要求パケットには、リレー エージェント情報オプションが含まれます。

例

次に、インターフェイスを信頼するよう指定する例を示します。

```
Router(config)# ip dhcp relay information trust
Router(config)#
```

関連コマンド

コマンド	説明
show ip dhcp relay information trusted-sources	設定済みの信頼されるインターフェイスをすべて一覧表示します。

ip dhcp route connected

接続ルートとしてルートを指定するには、**ip dhcp route connected** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip dhcp route connected

no ip dhcp route connected

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト ルータ上のインターフェイスはすべて信頼されていません。

コマンド モード グローバル コンフィギュレーション (config) (config)

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン **ip dhcp route connected** コマンドをイネーブルにすると、DHCP はデータベース エージェントからルート データベースをダウンロードし、スタティック ルートとして以前追加されていた可能性があるルートを接続ルートとして追加します。

例 次に、接続ルートとしてルートを指定する例を示します。

```
Router(config)# ip dhcp route connected
Router(config)#
```

ip dhcp snooping

DHCP スヌーピングをグローバルにイネーブルにするには、**ip dhcp snooping** コマンドを使用します。DHCP スヌーピングをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp snooping

no ip dhcp snooping

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

DHCP スヌーピング データベースに対応するエントリがある場合にだけ、無線クライアント（モバイル ノード）は信頼できない無線ネットワークにアクセスします。DHCP スヌーピングをグローバルにイネーブルにするには、**ip dhcp snooping** コマンドを入力し、トンネル インターフェイスの DHCP スヌーピングをイネーブルにするには、**ip dhcp snooping packets** コマンドを入力します。DHCP スヌーピングをイネーブルにしたあとで、プロセスはモバイル ノードで送受信される DHCP パケットをスヌーピングし、DHCP スヌーピング データベースにデータを入力します。

例

次に、DHCP スヌーピングをイネーブルにする例を示します。

```
Router(config) # ip dhcp snooping
Router(config) #
```

次に、DHCP スヌーピングをディセーブルにする例を示します。

```
Router(config) # no ip dhcp snooping
Router(config) #
```

関連コマンド

コマンド	説明
ip dhcp snooping packets	トンネル インターフェイス上で DHCP スヌーピングをイネーブルにします。
show ip dhcp snooping	DHCP スヌーピングの設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピングのバインディング エントリを表示します。
show ip dhcp snooping database	DHCP スヌーピング データベース エージェントのステータスを表示します。

ip dhcp snooping binding

DHCP バインディングの設定を確立および生成して、再起動後にバインディングを復元するには、**ip dhcp snooping binding** コマンドを使用します。バインディング設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ip dhcp snooping binding mac-address {vlan vlan} ip-address {interface interface
interface-number} {expiry seconds}
```

```
no ip dhcp snooping binding mac-address vlan vlan-# ip-address interface interface
```

シンタックスの説明	
<i>mac-address</i>	MAC アドレス
vlan <i>vlan</i>	有効な VLAN 番号を指定します。有効値は 1 ~ 4094 です。
<i>ip-address</i>	IP アドレス
interface <i>interface</i>	インターフェイス タイプを指定します。有効値は ethernet 、 fastethernet 、 gigabitethernet 、および tengigabitethernet です。
<i>interface-number</i>	モジュールおよびポート番号
expiry <i>seconds</i>	バインディングが無効になってからのインターバルを指定します。有効値は 1 ~ 4,294,967,295 秒です。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード 特権 EXEC (#)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドを使用してバインディングを追加または削除すると、バインディング データベースは変更済みとマークされ、書き込みが開始されます。

DHCP スヌーピング データベースでは、最大 512 のバインディングが許可されます。

例 次に、VLAN 1 のインターフェイス **gigabitethernet1/1** で期限切れ時間が 1000 秒の DHCP バインディング設定を生成する例を示します。

```
Router# ip dhcp snooping binding 0000.0c00.40af vlan 1 10.42.0.6 interface gi1/1 expiry 1000
Router#
```

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピングの設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピングのバインディング エントリを表示します。
show ip dhcp snooping database	DHCP スヌーピング データベース エージェントのステータスを表示します。

ip dhcp snooping database

DHCP スヌーピング データベースを設定するには、**ip dhcp snooping database** コマンドを使用します。

```
ip dhcp snooping database {bootflash:url | ftp:url | rcp:url | scp:url | sup-bootflash: | tftp:url}
```

```
ip dhcp snooping database {timeout timeout | write-delay time}
```

シンタックスの説明	
bootflash:url	ブートフラッシュを使用して、エントリを格納するためのデータベースの URL を指定します。
ftp:url	FTP を使用して、エントリを格納するためのデータベースの URL を指定します。
rcp:url	Remote Copy Protocol (RCP) を使用して、エントリを格納するためのデータベースの URL を指定します。
scp:url	Switch-Module Configuration Protocol or Serial Control Protocol (SCP) を使用して、エントリを格納するためのデータベースの URL を指定します。
sup-bootflash:	スーパーバイザ エンジンのブートフラッシュを使用して、エントリ格納用のデータベースの URL を指定します。
tftp:url	TFTP を使用して、エントリを格納するためのデータベースの URL を指定します。
timeout <i>timeout</i>	中断タイムアウト インターバルを指定します。有効値は 0 ~ 86,400 秒です。
write-delay <i>time</i>	ローカル DHCP スヌーピング データベースにデータが追加されてから、DHCP スヌーピング エントリを外部サーバに書き込みするまでの時間を指定します。有効値は 15 ~ 86,400 秒です。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドを入力する前に、インターフェイス上で DHCP スヌーピングをイネーブルにする必要があります。DHCP スヌーピングをイネーブルにするには、**ip dhcp snooping** コマンドを使用します。

例 次に、TFTP を使用してデータベースの URL を指定する例を示します。

```
Router(config)# ip dhcp snooping database tftp://90.90.90.90/snooping-rp2
Router(config)#
```

次に、DHCP スヌーピング エントリを外部サーバに書き込むまでの時間を指定する例を示します。

```
Router(config)# ip dhcp snooping database write-delay 15
```

■ ip dhcp snooping database

```
Router(config)#
```

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピングの設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピングのバインディング エントリを表示します。
show ip dhcp snooping database	DHCP スヌーピング データベース エージェントのステータスを表示します。

ip dhcp snooping information option

DHCP option 82 データ挿入をイネーブルにするには、**ip dhcp snooping information option** コマンドを使用します。DHCP option 82 データ挿入をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp snooping information option [allow-untrusted]

no ip dhcp snooping information option

シンタックスの説明	allow-untrusted	(任意) option 82 情報を含む着信 DHCP スヌーピング パケットをスイッチがエッジ スイッチから受信できるようにします。
------------------	------------------------	---

コマンドのデフォルト デフォルト設定は次のとおりです。

- **ip dhcp snooping information option** : イネーブル
- **ip dhcp snooping information option allow-untrusted** : ディセーブル

コマンド モード グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン DHCP option 82 は、RFC 3046 の一部です。DHCP はアプリケーション層プロトコルであり、Transmission Control Protocol/Internet Protocol (TCP/IP) ネットワークの動的構成に使用されます。このプロトコルにより、リレー エージェントは、DHCP クライアントと DHCP サーバの間で DHCP メッセージを渡すことが可能になります。リレー エージェントを使用すると、クライアントと同じネットワーク上にサーバを配置する必要がなくなります。セキュリティおよびスケーラビリティの問題には option 82 (82 はこのオプションのコード) で対処します。転送クライアントが発信した DHCP パケットがサーバに送信されるとき、option 82 はリレー エージェントに常駐します。option 82 を認識するサーバはこの情報を使用し、IP アドレスまたはその他のパラメータ割り当てポリシーを実装できます。DHCP サーバは、その応答でオプションをリレー エージェントにエコーします。リレー エージェントは、リレー エージェントからオプションを取り出してからクライアントにリレーを転送します。

信頼されていないインターフェイスでエッジ スイッチに接続している集約スイッチで **ip dhcp snooping information option allow-untrusted** を入力すると、集約スイッチは、option 82 情報を含むパケットをエッジ スイッチから受け取ります。集約スイッチは、信頼されていないスイッチ インターフェイスで接続しているホストのバインディングを学習します。ホストが接続されている、信頼されていない入力インターフェイスで option 82 情報を含むパケットをスイッチが受信する間は、ダイナミック ARP インスペクションや IP ソース ガードなどの DHCP セキュリティ機能を集約スイッチでイネーブルにできます。集約スイッチに接続するエッジ スイッチのポートは、信頼されているインターフェイスとして設定する必要があります。

**注意**

信頼されていないデバイスに接続している集約スイッチでは、**ip dhcp snooping information option allow-untrusted** コマンドを入力しないでください。このコマンドを入力すると、信頼されていないデバイスが option 82 情報をスプーフィングする可能性があります。

例

次に、DHCP option 82 データ挿入をイネーブルにする例を示します。

```
Router(config)# ip dhcp snooping information option
Router(config)#
```

次に、DHCP option 82 データ挿入をディセーブルにする例を示します。

```
Router(config)# no ip dhcp snooping information option
Router(config)#
```

次に、option 82 情報を含む着信 DHCP スヌーピング パケットをスイッチがエッジ スイッチから受信できるようにする例を示します。

```
Router(config)# ip dhcp snooping information option allow-trusted
Router(config)#
```

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピングの設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピングのバインディング エントリを表示します。
show ip dhcp snooping database	DHCP スヌーピング データベース エージェントのステータスを表示します。

ip dhcp snooping limit rate

インターフェイスが秒単位で受信できる DHCP メッセージ数を設定するには、**ip dhcp snooping limit rate** コマンドを使用します。DHCP メッセージ レートの制限をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp snooping limit rate rate

no ip dhcp snooping limit rate

シンタックスの説明	<i>rate</i> スイッチが秒単位で受信できる DHCP メッセージ数。有効値は 1 ～ 4,294,967,294 秒です。
------------------	--

コマンドのデフォルト	ディセーブル
-------------------	--------

コマンド モード	インターフェイス コンフィギュレーション (config-if)
-----------------	----------------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドは、レイヤ 2 スイッチポートおよびポートチャネル インターフェイスだけでサポートされます。

通常、レート制限は信頼できないインターフェイスに適用されます。信頼できるインターフェイスにレート制限を設定する場合、信頼できるインターフェイスはスイッチのすべての DHCP トラフィックを集約するため、インターフェイスのレート制限をより高い値に調整する必要があります。

例 次に、スイッチが秒単位で受信できる DHCP メッセージ数を指定する例を示します。

```
Router(config-if)# ip dhcp snooping limit rate 150
Router(config)#
```

次に、DHCP メッセージのレート制限をディセーブルにする例を示します。

```
Router(config-if)# no ip dhcp snooping limit rate
Router(config)#
```

関連コマンド	コマンド	説明
	show ip dhcp snooping	DHCP スヌーピングの設定を表示します。
	show ip dhcp snooping binding	DHCP スヌーピングのバインディング エントリを表示します。
	show ip dhcp snooping database	DHCP スヌーピング データベース エージェントのステータスを表示します。

ip dhcp snooping packets

トンネル インターフェイス上で DHCP スヌーピングをイネーブルにするには、**ip dhcp snooping packets** コマンドを使用します。DHCP スヌーピングをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp snooping packets

no ip dhcp snooping packets

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、レイヤ 2 スイッチポートおよびポートチャネル インターフェイスだけでサポートされます。

このコマンドは、Wireless LAN Services Module (WLSM) が搭載された Catalyst 6500 シリーズ スイッチだけでサポートされます。

DHCP スヌーピング データベースに対応するエントリがある場合にだけ、無線クライアント (モバイル ノード) は信頼できない無線ネットワークにアクセスします。DHCP スヌーピングをグローバルにイネーブルにするには、**ip dhcp snooping** コマンドを入力し、トンネル インターフェイスの DHCP スヌーピングをイネーブルにするには、**ip dhcp snooping packets** コマンドを入力します。DHCP スヌーピングをイネーブルにしたあとで、プロセスはモバイル ノードで送受信される DHCP パケットをスヌーピングし、DHCP スヌーピング データベースにデータを入力します。

例

次に、DHCP スヌーピングをイネーブルにする例を示します。

```
Router(config)# ip dhcp snooping packets
Router(config)#
```

次に、DHCP スヌーピングをディセーブルにする例を示します。

```
Router(config)# no ip dhcp snooping packets
Router(config)#
```

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピングの設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピングのバインディング エントリを表示します。
show ip dhcp snooping database	DHCP スヌーピング データベース エージェントのステータスを表示します。

ip dhcp snooping verify mac-address

DHCP パケットの送信元 MAC アドレスが、信頼できないポート上のクライアントのハードウェア アドレスに一致することを確認するには、**ip dhcp snooping verify mac-address** コマンドを使用します。確認をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

イネーブル

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

信頼できない DHCP スヌーピング ポートの場合、DHCP スヌーピングではクライアントのハードウェア アドレス フィールドの MAC アドレスを確認して、クライアントが単一の MAC アドレスから複数のアドレスを要求していることを確認します。ポートを信頼する場合は、**ip dhcp snooping verify mac-address** コマンドを使用します。または、クライアントのハードウェア アドレス フィールドでの MAC アドレス確認をディセーブルにしてポートを信頼できない状態にしておく場合は、**no ip dhcp snooping verify mac-address** コマンドを使用します。

例

次に、信頼できないポート上で DHCP パケットの送信元 MAC アドレスがクライアントのハードウェア アドレスに一致することを確認する例を示します。

```
Router(config)# ip dhcp snooping verify mac-address
Router(config)#
```

次に、クライアントのハードウェア アドレス フィールドの MAC アドレスの確認をオフにする例を示します。

```
Router(config)# no ip dhcp snooping verify mac-address
Router(config)#
```

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピングの設定を表示します。

コマンド	説明
<code>show ip dhcp snooping binding</code>	DHCP スヌーピングのバインディング エントリを表示します。
<code>show ip dhcp snooping database</code>	DHCP スヌーピング データベース エージェントのステータスを表示します。

ip dhcp snooping vlan

VLAN または VLAN のグループで DHCP スヌーピングをイネーブルにするには、**ip dhcp snooping vlan** コマンドを使用します。VLAN または VLAN のグループで DHCP スヌーピングをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp snooping vlan {number | vlanlist}

no ip dhcp snooping vlan {number | vlanlist}

シンタックスの説明

<i>number</i> <i>vlanlist</i>	VLAN 番号または VLAN のグループを指定します。有効値は、1 ~ 4094 です。詳細については、「使用上のガイドライン」を参照してください。
------------------------------------	---

コマンドのデフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

グローバル スヌーピングと VLAN スヌーピングの両方がイネーブルになっている場合だけ、DHCP スヌーピングが VLAN でイネーブルになります。

VLAN の範囲を指定するには、1,3-5,7,9-11 のように入力します。

例

次に、VLAN 上で DHCP スヌーピングをイネーブルにする例を示します。

```
Router(config)# ip dhcp snooping vlan 10
Router(config)#
```

次に、VLAN 上で DHCP スヌーピングをディセーブルにする例を示します。

```
Router(config)# no ip dhcp snooping vlan 10
Router(config)#
```

次に、VLAN のグループで DHCP スヌーピングをイネーブルにする例を示します。

```
Router(config)# ip dhcp snooping vlan 10,4-8,55
Router(config)#
```

次に、VLAN のグループで DHCP スヌーピングをディセーブルにする例を示します。

```
Router(config)# no ip dhcp snooping vlan 10,4-8,55
Router(config)#
```

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピングの設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピングのバインディング エントリを表示します。
show ip dhcp snooping database	DHCP スヌーピング データベース エージェントのステータスを表示します。

ip flow-aggregation cache

フロー集約キャッシュを作成し、集約キャッシュ コンフィギュレーション モードを開始するには、**ipflow-aggregation cache** コマンドを使用します。このコマンドを無効にするか、デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
ip flow-aggregation cache {as | destination-prefix | prefix | protocol-port |
source-prefix}
```

```
no ip flow-aggregation cache {as | destination-prefix | prefix | protocol-port |
source-prefix}
```

シンタックスの説明

as	Autonomous-System (AS; 自律システム) 集約キャッシュ方式を設定します。
destination-prefix	宛先プレフィクス集約キャッシュ方式を設定します。
prefix	プレフィクス集約キャッシュ方式を設定します。
protocol-port	プロトコル ポート集約キャッシュ方式を設定します。
source-prefix	送信元プレフィクス集約キャッシュ方式を設定します。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- **entries num** は 4096 エントリです。
- **active time** は 30 分です。
- **inactive time** は 15 秒です。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

送信元プレフィクス集約モードでは、送信元マスクだけが設定可能です。宛先プレフィクス集約モードでは、宛先マスクだけが設定可能です。

フロー集約キャッシュ コンフィギュレーション モードを開始すると、次のコマンドが使用できます。

- **cache {entries num} | {timeout {active time} | {inactive time}}**
- **default {cache {entries | timeout}} | enabled | {export destination}**
- **enabled**
- **export destination ip-addr udp-port-num**

構文は次のとおりです。

cache	NetFlow キャッシュ パラメータを設定します。
entries num	フロー キャッシュのエントリ数を指定します。有効値は、1024 ~ 524,288 です。
timeout	フロー キャッシュのタイムアウト パラメータを指定します。
active time	アクティブ フロー タイムアウトを指定します。有効値は、1 ~ 60 分です。
inactive time	非アクティブ フロー タイムアウトを指定します。有効値は、10 ~ 600 秒です。
default	コマンドをデフォルトに設定します。
enabled	集約キャッシュをイネーブルにします。
export destination	フロー統計情報を送信するホストまたはポートを指定します。
<i>ip-addr</i>	宛先 IP アドレスまたはホスト名。
<i>udp-port-num</i>	UDP ポート番号。有効値は 1 ~ 65,535 です。

例

次に、AS 集約キャッシュ方式をイネーブルにする例を示します。

```
Router(config)# ip flow-aggregation cache as
Router(config-flow-cache)# enable
Router(config-flow-cache)#
```

関連コマンド

コマンド	説明
show ip cache flow	NetFlow キャッシュ フロー エントリのサマリーを表示します。

ip flow-cache entries

NetFlow キャッシュに維持するエン트리数を変更するには、**ip flow-cache entries** コマンドを使用します。デフォルトのエン트리数に戻すには、このコマンドの **no** 形式を使用します。

ip flow-cache entries *number*

no ip flow-cache entries

シンタックスの説明

<i>number</i>	NetFlow キャッシュに維持するエン트리数。エントリの有効値は、1024 ~ 524288 です。
---------------	---

コマンドのデフォルト

65536 エントリー

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

通常は、NetFlow キャッシュはデフォルトのサイズで十分です。ただし、フロー トラフィック レートの必要性に応じて、キャッシュ内に維持するエントリを増減できます。多量のフロー トラフィックがある環境（インターネット コア ルータなど）では、131,072 などの大きな値を設定することを推奨します。フロー トラフィックに関する情報を入手するには、**show ip cache flow** コマンドを使用してください。

各キャッシュ エントリの記憶容量は、約 64 バイトです。デフォルトのエントリ数を持つキャッシュの場合、約 4 MB の dynamic RAM (DRAM) が必要です。フリー フローのキューから新規フローが取り出されるたびに、フリー フローの数がチェックされます。フリー フローの数が残り少なくなると、NetFlow は、タイムアウトを短縮し、30 個のフローをエージングしようとします。フリー フローが残り 1 個になった場合、NetFlow は、エージにかかわらず 30 個のフローを自動的にエージングします。これにより、フリー フロー エントリは常に使用できます。



注意

NetFlow のキャッシュ エントリ数は変更しないことを推奨します。この機能を誤って使用すると、ネットワークに問題が生じる可能性があります。NetFlow キャッシュ エントリ数をデフォルトに戻すには、**no ip flow-cache entries** コマンドを使用します。

例

次に、NetFlow キャッシュのエントリ数を 131,072 に増やす例を示します。

```
Router(config)# ip flow-cache entries 131072
Router(config)# exit
```

関連コマンド

コマンド	説明
show ip cache flow	NetFlow キャッシュ フロー エントリのサマリーを表示します。

ip flow-export

ハードウェアでスイッチングされるフローの NDE をグローバルにイネーブルにするには、**ip flow-export** コマンドを使用します。ハードウェアでスイッチングされるフローの NDE をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip flow-export

no ip flow-export

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- ディセーブル
- バージョン 7

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

デフォルトの NDE バージョンを変更するには、**ip flow-export hardware version** コマンドを使用します。

例

次に、ハードウェアでスイッチングされるフローの NDE をイネーブルにする例を示します。

```
Router(config)# ip flow-export
Router(config)#
```

次に、ハードウェアでスイッチングされるフローの NDE をディセーブルにする例を示します。

```
Router(config)# no ip flow-export
Router(config)#
```

関連コマンド

コマンド	説明
ip flow-export hardware version	ハードウェアでスイッチングされるフローの NDE バージョンを指定します。
show mls nde	NDE ハードウェアによってスイッチングされるフローに関する情報を表示します。

ip flow-export destination

NetFlow キャッシュ エントリを特定の宛先にエクスポートするには、**ip flow-export destination** コマンドを使用します。情報のエクスポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip flow-export destination {hostname | ip-address} udp-port

no ip flow-export destination

シンタックスの説明	
hostname	NetFlow 情報をエクスポートするワークステーションの IP ホスト名
ip-address	NetFlow 情報をエクスポートするワークステーションの IP アドレス
udp-port	UDP プロトコル専用のポート番号

コマンドのデフォルト ディセーブル

コマンド モード グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン 2 つの宛先 IP アドレスを入力して、冗長データ ストリームを提供することによりすべての NetFlow データを受信する確率を向上できます。

ルータに複数の NetFlow エクスポートの宛先を設定するには、**ip flow-export destination** コマンドを各宛先に 1 回ずつ、合計 2 回入力します。同じ IP アドレスを 2 回入力しないでください。ただし、同じ UDP ポート番号を持つ 2 つの異なる IP アドレスを入力することは可能です。

NetFlow キャッシュ エントリには、多くの情報が含まれます。フロー スイッチングが、**ip route-cache flow** コマンドでイネーブルにされている場合 **ip flow-export destination** コマンドを使用して、フローが期限切れになったときにフロー キャッシュ エントリをワークステーションにエクスポートするようにルータを設定できます。この機能は、たとえば統計情報、課金、およびセキュリティなどに有効です。

ip-address 値を入力する場合、次の注意事項に従ってください。

- 現在使用中のインターフェイスの IP アドレスを入力することはできません。未使用のインターフェイスによるサブネットからアドレスを使用する必要があります。
- ループバック インターフェイスからアドレスを使用することはできません。ループバック インターフェイスには内部 VLAN ID または MAC アドレスがありません。

データの送信元 IP アドレスを指定するには、**ip flow-export source** コマンドを使用します。NetFlow データを受信するワークステーションで使用されるバージョンを指定するには、**ip flow-export version** コマンドを使用します。

NDE の詳細については、『Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY』の「Configuring NDE」の章を参照してください。

■ ip flow-export destination

例

次に、IP アドレス 10.42.42.1 99917 のワークステーション上でバージョン 1 形式を使用して NetFlow キャッシュ エントリを UDP ポート 125 にエクスポートする例を示します。

```
Router# configure terminal
Router(config)# ip flow-export destination 10.42.42.1 9991 125
Router(config)# exit
```

関連コマンド

コマンド	説明
ip flow-export source	NDE データグラムで使用する送信元インターフェイス IP アドレスを指定します。
ip flow-export version	NetFlow キャッシュ エントリにおける情報のエクスポートのバージョンを指定します。
ip route-cache flow	IP ルーティングの NetFlow スイッチングをイネーブルにします。

ip flow-export hardware version

ハードウェアでスイッチングされるフローの NDE バージョンを指定するには、**ip flow-export hardware version** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip flow-export hardware version [5 | 7]

no ip flow-export hardware version

シンタックスの説明	5	7
	エクスポート パケットがバージョン 5 形式を使用するように指定します。詳細については、「使用上のガイドライン」を参照してください。	エクスポート パケットがバージョン 7 形式を使用するように指定します。詳細については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト バージョン 7

コマンドモード グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、ハードウェアでスイッチングされるフローの NDE バージョンを指定する例を示します。

```
Router(config)# ip flow-export hardware version 5
Router(config)#
```

関連コマンド	コマンド	説明
	ip flow-export interface	ハードウェアでスイッチングされるフローのインターフェイス ベースの入力 NDE をイネーブルにします。
	show mls nde	NDE ハードウェアによってスイッチングされるフローに関する情報を表示します。

ip flow-export interface

ハードウェアでスイッチングされるフローのインターフェイス ベースの入力 NDE をイネーブルにするには、**ip flow-export interface** コマンドを使用します。ハードウェアでスイッチングされるフローのインターフェイス ベースの NDE をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip flow-export interface

no ip flow-export interface

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

特定のインターフェイス上の NDE をイネーブルまたはディセーブルにするには、**ip flow-export interface** コマンドとともに、**ip flow ingress** コマンドを使用します。

例

次に、ハードウェアでスイッチングされるフローのインターフェイス ベースの NDE をイネーブルにする例を示します。

```
Router(config)# ip flow-export interface
Router(config)#
```

次に、ハードウェアでスイッチングされるフローのインターフェイス ベースの NDE をディセーブルにする例を示します。

```
Router(config)# no ip flow-export interface
Router(config)#
```

関連コマンド

コマンド	説明
ip flow-export hardware version	ハードウェアでスイッチングされるフローの NDE バージョンを指定します。
show ip flow-export	ハードウェア スイッチングおよびソフトウェア スイッチングされるデータ エクスポートのフローに関する情報 (メイン キャッシュや他のすべてのイネーブル化されたキャッシュなど) を表示します。
show mls nde	NDE ハードウェアによってスイッチングされるフローに関する情報を表示します。

ip flow-export source

NDE データグラムで使用される送信元インターフェイスの IP アドレスを指定するには、**ip flow-export source** コマンドを使用します。送信元アドレスを削除するには、このコマンドの **no** 形式を使用します。

```
ip flow-export source [{interface interface-number} | {null interface-number} |
{port-channel number} | {vlan vlan-id}]
```

```
no ip flow-export source [{interface interface-number} | {null interface-number} |
{port-channel number} | {vlan vlan-id}]
```

シンタックスの説明

<i>interface</i>	(任意) インターフェイス タイプ。有効値は、 ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 ge-wan 、および atm です。
<i>interface-number</i>	(任意) モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
null interface-number	(任意) スル インターフェイスを指定します。有効値は 0 です。
port-channel number	(任意) チャネル インターフェイスを指定します。有効値は 1 ~ 256 の範囲の最大 64 個の値です。
vlan vlan-id	(任意) VLAN を指定します。有効値は 1 ~ 4094 です。

コマンドのデフォルト

送信元インターフェイスは指定されていません。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

interface-number 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビットイーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

NDE を設定したあと、エクスポート データを含む UDP データグラムで使用される送信元インターフェイスを指定できます。ワークステーションの NetFlow Collector は、送信元インターフェイスの IP アドレスを使用してどのルータが情報を送信したかを判別します。NetFlow Collector は、送信元インターフェイスの IP アドレスを使用してルータに Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) クエリーを実行します。送信元インターフェイスの IP アドレスは変更することがあるので (たとえば、インターフェイスがフラップして、異なるインターフェイスがデータの送信に使用される場合など)、ループバック送信元インターフェイスを設定することを推奨します。ループバック インターフェイスは、常にアップの状態、ワークステーションの NetFlow Collector から SNMP クエリーに応答できます。

NDE の詳細については、『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*』の「Configuring NDE」の章を参照してください。

例

次に、ループバック送信元インターフェイスの設定例を示します。ループバック インターフェイスは、4.0.0.1 の IP アドレスを持ち、スロット 5、およびポート 0 のシリアル インターフェイスに使用されます。

```
Router# configure terminal
Router(config)# interface loopback0
Router(config-if)# ip address 4.0.0.1 255.0.0.0
Router(config-if)# exit
Router(config)# interface serial 5/0:0
Router(config-if)# ip unnumbered loopback0
Router(config-if)# no ip mroute-cache
Router(config-if)# encapsulation ppp
Router(config-if)# ip route-cache flow
Router(config-if)# exit
Router(config)# ip flow-export source loopback0
Router(config)# exit
```

関連コマンド

コマンド	説明
ip flow-export destination	特定の宛先に NetFlow キャッシュ エントリをエクスポートします。
ip flow-export version	NetFlow キャッシュ エントリにおける情報のエクスポートのバージョンを指定します。
ip route-cache flow	IP ルーティングの NetFlow スイッチングをイネーブルにします。

ip flow-export version

NetFlow キャッシュ エントリにおける情報のエクスポートのバージョンを指定するには、**ip flow-export version** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
ip flow-export version {1 | {5 [origin-as | peer-as]} | {9 [bgp-nextthop | origin-as | peer-as]}}
```

```
no ip flow-export version
```

シンタックスの説明

1	エクスポート パケットがバージョン 1 形式を使用するように指定します。詳細については、「使用上のガイドライン」を参照してください。
5	エクスポート パケットがバージョン 5 形式を使用するように指定します。詳細については、「使用上のガイドライン」を参照してください。
origin-as	(任意) 送信元および宛先のオリジン自律システムを含むエクスポート統計情報を指定します。
peer-as	(任意) 送信元および宛先のピア自律システムを含むエクスポート統計情報を指定します。
9	エクスポート パケットがバージョン 9 形式を使用するように指定します。詳細については、「使用上のガイドライン」を参照してください。
bgp-nextthop	(任意) 送信元および宛先の BGP ネクスト ホップを含むエクスポート統計情報を指定します。

コマンドのデフォルト

NetFlow キャッシュ エントリにおける情報のエクスポートはディセーブルです。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

バージョン 5 およびバージョン 9 の形式には、送信元と宛先の AS アドレス、および送信元と宛先のプレフィクス マスクが含まれます。バージョン 9 には BGP ネクスト ホップ情報も含まれます。

バージョン 1 の場合、データグラムに保存されるレコードの数は、1 ~ 24 までの変数です。バージョン 5 の場合、データグラムに保存されるレコードの数は、1 ~ 30 までの変数です。

NDE の詳細については、『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*』の「Configuring NDE」の章を参照してください。

■ ip flow-export version

例

次に、バージョン 5 形式を使用してデータをエクスポートする例を示します。

```
Router(config)# ip flow-export version 5
Router(config)#
```

関連コマンド

コマンド	説明
show mls nde	NDE ハードウェアによってスイッチングされるフローに関する情報を表示します。

ip flow ingress

ソフトウェアでスイッチングされるフローの作成をレイヤ 3 でイネーブルにするには、**ip flow ingress** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip flow ingress

no ip flow ingress

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト デイセーブル

コマンド モード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン NetFlow エントリを作成するには、**ip flow ingress** コマンドを入力する必要があります。次の注意事項に従ってマルチキャスト エントリを表示してください。

- **show mls netflow ip** コマンドを入力します。
- **ip flow ingress** コマンドをインターフェイスで入力します。
- **no ip multicast netflow ingress** コマンドを入力していないことを確認します。

例 次に、IPv4 ブリッジド フローに対して着信 NDE をイネーブルにして、NetFlow エントリ作成をイネーブルにする例を示します。

```
Router(config-if)# ip flow ingress
Router(config-if)#
```

次に、IPv4 ブリッジド フローに対して着信 NDE をデイセーブルにする例を示します。

```
Router(config-if)# no ip flow ingress
Router(config-if)#
```

ip flow layer2-switched

スイッチドフロー、ブリッジドフロー、レイヤ 2 IP フローの作成を特定の VLAN でイネーブルにするには、**ip flow layer2-switched** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
ip flow {ingress | export} layer2-switched {vlan {num | vlanlist}}
```

```
no ip flow {ingress | export} layer2-switched {vlan {num | vlanlist}}
```

シンタックスの説明

ingress	スイッチドフロー、ブリッジドフロー、IP フローの収集をレイヤ 2 でイネーブルにします。
export	スイッチドフロー、ブリッジドフロー、IP フローのエクスポートをレイヤ 2 でイネーブルにします。
vlan num vlanlist	VLAN または VLAN 範囲を指定します。有効値は 1 ~ 4094 です。詳細については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- **ip flow ingress layer2switch** はディセーブルです。
- **ip flow export layer2switched** はイネーブルです。

コマンドモード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドを使用する前に、対応する VLAN インターフェイスが使用可能であり、有効な IP アドレスが含まれていることを確認してください。

1 つまたは複数の VLAN を入力できます。次に、有効な VLAN リストの例を示します。1; 1,2,3; 1-3,7。

例

次に、特定の VLAN 上でレイヤ 2 スwitchドフローの収集をイネーブルにする例を示します。

```
Router(config)# ip flow ingress layer2-switched vlan 2
Router(config)#
```

次に、ある VLAN 範囲でレイヤ 2 スwitchドフローのエクスポートをイネーブルにする例を示します。

```
Router(config)# ip flow export layer2-switched vlan 1-3,7
Router(config)#
```

次に、特定の VLAN 上でレイヤ 2 スwitchドフローの収集をディセーブルにする例を示します。

```
Router(config)# no ip flow ingress layer2-switched vlan 2
Router(config)#
```

ip forward-protocol turbo-flood

スパニングツリー アルゴリズムを使用して UDP パケットのフラッディングを高速化するには、**ip forward-protocol turbo-flood** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip forward-protocol turbo-flood [udp-checksum]

no ip forward-protocol turbo-flood [udp-checksum]

シンタックスの説明

udp-checksum (任意) UDP チェックサムを指定します。

コマンドのデフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ip forward-protocol turbo-flood コマンドを入力した場合、送信 UDP パケットに NULL チェックサムが含まれます。すべての送信パケットに UDP チェックサムが含まれるようにするには、**ip forward-protocol turbo-flood udp-checksum** コマンドを入力する必要があります。

例

次に、スパニングツリー アルゴリズムを使用して UDP パケットのフラッディングを高速化する例を示します。

```
Router(config)# ip forward-protocol turbo-flood
Router(config)#
```

次に、スパニングツリー アルゴリズムを使用して UDP パケットのフラッディングを高速化し、すべての送信パケットに UDP チェックサムが含まれるようにする例を示します。

```
Router(config)# ip forward-protocol turbo-flood udp-checksum
Router(config)#
```

次に、**udp-checksum** キーワードおよび **ip forward-protocol turbo-flood** コマンドをオフにする例を示します。

```
Router(config)# no ip forward-protocol turbo-flood udp-checksum
Router(config)#
```

次に、**udp-checksum** キーワードなしの **ip forward-protocol turbo-flood** コマンドを回復する例を示します。

```
Router(config)# ip forward-protocol turbo-flood
Router(config)#
```

■ ip forward-protocol turbo-flood

関連コマンド

コマンド	説明
ip forward-protocol	ブロードキャスト パケットの転送時にルータが転送するプロトコルとポートを指定します。

ip igmp immediate-leave group-list

IGMP 脱退グループ メッセージの即時処理をイネーブルにするには、**ip igmp immediate-leave group-list** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip igmp immediate-leave group-list *acl*

no ip igmp immediate-leave group-list *acl*

シンタックスの説明	<i>acl</i>	グループ ACL 番号。有効値については、「使用上のガイドライン」を参照してください。
------------------	------------	---

コマンドのデフォルト	ディセーブル
-------------------	--------

コマンド モード	グローバルまたはインターフェイス コンフィギュレーション
-----------------	------------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン **ip igmp immediate-leave group-list** コマンドを入力した場合、VLAN インターフェイス コンフィギュレーション モードだけでこのコマンドを入力する必要があります。

acl 引数の有効値は次のとおりです。

- アクセス リスト番号 : 1 ~ 99
- 拡張範囲アクセス リスト番号 : 1300 ~ 1999
- 標準 IP アクセス リストの名前

設定できるのはどちらか一方で、両方のコンフィギュレーション モードを同時に設定することはできません。

即時脱退動作をマルチキャスト グループの簡易アクセス リストに制限するには、*acl* 値を指定します。*acl* 値で許可されていないマルチキャスト グループの IGMP 脱退グループ メッセージでは、標準的な問い合わせメカニズムおよび脱退遅延が適用されます。

例 次に、IGMP 脱退グループ メッセージの即時処理をイネーブルにする例を示します。

```
Router(config)# ip igmp immediate-leave group-list 3
Router(config)#
```

ip igmp last-member-query-interval

IGMP の最終メンバー クエリー インターバルを設定するには、**ip igmp last-member-query-interval** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip igmp last-member-query-interval *interval*

no ip igmp last-member-query-interval

シンタックスの説明

<i>interval</i>	最終メンバー クエリーのインターバル。有効値は、100 ~ 65,535 ミリ秒です (100 ミリ秒の倍数)。
-----------------	--

コマンドのデフォルト

1000 ミリ秒 (1 秒) です。詳細については、「使用上のガイドライン」を参照してください。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

マルチキャスト ホストがグループから脱退すると、ホストは IGMP 脱退メッセージを送信します。このホストがグループを脱退する最終ホストかどうかを確認するために、脱退が確認されタイマーが開始したときに IGMP クエリーが送信されます。タイマーの期限が切れる前にレポートが受信されないと、グループ レコードは削除されます。

interval は、Catalyst 6500 シリーズ スイッチがグループ固有のクエリーの応答を実際に待つ時間です。

100 の倍数でないインターバルを入力すると、100 未満の端数が切り捨てられます。たとえば、999 と入力した場合、端数が切り捨てられて 900 ミリ秒になります。

IGMP 高速脱退処理をイネーブルにして、**no ip igmp last-member-query-interval** コマンドを入力した場合、インターバルは 0 秒にセットされ、即時脱退が常に優先されます。

例

次に、最終メンバー クエリーのインターバルを 200 ミリ秒に設定する例を示します。

```
Router(config-if)# ip igmp last-member-query-interval 200
Router(config-if)#
```

関連コマンド

コマンド	説明
ip igmp immediate-leave group-list	IGMP 脱退グループ メッセージの即時処理をイネーブルにします。
show ip igmp interface	IGMP インターフェイス ステータスおよび設定に関する情報を表示します。

ip igmp snooping

IGMP スヌーピングをイネーブルにするには、**ip igmp snooping** コマンドを使用します。IGMP スヌーピングをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip igmp snooping

no ip igmp snooping

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト デフォルト設定は次のとおりです。

- IGMP スヌーピングは、Catalyst 6500 シリーズ スイッチでイネーブルです。
- マルチキャスト ルータ上で、IGMP スヌーピングは設定されていません。

コマンドのデフォルト インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン Catalyst 6500 シリーズ スイッチの IGMP スヌーピングをイネーブルにする前に、VLAN インターフェイスにマルチキャスト ルーティングを設定する必要があります。

このコマンドは、VLAN インターフェイス コンフィギュレーション モードだけで使用してください。

例 次に、IGMP スヌーピングをイネーブルにする例を示します。

```
Router(config-if)# ip igmp snooping
Router(config-if)#
```

次に、IGMP スヌーピングをディセーブルにする例を示します。

```
Router(config-if)# no ip igmp snooping
Router(config-if)#
```

関連コマンド	コマンド	説明
	ip igmp snooping fast-leave	IGMPv3 スヌーピングの高速脱退処理をイネーブルにします。
	ip igmp snooping mrouter	マルチキャスト ルータ ポートとしてレイヤ 2 ポートを設定します。
	show ip igmp snooping explicit-tracking	IGMPv3 ホストの明示的なホストトラッキング ステータスに関する情報を表示します。

ip igmp snooping explicit-tracking

明示的なホスト トラッキングをイネーブルにするには、**ip igmp snooping explicit-tracking** コマンドを使用します。明示的なホスト トラッキングをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip igmp snooping explicit-tracking

no ip igmp snooping explicit-tracking

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンド モード

イネーブル

コマンドのデフォルト

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

明示的なホスト トラッキングは、IGMPv3 ホストだけでサポートされています。

明示的なホスト トラッキングがイネーブルで、Catalyst 6500 シリーズ スイッチがプロキシ レポート モードで動作している場合、ルータは VLAN インターフェイスの背後のホストすべてをトラッキングできない場合があります。プロキシ レポート モードでは、Catalyst 6500 シリーズ スイッチはチャンネルの最初のレポートだけをルータへ転送し、同じチャンネルに対するその他のレポートはすべて抑制されます。

IGMPv3 プロキシ レポートを使用すると、Catalyst 6500 シリーズ スイッチは非請求レポート、および一般的なクエリー インターバルで受信されたレポートに対してプロキシ レポートを行います。

プロキシ レポートはデフォルトでオンになっています。プロキシ レポートをディセーブルにすると、Catalyst 6500 シリーズ スイッチはトランスペアレント モードで動作し、レポートを受信すると IGMP スヌーピング データベースを更新し、アップストリームのルータにこの情報を転送します。このようにして、ルータはレポートするホストをすべて明示的にトラッキングできます。

明示的なトラッキングをディセーブルにすると、高速脱退処理およびプロキシ レポートがディセーブルになります。

IGMPv3 はすべてのポートでメンバーシップ情報の明示的なホスト トラッキングをサポートしています。明示的なホスト トラッキング データベースは、IGMPv3 ホストの高速脱退処理、プロキシ レポート、および統計情報収集に使用されます。VLAN 上で、明示的なホスト トラッキングをイネーブルにすると、IGMP スヌーピング ソフトウェアはホストから受信する IGMPv3 レポートを処理し、次の情報が含まれる明示的なホスト トラッキング データベースを構築します。

- ホストが接続されているポート
- ホストによりレポートされるチャンネル
- ホストによりレポートされる各グループのフィルタ モード

- ホストによりレポートされる各グループの送信元リスト
- 各グループのルータ フィルタ モード
- グループごとの、送信元を要求するホスト リスト

例

次に、IGMPv3 の明示的なホスト トラッキングをイネーブルにする例を示します。

```
Router(config-if) # ip igmp snooping explicit-tracking
Router(config-if) #
```

次に、IGMPv3 の明示的なホスト トラッキングをディセーブルにする例を示します。

```
Router(config-if) # no ip igmp snooping explicit-tracking
Router(config-if) #
```

関連コマンド

コマンド	説明
ip igmp snooping limit track	明示的トラッキング データベースのサイズを制限します。
show ip igmp snooping explicit-tracking	IGMPv3 ホストの明示的なホストトラッキング ステータスに関する情報を表示します。

ip igmp snooping fast-leave

IGMPv3 スヌーピングの高速脱退処理をイネーブルにするには、**ip igmp snooping fast-leave** コマンドを使用します。高速脱退処理をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip igmp snooping fast-leave

no ip igmp snooping fast-leave

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドモード

デフォルト設定は次のとおりです。

- IGMP バージョン 2 : ディセーブル
- IGMP バージョン 3 : イネーブル

コマンドのデフォルト

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、VLAN インターフェイス コンフィギュレーション モードだけで使用してください。



(注)

高速脱退処理はデフォルトでイネーブルです。高速脱退処理をディセーブルにするには、**no ip igmp snooping fast-leave** コマンドを使用して高速脱退処理をディセーブルにする必要があります。

IGMPv3 スヌーピングの高速脱退処理機能は、特定 VLAN の MAC グループの単一レシーバーがある場合に使用してください。

例

次に、IGMPv3 スヌーピングの高速脱退処理をイネーブルにする例を示します。

```
Router(config-if)# ip igmp snooping fast-leave
Router(config-if)#
```

次に、IGMPv3 スヌーピングの高速脱退処理をディセーブルにする例を示します。

```
Router(config-if)# no ip igmp snooping fast-leave
Router(config-if)#
```

関連コマンド

コマンド	説明
ip igmp snooping	IGMP スヌーピングをイネーブルにします。
ip igmp snooping explicit-tracking	明示的なホスト トラッキングをイネーブルにします。
show ip igmp interface	IGMP インターフェイス ステータスおよび設定に関する情報を表示します。
show mac-address-table	MAC アドレス テーブルに関する情報を表示します。

ip igmp snooping flooding

マルチキャスト パケットの定期的なフラッディングを設定するには、**ip igmp snooping flooding** コマンドを使用します。定期的なフラッディングをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip igmp snooping flooding [timer seconds]

no ip igmp snooping flooding

シンタックスの説明

timer seconds	(任意) 送信元専用エントリに対する 24 時間内のフラッディング間隔を指定します。有効値は、0 ~ 86,400 秒です。
----------------------	--

コマンド モード

デフォルト設定は次のとおりです。

- ディセーブル
- イネーブルの場合、*seconds* は **600** 秒 (10 分) です。

コマンドのデフォルト

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは送信元専用 VLAN 上でサポートされます。

フラッディングをディセーブルにするには、**0** 秒を入力します。最大値の 86,400 秒を入力した場合、フラッディングは 24 時間ごとに実行されます。

例 次に、24 時間内のフラッディング間隔を指定する例を示します。

```
Router(config-if)# ip igmp snooping flooding timer 300
Router(config-if)#
```

ip igmp snooping l2-entry-limit

Catalyst 6500 シリーズスイッチによって作成されるレイヤ 2 エントリの最大数を設定するには、**ip igmp snooping l2-entry-limit** コマンドを使用します。

ip igmp snooping l2-entry-limit *max-entries*

シンタックスの説明	<i>max-entries</i>	Catalyst 6500 シリーズスイッチによって作成されるレイヤ 2 エントリの最大数。有効値は、1 ~ 100,000 です。
-----------	--------------------	--

コマンドのデフォルト	15488 のレイヤ 2 エントリ
------------	-------------------

コマンドモード	グローバル コンフィギュレーション (config)
---------	----------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン	<i>max-entries</i> を入力する場合、カンマ (,) を入力しないでください。 このコマンドは、VLAN インターフェイス コンフィギュレーション モードだけで使用してください。
------------	--

例	次に、Catalyst 6500 シリーズスイッチによって作成されるレイヤ 2 エントリの最大数を設定する例を示します。
---	--

```
Router(config-if)# ip igmp snooping l2-entry-limit 25000
Router(config-if)#
```

関連コマンド	<table><thead><tr><th>コマンド</th><th>説明</th></tr></thead><tbody><tr><td>show ip igmp interface</td><td>IGMP インターフェイス ステータスおよび設定に関する情報を表示します。</td></tr></tbody></table>	コマンド	説明	show ip igmp interface	IGMP インターフェイス ステータスおよび設定に関する情報を表示します。
コマンド	説明				
show ip igmp interface	IGMP インターフェイス ステータスおよび設定に関する情報を表示します。				

ip igmp snooping last-member-query-interval

IGMP スヌーピングの最終メンバー クエリー インターバルを設定するには、**ip igmp snooping last-member-query-interval** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip igmp snooping last-member-query-interval *interval*

no ip igmp snooping last-member-query-interval

シンタックスの説明

<i>interval</i>	最終メンバー クエリーのインターバル。有効値は、100 ～ 900 ミリ秒です (100 ミリ秒の倍数)。
-----------------	---

コマンドのデフォルト

1000 ミリ秒 (1 秒) です。詳細については、「使用上のガイドライン」を参照してください。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

マルチキャスト ホストがグループから脱退すると、ホストは IGMP 脱退メッセージを送信します。このホストがグループを脱退する最終ホストかどうかを確認するために、脱退が確認されタイマーが開始したときに IGMP クエリーが送信されます。タイマーの期限が切れる前にレポートが受信されないと、グループ レコードは削除されます。

interval は、Catalyst 6500 シリーズ スイッチがグループ固有のクエリーの応答を実際に待つ時間です。

100 の倍数でないインターバルを入力すると、100 未満の端数が切り捨てられます。たとえば、999 と入力した場合、端数が切り捨てられて 900 ミリ秒になります。

IGMP 高速脱退処理をイネーブルにして、**no ip igmp snooping last-member-query-interval** コマンドを入力した場合、インターバルは 0 秒にセットされ、高速脱退処理が常に優先されます。

有効値の範囲は 100 ～ 1000 ミリ秒ですが、**1000** の値は入力できません。この値にする場合は、**no ip igmp snooping last-member-query-interval** コマンドを入力して、デフォルト値 (1000 ミリ秒) に戻す必要があります。

例

次に、最終メンバー クエリー インターバルを 200 ミリ秒に設定する例を示します。

```
Router(config-if)# ip igmp snooping last-member-query-interval 200
Router(config-if)#
```

関連コマンド

コマンド	説明
ip igmp snooping fast-leave	IGMP v3 スヌーピングの高速脱退処理をイネーブルにします。
show ip igmp interface	IGMP インターフェイス ステータスおよび設定に関する情報を表示します。

ip igmp snooping limit track

明示的トラッキング データベースのサイズを制限するには、**ip igmp snooping limit track** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip igmp snooping limit track *max-entries*

no ip igmp snooping limit track

シンタックスの説明

max-entries 明示的トラッキング データベースの最大エントリ数。有効値は 0 ～ 128,000 です。

コマンドのデフォルト

max-entries は **32000** です。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

明示的なトラッキング データベースの各エントリは、送信元 IP、グループ IP、ポート、VLAN、およびレポータ IP により識別されます。

max-entries を **0** に設定すると、明示的なトラッキングはディセーブルになります。

明示的なトラッキング データベースが設定された *max-entries* を超えると、Syslog メッセージが生成されます。

max-entries を減らした場合、明示的なトラッキング データベースではただちにサイズを減らすことはできません。明示的なトラッキング データベースは、レポータがタイムアウトになるに従って徐々に縮小されます。

例

次に、明示的なトラッキング データベースの最大エントリ数を設定する例を示します。

```
Router(config)# ip igmp snooping limit track 20000
Router(config)#
```

関連コマンド

コマンド	説明
ip igmp snooping explicit-tracking	明示的なホストトラッキングをイネーブルにします。
show ip igmp snooping explicit-tracking vlan	IGMPv3 ホストの明示的なホストトラッキングに関する情報を表示します。

ip igmp snooping mrouter

レイヤ 2 ポートをマルチキャスト ルータ ポートとして設定するには、**ip igmp snooping mrouter** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

ip igmp snooping mrouter {*interface* {*interface interface-number*} |
{*port-channel number*}} | {**learn** {**cgmp** | **pim-dvmrp**}}

no ip igmp snooping mrouter {*interface* {*interface interface-number*} |
{*port-channel number*}} | {**learn** {**cgmp** | **pim-dvmrp**}}

シンタックスの説明	
interface	マルチキャスト ルータへのネクスト ホップ インターフェイスを指定します。
<i>interface</i>	インターフェイス タイプ。有効値は ethernet 、 fastethernet 、 gigabitethernet 、および tengigabitethernet です。その他の有効値については、「使用上のガイドライン」を参照してください。
<i>interface-number</i>	モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
port-channel number	ポート チャネル番号を指定します。有効値は 1 ~ 256 の範囲の最大 64 個の値です。
learn	マルチキャスト ルータの学習方式を指定します。
cgmp	マルチキャスト ルータのスヌーピング CGMP パケットを指定します。
pim-dvmrp	マルチキャスト ルータのスヌーピング PIM-DVMRP パケットを指定します。

コマンドのデフォルト **pim-dvmrp**

コマンド モード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドは、VLAN インターフェイス コンフィギュレーション モードだけで使用してください。ルータとのインターフェイスは、コマンドを入力する VLAN 内になければなりません。インターフェイスは管理上のアップ状態にあり、ラインプロトコルもアップになっている必要があります。

interface-number 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

ip igmp snooping mrouter

CGMP 学習方式により、制御トラフィックを減少させることができます。

設定された学習方式は、NVRAM に保存されます。

マルチキャスト ルータへのスタティック接続は、スイッチ ポート上だけでサポートされます。

例

次に、マルチキャスト ルータへのネクスト ホップ インターフェイスを指定する例を示します。

```
Router(config-if)# ip igmp snooping mrouter interface fastethernet 5/6
Router(config-if)#
```

次に、マルチキャスト ルータの学習方式を指定する例を示します。

```
Router(config-if)# ip igmp snooping mrouter learn cgmp
Router(config-if)#
```

関連コマンド

コマンド	説明
ip igmp snooping	IGMP スヌーピングをイネーブルにします。
ip igmp snooping fast-leave	IGMPv3 スヌーピングの高速脱退処理をイネーブルにします。
show ip igmp snooping mrouter	ダイナミックに学習された、および手動で設定されたマルチキャスト ルータ インターフェイスに関する情報を表示します。

ip igmp snooping querier

VLAN またはサブネット内でマルチキャスト ルーティング プロトコルが設定されていない場合に、サブネット内のマルチキャスト サポートをイネーブルにするには、**ip igmp snooping querier** コマンドを使用します。マルチキャスト ルーティング プロトコルが設定されていない場合に、サブネット内のマルチキャスト サポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip igmp snooping querier

no ip igmp snooping querier

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト ディセーブル

コマンド モード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、VLAN インターフェイス コンフィギュレーション モードだけで使用してください。Catalyst 6500 シリーズ スイッチ上で IGMP スヌーピングをイネーブルにし、VLAN 上で PIM をディセーブルにします。

VLAN はグローバル コンフィギュレーション モードで設定してください。

VLAN インターフェイス上で IP アドレスを設定してください。イネーブルになっている場合、IGMP スヌーピング クエリアはこの IP アドレスをクエリーの送信元アドレスとして使用します。VLAN インターフェイス上に IP アドレスが設定されていない場合、IGMP スヌーピング クエリアは起動しません。IP アドレスが消去されると、IGMP スヌーピング クエリアは自身をディセーブルにします。イネーブルになっている場合、IP アドレスを設定すると IGMP スヌーピング クエリアは再起動します。

IGMP スヌーピング クエリアは、IGMP version 2 (IGMPv2) をサポートしています。

イネーブルになっている場合、IGMP スヌーピング クエリアは次のように動作します。

- マルチキャスト ルータからの IGMP トラフィックを検出すると、IGMP スヌーピング クエリアは起動しません。
- マルチキャスト ルータから IGMP トラフィックが検出されなければ、IGMP スヌーピング クエリアは 60 秒後に起動します。
- マルチキャスト ルータからの IGMP トラフィックを検出すると、IGMP スヌーピング クエリアは自身をディセーブルにします。

IGMP スヌーピングがイネーブルのとき、QoS は IGMP パケットをサポートしません。

IGMP スヌーピング クエリアは、VLAN のすべての Catalyst 6500 シリーズ スイッチでイネーブルにできます。1 つの Catalyst 6500 シリーズ スイッチが、クエリアとして選定されます。

ip igmp snooping querier

マルチキャスト ルータが VLAN またはサブネットに存在しない場合に IGMP スヌーピング クエリアをイネーブルにすると、Catalyst 6500 シリーズスイッチは VLAN の IGMP クエリアになります。

IGMP スヌーピング クエリアをディセーブルにすると、IGMP スヌーピングは PIM をサブネットに設定した場合にだけ機能します。

ip igmp snooping querier コマンドはいつでも入力できますが、IGMP スヌーピング クエリアが起動するのは、他のマルチキャスト ルータが VLAN またはサブネットに存在しない場合だけです。

サブネットに PIM を設定する代わりにこのコマンドを使用できます。マルチキャストトラフィックがルーティングされる必要はないが、ネットワーク内のレイヤ 2 インターフェイスで IGMP スヌーピングのサポートが必要な場合に使用します。

例

次に、VLAN 上で IGMP スヌーピング クエリアをイネーブルにする例を示します。

```
Router(config-if)# ip igmp snooping querier
Router(config-if)#
```

関連コマンド

コマンド	説明
show ip igmp snooping mrouter	ダイナミックに学習された、および手動で設定されたマルチキャスト ルータ インターフェイスに関する情報を表示します。

ip igmp snooping rate

IGMP スヌーピング パケットのレート制限を設定するには、**ip igmp snooping rate** コマンドを使用します。ソフトウェア レートの制限をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip igmp snooping rate *pps*

no ip igmp snooping rate

シンタックスの説明	<i>pps</i>	着信 IGMP メッセージのレート制限。有効値は、100 ~ 6000 パケット/秒です。
-----------	------------	---

コマンドのデフォルト	ディセーブル
------------	--------

コマンド モード	グローバル コンフィギュレーション (config) (config)
----------	-------------------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、ソフトウェアのレート制限をイネーブルにする例を示します。

```
Router(config)# ip igmp snooping rate
Router(config)#
```

次に、ソフトウェアのレート制限をディセーブルにする例を示します。

```
Router(config)# no ip igmp snooping rate
Router(config)#
```

関連コマンド	コマンド	説明
	show ip igmp snooping rate-limit	IGMP スヌーピング レート制限に関する情報を表示します。

ip igmp snooping report-suppression

IP IGMP スヌーピング レポート抑制をオンに切り替えるには、**ip igmp snooping report-suppression** コマンドを使用します。レポート抑制をオフに切り替えるには、このコマンドの **no** 形式を使用します。

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

一般クエリーに応答するすべてのホスト レポートに対してレポート抑制をイネーブルにすると、IP IGMP スヌーピングは最初のレポートだけを転送し、残りのレポートを抑制して IGMP トラフィックをマルチキャスト ルータに制限します。

ip igmp snooping source-only-learning age-timer

マルチキャスト送信元専用でレシーバーが接続されていないレイヤ 2 セグメントにマルチキャストパケットを定期的にフラッディングするには、**ip igmp snooping source-only-learning age-timer** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip igmp snooping source-only-learning age-timer seconds

no ip igmp snooping source-only-learning age-timer

シンタックスの説明

<i>seconds</i>	秒単位の送信元専用エントリ エージング タイマー値。有効値は 0 ~ 86,400 秒です。
----------------	--

コマンドのデフォルト

seconds は 600 秒 (10 分) です。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

source_only_age_timer および *source_only_delete_timer* という 2 つの送信元専用タイマーがあり、交互に動作します。**ip igmp snooping source-only-learning age-timer** コマンドで設定した値では、*source_only_age_timer* が設定されます。*source_only_delete_timer* の値は 5 分 (300 秒) に固定されていて設定を変えることはできません。

片方のタイマーが満了すると、他方のタイマーが開始されます。常にどちらかのタイマーが動作しています。

エージング タイマーを **0** に設定すると、送信元専用 VLAN でフラッディングが停止します。



(注)

エージング タイマーをゼロ以外の値に設定すると、x (設定値) + 5 分 (*source_only_delete_timer*) の間隔ごとにフラッディングが発生します。

例

次に、マルチキャストパケットを定期的にフラッディングする例を示します。

```
Router(config)# ip igmp snooping source-only-learning age-timer 300
Router(config)#
```

次に、デフォルト設定に戻す例を示します。

```
Router(config)# no ip igmp snooping source-only-learning age-timer
Router(config)#
```

ip igmp ssm-map

Source Specific Multicast (SSM) マッピングをイネーブルにして設定するには、**ip igmp ssm-map** コマンドを使用します。SSM マッピングをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ip igmp ssm-map {enable | {query dns} | {static {group-access-list |
group-access-list-name} source-address}}
```

```
no ip igmp ssm-map {enable | {query dns}}
```

シンタックスの説明

enable	送信元マッピングに対して SSM グループをイネーブルにします。
query dns	DNS 検索をイネーブルにします。
static	送信元マッピングに対して SSM スタティック グループを指定します。
<i>group-access-list</i>	送信元アドレスにマッピングするグループのアクセス リスト
<i>group-access-list-name</i>	送信元アドレスにマッピングするグループのアクセス リスト名
<i>source-address</i>	送信元アドレス

コマンドのデフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

デフォルトでは、ローカルに設定されたスタティック SSM マッピングおよび DNS サーバがクエリーされます。ローカルに設定されたマッピングは、ダイナミック マッピングより優先されます。DNS サーバが使用できない場合、DNS サーバ検索はディセーブルにしておくことができます。DNS 検索をディセーブルにするには、**no ip igmp ssm-map query dns** コマンドを使用します。

DNS サーバが使用できない場合、ローカルに設定されたスタティック SSM マッピング データベースがクエリーに使用されます。データベース クエリーではグループ アドレスを使用し、それに対して送信元リストを受信します。スタティック SSM マッピングが設定されるとすぐに、このマップが検索用に使用されます。スタティック SSM マッピング データベースを確立するには、次のコマンドを使用します。

```
ip igmp ssm-map static acl-1 source-1-ip-address
```

```
ip igmp ssm-map static acl-2 source-2-ip-address
```

ACL では、表示される送信元にマッピングされる必要があるグループ (複数可) を指定します。コンテンツ サーバは同じ送信元アドレスを使用して複数のストリームを送信する必要があるため、マルチキャスト宛先アドレスを 1 つのグループとするためにアクセスリストが使用されます。アドレスが連続している場合は、ワイルドカードを使用できます。

1 つのマルチキャスト グループ アドレスが複数の送信元に参加する必要がある場合、送信元アドレスに関連付けられるすべての ACL にグループを配置する必要があります。上記の例では、グループ G が送信元 1 および 2 に参加する必要がある場合、グループ アドレスは `acl-1` および `acl-2` の両方に配置される必要があります。

ip igmp ssm-map enable コマンドを使用して SSM マッピングをイネーブルにしても、グループの送信元マッピング リストが空の場合、**no ip igmp ssm-map query dns** コマンドを入力します。**ip igmp ssm-map enable** コマンドは、スタティックに設定された SSM マッピングの送信元エントリだけでサポートされます。

例

次に、送信元マッピングに対して SSM グループをイネーブルにする例を示します。

```
Router(config)# ip igmp ssm-map enable
Router(config)#
```

次に、DNS 検索をイネーブルにする例を示します。

```
Router(config)# ip igmp ssm-map query dns
Router(config)#
```

次に、スタティック SSM マッピング データベースを確立する例を示します。

```
Router(config)# ip igmp ssm-map static acl1 255.255.255.0
Router(config)# ip igmp ssm-map static acl2 255.255.255.0
Router(config)#
```

次に、送信元マッピングに対して SSM グループをディセーブルにする例を示します。

```
Router(config)# no ip igmp ssm-map enable
Router(config)#
```

次に、DNS 検索をディセーブルにする例を示します。

```
Router(config)# no ip igmp ssm-map query dns
Router(config)#
```

ip igmp tcn query

設定間隔の間に実行する IGMP トポロジ変更クエリーの数を設定するには、**ip mp tcn query** コマンドを使用します。トポロジ変更クエリーを無効にするには、このコマンドの **no** 形式を使用します。

```
ip igmp tcn query {count count | interval interval}
```

```
no ip igmp tcn query {count | interval}
```

シンタックスの説明

count count	TCN イベント後のマルチキャスト トラフィックのフラッドイングを停止するのに必要なクエリー数を指定します。有効値は 1 ~ 10 です
interval interval	IGMP TCN クエリーが期限切れになるまでの時間を指定します。有効値は 1 ~ 255 秒です。

コマンドのデフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ip igmp tcn query コマンドは、レイヤ 2 スイッチポートおよび EtherChannel だけに適用され、VLAN インターフェイスおよびレイヤ 3 チャンネルには適用されません。

ip igmp tcn query count コマンドは、TCN イベント後にマルチキャスト トラフィックがフラッドイングするまでの時間を制御するために使用されます。**ip igmp tcn query count** コマンドを使用して TCN フラッド クエリー カウントを 1 に設定した場合、1 つの一般クエリーを受信した後にフラッドイングが停止します。カウントを 7 に設定した場合は、TCN イベントによるマルチキャスト トラフィックのフラッドイングは、7 つの一般クエリーが受信されるまで続きます。TCN イベント中に受信された一般クエリーに基づいて、グループが再学習されます。

例

次に、実行されるクエリーの数を設定する例を示します。

```
Router(config)# ip igmp tcn query count 5
Router(config)#
```

次に、クエリーが期限切れになるまでの時間を 120 秒に設定する例を示します。

```
ローカル プロキシ ARP をイネーブルにするには、Router(config)# ip igmp tcn query interval 120
Router(config)#
```

ip local-proxy-arp

ip local-proxy-arp コマンドを使用します。ローカル プロキシ ARP をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip local-proxy-arp

no ip local-proxy-arp

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト ディセーブル

コマンド モード インターフェイス コンフィギュレーション (config-if)

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン ホストが直接相互通信できないように設定されたサブネットでは、ローカル プロキシ ARP を使用します。たとえば、プライベート VLAN 環境でローカル プロキシ ARP を使用できます。ローカル プロキシ ARP を使用すると、PISA は通常ルーティングが必要とされないサブネット内部の IP アドレスに関する ARP 要求に応答できます。ローカル プロキシ ARP をイネーブルにすると、PISA はトラフィックが通常はルーティングされない共通のサブネット内で、IP アドレスに関する ARP 要求に応答できません。このような状況は、同じサブネット上の 2 つのホスト間で直接アドレス解決できない場合にだけ発生します。

Internet Control Message Protocol (ICMP) リダイレクトは、ローカル プロキシ ARP がイネーブルのインターフェイスでディセーブルです。

例 次に、ローカル プロキシ ARP をイネーブルにする例を示します。

```
Router(config-if)# ip local-proxy-arp
Router(config-if)#s
```

ip mroute

マルチキャスト スタティック ルート (mroute) を設定するには、**ip mroute** コマンドを使用します。ルート削除するには、このコマンドの **no** 形式を使用します。

```
ip mroute [vrf vrf-name] source-address mask [protocol as-number] {rpf-address | interface-type interface-number} [distance]
```

```
no ip mroute [vrf vrf-name] source-address mask [protocol as-number] {rpf-address | interface-type interface-number} [distance]
```

シンタックスの説明

<i>vrf vrf-name</i>	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
<i>source-address</i>	マルチキャスト送信元の IP アドレス
<i>mask</i>	マルチキャスト送信元の IP アドレスのマスク
<i>protocol</i>	(任意) 使用中のユニキャスト ルーティング プロトコル
<i>as-number</i>	(任意) 使用中のルーティング プロトコルの自律システム番号 (該当する場合)
<i>rpf-address</i>	mroute 用の着信インターフェイス
<i>interface-type interface-number</i>	mroute 用のインターフェイス タイプおよびインターフェイス番号
<i>distance</i>	(任意) 管理上の距離。有効値は 0 ~ 255 です。

コマンドのデフォルト

distance は **0** です。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドにより、マルチキャスト送信元の場所をスタティックに設定できます (ユニキャスト ルーティング テーブルでは一部異なって表示されます)。

送信元範囲が指定されている場合、*rpf-address* 引数はこれらの送信元だけに適用されます。

rpf-address が PIM ネイバである場合、PIM join、graft、および prune メッセージがこれに対して送信されます。*rpf-address* 引数は、直接接続されたシステムのホストの IP アドレスまたはネットワーク/サブネット番号になります。この引数がルートの場合、再帰検索がユニキャスト ルーティング テーブルから実行され、直接接続されたシステムを検出します。*rpf-address* 引数が指定されなければ、インターフェイスの *interface-type interface-number* 値が着信インターフェイスとして使用されます。

distance 引数により、reverse path forwarding (RPF) 検索に使用されるルート (ユニキャスト ルート、DVMRP ルート、またはスタティック mroute) が決定されます。距離が短いほど、優先順位は高くなります。スタティック mroute が他の 2 つの RPF 送信元と同じ距離である場合、スタティック mroute が優先されます。

例

次に、単一のインターフェイス（この場合はトンネル）からすべての送信元を設定する例を示します。

```
Router(config)# ip mroute 224.0.0.0 255.255.255.255 tunnel0
Router(config)#
```

次に、ネットワーク番号内の特定の送信元すべてが 172.30.10.13 経由で到達可能になるよう設定する例を示します。

```
Router(config)# ip mroute 172.16.0.0 255.255.0.0 172.30.10.13
Router(config)#
```

次に、任意で指定された宛先のユニキャスト ルートが削除された場合に、このマルチキャスト スタティック ルートを有効にする例を示します。

```
Router(config)# ip mroute 224.0.0.0 255.255.255.255 serial0 200
Router(config)#
```

ip msdp border

Protocol Independent Multicast sparse mode (PIM-SM; プロトコル独立マルチキャスト疎モード) リージョンと dense mode (PIM-DM; 密モード) リージョンの境界にあるルータで MSDP を使用するよう設定するには、**ip msdp border** コマンドを使用します。このアクションを防止するには、このコマンドの **no** 形式を使用します。

ip msdp [vrf vrf-name] border sa-address internet-type internet-number

no ip msdp [vrf vrf-name] border sa-address internet-type internet-number

シンタックスの説明

vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
sa-address	アクティブな送信元 IP アドレスを指定します。
internet-type internet-number	IP アドレスの取得元であり、 source-active メッセージ内のランデブーポイントアドレスとして使用されるインターフェイスタイプおよび番号

コマンドのデフォルト

dense (密) モード リージョンのアクティブな送信元は、MSDP に参加しません。

コマンドのデフォルト

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

PIM dense (密) モード リージョンでアクティブな送信元の **source-active** メッセージを MSDP ピアに送信する場合、このコマンドを使用します。

internet-type internet-number を指定すると、MSDP ピアはこの境界から **source-active** メッセージを転送できます。インターフェイスの IP アドレスは発信者 ID として使用されます。これは、MSDP **source-active** メッセージのランデブーポイント フィールドとなります。



(注)

sparse (疎) モード ドメインの境界ルータが dense (密) モード ドメイン内の送信元をプロキシ登録するように設定し、sparse (疎) モード ドメインが標準 MSDP 手順を使用してこれらの送信元をアドバタイズするよう設定することを推奨します。



(注)

このコマンドを使用する場合、**ip msdp redistribute** コマンドによりアドバタイズされる送信元を制限する必要があります。ローカルの送信元にだけ適用されるよう **ip msdp redistribute** コマンドを設定します。この設定の結果、dense (密) モード ドメインの送信元が送信を停止したあとも継続する (S,G) ステートとなることに留意してください。



(注)

ip msdp originator-id コマンドでは、ランデブー ポイント アドレスとして使用されるインターフェイス タイプおよび番号を識別します。**ip msdp border** および **ip msdp originator-id** コマンドの両方が設定されている場合、**ip msdp originator-id** コマンドが優先されます。**ip msdp originator-id** コマンドから取得されたアドレスが、ランデブー ポイントのアドレスを決定します。

例

この例では、ローカル ルータはランデブー ポイントではありません。ローカル ルータは、PIM sparse (疎) モード リージョンと dense (密) モード リージョンの境界にあり、イーサネット インターフェイス 0 の IP アドレスを source-active メッセージのランデブー ポイント アドレスとして使用します。

```
Router (config) # ip msdp border sa-address ethernet0
Router (config) #
```

関連コマンド

コマンド	説明
ip msdp originator-id	source-active メッセージを発信する MSDP スピーカーが、source-active メッセージのランデブー ポイント アドレスとしてインターフェイスの IP アドレスを使用できるようにします。
ip msdp redistribute	マルチキャスト ルーティング テーブルのどの (S,G) エントリが、MSDP ピアに発信される source-active メッセージでアドバタイズされるかを設定します。

ip msdp cache-sa-state

ルータで source-active ステートを作成するには、**ip msdp cache-sa-state** コマンドを使用します。

ip msdp cache-sa-state [vrf vrf-name]

シンタックスの説明

vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
---------------------	--

コマンドモード

ルータは、受信するすべての MSDP source-active メッセージに対して source-active ステートを作成します。

コマンドのデフォルト

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、少なくとも 1 つの MSDP ピアが設定されている場合に自動的に設定されます。このコマンドはディisableにできません。

例

次に、MSDP ピアが設定されたときに、**ip msdp cache-sa-state** コマンドがイネーブルとなる例を示します。MSDP の設定例の詳細については、『*Cisco IOS IP Configuration Guide*』Cisco IOS Release 12.2 の「Configuring Multicast Source Discovery Protocol」の章を参照してください。

```
.
.
.
Router(config)# ip classless
Router(config)# ip msdp peer 192.168.1.2 connect-source Loopback0
Router(config)# ip msdp peer 192.169.1.7
Router(config)# ip msdp mesh-group outside-test 192.168.1.2
Router(config)# ip msdp cache-sa-state
Router(config)# ip msdp originator-id Loopback0
.
.
.
```

関連コマンド

コマンド	説明
clear ip msdp sa-cache	MSDP ピアを設定します。
ip msdp filter-sa-request	ルータに source-active ステートを作成します。
show ip msdp sa-cache	MSDP ピアから学習した (S,G) 状態を表示します。

ip msdp default-peer

すべての MSDP source-active メッセージの受信元のデフォルト ピアを定義するには、**ip msdp default-peer** コマンドを使用します。デフォルト ピアを削除するには、このコマンドの **no** 形式を使用します。

```
ip msdp [vrf vrf-name] default-peer {peer-address | peer-name} [prefix-list list]
```

```
no ip msdp [vrf vrf-name] default-peer
```

シンタックスの説明	
vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
peer-address peer-name	MSDP のデフォルト ピアの IP アドレスまたは DNS 名
prefix-list list	(任意) BGP プレフィクス リストを指定します。

コマンド モード MSDP のデフォルト ピアは存在しません。

コマンドのデフォルト グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン 使用する MSDP ピアが BGP ピアにならないように設定する場合にも、**ip msdp default-peer** コマンドを使用します。

MSDP ピアが 1 つだけ設定されている場合 (**ip msdp peer** コマンドにより) は、これがデフォルト ピアとして使用されます。このコマンドを使用してデフォルト ピアを、設定する必要はありません。

prefix-list list キーワードおよび引数を指定しない場合、設定済みのデフォルト ピアから受信したすべての source-active メッセージが受け入れられます。

prefix-list list キーワードおよび引数により、このピアが **list** 引数で指定されたリストに表示されるプレフィクス専用のデフォルト ピアとなることが指定されます。この **prefix-list list** キーワードおよび引数を有効にするためには、BGP プレフィクス リストを設定する必要があります。

ip msdp default-peer コマンドで **prefix-list list** キーワードおよび引数を設定する場合は、BGP プレフィクス リストを設定する必要があります。

prefix-list list キーワードおよび引数を指定すると、**prefix-list list** キーワードおよび引数の対象となるランデブー ポイントから生成された source-active メッセージが、設定済みのデフォルト ピアから受信されます。**prefix-list list** キーワードおよび引数を指定しても、プレフィクス リストを設定しなければ、デフォルト ピアがすべてのプレフィクスに使用されます。

複数の **ip msdp default-peer** コマンドを **prefix-list** キーワードありで（またはなしで）入力できます。ただし、すべてのコマンドでキーワードを付加するかまたは付加しないかを定める必要があります。

- 複数の **ip msdp default-peer** コマンドに **prefix-list** キーワードを付加して使用する場合、すべてのデフォルトピアが異なるランデブーポイントプレフィクスに同時に使用されます。通常、この構文はスタブサイトを接続するサービスプロバイダークラウドで使用されます。
- 複数の **ip msdp default-peer** コマンドを **prefix-list** キーワードなしで使用する場合、単一のアクティブピアを使用してすべての **source-active** メッセージを受信します。このピアがダウンすると、次に設定されたデフォルトピアに移動してすべての **source-active** メッセージを受信します。通常、この構文はスタブサイトで使用されます。

例

次に、**router.cisco.com** という名前のルータをローカルルータに対するデフォルトピアとして設定する例を示します。

```
Router(config)# ip msdp peer 192.168.1.2
Router(config)# ip msdp peer 192.168.1.3
Router(config)# ip msdp default-peer router.cisco.com    !At a stub site
```

次に、IP アドレス **192.168.1.3** のルータをローカルルータのデフォルトピアとして設定する例を示します。

```
Router(config)# ip msdp peer 192.168.1.3
Router(config)# ip msdp peer 192.168.3.5
Router(config)# ip msdp default-peer 192.168.1.3
```

次に、2 つのデフォルトピアを設定する例を示します。

```
Router(config)# ip msdp peer 172.18.2.3
Router(config)# ip msdp peer 172.19.3.5
Router(config)# ip msdp default-peer 172.18.2.3 prefix-list site-c
Router(config)# ip prefix-list site-a permit 172.18.0.0/16
Router(config)# ip msdp default-peer 172.19.3.5 prefix-list site-a
Router(config)# ip prefix-list site-c permit 172.19.0.0/16
```

関連コマンド

コマンド	説明
ip msdp peer	MSDP ピアを設定します。
ip prefix-list	プレフィクスリストにエントリを作成します。

ip msdp description

MSDP ピアの設定に説明文を追加するには、**ip msdp description** コマンドを使用します。説明文を削除するには、このコマンドの **no** 形式を使用します。

```
ip msdp [vrf vrf-name] description {peer-name | peer-address} text
```

```
no ip msdp [vrf vrf-name] description {peer-name | peer-address}
```

シンタックスの説明		
<i>vrf vrf-name</i>	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。	
<i>peer-name</i> <i>peer-address</i>	この説明を適用するピアの名前およびアドレス	
<i>text</i>	MSDP ピアの説明	

コマンド モード MSDP ピアに説明文は関連付けられていません。

コマンドのデフォルト グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン MSDP ピアを識別しやすくするために、説明を設定します。この説明は、**show ip msdp peer** コマンドの出力に表示されます。

例 次に、IP アドレス 224.107.5.4 のルータにカスタマー A のルータであることを示す説明を付加する例を示します。

```
Router(config)# ip msdp description 224.107.5.4 router at customer a  
Router(config)#
```

関連コマンド	コマンド	説明
	show ip msdp peer	MSDP ピアに関する詳細情報を表示します。

ip msdp filter-sa-request

グループからの新規加入者がアクティブになった場合に、ルータが MSDP ピアに source-active 要求メッセージを送信するよう設定するには、**ip msdp filter-sa-request** コマンドを使用します。このアクションを防止するには、このコマンドの **no** 形式を使用します。

```
ip msdp [vrf vrf-name] filter-sa-request {peer-address | peer-name} [list access-list]
```

```
no ip msdp [vrf vrf-name] filter-sa-request {peer-address | peer-name}
```

シンタックスの説明

vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
peer-address	グループの新規加入者がアクティブになった場合に、ローカルルータが source-active メッセージを要求する MSDP ピアの IP アドレス
peer-name	グループの新規加入者がアクティブになった場合に、ローカルルータが source-active メッセージを要求する MSDP ピアの名前
list access-list	(任意) マルチキャスト グループ アドレスを説明する標準 IP アクセスリストの番号または名前を指定します。

コマンドモード

このコマンドが設定されていない場合、すべての source-active 要求メッセージが認識されます。このコマンドが設定されてもアクセス リストが指定されない場合、すべての source-active 要求メッセージは無視されます。

コマンドのデフォルト

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

デフォルトでは、ルータはピアからのすべての source-active 要求メッセージを認識します。ルータがどの source-active 要求メッセージを認識するかを制御する場合は、このコマンドを使用します。

アクセス リストが指定されなければ、すべての source-active 要求メッセージが無視されます。アクセス リストが指定された場合、許可されたグループからの source-active 要求メッセージだけが認識され、他のすべての source-active 要求メッセージは無視されます。

例

次に、172.16.2.2 の MSDP ピアからの source-active 要求メッセージをフィルタリングするようにルータを設定する例を示します。この例では、ネットワーク 192.168.22.0 の送信元からの source-active 要求メッセージが、アクセス リスト 1 を通過して認識されます。その他の source-active 要求メッセージはすべて無視されます。

```
Router(config)# ip msdp filter sa-request 224.69.2.2 list 1  
access-list 1 permit 228.4.22.0 0.0.0.255
```

関連コマンド

コマンド	説明
ip msdp peer	MSDP ピアを設定します。

ip msdp mesh-group

MSDP ピアがメッシュ グループのメンバーとなるよう設定するには、**ip msdp mesh-group** コマンドを使用します。メッシュ グループから MSDP ピアを削除するには、このコマンドの **no** 形式を使用します。

```
ip msdp [vrf vrf-name] mesh-group mesh-name {peer-address | peer-name}
```

```
no ip msdp [vrf vrf-name] mesh-group mesh-name {peer-address | peer-name}
```

シンタックスの説明

<i>vrf vrf-name</i>	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
<i>mesh-name</i>	メッシュ グループ名
<i>peer-address</i> <i>peer-name</i>	メッシュ グループのメンバーとなる MSDP ピアの IP アドレスまたは名前

コマンド モード

MSDP ピアは、メッシュ グループに属しません。

コマンドのデフォルト

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

メッシュ グループとは、MSDP スピーカー間の MSDP 接続が完全にメッシュ化されている MSDP スピーカーのグループです。メッシュ グループ内のピアから受信した **source-active** メッセージは、同じメッシュ グループ内の他のピアには転送されません。

メッシュ グループは、次の 2 つの目的に使用されます。

- **source-active** メッセージ フラッディングの軽減
- ピアの RPF フラッディングの簡略化 (MSDP ピア間で BGP またはマルチプロトコル BGP を実行する必要がなくなります)

例

次に、アドレス 224.1.1.1 の MSDP ピアが **internal** という名前のメッシュ グループのメンバーとなるよう設定する例を示します。

```
Router(config)# ip msdp mesh-group internal 224.1.1.1
Router(config)#
```

ip msdp originator-id

source-active メッセージを生成する MSDP スピーカーが、インターフェイスの IP アドレスを source-active メッセージのランデブー ポイントアドレスとして使用できるよう設定するには、**ip msdp originator-id** コマンドを使用します。この方法でランデブー ポイントアドレスが取得されることを防止するには、このコマンドの **no** 形式を使用します。

ip msdp [vrf vrf-name] originator-id interface-type interface-number

no ip msdp [vrf vrf-name] originator-id interface-type interface-number

シンタックスの説明	
vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
interface-type	その IP アドレスが source-active メッセージのランデブー ポイント
interface-number	アドレスとして使用されるローカルルータのインターフェイス タイプおよび番号

コマンド モード ランデブー ポイント アドレスは、発信者 ID として使用されます。

コマンドのデフォルト グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン **ip msdp originator-id** コマンドにより、source-active メッセージのランデブー ポイント アドレスとして使用されるインターフェイスのタイプおよび番号が識別されます。

論理ランデブー ポイントを設定する場合は、このコマンドを使用します。ランデブー ポイントおよび MSDP 境界ルータだけが source-active メッセージを生成するため、この目的に使用される ID を変更する必要があります。

ip msdp border sa-address コマンドおよび **ip msdp originator-id** コマンドの両方が設定されている場合、**ip msdp originator-id** コマンドが優先されます。**ip msdp originator-id** コマンドから取得されたアドレスにより、source-active メッセージで使用されるランデブー ポイントのアドレスが決定されます。

例 次に、イーサネット インターフェイス 1 の IP アドレスを source-active メッセージ内のランデブー ポイント アドレスとして設定する例を示します。

```
Router(config)# ip msdp originator-id ethernet1
Router(config)#
```

■ ip msdp originator-id

関連コマンド

コマンド	説明
ip msdp border	PIM sparse (疎) モードリージョンと dense (密) モードリージョンの境界にあるルータで MSDP を使用するよう設定します。

ip msdp peer

MSDP ピアを設定するには、**ip msdp peer** コマンドを使用します。ピア関係を削除するには、このコマンドの **no** 形式を使用します。

```
ip msdp [vrf vrf-name] peer {peer-name | peer-address} [connect-source interface-type
interface-number] [remote-as as-number]
```

```
no ip msdp [vrf vrf-name] peer {peer-name | peer-address}
```

シンタックスの説明	
vrf <i>vrf-name</i>	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
<i>peer-name</i> <i>peer-address</i>	MSDP ピアとなるルータの DNS 名または IP アドレス
connect-source <i>interface-type</i> <i>interface-number</i>	(任意) プライマリ アドレスが TCP 接続の送信元 IP アドレスとなるインターフェイスのタイプおよび番号を指定します。
remote-as <i>as-number</i>	(任意) MSDP ピアの自律システム番号を指定します。

コマンド モード MSDP ピアは設定されていません。

コマンドのデフォルト グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン 指定されたルータは、BGP ネイバとしても設定される必要があります。

interface-type は、設定されるルータ上にあります。

この MSDP ピアとともに BGP ピアリングも使用する場合、BGP に使用した IP アドレスと同じアドレスを MSDP に使用する必要があります。ただし、MSDP ピア間に BGP または MBGP パスがある場合は、MSDP ピアとともに BGP または MBGP を実行する必要はありません。パスがない場合は、**ipmsdp default-peer** コマンドを設定する必要があります。

remote-as *as-number* キーワードおよび引数は、表示目的だけに使用されます。

あるピアで MSDP ピアリングセッションはあり BGP ピアセッションがない場合、このピアが他の AS (実際とは異なる) に存在するように表示される場合があります。この場合、他の AS により投入されたピアのプレフィクスは、ピアの AS 番号のように表示されます。

例 次に、IP アドレス 224.108.1.2 のルータをローカル ルータに対する MSDP ピアとして設定する例を示します。ネイバは、AS 109 に属しています。

```
Router(config)# ip msdp peer 224.108.1.2 connect-source ethernet 0
router bgp 110
  network 224.108.0.0
  neighbor 224.108.1.2 remote-as 109
```

■ ip msdp peer

```
neighbor 224.108.1.2 update-source ethernet 0
```

次に、router.cisco.com という名前のルータをローカル ルータに対する MSDP ピアとして設定する例を示します。

```
Router(config)# ip msdp peer router.cisco.com  
Router(config)#
```

次に、router.cisco.com という名前のルータが AS 109 の MSDP ピアとなるよう設定する例を示します。イーサネット インターフェイス 0 のプライマリ アドレスは、TCP 接続の送信元アドレスとして使用されます。

```
Router(config)# ip msdp peer router.cisco.com connect-source ethernet0 remote-as 109  
Router(config)#
```

関連コマンド

コマンド	説明
neighbor remote-as	BGP またはマルチプロトコル BGP ネイバテーブルにエントリを追加します。

ip msdp redistribute

MSDP ピアに対して生成される `source-active` メッセージでアドバタイズされるマルチキャスト ルーティング テーブルからのエントリ (S,G) を設定するには、**ip msdp redistribute** コマンドを使用します。フィルタを削除するには、このコマンドの **no** 形式を使用します。

```
ip msdp [vrf vrf-name] redistribute [list access-list-name] [asn as-access-list-number]
[route-map map-name]
```

```
no ip msdp [vrf vrf-name] redistribute
```

シンタックスの説明

<i>vrf vrf-name</i>	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
<i>list access-list-name</i>	(任意) アドバタイズされるローカルの送信元およびこの送信元の送信先グループを制御する標準/拡張 IP アクセスリストの番号、または名前を指定します。
<i>asn as-access-list-number</i>	(任意) 標準/拡張 IP アクセスリスト番号を指定します。有効値は、1 ~ 199 です。
<i>route-map map-name</i>	(任意) ルート マップ名を指定します。

コマンド モード

デフォルト設定は次のとおりです。

- このコマンドがまったく設定されていない場合、ルータがランデブー ポイントであるグループに送信するローカルの送信元だけがアドバタイズされます。
- このコマンドがまったく設定されていない場合で、**ip msdp border sa-address** コマンドが設定されていると、すべてのローカルの送信元がアドバタイズされます。
- ip msdp redistribute** コマンドがキーワードなしで設定されている場合、マルチキャスト送信元はアドバタイズされません。

コマンドのデフォルト

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ip as-path コマンドでは *as-access-list-number* 引数を設定する必要があります。

このコマンドは `source-active` メッセージの転送ではなく、`source-active` メッセージの生成に影響します。MSDP ピアに転送される `source-active` メッセージをフィルタリングする場合、**ip msdp sa-filter in** または **ip msdp sa-filter out** コマンドを使用します。

ip msdp redistribute

ip msdp redistribute コマンドは、ルータがマルチキャストルーティングテーブルからアドバタイズする (S,G) ペアを制御します。デフォルトでは、ローカルドメイン内の送信元だけがアドバタイズされます。**ip msdp redistribute** コマンドについては、次の注意事項に従ってください。

- **list access-list-name** キーワードおよび引数だけを指定すると、アドバタイズされるローカルの送信元およびアドバタイズを送信されるグループがフィルタリングされます。アクセスリストにより、送信元アドレス、送信元マスク、グループアドレス、およびグループマスクが指定されます。
- **asn as-access-list-number** キーワードおよび引数だけを指定すると、自律システムパスアクセスリストを通過する任意のグループに送信するすべての送信元がアドバタイズされます。AS パスアクセスリスト番号とは、アクセスリストを指定する **ip as-path** コマンドを指します。**asn 0** キーワードを指定すると、すべての AS からの送信元がアドバタイズされます。**asn 0** キーワードは、dense (密) モードドメインが MSDP を実行する sparse (疎) モードドメインと接続する場合、または BGP が設定されていないルータで MSDP を使用する場合に役立ちます。この場合、送信元がローカルであるかどうか識別できません。
- **route-map map-name** キーワードおよび引数だけを指定する場合、ルートマップの **map-name** 引数の一致基準を満たすすべての送信元がアドバタイズされます。
- 3 つのすべてのキーワード (**list**、**asn**、および **route-map**) を指定する場合、任意のマルチキャスト送信元が source-active メッセージでアドバタイズされるには、すべての条件が当てはまる必要があります。
- **ip multicast redistribute** コマンドを他のキーワードまたは引数なしで指定する場合、マルチキャスト送信元はアドバタイズされません。

例

次に、MSDP ピアに対して生成される source-active メッセージ内でアドバタイズされるマルチキャストルーティングテーブルのエントリ (S,G) を設定する例を示します。

```
Router(config)# ip msdp redistribute route-map customer-sources

route-map customer-sources permit
match as-path customer-as

Router(config)# ip as-path access-list ^109$
```

関連コマンド

コマンド	説明
ip as-path	BGP AS パスアクセスリストを定義します。
ip msdp border	PIM sparse (疎) モードリージョンと dense (密) モードリージョンの境界にあるルータで MSDP を使用するよう設定します。

ip msdp sa-filter in

指定された MSDP ピアから受信した source-active メッセージの着信フィルタ リストを設定するには、**ip msdp sa-filter in** コマンドを使用します。フィルタを削除するには、このコマンドの **no** 形式を使用します。

```
ip msdp [vrf vrf-name] sa-filter in {peer-address | peer-name} [list access-list-name]
[route-map map-name]
```

```
no ip msdp [vrf vrf-name] sa-filter in {peer-address | peer-name} [list access-list-name]
[route-map map-name]
```

シンタックスの説明

vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
peer-address peer-name	source-active メッセージがフィルタリングされる MSDP ピアの IP アドレスまたは名前
list access-list-name	(任意) IP アクセスリストの番号または名前を指定します。
route-map map-name	(任意) ルート マップ名を指定します。

コマンド モード

デフォルト設定は次のとおりです。

- このコマンドが設定されていない場合、着信メッセージはフィルタリングされません。ピアからのすべての source-active メッセージが受け入れられます。
- このコマンドは設定されるが、アクセス リストまたはルート マップが指定されない場合、ピアからのすべての送信元/グループのペアがフィルタリングされます。
- **list** および **route-map** キーワードの両方が使用された場合、着信 source-active メッセージ内の任意の (S,G) ペアが通過するためには、すべての条件に当てはまる必要があります。

コマンドのデフォルト

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

access-list-name を指定しない場合、ピアからのすべての送信元/グループのペアがフィルタリングされます。

指定された MSDP ピアは、ルート マップの **map-name** 引数の一致基準を満たす source-active メッセージだけを通過させます。

すべての一致基準に当てはまる場合、ルート マップの **permit** キーワードがフィルタを通してルートを通過します。ルートをフィルタリングするには、**deny** キーワードを使用します。

■ ip msdp sa-filter in

例

次に、router.cisco.com という名前のピアからのすべての source-active メッセージをフィルタリングするようにルータを設定する例を示します。

```
Router(config)# ip msdp peer router.cisco.com connect-source ethernet 0
Router(config)# ip msdp sa-filter in router.cisco.com
Router(config)#
```

関連コマンド

コマンド	説明
ip msdp peer	MSDP ピアを設定します。
ip msdp sa-filter out	指定の MSDP ピアに送信される source-active メッセージの送信フィルタリストを設定します。

ip msdp sa-filter out

指定された MSDP ピアに送信される source-active メッセージの送信フィルタ リストを設定するには、**ip msdp sa-filter out** コマンドを使用します。フィルタを削除するには、このコマンドの **no** 形式を使用します。

```
ip msdp [vrf vrf-name] sa-filter out {peer-address | peer-name} [list access-list-name]
[route-map map-name]
```

```
no ip msdp [vrf vrf-name] sa-filter out {peer-address | peer-name} [list access-list-name]
[route-map map-name]
```

シンタックスの説明

vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
peer-address peer-name	source-active メッセージがフィルタリングされる MSDP ピアの IP アドレスまたは DNS 名
list access-list	(任意) 拡張 IP アクセスリストの番号または名前を指定します。
route-map map-name	(任意) ルート マップ名を指定します。

コマンド モード

デフォルト設定は次のとおりです。

- このコマンドが設定されていない場合、送信メッセージはフィルタリングされません。受信されるすべての source-active メッセージはピアに転送されます。
- このコマンドは設定されるが、アクセス リストまたはルート マップが指定されない場合、すべての送信元/グループのペアがフィルタリングされます。
- **list** および **route-map** キーワードの両方が使用された場合、送信 source-active メッセージ内の任意の (S,G) ペアが通過するためには、すべての条件に当てはまる必要があります。

コマンドのデフォルト

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

access-list を指定しない場合、すべての送信元/グループのペアがフィルタリングされます。指定された MSDP ペアは、拡張アクセス リストを通過する source-active メッセージだけを通過させます。

list および **route-map** キーワードの両方が使用された場合、送信 source-active メッセージ内の任意の (S,G) ペアが通過するためには、すべての条件に当てはまる必要があります。

指定された MSDP ピアに対して、ルート マップの **map-name** 引数の一致基準を満たす source-active メッセージだけが通されます。

すべての一致基準に当てはまる場合、ルート マップの **permit** キーワードがフィルタを通してルートを通します。ルートをフィルタリングするには、**deny** キーワードを使用します。

■ ip msdp sa-filter out

例

次に、アクセスリスト 100 を通過する (S,G) ペアだけが source-active メッセージ内で router.cisco.com という名前のピアに転送できるようにする例を示します。

```
Router(config)# ip msdp peer router.cisco.com connect-source ethernet 0
Router(config)# ip msdp sa-filter out router.cisco.com list 100
access-list 100 permit ip 224.69.0.0 0.0.255.255 224.2.0.0 0.0.255.255
```

関連コマンド

コマンド	説明
ip msdp peer	MSDP ピアを設定します。
ip msdp sa-filter in	指定の MSDP ピアから受信する source-active メッセージの着信フィルタリストを設定します。

ip msdp sa-request

グループからの新規加入者がアクティブになった場合に、ルータが MSDP ピアに source-active 要求メッセージを送信するよう設定するには、**ip msdp sa-request** コマンドを使用します。このアクションを防止するには、このコマンドの **no** 形式を使用します。

```
ip msdp [vrf vrf-name] sa-request {peer-address | peer-name}
```

```
no ip msdp [vrf vrf-name] sa-request {peer-address | peer-name}
```

シンタックスの説明	vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
	peer-address peer-name	グループの新規加入者がアクティブになった場合に、ローカル ルータが source-active メッセージを要求する MSDP ピアの IP アドレスまたは名前

コマンド モード source-active 要求メッセージは、MSDP ピアに送信されません。

コマンドのデフォルト グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン デフォルトでは、グループに加入した新規メンバーがマルチキャストトラフィックを受信しようと、source-active 要求メッセージは MSDP ピアに送信されません。新規メンバーは、最終的に到達する任意の source-active メッセージの受信を待機します。

グループに送信する接続された PIM-SM ドメイン内の現在のアクティブ マルチキャスト送信元を、グループの新メンバーに学習させる場合は、このコマンドを使用します。新メンバーがグループに加入すると、source-active 要求メッセージが指定された MSDP ピアに送信されます。ピアは、source-active キャッシュ内の情報により応答します。ピアでキャッシュが設定されていない場合、このコマンドは機能しません。

ルータ キャッシュ メッセージを受け取る場合には、**ip msdp cache-sa-state** コマンドも使用できます。

例 次に、source-active 要求メッセージを 224.69.1.1 の MSDP ピアに送信するようルータを設定する例を示します。

```
Router(config)# ip msdp sa-request 224.69.1.1
Router(config)#
```

■ ip msdp sa-request

関連コマンド

コマンド	説明
ip msdp cache-sa-state	ルータに source-active ステートを作成します。
ip msdp peer	MSDP ピアを設定します。

ip msdp shutdown

設定済みの MSDP ピアを管理上シャットダウンするには、**ip msdp shutdown** コマンドを使用します。ピアをアップに戻すには、このコマンドの **no** 形式を使用します。

```
ip msdp [vrf vrf-name] shutdown {peer-address | peer-name}
```

```
no ip msdp [vrf vrf-name] shutdown {peer-address | peer-name}
```

シンタックスの説明	vrf <i>vrf-name</i>	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
	<i>peer-address</i> <i>peer-name</i>	シャットダウンする MSDP ピアの IP アドレスまたは名前

コマンドモード MSDP ピアをシャットダウンするアクションは実行されません。

コマンドのデフォルト グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、IP アドレス 224.5.7.20 の MSDP ピアをシャットダウンする例を示します。

```
Router(config)# ip msdp shutdown 224.5.7.20  
Router(config)#
```

関連コマンド	コマンド	説明
	ip msdp peer	MSDP ピアを設定します。

ip msdp ttl-threshold

MSDP ピアに送信される source-active メッセージ内のマルチキャスト データ パケットを制限するには、**ip msdp ttl-threshold** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

```
ip msdp [vrf vrf-name] ttl-threshold {peer-address | peer-name} ttl-value
```

```
no ip msdp [vrf vrf-name] ttl-threshold {peer-address | peer-name}
```

シンタックスの説明

vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
peer-address peer-name	ttl-value 引数を適用する MSDP ピアの IP アドレスまたは名前
ttl-value	Time to Live (TTL; 存続可能時間) 値。有効値は、0 ~ 255 です。

コマンドのデフォルト

ttl-value は **0** です。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、データがカプセル化された source-active メッセージ内のマルチキャスト データ パケットを制限します。IP ヘッダーの TTL が **ttl-value** 引数以上であるマルチキャスト パケットだけが、IP アドレスまたは名前により指定された MSDP ピアに送信されます。

TTL によりマルチキャスト データ トラフィックを制限する場合、このコマンドを使用します。たとえば、内部トラフィックの TTL を 8 に制限したとします。他のグループを外部に設定する場合、これらのパケットの TTL は 9 以上で送信する必要があります。

ttl-value 引数のデフォルト値は、**0** です。これは TTL が尽きるまで、すべてのマルチキャスト データ パケットがピアに転送されることを意味します。

例

次に、TTL しきい値を 8 ホップに設定する例を示します。

```
Router(config)# ip msdp ttl-threshold 224.5.7.20 8
Router(config)#
```

関連コマンド

コマンド	説明
ip msdp peer	MSDP ピアを設定します。

ip multicast boundary

管理用スコープの境界を設定するには、**ip multicast boundary** コマンドを使用します。境界を削除するには、このコマンドの **no** 形式を使用します。

ip multicast boundary access-list [filter-autorp]

no ip multicast boundary access-list [filter-autorp]

シンタックスの説明	説明
<i>access-list</i>	境界によって影響されたグループ アドレスの範囲を制御するアクセス リストを識別する番号または名前
<i>filter-autorp</i>	(任意) 境界 ACL によって拒否された自動 RP メッセージをフィルタリングします。

コマンドのデフォルト 境界はありません。

コマンド モード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン *access-list* 引数で定義された範囲のマルチキャスト グループ アドレスをフィルタリングするには、このコマンドを使用して、管理用スコープの境界をインターフェイスに設定します。標準のアクセス リストは、影響されたアドレスの範囲を定義します。このコマンドを設定すると、マルチキャスト データ パケットはどの方向からもインターフェイスに流れることができなくなります。マルチキャスト データ パケットのフローを制限することによって、異なる管理ドメインで同じマルチキャスト グループのアドレスを再利用できます。



(注) 拡張アクセス リストは、**filter-autorp** キーワードまたは **no** キーワードを使用している場合は使用できません。

filter-autorp キーワードを設定すると、管理用スコープの境界は Auto-RP 検出およびアナウンスメント メッセージも調べて、境界 ACL によって拒否された Auto-RP パケットから Auto-RP グループ範囲のアナウンスメントを削除します。Auto-RP グループ範囲のすべてのアドレスが境界 ACL によって許可された場合、Auto-RP グループ範囲のアナウンスメントは許可され、その境界だけを通過します。アドレスが許可されなかった場合、Auto-RP メッセージが転送される前に、グループ範囲全体がフィルタリングされ、Auto-RP メッセージから削除されます。

ip multicast boundary コマンドを入力する場合は、次の注意事項に従ってください。

- **filter-autorp** キーワードまたは **no** キーワードを使用する場合、標準のアクセス リストだけが許可されます。
- コマンドのすべてのインスタンスは、制御トラフィックおよびデータ プレーン トラフィックの両方に適用されます。

ip multicast boundary

- 拡張アクセス リストのプロトコル情報は解析され、IOS 一貫性の再利用とフィルタリングが許可されます。アクセス リストがすべてのプロトコルの (S,G) トラフィックをフィルタリングする場合、(S,G) オペレーションは、キーワードについて記述されたすべての条件で拡張アクセス リストによってフィルタリングされます。

例

次に、管理用スコープのアドレスに対する境界を設定する例を示します。

```
Router(config-if)# ip multicast boundary 1
Router(config-if)#
```

次に、拡張 ACL の境界を設定する例を示します。

```
Router(config-if)# ip multicast boundary 101
Router(config-if)#
```

次に、境界 ACL によって拒否された自動 RP メッセージをフィルタリングする例を示します。

```
Router(config-if)# ip multicast boundary acc_grp10 filter-autorp
Router(config-if)#
```

関連コマンド

コマンド	説明
access-list (IP 標準)	標準 IP アクセス リストを定義します。

ip multicast cache-headers

ルータが受信する IP マルチキャスト パケット ヘッダーを格納するために循環バッファを割り当てるには、**ip multicast cache-headers** コマンドを使用します。バッファを削除するには、このコマンドの **no** 形式を使用します。

ip multicast [vrf vrf-name] cache-headers [rtp]

no ip multicast [vrf vrf-name] cache-headers

シンタックスの説明	パラメータ	説明
vrf vrf-name	(任意)	マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
rtp	(任意)	Real-Time Transport Protocol (RTP) ヘッダーをキャッシュします。

コマンドのデフォルト デイセーブル

コマンドモード グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン 次の情報を決定する場合、IP マルチキャスト パケット ヘッダーをキャッシュに格納し、表示します。

- IP マルチキャスト パケットの送信者と送信先グループ
- パケット内遅延
- IP マルチキャスト パケットの複製 (存在する場合)
- ネットワーク内のマルチキャスト転送ループ (存在する場合)
- グループのサイズ
- UDP ポート番号
- パケット長



(注) このコマンドにより、約 32 KB の循環バッファが割り当てられます。メモリが不足している場合は、このコマンドを設定しないでください。

バッファを表示するには、**show ip mpacket** コマンドを使用します。

例 次に、IP マルチキャスト パケット ヘッダーを格納するバッファを割り当てる例を示します。

```
Router(config)# ip multicast cache-headers
Router(config)#
```

■ ip multicast cache-headers

関連コマンド

コマンド	説明
show ip mpacket	循環キャッシュヘッダー バッファの内容を表示します。

ip multicast helper-map

2つのブロードキャスト専用インターネットワーク間のマルチキャスト対応インターネットワークにおいて IP マルチキャストルーティングを許可するには、**ip multicast helper-map** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip multicast helper-map broadcast *multicast-address access-list* [ttl *x*]

no ip multicast helper-map broadcast *multicast-address access-list*

シンタックスの説明

broadcast	トラフィックがブロードキャストからマルチキャストに変換されることを指定します。このキーワードは <i>multicast-address</i> 引数と併用してください。
<i>multicast-address</i>	変換済みトラフィックの転送先となる IP マルチキャストアドレス。この引数は broadcast キーワードと併用してください。
<i>access-list</i>	UDP ポート番号に基づき、どのブロードキャストパケットを変換するかを制御する IP 拡張アクセスリストの番号または名前。
ttl <i>x</i>	(任意) TTL が 1 であるパケットを変換し、TTL をリセットします。有効値は 1 ~ 50 です。

コマンドのデフォルト

ブロードキャストとマルチキャストの間で変換は行われません。

コマンドモード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

マルチキャスト対応インターネットワークが 2 つのブロードキャスト専用インターネットワークの間にある場合は、最初のホップのルータでブロードキャストトラフィックをマルチキャストに変換し、最終ホップルータでブロードキャストに変換しなおしてから、ブロードキャストクライアントにパケットを配信できます。しかし IP 送信元アドレスが 0.0.0.0 であるブロードキャストパケット (DHCP 要求など) は、マルチキャストグループに変換されません。

転送されたブロードキャストをサブネットに送信する場合は、IP ブロードキャストアドレスを x.x.x.255 にして最終ホップルータの発信インターフェイスを設定できます。x.x.x.0 は、到達しようとしているサブネットです。その他の場合、パケットは 255.255.255.255 に変換されます。

ip multicast helper-map コマンドで **ttl** キーワードを使用しない場合、TTL が 1 であるブロードキャストパケットはコマンドで変換されません。

■ ip multicast helper-map

例

次に、2 つのブロードキャスト専用インターネットワーク間のマルチキャスト対応インターネットワークで IP マルチキャストルーティングを可能にする例を示します。

```
Router(config-if)# ip multicast helper-map broadcast 224.5.5.5 120 ttl 2
Router(config-if)#
```

関連コマンド

コマンド	説明
ip directed-broadcast	転送ブロードキャストから物理ブロードキャストへの変換をイネーブルにします。
ip forward-protocol turbo-flood	スパニングツリーアルゴリズムを使用し、UDP パケットのフラッディングを高速化します。

ip multicast mrinfo-filter

multicast router information (mrinfo; マルチキャストルータ情報) 要求パケットをフィルタリングするには、**ip multicast mrinfo-filter** コマンドを使用します。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ip multicast mrinfo-filter access-list
```

```
no ip multicast mrinfo-filter access-list
```

シンタックスの説明	<i>access-list</i>	フィルタリングされる送信元 IP アドレスのアクセス リスト
-----------	--------------------	--------------------------------

コマンド モード	このコマンドにはデフォルト設定がありません。
----------	------------------------

コマンド モード	グローバル コンフィギュレーション (config) (config)
----------	-------------------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン	ip multicast mrinfo-filter コマンドは、指定されたアクセス リスト内のすべての送信元の mrinfo 要求パケットをフィルタリングします。
------------	---

例	次に、mrinfo 要求パケットがアクセスリスト No.4 に表示されたすべての送信元用にフィルタリングされる例を示します。
---	--

```
Router(config)# ip multicast mrinfo-filter 4
Router(config)#
```

ip multicast multipath

複数の等価コストパス間で IP マルチキャストトラフィックの負荷を分割するには、**ip multicast multipath** コマンドを使用します。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip multicast [vrf vrf-name] multipath

no ip multicast [vrf vrf-name] multipath

シンタックスの説明

vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
---------------------	--

コマンドのデフォルト

複数の等価コストパスが存在する場合、マルチキャストトラフィックはこれらのパス間で分割されません。

コマンドのデフォルト

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ip multicast multipath コマンドを入力し、複数の等価コストパスがネットワークに存在する場合、異なる送信元から同じマルチキャストグループへのマルチキャストトラフィックの等価コストパス間では、負荷分割が行われますが、同じ送信元から異なるマルチキャストグループへのトラフィックの場合には行われません。このコマンドにより RPF ネイバの選択方法が変更されるため、冗長トポロジー内のすべてのルータ上の等価コストパス間では常に IP マルチキャストトラフィックの負荷を分割して、ループを回避する必要があります。

例

次に、複数の等価コストパス間で IP マルチキャストトラフィックの負荷を分割する例を示します。

```
Router(config)# ip multicast multipath
Router(config)#
```

関連コマンド

コマンド	説明
show ip rpf	誘発型 RPF 統計を表示します。

ip multicast netflow

マルチキャスト出力または入力の NetFlow アカウンティングをインターフェイスでイネーブルにするには、**ip multicast netflow** コマンドを使用します。マルチキャスト NetFlow アカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip multicast netflow {egress | ingress}

no ip multicast netflow {egress | ingress}

シンタックスの説明

egress	マルチキャスト出力 NetFlow アカウンティングを指定します。
ingress	マルチキャスト入力 NetFlow アカウンティングを指定します。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- マルチキャスト出力 NetFlow アカウンティングはディセーブルです。
- マルチキャスト入力 NetFlow アカウンティングはイネーブルです。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

show running-config コマンドの出力では、マルチキャスト入力アカウンティングがイネーブルであることが示されませんが、マルチキャスト入力 NetFlow アカウンティングがディセーブルであることは示されます。

発信マルチキャスト ストリームをカウントするすべてのインターフェイスで、マルチキャスト出力 NetFlow アカウンティングをイネーブルにする必要があります。

マルチキャスト エントリを表示するには、**show mls netflow ip** コマンドを入力します。

例

次に、入力イーサネット 1/0 インターフェイスでマルチキャスト入力 NetFlow アカウンティングをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# interface ethernet 1/0
Router(config-if)# ip multicast netflow ingress
Router(config-if)# end
```

関連コマンド

コマンド	説明
ip multicast netflow rpf-failure	RPF チェックで不合格になるマルチキャストデータの NetFlow アカウンティングをイネーブルにします。
show ip flow interfaces	インターフェイスの NetFlow アカウンティング設定を表示します。

ip multicast route-limit

マルチキャスト ルーティング テーブルに追加できるマルチキャスト ルート (mroute) 数を制限するには、**ip multicast route-limit** コマンドを使用します。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ip multicast [vrf vrf-name] route-limit limit [threshold]
```

```
no ip multicast [vrf vrf-name] route-limit limit [threshold]
```

シンタックスの説明

<i>vrf vrf-name</i>	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
<i>limit</i>	追加できる mroute 数。有効値は 1 ~ 2,147,483,647 です。
<i>threshold</i>	(任意) 警告メッセージの原因となる mroute 数。有効値は 1 ~ 2,147,483,647 です。

コマンドモード

limit は 2,147,483,647 です。

コマンドモード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ip multicast route-limit コマンドにより、ルータに追加されるマルチキャスト ルート数が制限され、この制限を超えた場合にはエラー メッセージが生成されます。*threshold* 引数を設定した場合は、しきい値を超えた場合にしきい値エラー メッセージが生成されます。このメッセージは、mroute 数が *limit* 引数により設定された限度に達するまで継続して表示されます。

mroute 警告 *threshold* は、mroute *limit* を超過できません。

例

次に、cisco という名前の VRF インスタンスに mroute 限度を 200,000 に、しきい値を 20,000 に設定する例を示します。

```
Router(config)# ip multicast vrf cisco route-limit 200000 20000
Router(config)#
```

ip multicast-routing

IP マルチキャストルーティングをイネーブルにするには、**ip multicast-routing** コマンドを使用します。IP マルチキャストルーティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip multicast-routing [vrf vrf-name] [distributed]

no ip multicast-routing [vrf vrf-name]

シンタックスの説明	説明
vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
distributed	(任意) multicast distributed switching (MDS; マルチキャスト配信スイッチング) をイネーブルにします。

コマンドのデフォルト このコマンドはディセーブルです。

コマンドのデフォルト グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン IP マルチキャストルーティングがディセーブルの場合、マルチキャストパケットは転送されません。

例 次に、IP マルチキャストルーティングをイネーブルにする例を示します。

```
Router(config)# ip multicast-routing
Router(config)#
```

次に、特定の VRF で IP マルチキャストルーティングをイネーブルにする例を示します。

```
Router(config)# ip multicast-routing vrf vrf1
Router(config)#
```

次に、IP マルチキャストルーティングをディセーブルにする例を示します。

```
Router(config)# no ip multicast-routing
Router(config)#
```

関連コマンド	コマンド	説明
	ip pim	インターフェイス上の PIM をイネーブルにします。

ip multicast rpf backoff

PIM バックオフ インターバルを設定するには、**ip multicast rpf backoff** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip multicast rpf backoff *{min max}* | **disable**

no ip multicast rpf backoff

シンタックスの説明

<i>min</i>	初期 RPF バックオフ遅延時間 (ミリ秒単位)。指定できる値は、1 ~ 65,535 ミリ秒です。
<i>max</i>	最大 RPF 遅延時間 (ミリ秒単位)。指定できる値は、1 ~ 65,535 ミリ秒です。
disable	誘発型 RPF チェックをディセーブルにします。

コマンドモード

誘発型 RPF チェックをイネーブルにした場合、デフォルトは次のとおりです。

- *min* は **500** ミリ秒です。
- *max* は **5000** ミリ秒です。

コマンドモード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

誘発型 RPF チェックをイネーブルにしない場合、PIM が定期的にルーティング テーブルに変化がないかポーリングします (**ip multicast rpf interval** コマンドを使用して設定します)。誘発型 RPF チェックをイネーブルにした場合、ルーティング テーブルが変更されたときに PIM がルーティング テーブルをポーリングします。*min* 引数は、初期バックオフ時間を設定します。いったん誘発されると、PIM はさらにルーティング テーブルが変更されるのを待ちます。ルーティング テーブルの変更が行われず *min* 時間が切れると、PIM はルーティング変更をスキャンします。バックオフ時間内にさらにルーティング変更が行われた場合、PIM はバックオフ時間を 2 倍に延長します。*max* 引数で、2 倍にされたバックオフ時間に対して最大インターバルを設定できます。

次のような場合、このコマンドを使用します。

- 装置でルート変更が頻繁に行われる場合 (たとえば、ダイヤルイン ルータなど)
- 新たに構築されたルートでより高速な IP マルチキャストを実現させるため、最大 RPF チェック インターバルを減らす場合、または RPF チェックによって生じる CPU 負荷を減らすため、RPF チェック インターバルを増やす場合

例

次に、PIM バックオフ インターバルをミリ秒単位で設定する例を示します。

```
Router(config)# ip multicast rpf backoff 100
Router(config)#
```

関連コマンド

コマンド	説明
ip multicast rpf interval	RPF 一貫性チェック インターバルを設定します。
show ip rpf events	誘発型 RPF 統計を表示します。

ip multicast rpf interval

RPF 一貫性チェック インターバルを設定するには、**ip multicast rpf interval** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip multicast rpf interval *interval*

no ip multicast rpf interval

シンタックスの説明

interval RPF チェック間のインターバル (秒単位)。有効値は、1 ~ 10 秒です。

コマンドのデフォルト

10 秒

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ip multicast rpf interval コマンドは、インターバル PIM を設定し、ルーティング テーブルに変化がないかポーリングします。

例

次に、RPF 一貫性チェック インターバルを秒単位で設定する例を示します。

```
Router(config)# ip multicast rpf interval 5
Router(config)#
```

関連コマンド

コマンド	説明
ip multicast rpf backoff	PIM 待機インターバルを設定します。

ip pim accept-register

候補ランデブー ポイント ルータで PIM 登録メッセージをフィルタリングするよう設定するには、**ip pim accept-register** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ip pim [vrf vrf-name] accept-register {list access-list | route-map map-name}
```

```
no ip pim [vrf vrf-name] accept-register {list access-list | route-map map-name}
```

シンタックスの説明	
vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
list access-list	拡張アクセスリストの番号または名前を指定します。
route-map map-name	ルート マップ名を指定します。

コマンドのデフォルト ディセーブル

コマンド モード グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン 非認証の送信元がランデブー ポイントに登録されないようにするには、このコマンドを使用します。非認証の送信元がランデブー ポイントに登録メッセージを送信すると、ランデブー ポイントはただちに登録中止メッセージを送信します。

例 次に、アドレスが SSM 範囲内の送信元がランデブー ポイントにより登録されないようにランデブー ポイントを制限する例を示します。次のステートメントは、ランデブー ポイントだけで設定される必要があります。

```
Router(config)# ip pim accept-register list no-ssm-range
Router(config)# ip access-list extended no-ssm-range
    deny ip any 232.0.0.0 0.255.255.255
    permit ip any any
Router(config)#
```

ip pim accept-rp

ルータが、指定されたランデブー ポイントおよび特定のグループ リスト宛の join/prune メッセージを受け入れるよう設定するには、**ip pim accept-rp** コマンドを使用します。チェックを削除するには、このコマンドの **no** 形式を使用します。

```
ip pim [vrf vrf-name] accept-rp {rp-address | auto-rp} [access-list]
```

```
no ip pim [vrf vrf-name] accept-rp {rp-address | auto-rp} [access-list]
```

シンタックスの説明

vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
rp-address	グループのアクセス リストにより指定された範囲のグループに join メッセージを送信できるランデブー ポイントのアドレス
auto-rp	Auto-RP キャッシュ内のランデブー ポイントに対してだけ、join および登録メッセージを受け入れるよう指定します。
access-list	(任意) チェックされるグループを定義するアクセスリストの番号または名前

コマンドのデフォルト

ディセーブル：すべての join/prune メッセージが処理されます。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドにより、ルータは指定のランデブー ポイント アドレス宛の (*,G) join メッセージだけを受け入れるようになります。グループ アドレスはアクセス リストで指定された範囲内にある必要があります。

rp-address 引数がシステム アドレスの 1 つである場合、システムはアクセス リストで指定された指定グループ範囲だけに対するランデブー ポイントとなります。グループ アドレスがこのグループ範囲にない場合、ランデブー ポイントでは join または登録メッセージを受け入れずに、ただちに登録中止メッセージ付きの登録メッセージに応答します。

例

次に、ルータがマルチキャスト グループ 224.2.2.2 のアドレス 172.17.1.1 のランデブー ポイント宛の join/prune メッセージを受け入れるよう設定する例を示します。

```
Router(config)# ip pim accept-rp 172.17.1.1 3
access-list 3 permit 224.2.2.2
```

関連コマンド

コマンド	説明
access-list (IP 標準)	標準 IP アクセス リストを定義します。

ip pim bidir-enable

bidirectional PIM (bidir-PIM; 双方向 PIM) をイネーブルにするには、**ip pim bidir-enable** コマンドを使用します。bidir-PIM をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip pim [vrf vrf-name] bidir-enable

no ip pim [vrf vrf-name] bidir-enable

シンタックスの説明

vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
---------------------	--

コマンドのデフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

bidir-PIM がディセーブルの場合、このスイッチは bidir-PIM のサポートがないルータと同様に動作します。次の条件が適用されます。

- ルータが送信する PIM hello メッセージには、双方向モード オプションが含まれません。
- ルータは designated forwarder (DF; 指定フォワード) 選定メッセージを送信せず、受信した指定フォワード選定メッセージを無視します。
- ip pim rp-address**、**ip pim send-rp-announce**、および **ip pim rp-candidate** コマンドは次のように処理されます。
 - bidir-PIM がディセーブルでこれらのコマンドを設定する場合、双方向モードはコンフィギュレーション オプションにはなりません。
 - bidir-PIM がイネーブルからディセーブルになった場合に、双方向モード オプションとともにこれらのコマンドを設定すると、これらのコマンドは CLI から削除されます。bidir-PIM を再度イネーブルにする場合は、これらのコマンドを双方向モード オプションを指定して再入力する必要があります。
- show ip pim interface** コマンドの **df** キーワードは、サポートされません。

例

次に、bidir-PIM をイネーブルにする例を示します。

```
Router(config)# ip pim bidir-enable
Router(config)#
```

次に、bidir-PIM をディセーブルにする例を示します。

```
Router(config)# no ip pim bidir-enable
Router(config)#
```

関連コマンド

コマンド	説明
ip pim rp-address	特定グループの PIM ランデブー ポイントのアドレスを設定します。
ip pim rp-candidate	ルータが自身を PIM バージョン 2 ランデブー ポイント候補として Bootstrap Router (BSR; ブートストラップ ルータ) にアドバタイズするよう設定します。
ip pim send-rp-announce	Auto-RP を使用し、ルータがランデブー ポイントとして動作するグループを設定します。

ip pim bsr-candidate

ルータが BSR として候補であることをアナウンスするよう設定するには、**ip pim bsr-candidate** コマンドを使用します。候補ブートストラップルータとしてのこのルータを削除するには、このコマンドの **no** 形式を使用します。

```
ip pim [vrf vrf-name] bsr-candidate interface-type interface-number [hash-mask-length]
[priority]
```

```
no ip pim [vrf vrf-name] bsr-candidate
```

シンタックスの説明

<i>vrf vrf-name</i>	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
<i>interface-type</i> <i>interface-number</i>	BSR アドレスを取得して候補にするルータ上のインターフェイス タイプおよび番号
<i>hash-mask-length</i>	(任意) ハッシュ機能がコールされる前にグループアドレスと論理積をとるマスク長 (最大 32 ビット)
<i>priority</i>	(任意) BSR のプライオリティ。有効値は 0 ~ 255 です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- ディセーブル
- イネーブルの場合、*priority* は **0** です。

コマンドモード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドにより、ブートストラップメッセージは BSR アドレスとして指定されたインターフェイスのアドレスをつけてすべての PIM ネイバに送信されます。各ネイバは、以前のブートストラップメッセージから受信したアドレスと BSR アドレスを比較します (同じインターフェイスで受信される必要はない)。現在のアドレスが同じかまたはより高位のアドレスである場合、現在のアドレスはキャッシュに格納され、ブートストラップメッセージは転送されます。それ以外の場合、ブートストラップメッセージは廃棄されます。

このルータよりもプライオリティが高い (プライオリティが同じ場合は、より高位の IP アドレスを持つ) とされる他の候補 BSR からブートストラップメッセージを受信するまで、このルータは BSR のままです。

このコマンドは、PIM ドメインのすべての部分との接続が良好であるバックボーンルータだけで使用してください。残りの PIM ドメインとの接続でオンデマンドのダイヤルアップリンクを信頼するスタブルータは、BSR 候補にふさわしくありません。

PIM では *interface-type* をイネーブルにする必要があります。

hash-mask-length 引数を設定する場合、同じシード ハッシュを持つすべてのグループは、同じランデブーポイントに対応します。たとえばこの値が 24 である場合は、グループアドレスの最初の 24 ビットだけが適用可能です。この設定を使用すると、複数のグループに 1 つのランデブーポイントを取得できます。

priority を設定する場合、プライオリティが高い BSR が選択されます。プライオリティ値が同じ場合は、IP アドレスがより高位であるルータが BSR となります。

例

次に、プライオリティが 10 である候補 BSR とするように、イーサネット インターフェイス 0 上のルータの IP アドレスを設定する例を示します。

```
Router (config) # ip pim bsr-candidate ethernet 0 10
Router (config) #
```

関連コマンド

コマンド	説明
ip pim bsr border	BSR メッセージがインターフェイスで送受信されることを防止します。
ip pim rp-candidate	ルータが自身を PIM バージョン 2 ランデブーポイント候補として BSR にアドバタイズするよう設定します。
ip pim send-rp-discovery	ランデブーポイント マッピング エージェントとしてルータを設定します。
show ip pim bsr	BSR 情報を表示します。
show ip pim rp	関連マルチキャスト ルーティング エントリとともにキャッシュされているアクティブ ランデブーポイントを表示します。

ip pim register-rate-limit

各ルーティング エントリ (S,G) に毎秒送信される PIM-SM 登録メッセージの最大数の制限を設定するには、**ip pim register-rate-limit** コマンドを使用します。この制限をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ip pim [vrf vrf-name] register-rate-limit rate
```

```
no ip pim [vrf vrf-name] register-rate-limit
```

シンタックスの説明

vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
rate	ルータから毎秒送信される登録メッセージの最大数。有効値は、1 ~ 65,535 メッセージ/秒です。

コマンドのデフォルト

制限は定義されていません。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、指定ルータが各エントリ (S,G) に許可する登録メッセージ数を制限する場合に使用します。このコマンドをイネーブルにすると、指定ルータおよびランデブー ポイント上の負荷は制限されますが、設定限度を超過する登録メッセージは廃棄されます。登録メッセージがバースト性のある送信元から送信されて 1 秒以内に、レシーバーでデータ パケット損失が発生する可能性があります。

ip pim dense-mode proxy-register コマンドを入力すると、次に **ip pim register-rate-limit** コマンドを入力する必要があります。これは、sparse (疎) モードリージョンにデータを送信する (および境界ルータでの登録が必要である) dense (密) モード エリアからは、送信元が多数となる可能性があるためです。

このコマンドは、sparse (疎) モード (S,G) マルチキャスト ルーティング エントリに対してだけ適用されます。

例

次に、PIM-SM 登録メッセージで毎秒 2 つの登録メッセージを最大レートとする制限を設定する例を示します。

```
Router(config)# ip pim register-rate-limit 2
Router(config)#
```

関連コマンド

コマンド	説明
ip pim	インターフェイス上の PIM をイネーブルにします。

ip pim register-source

登録メッセージの IP 送信元アドレスを、ランデブー ポイントへと続く指定ルータの発信インターフェイス アドレス以外のインターフェイス アドレスに設定するには、**ip pim register-source** コマンドを使用します。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip pim [vrf vrf-name] register-source interface-type interface-number

no ip pim [vrf vrf-name] register-source

シンタックスの説明	
<i>vrf vrf-name</i>	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
<i>interface-type</i>	登録メッセージの IP 送信元アドレスを識別するインターフェイス タイプ
<i>interface-number</i>	およびインターフェイス番号

コマンドのデフォルト ランデブー ポイントへと続く指定ルータの発信インターフェイスの IP アドレスが、登録メッセージの IP 送信元アドレスとして使用されます。

コマンド モード グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドは、登録メッセージの IP 送信元アドレスが、ランデブー ポイントがパケットを送信できる一意のルーテッドアドレスではない場合だけ必要となります。このような状況は、受信したパケットが転送されないように送信元アドレスがフィルタリングされる場合、または送信元アドレスがネットワークに対して一意でない場合に発生します。この場合、ランデブー ポイントから送信元アドレスへ送信される応答は指定ルータに到着せず、PIM-SM プロトコル障害となります。

IP 送信元アドレスを設定していない場合、または設定された送信元アドレスが機能しない場合は、ランデブー ポイントに続く指定ルータの発信インターフェイスの IP アドレスは、登録メッセージの IP 送信元アドレスとして使用されます。ループバック インターフェイスには PIM-SM ドメイン全体で一意にルーティングされた IP アドレスを使用することを推奨します。

例 次に、登録メッセージの IP 送信元アドレスを指定ルータのループバック 3 インターフェイスに設定する例を示します。

```
Router(config)# ip pim register-source loopback 3
Router(config)#
```

ip pim rp-announce-filter

ランデブー ポイントからの着信 Auto-RP アナウンスメント メッセージをフィルタリングするには、**ip pim rp-announce-filter** コマンドを使用します。フィルタを削除するには、このコマンドの **no** 形式を使用します。

ip pim [vrf vrf-name] rp-announce-filter rp-list access-list group-list access-list

no ip pim [vrf vrf-name] rp-announce-filter rp-list access-list group-list access-list

シンタックスの説明

vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
rp-list access-list	group-list access-list の組み合わせで提供されるグループ範囲に許容されるランデブー ポイント アドレスの標準アクセス リストの番号または名前を指定します。
group-list access-list	ランデブー ポイントが提供するマルチキャストグループを説明する標準アクセス リストの番号または名前を指定します。

コマンドのデフォルト

すべての RP アナウンスメントが受け入れられます。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、PIM ランデブー ポイント マッピング エージェントに設定します。複数のランデブー ポイント マッピング エージェントを使用する場合は、アナウンスメント エージェントが削除された際にマッピング ステート内で競合しないように、これらのエージェント間のフィルタを一貫させることを推奨します。

例

次に、ルータがアクセス リスト 2 で説明されたグループ範囲用のアクセス リスト 1 のランデブー ポイントからのランデブー ポイント アナウンスメントを受け入れるよう設定する例を示します。

```
Router(config)# ip pim rp-announce-filter rp-list 1 group-list 2
Router(config)#
```

関連コマンド

コマンド	説明
access-list (IP 標準)	標準 IP アクセス リストを定義します。

ip pim rp-candidate

ルータが、自身を PIM バージョン 2 ランデブー ポイント候補として BSR にアドバタイズするよう設定するには、**ip pim rp-candidate** コマンドを使用します。ランデブー ポイント候補としてのこのルータを削除するには、このコマンドの **no** 形式を使用します。

```
ip pim [vrf vrf-name] rp-candidate interface-type interface-number [group-list access-list] [bidir]
```

```
no ip pim [vrf vrf-name] rp-candidate
```

シンタックスの説明

vrf <i>vrf-name</i>	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
interface-type interface-number	このインターフェイス タイプおよびインターフェイス番号に関連付けられた IP アドレスは、候補ランデブー ポイントアドレスとしてアドバタイズされます。
group-list <i>access-list</i>	(任意) ランデブー ポイントアドレスを使用してアドバタイズされるグループプレフィクスを定義する標準 IP アクセス リストの番号または名前を指定します。
bidir	(任意) <i>access-list</i> 引数で指定されるマルチキャスト グループが、双方向モードで動作することを示します。

コマンドのデフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドにより、ルータは自身をランデブー ポイント候補としてアドバタイズする PIM バージョン 2 メッセージを BSR に送信します。アクセス リストで許容されたアドレスは、タイプおよび番号により識別されたルータとともにランデブー ポイントおよびランデブー ポイントが関連するアドレス範囲を構成します。

このコマンドは、PIM ドメインのすべての部分との接続が良好であるバックボーン ルータだけで使用してください。残りの PIM ドメインとの接続でオンデマンドのダイヤルアップ リンクを信頼するスタブルータは、ランデブー ポイント候補としてふさわしくありません。

このコマンドは、双方向転送を行う場合、および PIM バージョン 2 BSR メカニズムを使用してグループ/ランデブー ポイントのマッピングを分散する場合に、**bidir** キーワードを指定して使用します。他のオプションは、次のとおりです。

- Auto-RP によりグループ/ランデブー ポイントのマッピングを分散する場合は、**ip pim send-rp-announce** コマンドで **bidir** キーワードを使用します。

ip pim rp-candidate

- Auto-RP または PIM バージョン 2 BSR メカニズムのどちらによってもグループ/ランデブー ポイントのマッピングを分散しない場合は、**ip pim rp-address** コマンドで **bidir** キーワードを使用します。

access-list 名には、スペースまたは引用符を含めることができず、番号付けされたアクセス リストと混乱しないように、英文字で始める必要があります。

このコマンドを **bidir** キーワードなしで入力すると、指定されたグループは PIM sparse (疎) モードで動作します。

例

次に、ルータが自身をランデブー ポイント候補として PIM ドメイン内の BSR にアドバタイズする例を示します。標準アクセス リスト番号 4 は、イーサネット インターフェイス 2 により識別されるアドレスを持つランデブー ポイントに関連付けられたグループ プレフィクスを指定します。このランデブー ポイントは、プレフィクス 239 を持つグループに関連します。

```
Router(config)# ip pim rp-candidate 192.168.37.33 ethernet 2 group-list 4
access-list 4 permit 239.0.0.0 0.255.255.255
Router(config)#
```

関連コマンド

コマンド	説明
ip pim bsr-candidate	ルータが BSR として候補であることをアナウンスするよう設定します。
ip pim rp-announce-filter	ランデブー ポイントから着信した Auto-RP アナウンスメント メッセージをフィルタ処理します。
ip pim send-rp-announce	Auto-RP を使用し、ルータがランデブー ポイントとして動作するグループを設定します。

ip pim send-rp-announce

Auto-RP を使用して、ルータがランデブー ポイントとして動作するグループを設定するには、**ip pim send-rp-announce** コマンドを使用します。ランデブー ポイントとしてのこのルータの設定を解除するには、このコマンドの **no** 形式を使用します。

```
ip pim [vrf vrf-name] send-rp-announce interface-type interface-number scope ttl-value
[group-list access-list] [interval seconds] [bidir]
```

```
no ip pim [vrf vrf-name] send-rp-announce
```

シンタックスの説明	
vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
interface-type interface-number	ランデブー ポイント アドレスを定義するのに使用されるインターフェイス タイプおよびインターフェイス番号
scope ttl-value	Auto-RP アナウンスメント数を制限する存続可能時間 (TTL) 値を指定します。有効値は、1 ~ 255 です。
group-list access-list	(任意) ランデブー ポイント アドレスに関連してアドバタイズされるグループプレフィックスを定義する標準 IP アクセスリストの番号または名前を指定します。
interval seconds	(任意) ランデブー ポイント アナウンスメント間のインターバル (秒) を指定します。有効値は、1 ~ 16,383 秒です。
bidir	(任意) <i>access-list</i> 引数で指定されるマルチキャスト グループが、双方向モードで動作することを示します。

コマンドのデフォルト デフォルト設定は次のとおりです。

- Auto-RP はディセーブルです。
- イネーブルの場合、*seconds* は 60 秒です。

コマンド モード グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドは、ランデブー ポイントとするルータで使用します。Auto-RP を使用してグループ/ランデブー ポイント マッピングを分散すると、ルータはこのコマンドにより既知のグループ CISCO-RP-ANNOUNCE (224.0.1.39) に Auto-RP アナウンスメント メッセージを送信します。このメッセージは、ルータがアクセス リストで説明された範囲内のグループに対するランデブー ポイント候補であることをアナウンスします。

このコマンドは、双方向転送を行う場合、および Auto-RP を使用してグループ/ランデブーポイントのマッピングを分散する場合に、**bidir** キーワードを指定して使用します。他のオプションは、次のとおりです。

- PIM バージョン 2 ブートストラップ ルータ (PIMv2 BSR) メカニズムによりグループ/ランデブーポイントのマッピングを分散する場合は、**ip pim rp-candidate** コマンドで **bidir** キーワードを使用します。
- Auto-RP または PIMv2 BSR メカニズムのどちらによってもグループ/ランデブーポイントのマッピングを分散しない場合は、**ip pim rp-address** コマンドで **bidir** キーワードを使用します。

このコマンドを **bidir** キーワードなしで入力すると、指定されたグループは PIM-SM で動作します。

access-list 名には、スペースまたは引用符を含めることができず、番号付けされたアクセスリストと混乱しないように、英文字で始める必要があります。

ランデブーポイントアナウンスメントの合計保持時間は、インターバル値の 3 倍に自動設定されます。

例

次に、最大ホップ数が 31 の PIM 対応のすべてのインターフェイスにランデブーポイントアナウンスメントを送信する例を示します。ルータがランデブーポイントとして識別される IP アドレスは、イーサネットインターフェイス 0 に関連付けられた IP アドレスです。アクセスリスト 5 は、このルータがランデブーポイントとして機能するグループを説明します。

```
Router(config)# ip pim send-rp-announce ethernet0 scope 31 group-list 5
access-list 5 permit 224.0.0.0 15.255.255.255
```

関連コマンド

コマンド	説明
access-list (IP 標準)	標準 IP アクセスリストを定義します。
ip pim rp-address	特定グループの PIM ランデブーポイントのアドレスを設定します。
ip pim rp-candidate	ルータが自身を PIM バージョン 2 ランデブーポイント候補として BSR にアダプタイズするよう設定します。

ip pim send-rp-discovery

ルータをランデブー ポイント マッピング エージェントとして設定するには、**ip pim send-rp-discovery** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ip pim [vrf vrf-name] send-rp-discovery [interface-type interface-number] scope ttl-value

no ip pim [vrf vrf-name] send-rp-discovery

シンタックスの説明

vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
interface-type	(任意) ランデブー ポイント マッピング エージェント アドレスを定義するのに使用されるインターフェイス タイプおよびインターフェイス番号
interface-number	
scope ttl-value	検出メッセージをこのホップ数以内に維持する IP ヘッダーの存続可能時間 (TTL) 値を指定します。有効値は 1 ~ 255 です。

コマンドのデフォルト

ルータは、ランデブー ポイント マッピング エージェントではありません。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、ランデブー ポイント マッピング エージェントとして指定されたルータで設定します。PIM ドメインを対象とするのに十分な TTL を指定します。

Auto-RP が使用されている場合の動作は、次のとおりです。

1. ランデブー ポイント マッピング エージェントは、ランデブー ポイント候補が送信する既知のグループ アドレス CISCO-RP-ANNOUNCE (224.0.1.39) を待ち受けます。
2. ランデブー ポイント マッピング エージェントは、既知のグループ CISCO-RP-DISCOVERY (224.0.1.40) に Auto-RP ランデブー ポイント検出メッセージのランデブー ポイント/グループ マッピングを送信します。TTL 値は、メッセージが含むことができるホップ数を制限します。
3. PIM 指定ルータはこのグループを待ち受け、検出メッセージから学習したランデブー ポイントを使用します。

例

次に、Auto-RP ランデブー ポイント検出メッセージを 20 ホップに制限する例を示します。

```
Router(config)# ip pim send-rp-discovery scope 20
Router(config)#
```

ip pim snooping (global configuration mode)

PIM スヌーピングをグローバルにイネーブルにするには、**ip pim snooping** コマンドを使用します。
PIM スヌーピングをグローバルにディセーブルにするには、このコマンドの **no** 形式を使用します。

ip pim snooping

no ip pim snooping

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

予約されている MAC アドレス範囲（たとえば 0100.5e00.00xx）に接続しているグループでは、PIM スヌーピングはサポートされません。

PIM スヌーピングをグローバルにディセーブルにすると、PIM スヌーピングはすべての VLAN 上でディセーブルになります。

例

次に、PIM スヌーピングをグローバルにイネーブルにする例を示します。

```
Router(config)# ip pim snooping
Router(config)#
```

次に、PIM スヌーピングをグローバルにディセーブルにする例を示します。

```
Router(config)# no ip pim snooping
Router(config)#
```

関連コマンド

コマンド	説明
show ip pim snooping	IP PIM スヌーピングに関する情報を表示します。

ip pim snooping (interface configuration mode)

インターフェイス上で PIM スヌーピングをイネーブルにするには、**ip pim snooping** コマンドを使用します。PIM スヌーピングをインターフェイスでディセーブルにするには、このコマンドの **no** 形式を使用します。

ip pim snooping

no ip pim snooping

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト ディセーブル

コマンド モード インターフェイス コンフィギュレーション (config-if)

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン 予約されている MAC アドレス範囲（たとえば 0100.5e00.00xx）に接続しているグループでは、PIM スヌーピングはサポートされません。

インターフェイス上で PIM スヌーピングをイネーブルにする前に、PIM スヌーピングをグローバルにイネーブルにする必要があります。PIM スヌーピングをグローバルにディセーブルにすると、PIM スヌーピングはすべての VLAN 上でディセーブルになります。

PIM スヌーピングは VLAN インターフェイス上だけでイネーブルにできます。

例 次に、VLAN インターフェイス上で PIM スヌーピングをイネーブルにする例を示します。

```
Router(config)# interface vlan 101
Router(config-if)# ip pim snooping
Router(config-f)#
```

次に、VLAN インターフェイス上で PIM スヌーピングをディセーブルにする例を示します。

```
Router(config-if)# no ip pim snooping
Router(config-f)#
```

コマンド	説明
show ip pim snooping	IP PIM スヌーピングに関する情報を表示します。

ip pim snooping dr-flood

指定ルータへのパケットのフラッディングをイネーブルにするには、**ip pim snooping dr-flood** コマンドを使用します。指定ルータへのパケットのフラッディングをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip pim snooping dr-flood

no ip pim snooping dr-flood

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト イネーブル

コマンド モード グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン 予約されている MAC アドレス範囲 (たとえば 0100.5e00.00xx) に接続しているグループでは、PIM スヌーピングはサポートされません。

指定ルータが接続していないスイッチだけに、**no ip pim snooping dr-flood** コマンドを入力してください。

指定ルータは、(S,G) O リストで自動的にプログラムされます。

例 次に、指定ルータへのパケットのフラッディングをイネーブルにする例を示します。

```
Router(config)# ip pim snooping dr-flood
Router(config)#
```

次に、指定ルータへのパケットのフラッディングをディセーブルにする例を示します。

```
Router(config)# no ip pim snooping dr-flood
Router(config)#
```

関連コマンド	コマンド	説明
	show ip pim snooping	IP PIM スヌーピングに関する情報を表示します。

ip pim snooping suppress sgr-prune

指定ルータへの SGR-prune パケットの抑制をイネーブルにするには、グローバル コンフィギュレーション モードで **ip pim snooping suppress sgr-prune** コマンドを使用します。指定ルータへのパケットの抑制をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip pim snooping suppress sgr-prune

no ip pim snooping suppress sgr-prune

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト 指定ルータへのパケットの抑制は、デフォルトではディセーブルです。

コマンド モード グローバル コンフィギュレーション モード

リリース	変更内容
12.2(18)ZY	このコマンドが追加されました。
12.2(18)SXF	このコマンドが追加されました。

使用上のガイドライン 共有ツリーおよび SPT がスイッチ ルータ上で VLAN へ分かれている場合で、PIM にスヌーピングが設定されているときは、マルチキャスト パケットの複製がネットワークに配信されます。PIM スヌーピングは、共有ツリーの到達アップストリーム スイッチ ルータからレシーバーによって送信された prune メッセージを停止することがあります。これによって、1 つ以上のアップストリーム スイッチ ルータがマルチキャスト トラフィックを送信します。この状況は、マルチキャスト パケットの複製がレシーバーに送信される原因となります。PIM-ASSERT メカニズムが開始され、無関係のフローが停止されるため、マルチキャストパケットの複製の送信は数秒間だけ続きます。しかし、次の prune メッセージが送信されると、サイクルが繰り返されます。この状況の発生を停止するには、**no ip pim snooping suppress sgr-prune** コマンドを入力します。

例 次に、指定ルータへの SGR-prune パケットの抑制をイネーブルにする例を示します。

```
Router(config)# ip pim snooping suppress sgr-prune
```

コマンド	説明
show ip pim snooping	IP PIM スヌーピングに関する情報を表示します。

ip pim spt-threshold

PIM リーフ ルータが指定されたグループの最短パス送信元ツリーに加入する時期を設定するには、**ip pim spt-threshold** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

```
ip pim [vrf vrf-name] spt-threshold {kbps | infinity} [group-list access-list]
```

```
no ip pim [vrf vrf-name] spt-threshold
```

シンタックスの説明

vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
kbps	トラフィック レート。有効値は、0 ~ 4,294,967 kbps です。
infinity	指定されたグループのすべての送信元が共有ツリーを使用するようになります。
group-list access-list	(任意) しきい値が適用されるグループを指定します。

コマンドのデフォルト

このコマンドが使用されない場合は、最初の packets が新しい送信元から到着するとすぐに、PIM リーフ ルータが最短パス ツリーに加入します。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

送信元がトラフィック レート (*kbps* 値) 以上のレートで送信する場合、PIM join メッセージがトリガーされ、送信元ツリーを構築します。

group-list access-list は、IP 標準アクセスリストの番号または名前である必要があります。この値が 0、または省略されている場合、すべてのグループにしきい値が適用されます。

infinity キーワードを指定すると、指定グループのすべての送信元は共有ツリーを使用します。グループ リスト アクセス リストを指定すると、しきい値が適用されるグループが示されます。

送信元からのトラフィック レートが、しきい値のトラフィック レートを下回ると、しばらくあとにリーフ ルータが共有ツリーにスイッチ バックして、送信元に **prune** メッセージを送信します。

例

次に、しきい値を 4 kbps に設定する例を示します。トラフィック レートがこのしきい値を上回る場合、送信元からグループへのトラフィックによりルータはこの送信元への最短パス ツリーに切り替わります。

```
Router(config)# ip pim spt-threshold 4
Router(config)#
```

ip pim ssm

IP マルチキャストアドレスの SSM 範囲を定義するには、**ip pim ssm** コマンドを使用します。SSM 範囲をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ip pim [vrf vrf-name] ssm {default | range access-list}
```

```
no ip pim [vrf vrf-name] ssm
```

シンタックスの説明	
vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
default	SSM 範囲アクセス リストを 232/8 として定義します。
range access-list	SSM 範囲を定義する標準 IP アクセスリストの番号または名前を指定します。

コマンドのデフォルト ディセーブル

コマンド モード グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン IP マルチキャストアドレスの SSM 範囲が **ip pim ssm** コマンドにより定義されている場合、MSDP source-active メッセージが SSM 範囲で受け入れられるか、または生成されます。

例 次に、アクセス リスト 4 で定義される IP アドレス範囲の SSM サービスを設定する例を示します。

```
access-list 4 permit 224.2.151.141
Router(config)# ip pim ssm range 4
```

関連コマンド	コマンド	説明
	ip igmp v3lite	IGMP v3lite メンバシップ レポートをインターフェイスで受信して処理できるようにします。
	ip urd	インターフェイスで予約されている URL Rendezvous Directory (URD) ポート 465 に送信された TCP パケットを代行受信し、URD チャネル加入レポートを処理できるようにします。

ip pim state-refresh disable

PIM ルータ上で PIM dense (密) モード リフレッシュ制御メッセージの処理および転送をディセーブルにするには、**ip pim state-refresh disable** コマンドを使用します。PIM dense (密) モード リフレッシュ制御メッセージの処理および転送を再びイネーブルにするには、このコマンドの **no** 形式を使用します。

ip pim [vrf vrf-name] state-refresh disable

no ip pim [vrf vrf-name] state-refresh disable

シンタックスの説明

vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
---------------------	--

コマンドのデフォルト

PIM dense (密) モード リフレッシュ制御メッセージの処理および転送は、PIM dense (密) モード リフレッシュ制御機能をサポートする CiscoIOS ソフトウェア リリースが稼動する PIM ルータ上でイネーブルです。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドを設定すると、PIM hello メッセージから PIM dense (密) モード リフレッシュ制御情報が削除されます。

例

次に、送信元ベースの IP マルチキャスト分散ツリーの下方の PIM dense (密) モード リフレッシュ制御メッセージの定期的な転送をディセーブルにする例を示します。

```
Router(config)# ip pim state-refresh disable
Router(config)#
```

関連コマンド

コマンド	説明
ip pim state-refresh origination-interval	PIM ルータにおける PIM dense (密) モード ステート リフレッシュ制御メッセージの発信およびインターバルを設定します。
show ip pim interface	PIM 用に設定されているインターフェイスに関する情報を表示します。
show ip pim neighbor	PIM ネイバが検出したリストを表示します。

ip rgmp

インターフェイス上で Router-Ports Group Management Protocol (RGMP) をイネーブルにするには、**ip rgmp** コマンドを使用します。RGMP をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip rgmp

no ip rgmp

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- レイヤ 2 インターフェイス上でイネーブル (設定変更不可)
- レイヤ 3 インターフェイス上でディセーブル

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

次の制限事項が PISA の RGMP に適用されます。

- マルチキャスト ルーティングをサポートするように設定されたインターフェイスで RGMP をイネーブルにできます。
- Catalyst 6500 シリーズ スイッチで IGMP スヌーピングをイネーブルにする必要があります。
- Catalyst 6500 シリーズ スイッチで PIM をイネーブルにする必要があります。
- RGMP がサポートするのは、PIM sparse (疎) モードだけです。RGMP は、PIM dense (密) モードをサポートしません。RGMP は、2 つの AutoRP グループを明示的に dense (密) モードでサポートします。トラフィックにはこれらのグループに制限されず、すべてのルータ ポートにフラッディングされます。そのため、PIM sparse-dense モードを設定する必要があります。AutoRP グループ以外のグループを dense (密) モードに設定すると、これらのトラフィックは、RGMP 対応ルータ ポートからは正しく転送されません。
- RGMP を使用してマルチキャスト トラフィックを効率的に抑制するには、RGMP 対応 Catalyst 6500 シリーズ スイッチ上の個別のポートに RGMP 対応ルータを接続してください。
- RGMP は、RGMP 対応ルータを検出したポートからのトラフィックだけを抑制します。ポート上で非 RGMP 対応ルータが検出されると、そのポートはすべてのマルチキャスト トラフィックを受信します。
- RGMP は、直接接続されたネットワーク上の送信元をサポートしません。直接接続された送信元は、RGMP または PIM によるこの情報のシグナリングをせずにネットワークにトラフィックを送信します。このトラフィックは、ルータが RGMP を介してグループの受信を要求していた場合を

除いて、RGMP 対応ルータでは受信されません。この制限は、ホスト、ルータのマルチキャストトラフィック送信機能 (**ping** および **mtrace** コマンド) および UDPTN などのマルチキャストトラフィックを送信するマルチキャストアプリケーションなどに適用されます。

- RGMP は、直接接続されたネットワーク上のレシーバーをサポートします。これらのレシーバーへのトラフィックは、IGMP スヌーピングによって抑制されるか、レシーバーがルータの場合には、PIM および RGMP によって抑制されます。ルータ上で RGMP がイネーブルになっているネットワークでは、CGMP はサポートされません。
- ルータ インターフェイス上で RGMP および CGMP の両方をイネーブルにすることはできません。インターフェイス上で RGMP をイネーブルにすると、CGMP は自動的にディセーブルになります。逆の場合も同様です。

例

次に、RGMP をイネーブルにする例を示します。

```
Router(config-if)# ip rgmp
Router(config-if)#
```

次に、RGMP をディセーブルにする例を示します。

```
Router(config-if)# no ip rgmp
Router(config-if)#
```

関連コマンド

コマンド	説明
show running-config	モジュールまたはレイヤ 2 VLAN のステータスおよび設定を表示します。

ip route-cache flow

IP ルーティングの NetFlow スイッチングをイネーブルにするには、**ip route-cache flow** コマンドを使用します。NetFlow スイッチングをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip route-cache flow

no ip route-cache flow

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト ディセーブル

コマンド モード インターフェイス コンフィギュレーション (config-if)

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン NetFlow スイッチングは、スイッチング機能の一部として一連のトラフィック統計情報をキャプチャします。トラフィック統計情報には、ユーザ、プロトコル、ポートおよびネットワーク解析、プランニング、アカウントリング、および課金に使用されるサービス情報のタイプが含まれます。NetFlow データをエクスポートするには、グローバル コンフィギュレーション モードで **ip flow-export destination** または **ip flow-export source** コマンドを使用します。

NetFlow スイッチングは、ISL/VLAN、ATM、インターフェイスで複数の入力アクセス制御リストが使用されている場合のフレーム リレー インターフェイス、および ATM LAN Emulation (LANE) 以外のすべてのインターフェイス タイプおよびカプセル化上の IP および IP カプセル化トラフィックでサポートされます。

NetFlow スイッチングの詳細については、『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*』を参照してください。



(注) NetFlow は、他のスイッチング モードに比べて、メモリおよび CPU リソースを多く消費します。ルータが必要とするリソースについて十分に理解したうえで、NetFlow をイネーブルにすることを推奨します。

例 次に、インターフェイス上で NetFlow スイッチングをイネーブルにする例を示します。

```
Router(config-if)# ip route-cache flow
Router(config-if)#
```

次に、インターフェイスをデフォルト（高速スイッチングがイネーブルで、自律スイッチングがディセーブル）に戻す例を示します。

```
Router(config-if)# no ip route-cache flow
```

■ ip route-cache flow

```
Router(config-if)#
```

関連コマンド

コマンド	説明
ip flow-export destination	特定の宛先に NetFlow キャッシュ エントリをエクスポートします。
show ip cache flow	NetFlow キャッシュ フロー エントリのサマリーを表示します。

ip sticky-arp (global configuration)

スティッキ ARP をイネーブルにするには、**ip sticky-arp** コマンドを使用します。スティッキ ARP をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip sticky-arp

no ip sticky-arp

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンド モード イネーブル

コマンドのデフォルト グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

特定のインターフェイスでスティッキ ARP をディセーブルにするには、**ip sticky-arp (interface configuration)** コマンドを入力します。

レイヤ 3 インターフェイスで学習した ARP エントリは、スティッキ ARP エントリです。**show arp** コマンドを使用し、レイヤ 3 インターフェイスで ARP エントリの表示と確認を行うことを推奨します。

セキュリティ上の理由から、レイヤ 3 インターフェイス上のスティッキ ARP エントリには期限切れがありません。同じ IP アドレスを使用して新しい装置を接続すると、メッセージが生成され、ARP エントリは作成されません。

レイヤ 3 インターフェイス上の ARP エントリには期限がないため、MAC アドレスが変更された場合は、レイヤ 3 インターフェイス上の ARP エントリを手動で削除する必要があります。

スタティック エントリとは異なり、スティッキ ARP エントリは、**reboot** および **restart** コマンドを入力した場合に、保存および復元されません。

例 次に、スティッキ ARP をイネーブルにする例を示します。

```
Router(config) ip sticky-arp
Router(config)
```

次に、スティッキ ARP をディセーブルにする例を示します。

```
Router(config) no ip sticky-arp
Router(config)
```

■ ip sticky-arp (global configuration)

関連コマンド

コマンド	説明
arp	SMDS ネットワークでスタティック ルーティングの ARP エントリを有効にします。
ip sticky-arp (interface configuration)	インターフェイスでスティッキ ARP をイネーブルにします。
show arp	ARP テーブルを表示します。

ip sticky-arp (interface configuration)

インターフェイスでスティッキ ARP をイネーブルにするには、**ip sticky-arp** コマンドを使用します。このコマンドを削除するには、このコマンドの **no** 形式を使用します。

ip sticky-arp [ignore]

no ip sticky-arp [ignore]

シンタックスの説明	ignore (任意) ip sticky-arp (global configuration) コマンドを上書きします。
-----------	---

コマンドのデフォルト	このコマンドにはデフォルト設定がありません。
------------	------------------------

コマンド モード	インターフェイス コンフィギュレーション (config-if)
----------	----------------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン	このコマンドはレイヤ 3 インターフェイスで入力できます。 特定のインターフェイスで PVLAN スティッキ ARP グローバル設定を上書きするには、 ip sticky-arp ignore コマンドを入力します。
------------	--

例	次に、インターフェイス上でスティッキ ARP をイネーブルにする例を示します。 <pre>Router(config-if) ip sticky-arp Router(config-if)</pre> 次に、インターフェイスで以前設定したコマンドを削除する例を示します。 <pre>Router(config-if) no ip sticky-arp Router(config-if)</pre> 次に、インターフェイス上でスティッキ ARP をディセーブルにする例を示します。 <pre>Router(config-if) ip sticky-arp ignore Router(config-if)</pre>
---	---

関連コマンド	コマンド	説明
	arp	SMDS ネットワークでスタティック ルーティングの ARP エントリを有効にします。
	ip sticky-arp (global configuration)	スティッキ ARP をイネーブルにします。
	show arp	ARP テーブルを表示します。

ip unnumbered

インターフェイスに明示的な IP アドレスを割り当てずに、シリアル インターフェイス上での IP 処理をイネーブルにするには、**ip unnumbered** コマンドを使用します。IP 処理をインターフェイスでディセーブルにするには、このコマンドの **no** 形式を使用します。

ip unnumbered interface-type number

no ip unnumbered interface-type number

シンタックスの説明

interface-type number ルータが割り当てられた IP アドレスを持つ別のインターフェイスのタイプおよび番号。このインターフェイスを別の unnumbered インターフェイスにすることはできません。

コマンドのデフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション (config-if) またはイーサネット VLAN サブインターフェイス (config-subif)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

interface-type number 引数で指定するインターフェイスは、イネーブルである必要があります (**show interfaces** コマンド出力で [up] と表示)。

unnumbered インターフェイスおよびサブインターフェイスは、DHCP を介するピア IP アドレス割り当ておよび DHCP option 82 をサポートします。

IP unnumbering を使用する場合、次の制限事項が適用されます。

- インターフェイスまたはサブインターフェイスの範囲設定により設定されたインターフェイスまたはサブインターフェイスの範囲では、IP unnumbering をイネーブルにできません。
- インターフェイスにアドレスがないため、インターフェイスがアップかどうかを判別するのに pingEXEC コマンドを使用できません。SNMP を使用して、リモートでインターフェイス ステータスをモニタできます。
- unnumbered シリアル インターフェイス上では、実行可能なイメージをブートできません。
- IP セキュリティ オプションは、unnumbered インターフェイス上でサポートできません。

例

次に、イーサネット VLAN サブインターフェイスのサブインターフェイス モードで IP unnumbered 機能をイネーブルにする例を示します。

```
Router (config)# interface fastethernet1/0.1
Router (config-subif)# encapsulation dot1q 10
Router (config-subif)# ip unnumbered ethernet 3/0
```

次に、イーサネット物理インターフェイスで IP unnumbered 機能をディセーブルにする例を示します。

```
Router (config)# interface fastethernet 1
Router (config-if)# no ip unnumbered loopback 0
Router (config-if)#
```

関連コマンド

コマンド	説明
show ipv6 mld snooping explicit-tracking vlan	Multicast Listener Discovery version 2 (MLDv2; マルチキャストリスナーディスカバリーバージョン 2) スヌーピング情報を表示します。

ipv6 mfib-cef

送信パケットに対する CEF ベースの（割り込みレベル）IPv6 マルチキャスト転送を特定のインターフェイス上でイネーブルにするには、**ipv6 mfib-cef** コマンドを使用します。CEF ベースの IPv6 マルチキャスト転送をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 mfib-cef

no ipv6 mfib-cef

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト イネーブル

コマンド モード インターフェイス コンフィギュレーション (config-if)

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン CEF ベースの IPv6 マルチキャスト ルーティングがイネーブルの場合、CEF ベースの（割り込みレベル）IPv6 マルチキャスト転送はデフォルトでイネーブルです。

マルチキャスト転送インターフェイス ステータスを表示するには、**show ipv6 mfib interface** コマンドを使用します。

例 次に、CEF ベースの IPv6 マルチキャスト転送をイネーブルにする例を示します。

```
Router(config-if) ipv6 mfib-cef
Router(config-if)
```

次に、CEF ベースの IPv6 マルチキャスト転送をディセーブルにする例を示します。

```
Router(config-if) no ipv6 mfib-cef
Router(config-if)
```

関連コマンド	コマンド	説明
	show ipv6 mfib interface	IPv6 マルチキャスト対応インターフェイスおよびその転送ステータスに関する情報を表示します。

ipv6 mfib hardware-switching

IPv6 マルチキャスト パケットのハードウェア スイッチングをグローバル単位で設定するには、**ipv6 mfib hardware-switching** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ipv6 mfib hardware-switching [**connected** | {**replication-mode ingress**}]

no ipv6 mfib hardware-switching [**connected** | {**replication-mode ingress**}]

シンタックスの説明

connected	(任意) インターフェイスおよびマスク エントリをダウンロードできます。
replication-mode ingress	(任意) ハードウェア レプリケーション モードを入力に設定します。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- **connected** : イネーブルに設定されています。ACL-TCAM のサブネット エントリを組み込みます。
- **replication-mode** : 自動検出されますが、強制的に入力にできます。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

サブネット エントリの組み込みをグローバル単位で禁止するには、PIM SSM および PIM Bidir に関して **ipv6 mfib hardware-switching** コマンドを使用します。

例

次に、サブネット エントリの組み込みをグローバル単位で禁止する例を示します。

```
Router(config) ipv6 mfib hardware-switching
Router(config)
```

次に、ハードウェア レプリケーション モードを入力に設定する例を示します。

```
Router(config) ipv6 mfib hardware-switching replication-mode
Router(config)
```

関連コマンド

コマンド	説明
show platform software ipv6-multicast	プラットフォーム ソフトウェア IPv6 マルチキャストに関する情報を表示します。

ipv6 mld snooping

MLDv2 スヌーピングをグローバルにイネーブルにするには、**ipv6 mld snooping** コマンドを使用します。MLDv2 スヌーピングをグローバルにディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping

no ipv6 mld snooping

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

イネーブル

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

MLDv2 スヌーピングを使用するには、IPv6 マルチキャスト ルーティング用のサブネットでレイヤ 3 インターフェイスを設定するか、またはサブネットで MLDv2 スヌーピング クエリアをイネーブルにします。

例

次に、MLDv2 スヌーピングをグローバルにイネーブルにする例を示します。

```
Router(config)# ipv6 mld snooping
Router(config)#
```

関連コマンド

コマンド	説明
show ipv6 mld snooping	MLDv2 スヌーピング情報を表示します。

ipv6 mld snooping explicit-tracking

明示的なホスト トラッキングをイネーブルにするには、**ipv6 mld snooping explicit-tracking** コマンドを使用します。明示的なホスト トラッキングをディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping explicit-tracking

no ipv6 mld snooping explicit-tracking

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト イネーブル

コマンド モード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン 明示的なホスト トラッキングは、MLDv2 ホストだけでサポートされています。

明示的なホスト トラッキングがイネーブルで、Catalyst 6500 シリーズスイッチがプロキシ レポート モードで動作している場合、ルータは VLAN インターフェイスの背後のホストすべてをトラッキング できない場合があります。プロキシ レポート モードでは、Catalyst 6500 シリーズスイッチはチャンネルの最初のレポートだけをルータへ転送し、同じチャンネルに対するその他のレポートはすべて抑制され ます。

MLDv2 プロキシ レポートを使用すると、Catalyst 6500 シリーズスイッチは非請求レポート、および 一般的なクエリー インターバルで受信されたレポートに対してプロキシ レポートを行います。

プロキシ レポートはデフォルトでオンになっています。プロキシ レポートをディセーブルにすると、 Catalyst 6500 シリーズスイッチはトランスペアレント モードで動作し、レポートを受信すると MLDv2 スヌーピング データベースを更新し、アップストリームのルータにこの情報を転送します。こ のようにして、ルータはレポートするホストをすべて明示的にトラッキングできます。

明示的なトラッキングをディセーブルにすると、高速脱退処理およびプロキシ レポートがディセーブル になります。

MLDv2 はすべてのポートでメンバーシップ情報の明示的なホスト トラッキングをサポートしていま す。明示的なホスト トラッキング データベースは、MLDv2 ホストの高速脱退処理、プロキシ レポー ト、および統計情報収集に使用されます。VLAN 上で、明示的なホスト トラッキングをイネーブルに すると、MLDv2 スヌーピング ソフトウェアはホストから受信する MLDv2 レポートを処理し、次の情 報が含まれる明示的なホスト トラッキング データベースを構築します。

- ホストが接続されているポート
- ホストによりレポートされるチャンネル
- ホストによりレポートされる各グループのフィルタ モード

■ ipv6 mld snooping explicit-tracking

- ホストによりレポートされる各グループの送信元リスト
- 各グループのルータ フィルタ モード
- 送信元を要求する各グループのホスト リスト

例

次に、明示的なホスト トラッキングをイネーブルにする例を示します。

```
Router(config-if)# ipv6 mld snooping explicit-tracking  
Router(config-if)#
```

関連コマンド

コマンド	説明
ipv6 mld snooping limit	MLDv2 制限を設定します。
show ipv6 mld snooping explicit-tracking	MLDv2 スヌーピング情報を表示します。

ipv6 mld snooping last-member-query-interval

MLDv2 スヌーピングの最終メンバー クエリー インターバルを設定するには、**ipv6 mld snooping last-member-query-interval** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping last-member-query-interval *interval*

no ipv6 mld snooping last-member-query-interval

シンタックスの説明

interval 最終メンバー クエリーのインターバル。有効値は、100 ～ 900 ミリ秒です (100 ミリ秒の倍数)。

コマンドのデフォルト

1000 ミリ秒 (1 秒) です。詳細については、「使用上のガイドライン」を参照してください。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

マルチキャスト ホストがグループから脱退すると、ホストは MLDv2 脱退メッセージを送信します。これがグループを脱退する最終ホストかを確認するために、脱退が確認されてタイマーが開始したときに MLDv2 クエリーが送信されます。タイマーの期限が切れる前にレポートが受信されないと、グループ レコードは削除されます。

interval は、Catalyst 6500 シリーズスイッチがグループ固有のクエリーの応答を実際に待つ時間です。100 の倍数でないインターバルを入力すると、100 未満の端数が切り捨てられます。たとえば、999 と入力した場合、端数が切り捨てられて 900 ミリ秒になります。

MLDv2 高速脱退処理をイネーブルにして、**no ipv6 mld snooping last-member-query-interval** コマンドを入力した場合、インターバルは 0 秒にセットされ、高速脱退処理が常に優先されます。

有効値の範囲は 100 ～ 1000 ミリ秒ですが、**1000** の値は入力できません。この値を指定するには、**no ipv6 mld snooping last-member-query-interval** コマンドを入力して、デフォルト値 (1000 ミリ秒) に戻す必要があります。

例

次に、最終メンバー クエリー インターバルを 200 ミリ秒に設定する例を示します。

```
Router(config-if)# ipv6 mld snooping last-member-query-interval 200
Router(config-if)#
```

関連コマンド

コマンド	説明
show ipv6 mld snooping	MLDv2 スヌーピング情報を表示します。

ipv6 mld snooping limit

MLDv2 制限を設定するには、**ipv6 mld snooping limit** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
ipv6 mld snooping limit {{l2-entry-limit max-entries} | {rate pps} | {track max-entries}}
```

```
no ipv6 mld snooping limit {l2-entry-limit | rate | track}
```

シンタックスの説明

l2-entry-limit <i>max-entries</i>	MLD スヌーピングにより組み込まれるレイヤ 2 エントリの最大数を指定します。有効値は、1 ~ 100,000 エントリです。
rate <i>pps</i>	着信 MLDv2 メッセージのレート制限を指定します。有効値は、100 ~ 6000 パケット/秒です。
track <i>max-entries</i>	明示的なトラッキング データベースの最大エントリ数を指定します。有効値は、0 ~ 128,000 です。

コマンド モード

max-entries は **32000** です。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

明示的なトラッキング データベースの各エントリは、送信元 IP、グループ IP、ポート、VLAN、およびレポータ IP により識別されます。

max-entries を **0** に設定すると、明示的なトラッキングはディセーブルになります。

明示的なトラッキング データベースが設定された *max-entries* を超えると、Syslog メッセージが生成されます。

max-entries を減らした場合、明示的なトラッキング データベースではただちにサイズを減らすことはできません。明示的なトラッキング データベースは、レポータがタイムアウトになるに従って徐々に縮小されます。

例

次に、MLD スヌーピングによって組み込まれるレイヤ 2 エントリの最大数を設定する例を示します。

```
Router(config)# ipv6 mld snooping limit l2-entry-limit 20000
Router(config)#
```

次に、着信 MLDv2 スヌーピング パケットのレート制限を設定する例を示します。

```
Router(config)# ipv6 mld snooping limit rate 200
Router(config)#
```

次に、明示的なトラッキング データベースの最大エントリ数を設定する例を示します。

```
Router(config)# ipv6 mld snooping limit track 20000  
Router(config)#
```

次に、ソフトウェアのレート制限をディセーブルにする例を示します。

```
Router(config)# no ipv6 mld snooping limit rate  
Router(config)#
```

関連コマンド

コマンド	説明
ipv6 mld snooping explicit-tracking	明示的なホスト トラッキングをイネーブルにします。
show ipv6 mld snooping	MLDv2 ホストのスヌーピング ステータスに関する情報を表示します。

ipv6 mld snooping mrouter

レイヤ 2 ポートをマルチキャスト ルータ ポートとして設定するには、**ipv6 mld snooping mrouter** コマンドを使用します。

ipv6 mld snooping mrouter {interface type slot/port}

シンタックスの説明

interface type	インターフェイス タイプを指定します。有効値は、 ethernet 、 fastethernet 、 gigabitethernet 、または tengigabitethernet です。
slot/ports	モジュールおよびポート番号

コマンドのデフォルト

設定されていません。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

マルチキャスト ルータにスタティック接続を設定するには、**mac-address-table static** コマンドを使用します。

例

次に、レイヤ 2 ポートをマルチキャスト ルータ ポートとして設定する例を示します。

```
Router(config-if)# ipv6 mld snooping mrouter interface fastethernet 5/6
Router(config-if)#
```

関連コマンド

コマンド	説明
show ipv6 mld snooping	MLDv2 スヌーピング情報を表示します。

ipv6 mld snooping querier

MLDv2 スヌーピング クエリアをイネーブルにするには、**ipv6 mld snooping querier** コマンドを使用します。MLDv2 スヌーピング クエリアをディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping querier

no ipv6 mld snooping querier

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト ディセーブル

コマンド モード インターフェイス コンフィギュレーション (config-if)

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

VLAN インターフェイス上で IPv6 アドレスを設定してください。イネーブルになっている場合、MLDv2 スヌーピング クエリアはこの IPv6 アドレスをクエリーの送信元アドレスとして使用します。

VLAN インターフェイス上に IPv6 アドレスが設定されていない場合、MLDv2 スヌーピング クエリアは起動しません。IPv6 アドレスがクリアされると、MLDv2 スヌーピング クエリアは自身でディセーブルになります。イネーブルになった状態で IPv6 アドレスを設定すると、MLDv2 スヌーピング クエリアは再起動します。

イネーブルになっている場合、IPv6 マルチキャスト ルータからの MLDv2 トラフィックを検出すると MLDv2 スヌーピング クエリアは起動しません。

イネーブルになっている場合、IPv6 マルチキャスト ルータからの MLDv2 トラフィックを検出しなければ MLDv2 スヌーピング クエリアは 60 秒後に起動します。

イネーブルになっている場合、IPv6 マルチキャスト ルータからの MLDv2 トラフィックを検出すると MLDv2 スヌーピング クエリアは自身をディセーブルにします。

MLDv2 スヌーピング クエリアは、これをサポートする VLAN のすべての Catalyst 6500 シリーズスイッチでイネーブルにできます。1 台のスイッチがクエリアとして選定されます。

例 次に、VLAN 200 で MLDv2 スヌーピング クエリアをイネーブルにする例を示します。

```
Router# interface vlan 200
Router(config-if)# ipv6 mld snooping querier
```

■ ipv6 mld snooping querier

関連コマンド

コマンド	説明
<code>show ipv6 mld snooping</code>	MLDv2 スヌーピング情報を表示します。

ipv6 mld snooping report-suppression

VLAN 上でレポート抑制をイネーブルにするには、**ipv6 mld snooping report-suppression** コマンドを使用します。VLAN 上でレポート抑制をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping report-suppression

no ipv6 mld snooping report-suppression

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト イネーブル

コマンド モード インターフェイス コンフィギュレーション (config-if)

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン レポート抑制をイネーブルにするには、事前に明示的トラッキングをイネーブルにする必要があります。このコマンドをサポートするのは、VLAN インターフェイスだけです。

例 次に、明示的なホストトラッキングをイネーブルにする例を示します。

```
Router(config-if)# ipv6 mld snooping report-suppression  
Router(config-if)#
```

ip verify unicast reverse-path

ユニキャスト RPF をイネーブルにするには、**ip verify unicast reverse-path** コマンドを使用します。ユニキャスト RPF をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip verify unicast reverse-path [allow-self-ping] [list]

no ip verify unicast reverse-path [allow-self-ping] [list]

シンタックスの説明

allow-self-ping	(任意) Catalyst 6500 シリーズ スイッチが自身を ping できるようにします。
<i>list</i>	(任意) アクセスリスト番号。標準または拡張 IP アクセスリスト番号の場合、有効値は 1 ~ 199 で、標準または拡張 IP 拡張アクセスリスト番号の有効値は、1300 ~ 2699 です。

コマンドのデフォルト

ディセーブル

コマンドモード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ip verify unicast reverse-path コマンドを使用して、Catalyst 6500 シリーズ スイッチを通過する変造または偽造 (スプーフィング) された IP 送信元アドレスによって発生する問題を減少させます。変造または偽造された送信元アドレスは、送信元 IP アドレス スプーフィングを利用した DoS 攻撃である可能性があります。



(注)

ユニキャスト RPF は入力機能であり、接続のアップストリーム側になる Catalyst 6500 シリーズ スイッチの入力インターフェイスだけに適用されます。

ip verify unicast reverse-path コマンドに ACL を指定しない場合、Catalyst 6500 シリーズ スイッチは偽造および変造されたパケットをただちに廃棄し、ACL ログイングが行われません。Catalyst 6500 シリーズ スイッチおよびインターフェイス ユニキャスト RPF のカウンタは更新されます。

ip verify unicast reverse-path コマンドによって使用される ACL エントリのログイング オプションを指定してユニキャスト RPF イベントを記録できます。ログイング オプションを使用して、送信元アドレス、時間などの攻撃情報を収集できます。



(注)

ユニキャスト RPF では、すべての等価コストに対して「最良の」リターンパスが有効であると考えられます。ユニキャスト RPF は、各パスがルーティング コスト (ホップ数、重みなど) において他と同等であり、ルートが FIB にあるという条件で複数のリターンパスが存在する場合に動作します。ユニキャスト RPF は、異なる Enhanced Interior Gateway Routing Protocol (EIGRP) 変数が使用され、送信元 IP アドレスに戻る異なる候補パスが存在する場合にも機能します。

ユニキャスト RPF をネットワーク内部のインターフェイスで使用しないでください。内部インターフェイスでは、ルーティングが非対称である場合があります、パケットの送信元に複数のルートが存在します。ユニキャスト RPF を適用するのは、もともと対称か、または対称に設定されている場合だけにしてください。

サービス プロバイダー ネットワークのエッジにあるルータは、ネットワークのコアにあるルータに比べて対称的な逆パスを持つ可能性が高くなります。サービス プロバイダー ネットワークのコアにあるルータでは、ルータからの最善転送パスがルータに戻るパケットに選択されたパスである保証はありません。

ユニキャスト RPF を非対称ルーティングの可能性のある場所には適用しないことを推奨します。ユニキャスト RPF はネットワークのエッジだけに配置してください。サービス プロバイダー ネットワークに関しては、ユニキャスト RPF をネットワークのカスタマー エッジに配置してください。

例 次に、シリアル インターフェイスでユニキャスト RPF をイネーブルにする例を示します。

```
Router(config-if)# ip verify unicast reverse-path
Router(config-if)#
```

関連コマンド

コマンド	説明
ip cef	ルート プロセッサで CEF をイネーブルにします。

ip verify unicast source reachable-via

RPF チェックをイネーブルにして設定するには、**ip verify unicast source reachable-via** コマンドを使用します。RPF をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip verify unicast source reachable-via {rx | any} [allow-default] [allow-self-ping] [list]

no ip verify unicast source reachable-via

シンタックスの説明

rx	送信元アドレスがパケットが受信されたインターフェイスに到達可能かチェックします。
any	任意のパスで送信元アドレスが到達可能かどうかをチェックします。
allow-default	(任意) デフォルトのルートが送信元アドレスに一致するかどうかをチェックします。
allow-self-ping	(任意) ルータの自身への ping を許可します。
list	(任意) アクセス リスト番号。標準 IP アクセス リスト番号の場合、有効値は 1 ~ 199 で、標準 IP 拡張アクセス リスト番号の有効値は、1300 ~ 2699 です。

コマンドのデフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ユニキャスト RPF は、PVLAN ホスト ポートではサポートされていません。

ユニキャスト RPF は、次に示す 3 つの基本モードを提供します。

- **exists-only** モード：送信元アドレスが FIB にだけ存在し、「実物の」インターフェイスから到達可能であることが必要とされます。これは、**ip verify unicast source reachable-via any allow-default** コマンドに対しても同様です。**exists-only** モードでは、解決済みの到達可能な送信元アドレスが FIB テーブルに存在している必要があります。送信元アドレスは、設定されたインターフェイスから到達可能である必要があります。
- **any** モード：送信元が、任意のパスで到達可能である必要があります。たとえば、送信元には宛先別ロード バランスが備えられています。
- **rx** モード：送信元アドレスは、到達したインターフェイスに到達可能である必要があります。たとえば、送信元はロード バランスなしで到達可能である必要があります。



(注)

ユニキャスト RPF は入力機能であり、接続のアップストリーム側になるルータの入力インターフェイスだけに適用されます。

unicast reverse path forwarding (uRPF) チェックを設定する場合、次の注意事項および制限事項に従ってください。

- uRPF チェックを設定して、ACL によるフィルタリングを行う場合、トラフィックが ACL に一致するかどうかは PFC によって判別されます。PFC は RPF ACL によって拒否されたトラフィックを PISA に送信して、uRPF チェックを行います。ACL によって許可されたパケットは、uRPF チェックなしでハードウェアに転送されます。**mls ip cef rpf hw-enable-rpf-acl** コマンドを入力して、RPF チェックとハードウェアでの転送を指定し、uRPF ACL によって拒否されたパケットがハードウェアに転送され、ACL によって許可されたパケットがソフトウェアに送信されるように設定できます。
- DoS 攻撃のパケットは通常、拒否 ACE に一致し、uRPF チェック用に PISA に送信されるので、PISA が過負荷になる可能性があります。拒否 ACE に一致する DOS パケットはハードウェアで処理されるので、このような場合は、**mls ip cef rpf hw-enable-rpf-acl** コマンドを入力できます。

ユニキャスト RPF をネットワーク内部のインターフェイスで使用しないでください。内部インターフェイスでは、ルーティングが非対称である場合があり、パケットの送信元に複数のルートが存在します。ユニキャスト RPF を適用するのは、もともと対称か、または対称に設定されている場合だけにしてください。

例 次に、ユニキャスト RPF exist-only チェック モードをイネーブルにする例を示します。

```
Router(config-if)# ip verify unicast source reachable-via any
Router(config-if)#
```

関連コマンド

コマンド	説明
ip cef	ルートプロセッサで CEF をイネーブルにします。
show running-config	モジュールまたはレイヤ 2 VLAN のステータスおよび設定を表示します。

ip wccp group-listen

Web Cache Coprocessor Protocol (WCCP) の IP マルチキャスト パケットの受信をイネーブルにするには、**ip wccp group-listen** コマンド モードを使用します。WCCP の IP マルチキャスト パケットの受信をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip wccp {web-cache | {service-number | service-name}} group-listen

no ip wccp {web-cache | {service-number | service-name}} group-listen

シンタックスの説明

web-cache	Web キャッシュ サービスにパケットを送信するようにルータに指示します。
<i>service-number</i>	WCCP サービス番号。有効値は 0 ~ 99 です。
<i>service-name</i>	WCCP サービス名。有効値は web-cache です。

コマンドのデフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



(注)

コマンドを正しく動作させるには、**ip wccp group-listen** コマンドに加えて **ip pim mode** コマンドを入力する必要があります。

service-number は、**web-cache**、または動的に定義されたキャッシュ エンジンを表す番号にすることができます。サービスがイネーブルになると、Catalyst 6500 シリーズ スイッチはサービス グループの確立に参加できます。

IP マルチキャストの使用時、サービス グループのメンバーになる Catalyst 6500 シリーズ スイッチでは、次の設定が必要になります。

- WCCP サービス グループが使用する IP マルチキャスト アドレスを設定する必要があります。
- IP マルチキャスト アドレスを受信するインターフェイスで、**ip wccp {web-cache | service-number} group-listen** コマンドを設定する必要があります。

例 次に、マルチキャストアドレスが 224.1.1.100 である Web キャッシュでマルチキャスト パケットをイネーブルにする例を示します。

```
router# configure terminal
router(config)# ip wccp web-cache group-address 224.1.1.100
router(config)# interface ethernet 0
router(config-if)# ip wccp web-cache group-listen
```

関連コマンド

コマンド	説明
ip wccp	キャッシュ エンジン サービス グループに対するサポートをイネーブルまたはディセーブルにするようにルータに指示します。
ip wccp redirect	WCCP を使用して発信または着信インターフェイス上でパケット リダイレクションをイネーブルにします。

ip wccp redirect

WCCP を使用して発信または着信インターフェイス上でパケット リダイレクションをイネーブルにするには、**ip wccp redirect** コマンドを使用します。WCCP リダイレクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ip wccp {web-cache | service-number} redirect {in | out}
```

```
no ip wccp {web-cache | service-number} redirect {in | out}
```

シンタックスの説明

web-cache	Web キャッシュ サービスをイネーブルにします。
service-number	ルータに制御されているキャッシュ エンジン サービス グループの識別番号を指定します。有効値は 0 ～ 99 です。キャッシュ エンジン クラスタでシスコ製キャッシュ エンジンが使用されている場合、リバース プロキシ サービスは、値 99 で指定されます。
redirect	発信または着信インターフェイス上でパケット リダイレクション チェックをイネーブルにします。
in	着信インターフェイスでパケット リダイレクションを指定します。
out	発信インターフェイスでパケット リダイレクションを指定します。

コマンドのデフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ip wccp redirect in コマンドを使用すると、着信ネットワーク トラフィックを受信するインターフェイス上で WCCP リダイレクションを設定できます。コマンドがインターフェイスに適用される場合、そのインターフェイスに到達したすべてのパケットが、指定した WCCP サービスで定義された基準と比較されます。パケットは、基準と一致した場合にリダイレクトされます。

ip wccp redirect out コマンドを使用すると、発信インターフェイスで WCCP リダイレクション チェックを設定できます。



(注)

このコマンドは、**ip wccp redirect exclude in** コマンドに影響する可能性があります。インターフェイス上で **ip wccp redirect exclude in** コマンドを設定してから、**ip wccp redirect in** コマンドを設定すると、**ip wccp redirect exclude in** コマンドは上書きされます。逆も同様で、**ip wccp redirect exclude in** コマンドを設定すると、**ip wccp redirect in** コマンドは上書きされます。

Cisco IOS Release 12.0 以降に変更されたコマンドのリストを含む、WCCP コンフィギュレーション コマンドの詳細については、『Cisco IOS Release 12.2 Command Reference』の「Cisco IOS System Management Commands」の「WCCP Commands」の章を参照してください。

例 次に、イーサネット インターフェイス 0 上の逆プロキシ パケットのリダイレクションがチェックされ、シスコのキャッシュ エンジンにリダイレクトされるセッションを設定する例を示します。

```
Router# configure terminal
Router(config)# ip wccp 99
Router(config)# interface ethernet 0
Router(config-if)# ip wccp 99 redirect out
```

次に、インターフェイス 0/1 に到達する HTTP トラフィックがシスコのキャッシュ エンジンにリダイレクトされるセッションを設定する例を示します。

```
Router# configure terminal
Router(config)# ip wccp web-cache
Router(config)# interface ethernet 0/1
Router(config-if)# ip wccp web-cache redirect in
```

関連コマンド

コマンド	説明
show ip interface	IP 用に設定したインターフェイスのユーザビリティ ステータスを表示します。
show ip wccp	WCCP 統計情報を表示します。

ip wccp web-cache accelerated

WCCP バージョン 1 のハードウェア アクセラレーションをイネーブルにするには、**ip wccp web-cache accelerated** コマンドを使用します。ハードウェア アクセラレーションをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ip wccp web-cache accelerated {[group-address groupaddress] [redirect-list access-list]
[group-list access-list] [password password]}
```

```
no ip wccp web-cache accelerated
```

シンタックスの説明

group-address <i>groupaddress</i>	(任意) WCCP サービス グループとの通信に、指定されたマルチキャスト IP アドレスを使用するようにルータに指示します。詳細については、「使用上のガイドライン」を参照してください。
redirect-list <i>access-list</i>	(任意) このサービス グループにリダイレクトされるトラフィックの制御に、アクセス リストを使用するようにルータに指示します。詳細については、「使用上のガイドライン」を参照してください。
group-list <i>access-list</i>	(任意) サービス グループへの参加を許可されるキャッシュ エンジンの決定に、アクセス リストを使用するようにルータに指示します。詳細については、「使用上のガイドライン」を参照してください。
password <i>password</i>	(任意) サービス名で指定されたサービス グループから受信したメッセージに MD5 認証を適用するようルータに指示するストリングを指定します。詳細については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、キャッシュ エンジン ソフトウェア リリース Application and Content Networking System (ACNS) 4.2.1 よりあとのソフトウェア リリースでサポートされます。

group-address groupaddress オプションには、リダイレクトされたメッセージを受信するキャッシュ エンジンの決定に、ルータで使用されるマルチキャスト アドレスが必要です。このオプションは、このグループ アドレスで受信した「Here I Am」メッセージに対する「I See You」応答を結合するために、指定されたマルチキャスト IP アドレスを使用するようにルータに指示します。この応答は、グループ アドレスにも送信されます。デフォルトでは、**group-address** は設定されていないため、すべての「Here I Am」メッセージにユニキャスト応答が返されます。

redirect-list access-list オプションは、**service-name** で指定されたサービス グループのキャッシュ エンジンにリダイレクトされるトラフィックを制御するのに、アクセス リストを使用するようにルータに指示します。**access-list** 引数では、1 ~ 99 の数値を指定して標準または拡張アクセス リスト番号を表すか、または名前を指定して名前付きの標準または拡張アクセス リストを表します。アクセス リストは、リダイレクトを許可されるトラフィックを指定します。デフォルトでは、**redirect-list** は設定されていません (すべてのトラフィックがリダイレクトされます)。

group-list access-list オプションは、指定されたサービス グループへの参加を許可されるキャッシュ エンジンを制御するのに、アクセス リストを使用するようにルータに指示します。**access-list** 引数では、1 ~ 99 の数値を指定して標準アクセス リスト番号を表すか、または名前を指定して名前付きの標準アクセス リストを表します。アクセス リストは、サービス グループへの参加を許可されるキャッシュ エンジンを指定します。デフォルトでは、**group-list** は設定されていないため、すべてのキャッシュ エンジンがサービス グループに参加する可能性があります。

パスワードは最大 7 文字まで指定できます。パスワードを指定すると、認証で受け入れられないメッセージは廃棄されます。パスワード名は HMAC MD5 値と結合され、ルータとキャッシュ エンジン間の接続にセキュリティを確立します。

例

次に、WCCP バージョン 1 のハードウェア アクセラレーションをイネーブルにする例を示します。

```
Router (config)# ip wccp web-cache accelerated
Router (config)#
```

関連コマンド

コマンド	説明
ip wccp version	ルータで設定する WCCP のバージョンを指定します。

l2protocol-tunnel

インターフェイス上でプロトコル トンネリングをイネーブルにし、トンネリングするプロトコルのタイプを指定するには、**l2protocol-tunnel** コマンドを使用します。プロトコル トンネリングをディセーブルにするには、このコマンドの **no** 形式を使用します。

l2protocol-tunnel [{cdp | stp | vtp}]

no l2protocol-tunnel [{cdp | stp | vtp}]

シンタックスの説明

cdp	(任意) CDP トンネリングをイネーブルにします。
stp	(任意) STP トンネリングをイネーブルにします。
vtp	(任意) VTP トンネリングをイネーブルにします。

コマンドのデフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

サービス プロバイダーのすべてのエッジ スイッチでは、次のコマンドを入力して、802.1Q トンネル ポート上で PortFast BPDU フィルタリングをイネーブルにする必要があります。

```
Router(config-if)# spanning-tree bpdupfilter enable
Router(config-if)# spanning-tree portfast
```



(注)

PortFast BPDU フィルタリングは、トンネル ポートで自動的にイネーブルになります。

特定のプロトコルを指定しない場合、すべてのプロトコルがトンネリングされます。

プロトコル トンネリングは、VLAN およびトランク インターフェイス上に設定できます。

LAN ポートをレイヤ 2 インターフェイスとして設定するには、キーワードを指定しないで **switchport** コマンドを一度入力する必要があります。そのあとで、キーワードとともにさらに **switchport** コマンドを入力できます。この処理は、インターフェイスに対して **switchport** コマンドをまだ入力していない場合だけ必要となります。

例

次に、インターフェイス上でトンネリング プロトコルをイネーブルにする例を示します。

```
Router(config-if)# l2protocol-tunnel cdp
Router(config-if)#
```

次に、インターフェイス上でトンネリング プロトコルをディセーブルにする例を示します。

```
Router(config-if)# no l2protocol-tunnel
Protocol tunneling disabled on interface fastEthernet 4/1
Router(config-if)#
```

関連コマンド

コマンド	説明
show l2protocol-tunnel	1 つのインターフェイスまたはすべてのインターフェイスでトンネリングされるプロトコルを表示します。
switchport	レイヤ 2 スイッチド インターフェイスのスイッチング特性を変更します。

l2protocol-tunnel cos

すべての入力レイヤ 2 プロトコル トンネリング ポートに対してグローバルに class of service (CoS; サービス クラス) 値を指定するには、**l2protocol-tunnel cos** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

l2protocol-tunnel cos *cos-value*

no l2protocol-tunnel cos

シンタックスの説明

cos-value CoS 値。有効値は 0 ~ 7 です。

コマンドのデフォルト

cos-value は 5 です。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

cos-value は、サービス プロバイダー ネットワークを通じて protocol data unit (PDU; プロトコル データ ユニット) をトンネリングする前に、レイヤ 2 プロトコル トンネリング ポートに PDU を割り当てる CoS 値です。

すべての入力レイヤ 2 プロトコル トンネリング ポートにグローバルに CoS 値を指定できます。CoS 値がすべての入力トンネリング ポートに適用されるので、Catalyst 6500 シリーズ スイッチによって送出されたカプセル化 PDU の CoS 値はすべて同じになります。

サービス プロバイダーのすべてのエッジ スイッチでは、次のコマンドを入力して、802.1Q トンネル ポート上で PortFast BPDU フィルタリングをイネーブルにする必要があります。

```
Router(config-if)# spanning-tree bpdupfilter enable
Router(config-if)# spanning-tree portfast
```



(注) PortFast BPDU フィルタリングは、トンネル ポートで自動的にイネーブルになります。

例

次に、すべての入力レイヤ 2 プロトコル トンネリング ポートに CoS 値を指定する例を示します。

```
Router(config)# l2protocol-tunnel cos 6
Router(config)#
```

関連コマンド

コマンド	説明
show l2protocol-tunnel	1 つのインターフェイスまたはすべてのインターフェイスでトンネリングされるプロトコルを表示します。

l2protocol-tunnel drop-threshold

インターフェイス上で、廃棄される前に特定のプロトコルで処理される最大のパケット数を指定するには、**l2protocol-tunnel drop-threshold** コマンドを使用します。すべてのしきい値を 0 にリセットし、廃棄しきい値をディセーブルにするには、このコマンドの **no** 形式を使用します。

l2protocol-tunnel drop-threshold [cdp | stp | vtp] packets

no l2protocol-tunnel drop-threshold [cdp | stp | vtp]

シンタックスの説明

cdp	(任意) CDP パケットを指定します。
stp	STP パケットを指定します。
vtp	(任意) VTP パケットを指定します。
packets	最大パケット数。有効値は 1 ~ 4096 です。

コマンドのデフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

サービス プロバイダーのすべてのエッジ スイッチでは、次のコマンドを入力して、802.1Q トンネルポート上で PortFast BPDU フィルタリングをイネーブルにする必要があります。

```
Router(config-if)# spanning-tree bpdupfilter enable
Router(config-if)# spanning-tree portfast
```



(注)

PortFast BPDU フィルタリングは、トンネル ポートで自動的にイネーブルになります。

プロトコルを指定しない場合、しきい値がすべてのプロトコルに適用されます。

スイッチ ポートだけにプロトコル トンネリングを設定できます。LAN ポートをレイヤ 2 インターフェイスとして設定するには、キーワードを指定しないで **switchport** コマンドを一度入力する必要があります。そのあとで、キーワードとともにさらに **switchport** コマンドを入力できます。この処理は、インターフェイスに対して **switchport** コマンドをまだ入力していない場合だけ必要となります。

ドロップしきい値の設定についての詳細は、『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*』の「Configuring IEEE 802.1Q Tunneling and Layer 2 Protocol Tunneling」の章を参照してください。

■ **l2protocol-tunnel drop-threshold**

例

次に、ドロップしきい値を設定する例を示します。

```
Router(config-if)# switchport
Router(config-if)# l2protocol-tunnel drop-threshold 3000
Router(config-if)#
```

関連コマンド

コマンド	説明
l2protocol-tunnel	インターフェイス上でプロトコル トンネリングをイネーブルにし、トンネリングするプロトコルのタイプを指定します。
l2protocol-tunnel cos	すべての入力レイヤ 2 プロトコル トンネリング ポートにグローバルに CoS 値を指定します。
l2protocol-tunnel global drop-threshold	ソフトウェア レベルでのレート制限をイネーブルにします。
l2protocol-tunnel shutdown-threshold	特定のインターフェイス上で、指定されたプロトコルに対して、1 秒以内で処理可能な最大のパケット数を指定します。
show l2protocol-tunnel	1 つのインターフェイスまたはすべてのインターフェイスでトンネリングされるプロトコルを表示します。
switchport	レイヤ 2 スイッチド インターフェイスのスイッチング特性を変更します。

l2protocol-tunnel global drop-threshold

ソフトウェア レベルでのレート制限をイネーブルにするには、**l2protocol-tunnel global drop-threshold** コマンドを使用します。Catalyst 6500 シリーズスイッチでソフトウェア レート リミッタをディセーブルにするには、このコマンドの **no** 形式を使用します。

l2protocol-tunnel global drop-threshold *threshold*

no l2protocol-tunnel global drop-threshold

シンタックスの説明	<i>threshold</i>	超過 PDU を廃棄するまでの着信 PDU の最大レート。有効値は、100 ~ 20,000 PDU です。
------------------	------------------	--

コマンドのデフォルト グローバルなしきい値は設定されていません。

コマンド モード グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン レイヤ 2 プロトコル トンネリング対応ポートに着信する 3 つの PDU（標準 BPDU、CDP、および VTP パケット）はすべて、レート制限されます。レート制限は、レイヤ 2 プロトコル トンネリングの入力方向で行われます。着信 PDU のレートが設定したしきい値を超えると、超過した PDU は廃棄されます。

例 次に、レート制限をグローバルにイネーブルにする例を示します。

```
Router(config)# l2protocol-tunnel global drop-threshold 3000
Router(config)#
```

関連コマンド	コマンド	説明
	l2protocol-tunnel	インターフェイス上でプロトコル トンネリングをイネーブルにし、トンネリングするプロトコルのタイプを指定します。
	l2protocol-tunnel cos	すべての入力レイヤ 2 プロトコル トンネリング ポートにグローバルに CoS 値を指定します。
	l2protocol-tunnel drop-threshold	特定のインターフェイス上で、指定されたプロトコルに対し、廃棄される前に処理される最大の packets 数を指定します。
	l2protocol-tunnel shutdown-threshold	特定のインターフェイス上で、指定されたプロトコルに対して、1 秒以内で処理可能な最大の packets 数を指定します。
	show l2protocol-tunnel	1 つのインターフェイスまたはすべてのインターフェイスでトンネリングされるプロトコルを表示します。

l2protocol-tunnel shutdown-threshold

インターフェイス上で、1 秒間に指定したプロトコルで、処理される最大のパケット数を指定するには、**l2protocol-tunnel shutdown-threshold** コマンドを使用します。すべてのしきい値を 0 にリセットし、シャットダウンしきい値をディセーブルにするには、このコマンドの **no** 形式を使用します。

l2protocol-tunnel shutdown-threshold [cdp | stp | vtp] packets

no l2protocol-tunnel shutdown-threshold [cdp | stp | vtp] packets

シンタックスの説明

cdp	(任意) CDP トンネリングを指定します。
stp	(任意) STP トンネリングを指定します。
vtp	(任意) VTP トンネリングを指定します。
packets	シャットダウンしきい値。有効値は 1 ~ 4096 です。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

packets が一定値を超えると、ポートは **errdisable** ステートになります。

サービス プロバイダーのすべてのエッジ スイッチでは、次のコマンドを入力して、802.1Q トンネルポート上で PortFast BPDU フィルタリングをイネーブルにする必要があります。

```
Router(config-if)# spanning-tree bpdupfilter enable
Router(config-if)# spanning-tree portfast
```



(注)

PortFast BPDU フィルタリングは、トンネル ポートで自動的にイネーブルになります。

プロトコルを指定しない場合、**packets** 値がすべてのプロトコルに適用されます。

スイッチ ポートだけにプロトコル トンネリングを設定できます。LAN ポートをレイヤ 2 インターフェイスとして設定するには、キーワードを指定しないで **switchport** コマンドを一度入力する必要があります。そのあとで、キーワードとともにさらに **switchport** コマンドを入力できます。この処理は、インターフェイスに対して **switchport** コマンドをまだ入力していない場合だけ必要となります。

ドロップしきい値の設定についての詳細は、『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*』の「Configuring IEEE 802.1Q Tunneling and Layer 2 Protocol Tunneling」の章を参照してください。

例 次に、インターフェイス上で、1 秒間に処理される CDP パケットの最大数を指定する例を示します。

```
Router(config-if)# switchport  
Router(config-if)# l2protocol-tunnel shutdown-threshold cdp 200  
Router(config-if)#
```

関連コマンド

コマンド	説明
l2protocol-tunnel	インターフェイス上でプロトコル トンネリングをイネーブルにし、トンネリングするプロトコルのタイプを指定します。
show l2protocol-tunnel	1 つのインターフェイスまたはすべてのインターフェイスでトンネリングされるプロトコルを表示します。
switchport	レイヤ 2 スイッチド インターフェイスのスイッチング特性を変更します。

l2 vfi manual

レイヤ 2 Virtual Forwarding Instance (VFI) を作成し、レイヤ 2 マニュアル コンフィギュレーション サブモードを開始するには、**l2 vfi manual** コマンドを使用します。レイヤ 2 VFI を削除するには、このコマンドの **no** 形式を使用します。

l2 vfi name manual

no l2 vfi name manual

シンタックスの説明

<i>name</i>	新規レイヤ 2 VFI または既存のレイヤ 2 VFI の名前
-------------	---------------------------------

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

VFI は、1 つまたは複数の VC にパケットを転送するために、ソフトウェアベースまたはハードウェアベースのデータ プレーンによって使用されるデータ構造体の集合です。コントロールプレーンおよびデータ プレーンの両方によってデータ入力と更新が行われ、コントロールプレーンとデータ プレーンの間でデータ構造体インターフェイスとしても機能します。

レイヤ 2 VFI 手動コンフィギュレーション サブモードでは、次のパラメータを設定できます。

- Virtual Private LAN Service (VPLS) ドメインの Virtual Private Network (VPN; 仮想私設網) ID
- このドメイン内にあるその他の Provider Edge Router (PE Router; PE ルータ) のアドレス
- ピアごとのトンネルシグナリングおよびカプセル化メカニズムのタイプ

レイヤ 2 VFI 手動コンフィギュレーション サブモードでは、次のコマンドを使用できます。

- **[no] vpn id *vpn-id*** : RFC 2685 フォーマットで VPN ID を設定します。設定から VPN ID を削除するには、このコマンドの **no** 形式を使用します。
- **[no] neighbor remote-router-id {encapsulation {l2tpv3 | mpls} | {pw-class *pw-name*} | no-split-horizon}** : ピアごとにトンネルシグナリングおよびカプセル化メカニズムのタイプを指定します。**neighbor** コマンドを参照してください。

例

次に、レイヤ 2 VFI を作成してレイヤ 2 VFI 手動コンフィギュレーション サブモードを開始し、VPN ID を設定する例を示します。

```
Router(config)# l2 vfi vfitest1 manual
Router(config-vfi)# vpn id 303
```

lacp max-bundle

ポート チャネルで許可されるバンドル LACP ポートの最大数を定義するには、**lacp max-bundle** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

lacp max-bundle max-bundles

no lacp max-bundle

シンタックスの説明

<i>max-bundles</i>	ポート チャネルで許可されるバンドル ポートの最大数。有効値は 1 ~ 8 です。
--------------------	---

コマンドのデフォルト

デフォルト設定は次のとおりです。

- 最大 8 個のバンドル ポート
- ポート チャネルごとに最大 8 個のバンドル ポートおよび 8 個のホットスタンバイ ポート (LACP バンドルの両側のポート チャネルが同一設定である場合)

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、ポート チャネルでバンドルするポートの最大数を設定する例を示します。

```
Router(config-if)# lacp max-bundle 4
Router(config-if)#
```

関連コマンド

コマンド	説明
show lacp	LACP 情報を表示します。

lACP port-priority

物理インターフェイスのプライオリティを設定するには、**lACP port-priority** コマンドを使用します。

lACP port-priority priority

シンタックスの説明

priority 物理インターフェイスのプライオリティ。有効値は、1 ~ 65,535 です。

コマンドのデフォルト

32768

コマンドモード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

Catalyst 6500 シリーズ スイッチの各ポートには、ポート プライオリティを割り当てる必要があります。ポート プライオリティは、自動的に設定することも、**lACP port-priority** コマンドを入力して指定することもできます。ポート プライオリティはポート番号とともに使用され、ポート ID を形成します。ポート プライオリティは、ハードウェア制限上すべてのポートを集めることができない場合に、スタンバイ モードにする必要があるポートを決定します。

このコマンドはグローバル コンフィギュレーション コマンドですが、*priority* をサポートするのは、LACP 対応物理インターフェイスがあるポート チャネルだけです。

このコマンドは、LACP 対応インターフェイスでサポートされます。

プライオリティの設定では、数が大きいほどプライオリティは低くなります。

例

次に、インターフェイスのプライオリティを設定する例を示します。

```
Router(config-if)# lACP port-priority 23748
Router(config-if)#
```

関連コマンド

コマンド	説明
channel-group	EtherChannel インターフェイスの EtherChannel グループへの割り当ておよび設定を行います。
channel-protocol	チャネルを管理するためにインターフェイスで使用するプロトコルを設定します。
lACP system-priority	システムのプライオリティを設定します。
show lACP	LACP 情報を表示します。

lacp rate

LACP パケットがインターフェイスに入力されるレートを設定するには、**lacp rate** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

lacp rate {normal | fast}

no lacp rate

シンタックスの説明	normal	通常レート of 30 秒レートの LACP パケットが入力されることを指定します。
	fast	リンクが確立してから高速レートの 1 秒レートの LACP パケットが入力されることを指定します。

コマンドのデフォルト 90 秒

コマンドモード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドは、LACP 対応インターフェイスでサポートされます。

例 次に、LACP パケットが 1 秒レートの入力されるように指定する例を示します。

```
Router(config-if)# lacp rate fast
Router(config-if)#
```

関連コマンド	コマンド	説明
	show lacp	LACP 情報を表示します。

lacp system-priority

システムのプライオリティを設定するには、**lacp system-priority** コマンドを使用します。

lacp system-priority priority

シンタックスの説明	<i>priority</i>	システムのプライオリティ。有効値は、1 ~ 65,535 です。
-----------	-----------------	----------------------------------

コマンドのデフォルト	32768
------------	-------

コマンド モード	グローバル コンフィギュレーション (config) (config)
----------	-------------------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

LACP を実行する各 Catalyst 6500 シリーズ スイッチに、システム プライオリティを割り当てる必要があります。システム プライオリティは、自動的に設定することも、**lacp system-priority** コマンドを入力して指定することもできます。システム プライオリティは Catalyst 6500 シリーズ スイッチ MAC アドレスとともに使用され、システム ID を形成します。他のシステムとのネゴシエーション時にも使用されます。

このコマンドはグローバル コンフィギュレーション コマンドですが、*priority* は、LACP 対応物理インターフェイスがあるポート チャネルでサポートされます。

プライオリティの設定では、数が大きいほどプライオリティは低くなります。

lacp system-priority コマンドを入力することもできます。このコマンドを入力すると、デフォルトでグローバル コンフィギュレーション モードになります。

例	次に、システム プライオリティを設定する例を示します。
---	-----------------------------

```
Router(config)# lacp system-priority 23748
Router(config)#
```

関連コマンド

コマンド	説明
channel-group	EtherChannel インターフェイスの EtherChannel グループへの割り当ておよび設定を行います。
channel-protocol	チャンネルを管理するためにインターフェイスで使用するプロトコルを設定します。
lacp port-priority	物理インターフェイスのプライオリティを設定します。
show lacp	LACP 情報を表示します。

line

設定する回線を特定し、ライン コンフィギュレーション コレクション モードを開始するには、**line** コマンドを使用します。

```
line {{first-line-number [ending-line-number]} | {console first-line-number} | {vtty
first-line-number [ending-line-number]}}
```

シンタックスの説明		
<i>first-line-number</i>	回線タイプの指定時に設定する端末回線（または連続したグループの最初の回線）の相対番号。有効値は、0 ~ 1510 です。	
<i>ending-line-number</i>	(任意) 設定する連続したグループの最終回線の相対番号。有効値は、101 ~ 1510 です。	
console <i>first-line-number</i>	コンソール端末回線を指定します。有効値は、0 です。	
vtty	リモート コンソール アクセスに仮想端末回線を指定します。	

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン コンソール ポートは、DCE（データ通信装置）です。

console または **vtty** を指定しない場合、*first-line-number* および *ending-line-number* は相対回線番号ではなく絶対回線番号となります。

line コマンドにより、単一回線または連続した回線範囲を指定できます。ただし、回線番号が必要です。回線番号を入力しないと、エラー メッセージが送信されます。

オプションの回線タイプ (**console** または **vtty**) とともに **line** コマンドを入力すると、相対回線番号としての回線番号が指定されます。たとえば、回線 7 (TTY 回線) に回線パラメータを設定する場合、**line tty 7** コマンドを入力できます。

また、回線タイプを指定しないで **line** コマンドを使用することもできます。この場合、回線番号は絶対回線番号として処理されます。たとえば、回線 5 (タイプは問わない) に回線パラメータを設定する場合、**line 5** コマンドを入力できます。

絶対回線番号は連続的に増加するため、大規模システムでは管理が困難になります。相対回線番号は、設定時に使用される簡単な表記法です。Cisco IOS ソフトウェアでは内部的に絶対回線番号を使用します。相対回線番号はどこでも使用できるわけではありませんが、絶対回線番号は使用できます。

絶対回線番号および相対回線番号の表を表示するには、**show users all** コマンドを入力します。絶対回線番号は左端に表示され、そのあとに回線タイプ、次に相対回線番号が表示されます。相対回線番号は常に 0 で始まり、回線タイプを定義します。たとえば 2 番めの仮想回線を回線 VTY 1 と指定することは、回線 143 (絶対回線番号) と覚えるよりも容易です。

ルータをローカルに設定する端末は、コンソール ポートに接続されます。コンソール ポートに回線パラメータを設定するには、**line console 0** コマンドを入力します。コンソールの相対回線番号は、**0** にしてください。

ライン コンソール コンフィギュレーション モードを開始すると、送信/受信速度を設定できます。有効値は **0 ~ 9600** で、デフォルトのレートは **9600** です。

仮想端末回線を使用すると、ルータへのリモート アクセスが可能になります。仮想端末回線は、補助ポートまたはコンソール ポートのいずれとも対応付けられません。デフォルトでは、ルータには仮想端末回線が **5** つあります。ただし、仮想端末回線は追加で作成できます。『*Cisco IOS Terminal Services Configuration Guide*』の「Configuring Protocol Translation and Virtual Asynchronous Devices」の章を参照してください。

コンソール ポートまたは仮想端末回線を設定すると、通信パラメータの設定、自動ボー接続の指定、および使用している端末の端末動作パラメータの設定などの処理を実行できます。

例 次に、仮想端末回線 **0 ~ 4** の設定を開始する例を示します。

```
Router(config)# line vty 0 4
Router(config-line)#
```

次に、**no login** コマンドにより最大 **100** の仮想端末回線の作成および設定を行う例を示します。

```
Router(config)# line vty 0 99
Router(config-line)# no login
Router(config-line)#
```

次に、仮想端末回線番号 **5** およびそれ以降の番号がついたすべての仮想端末回線を削除する例を示します。仮想端末回線 **0 ~ 4** だけが残ります。

```
Router(config-line)# no line vty 5
Router(config)#
```

次に、コンソール ポートの送信/受信速度を設定する例を示します。

```
Router(config)# line console 0
Router(config-line)# speed 9600
Router(config-line)#
```

関連コマンド

コマンド	説明
show line	端末回線のパラメータを表示します。
show users	ルータのアクティブ回線に関する情報を表示します。

link debounce

インターフェイス上のデバウンス タイマーをイネーブルにするには、**link debounce** コマンドを使用します。タイマーをディセーブルにするには、このコマンドの **no** 形式を使用します。

link debounce [*time time*]

no link debounce

シンタックスの説明 **time time** (任意) 拡張デバウンス タイマーを指定します。有効値は、100 ~ 5000 ミリ秒です。

コマンドのデフォルト 表 2-13 にデバウンス タイマーのデフォルト値を一覧表示します。

表 2-13 ポート デバウンス タイマー遅延時間

ポート タイプ	デバウンス タイマーがディセーブルの場合	デバウンス タイマーがイネーブルの場合
10BASE-FL ポート	300 ミリ秒	3100 ミリ秒
10/100BASE-TX ポート	300 ミリ秒	3100 ミリ秒
100BASE-FX ポート	300 ミリ秒	3100 ミリ秒
10/100/1000BASE-TX ポート	300 ミリ秒	3100 ミリ秒
1000BASE-TX ポート	300 ミリ秒	3100 ミリ秒
ファイバ ギガビット ポート	10 ミリ秒	100 ミリ秒
WS-X6501-10GEX4 および WS-X6502-10GE を除く 10 ギガビット ポート	10 ミリ秒	100 ミリ秒
WS-X6501-10GEX4 および WS-X6502-10GE 10 ギガビット ポート	1000 ミリ秒	3100 ミリ秒

コマンド モード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

link debounce

使用上のガイドライン

time time キーワードおよび引数をサポートするのは、ギガビット イーサネットおよび 10 ギガビット イーサネットのインターフェイスだけです。

time time キーワードおよび引数は、銅線メディアでサポートされません。

デバウンス タイマーは、ファームウェアがソフトウェアにリンクダウンを通知するまで待機する時間を設定します。リンクアップはファームウェアによってただちに通知されるので、デバウンス タイマーはリンクアップには適用されません。

デフォルトのデバウンス時間は、引数のない **link debounce** コマンドを入力すると適用されます。たとえば **link debounce time 100** コマンドを入力することは、引数を指定せずに **link debounce** コマンドを入力することと同じです。次のように設定のリンク デバウンス エントリが表示されます。

```
interface GigabitEthernet1/1
  no ip address
  link debounce
```

インターフェイスのデバウンス コンフィギュレーションを表示するには、**show interfaces debounce** コマンドを入力します。

例

次に、ギガビット イーサネット ファイバインターフェイスにデバウンス タイマーを設定する例を示します。

```
Router (config-if)# link debounce time 100
Router (config-if)#
```

関連コマンド

コマンド	説明
show interfaces debounce	デバウンス タイマーのステータスおよび設定を表示します。

load-interval

インターフェイスの平均負荷の計算に使用する時間を指定するには、**load-interval** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

load-interval seconds

no load-interval

シンタックスの説明	<i>seconds</i>	負荷統計の計算に使用する時間。有効値は 30 ~ 600 秒 (30 秒単位) です。
-----------	----------------	---

コマンドのデフォルト	300 seconds (5 minutes)
------------	-------------------------

コマンド モード	インターフェイス コンフィギュレーション (config-if) フレームリレー DLCI コンフィギュレーション (config-fr-dlci)
----------	---

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン デフォルトでは、負荷データは 5 分ごと、つまり 300 秒ごとに収集されます。このデータを使用して、1 秒ごとのビット数およびパケット数の入力レート、および秒、負荷、信頼性ごとのビット数およびパケットの出力レートなど、負荷統計を算出できます。負荷データは加重平均計算を使用して算出され、最近の負荷データは古い負荷データより過重が大きくなります。

5 分間にわたる平均ではなく、トラフィックの短期バーストに負荷計算がよりよく反応するようにするには、負荷平均計算の時間を短縮します。たとえば負荷インターバルを 30 秒に設定すると、直近の 30 秒間の加重平均負荷を反映できます。

デフォルト値の 5 分 (300 秒) より短い時間または長い時間に計算インターバルを変更するには、**load-interval** コマンドを入力します。時間を短縮すると、**show interface** コマンドまたは **show frame-relay pvc** コマンドを使用したときに表示される入出力統計はより最近のものになり、長期間にわたる平均負荷は反映されなくなります。

バックアップ インターフェイスがアクティブになる可能性を増減するには、**load-interval** コマンドを入力します。たとえば、アクティブ インターフェイスにおける負荷の急増によってバックアップ ダイアル インターフェイスをトリガーすることができます。

例

次に、シリアル インターフェイス 0 の負荷インターバルを設定し、30 秒のインターバルで平均が計算されるようにする例を示します。

```
Router(config)# interface serial 0  
Router(config-if)# load-interval 30
```

次に、DLCI が 100 であるフレーム リレー PVC で負荷インターバルを 60 秒に設定する例を示します。

```
Router(config)# interface serial 1/1  
Router(config-if)# encapsulation frame-relay ietf  
Router(config-if)# frame-relay interface-dlci 100  
Router(config-fr-dlci)# load-interval 60
```

関連コマンド

コマンド	説明
show frame-relay pvc	フレーム リレー インターフェイスの PVC に関する統計情報を表示します。

logging event link-status (global configuration)

デフォルトを変更する、またはシステムの初期化中の link-status イベント メッセージングを設定するには、**logging event link-status** コマンドを使用します。link-status イベント メッセージングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging event link-status {default | boot}

no logging event link-status {default | boot}

シンタックスの説明

default	システムのすべてのインターフェイス上で、インターフェイス state-change イベントのシステム ロギングをイネーブルにします。
boot	システムのすべてのインターフェイス上で、システムの初期化中のインターフェイス state-change イベントのシステム ロギングをイネーブルにします。

コマンドのデフォルト

インターフェイス state-change メッセージは送信されません。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

システム初期化中の link-status メッセージングをイネーブルにする場合、**logging event link-status boot** コマンドを入力する必要はありません。**logging event link-status default** コマンドは、システムの初期化中でもシステム メッセージを記録します。

logging event link-status default コマンドと **no logging event link-status boot** コマンドの両方を入力すると、システムの初期化後 Catalyst 6500 シリーズ スイッチのすべてのモジュールが動作してから、インターフェイス state-change イベントが記録されます。**logging event link-status default** および **no logging event link-status boot** コマンドは、システムの実行コンフィギュレーションに保存および保持されます。

実行コンフィギュレーションに **logging event link-status default** コマンドと **no logging event link-status boot** コマンドの両方が存在し、システムの初期化中にインターフェイス state-change メッセージを表示する場合は、**logging event link-status boot** コマンドを入力します。

例

次に、システムのすべてのインターフェイス上でインターフェイス state-change イベントのシステム ロギングをイネーブルにする例を示します。

```
Router(config)# logging event link-status default
Router(config)#
```

■ logging event link-status (global configuration)

次に、すべてのインターフェイス上でシステム初期化中のインターフェイス state-change イベントのシステム ロギングをイネーブルにする例を示します。

```
Router(config)# logging event link-status boot
Router(config)#
```

次に、すべてのインターフェイス上でインターフェイス state-change イベントのシステム ロギングをディセーブルにする例を示します。

```
Router(config)# no logging event link-status default
Router(config)#
```

次に、システム初期化中のインターフェイス state-change イベントのシステム ロギングをディセーブルにする例を示します。

```
Router(config)# no logging event link-status boot
Router(config)#
```

関連コマンド

コマンド	説明
show running-config	モジュールまたはレイヤ 2 VLAN のステータスおよび設定を表示します。

logging event link-status (interface configuration)

インターフェイス上で link-status イベント メッセージングをイネーブルにするには、**logging event link-status** コマンドを使用します。link-status イベント メッセージングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging event link-status

no logging event link-status

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト インターフェイス state-change メッセージは送信されません。

コマンド モード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン 特定のインターフェイス上でインターフェイス state-change イベントのシステム ロギングをイネーブルにするには、**logging event link-status** コマンドを入力します。

システムのすべてのインターフェイス上でインターフェイス state-change イベントのシステム ロギングをイネーブルにするには、**logging event link-status** コマンドを入力します。

例 次に、インターフェイス上でインターフェイス state-change イベントのシステム ロギングをイネーブルにする例を示します。

```
Router(config-if)# logging event link-status
Router(config-if)#
```

次に、インターフェイス上でインターフェイス state-change イベントのシステム ロギングをディセーブルにする例を示します。

```
Router(config-if)# no logging event link-status default
Router(config-if)#
```

関連コマンド	コマンド	説明
	show running-config	モジュールまたはレイヤ 2 VLAN のステータスおよび設定を表示します。

logging event subif-link-status

サブインターフェイス上で link-status イベント メッセージングをイネーブルにするには、**logging event subif-link-status** コマンドを使用します。サブインターフェイスで link-status イベント メッセージングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging event subif-link-status

no logging event subif-link-status

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

サブインターフェイス state-change メッセージは送信されません。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、次のサブインターフェイスでサポートされています。

- フレーム リレー サブインターフェイス
- OSM-GE-WAN サブインターフェイス
- SIP サブインターフェイス
- LAN サブインターフェイス

特定のサブインターフェイス上でインターフェイス state-change イベントのシステム ロギングをイネーブルにするには、**logging event subif-link-status** コマンドを入力します。

特定のインターフェイス上でインターフェイス state-change イベントのシステム ロギングをイネーブルにするには、**logging event link-status** コマンドを入力します。

システムのすべてのインターフェイス上でインターフェイス state-change イベントのシステム ロギングをイネーブルにするには、**logging event link-status** コマンドを入力します。

例

次に、サブインターフェイス上でインターフェイス state-change イベントのシステム ロギングをイネーブルにする例を示します。

```
Router(config-if)# logging event subif-link-status
Router(config-if)#
```

次に、サブインターフェイス上でインターフェイス state-change イベントのシステム ログをディセーブルにする例を示します。

```
Router(config-if)# no logging event subif-link-status
Router(config-if)#
```

関連コマンド

コマンド	説明
show running-config	モジュールまたはレイヤ 2 VLAN のステータスおよび設定を表示します。

logging ip access-list cache (global configuration mode)

OAL パラメータを設定するには、**logging ip access-list cache** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
logging ip access-list cache {{entries entries} | {interval seconds} | {rate-limit pps} |
{threshold packets}}
```

```
no logging ip access-list cache [entries | interval | rate-limit | threshold]
```

シンタックスの説明

entries <i>entries</i>	ソフトウェアにキャッシュされるログ エントリの最大数を指定します。有効値は 0 ~ 1,048,576 エントリです。
interval <i>seconds</i>	エントリが Syslog に送信されるまでの最大間隔を指定します。有効値は 5 ~ 86,400 秒です。
rate-limit <i>pps</i>	ソフトウェアで記録されるパケット数/秒を指定します。有効値は 10 ~ 1,000,000 pps です。
threshold <i>packets</i>	エントリが Syslog に送信されるまでに一致するパケットの数を指定します。有効値は 1 ~ 1,000,000 パケットです。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- **entries** : **8000** エントリ
- **seconds** : **300** 秒 (5 分)
- **rate-limit pps** : **0** (レート制限はオフ) で、すべてのパケットが記録されます。
- **threshold packets** : **0** (レート制限はオフ) で、システム ログは一致するパケットの数ではトリガーされません。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

OAL は、IPv4 ユニキャスト トラフィックだけでサポートされます。

同じシャーシで OAL および VACL キャプチャを設定することはできません。OAL キャプチャと VACL キャプチャは、互換性がありません。OAL を設定した場合は、Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) を使用してトラフィックをキャプチャします。

update-interval *seconds* コマンドで指定された期間エントリが非アクティブである場合、そのエントリはキャッシュから削除されます。

キーワードを指定せずに **no logging ip access-list cache** コマンドを入力すると、すべてのパラメータがデフォルト値に戻ります。

拒否されたパケットを記録するように OAL が設定されている場合は、ICMP 到達不能レート制限を 0 に設定しておく必要があります。

例

次に、ソフトウェアにキャッシュされるログ エントリの最大数を指定する例を示します。

```
Router(config)# logging ip access-list cache entries 200
Router(config)#
```

次に、エントリがシステム ログに送信されるまでの最大間隔を指定する例を示します。

```
Router(config)# logging ip access-list cache interval 350
Router(config)#
```

次に、ソフトウェアで記録されるパケット数/秒を指定する例を示します。

```
Router(config)# logging ip access-list cache rate-limit 100
Router(config)#
```

次に、エントリがシステム ログに送信されるまでに一致するパケットの数を指定する例を示します。

```
Router(config)# logging ip access-list cache threshold 125
Router(config)#
```

関連コマンド

コマンド	説明
clear logging ip access-list cache	OAL キャッシュからすべてのエントリをクリアして、Syslog に送信します。
logging ip access-list cache (interface configuration mode)	方向に基づいてインターフェイス上で OAL ロギング キャッシュをイネーブルにします。
show logging ip access-list	ロギング IP アクセス リストに関する情報を表示します。

logging ip access-list cache (interface configuration mode)

インターフェイス上で方向に基づいた OAL ロギング キャッシュをイネーブルにするには、**logging ip access-list cache** コマンドを使用します。OAL をディセーブルにするには、このコマンドの **no** 形式を使用します。

logging ip access-list cache [in | out]

no logging ip access-list cache

シンタックスの説明

in	(任意) 入力パケットの OAL をイネーブルにします。
out	(任意) 出力パケットの OAL をイネーブルにします。

コマンドのデフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、適用される ACL で **log** キーワードが一致するトラフィックでサポートされます。拒否されたパケットを記録するように OAL が設定されている場合は、ICMP 到達不能レート制限を 0 に設定しておく必要があります。

PFC3A が搭載されたシステムでは、トンネル インターフェイス上の出力方向はサポートされていません。

OAL は、IPv4 ユニキャスト トラフィックだけでサポートされます。

同じシャーシで OAL および VACL キャプチャを設定することはできません。OAL キャプチャと VACL キャプチャは、互換性がありません。OAL を設定した場合は、SPAN を使用してトラフィックをキャプチャします。

update-interval seconds コマンドで指定された期間エントリが非アクティブである場合、そのエントリはキャッシュから削除されます。

キーワードを指定せずに **no logging ip access-list cache** コマンドを入力すると、すべてのパラメータがデフォルト値に戻ります。

例 次に、入力パケットの OAL をイネーブルにする例を示します。

```
Router(config-if)# logging ip access-list cache in
Router(config-if)#
```

次に、出力パケットの OAL をイネーブルにする例を示します。

```
Router(config-if)# logging ip access-list cache out  
Router(config-if)#
```

関連コマンド

コマンド	説明
clear logging ip access-list cache	OAL キャッシュからすべてのエントリをクリアして、Syslog に送信します。
logging ip access-list cache (global configuration mode)	OAL パラメータを設定します。
show logging ip access-list	ロギング IP アクセス リストに関する情報を表示します。

mac access-list extended

サブコマンドにアクセスして、拡張 MAC アクセス リストを定義するには、**mac access-list extended** コマンドを使用します。MAC アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

mac access-list extended name

no mac access-list extended name

シンタックスの説明

<i>name</i>	エントリが属する ACL 名
-------------	----------------

コマンドのデフォルト

デフォルト ACL はありません。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ACL 名を入力する場合、次の命名規則に従います。

- 最大 31 文字で、a ~ z、A ~ Z、0 ~ 9、ダッシュ文字 (-)、アンダースコア (_)、ピリオド文字 (.) を含むことができます。
- 英文字で始まり、すべてのタイプのすべての ACL で一意である必要があります。
- 大文字と小文字を区別します。
- 番号は使用できません。
- キーワードは使用できません。避けるべきキーワードは、**all**、**default-action**、**map**、**help**、および **editbuffer** です。

MAC アドレスに基づいて、IPX、DECnet、AppleTalk、VINES、または XNS トラフィックをフィルタリングする名前付き ACL を設定できます (MAC ACL による IPX フィルタリングは、PFC3 搭載の場合にだけサポートされます)。

PFC3 を搭載しているシステムで、EtherType 0x8137 に適合する MAC アクセス リストを使用して IPX トラフィックを分類する場合、**ipx-arp** または **ipx-non-arp** プロトコルを使用します。

mac access-list extended name コマンドを入力したら、次のサブセットを使用して、MAC アクセス リストのエントリを作成または削除します。

```
[no] {permit | deny} {{src-mac mask | any} {dest-mac mask} | any} [protocol [vlan vlan]
[cos value]]
```

vlan vlan および **cos value** キーワードと引数は、PFC3BXL または PFC3B モードでサポートされています。

vlan vlan および **cos value** キーワードおよび引数は、MAC VACL ではサポートされません。

表 2-14 に、**mac access-list extended** サブコマンドの構文を示します。

表 2-14 **mac access-list extended** サブコマンド

サブコマンド	説明
no	(任意) アクセス リストからステートメントを削除します。
permit	条件が一致した場合にアクセスを許可します。
deny	条件が一致した場合にアクセスを禁止します。
<i>src-mac mask</i>	次の形式の送信元 MAC アドレス。 <i>source-mac-address source-mac-address-mask</i>
any	任意のプロトコル タイプを指定します。
<i>dest-mac mask</i>	(任意) 次の形式の宛先 MAC アドレス。 <i>dest-mac-address dest-mac-address-mask</i>
<i>protocol</i>	(任意) プロトコル名または番号。有効値のリストについては、以下を参照してください。
vlan vlan	(任意) VLAN ID を指定します。有効値は 0 ~ 4095 です。
cos value	(任意) CoS 値を指定します。有効値は 0 ~ 7 です。

有効なプロトコル名は次のとおりです。

- 0x0-0xFFFF - 任意の EtherType (16 進数)
- **aarp** - EtherType: AppleTalk ARP
- **amber** - EtherType: DEC-Amber
- **appletalk** - EtherType: AppleTalk/EtherTalk
- **dec-spanning** - EtherType: DEC-Spanning-Tree
- **decnet-iv** - EtherType: DECnet Phase IV
- **diagnostic** - EtherType: DEC-Diagnostic
- **dsm** - EtherType: DEC-DSM
- **etype-6000** - EtherType: 0x6000
- **etype-8042** - EtherType: 0x8042
- **ip** - EtherType: 0x0800
- **ipx-arpa** - IPX arpa
- **ipx-non-arpa** - IPX 非 arpa
- **lat** - EtherType: DEC-LAT
- **lavr-sca** - EtherType: DEC-LAVC-SCA
- **mop-console** - EtherType: DEC-MOP Remote Console
- **mop-dump** - EtherType: DEC-MOP Dump
- **msdos** - EtherType: DEC-MSDOS
- **mumps** - EtherType: DEC-MUMPS
- **netbios** - EtherType: DEC-NETBIOS
- **vines-echo** - EtherType: VINES Echo
- **vines-ip** - EtherType: VINES IP

- **xns-idp** - EtherType: XNS Internet Datagram Protocol (IDP)

src-mac mask または *dest-mac mask* 値を入力する場合は、次の注意事項および制限事項に注意してください。

- MAC アドレスは、0030.9629.9f84 などのドット付き 16 進表記で 3 つの 4 バイト値として入力します。
- MAC アドレス マスクは、ドット付き 16 進表記で 3 つの 4 バイト値として入力します。1 ビットをワイルドカードとして使用します。たとえば、アドレスを完全に一致させるには、0000.0000.0000 を使用します (0.0.0 として入力できます)。
- 省略可能な *protocol* については、EtherType またはキーワードのいずれかを入力できます。
- *protocol* なしのエントリはどのプロトコルとも一致します。
- アクセス リスト エントリは入力順にスキャンされます。最初に一致したエントリが使用されます。パフォーマンスを高めるには、アクセス リストの初めの方に、最もよく使用されるエントリを置きます。
- リストの最後に明示的な **permit any any** エントリを含めないかぎり、アクセス リストの最後には暗示的な **deny any any** エントリが存在します。
- 新しいエントリはすべて既存のリストの最後に置かれます。リストの中間にエントリを追加できません。

変造されたり、無効であったり、故意に破壊されたりした EtherType 0x800 IP フレームは、IP トラフィックとして認識されず、IP ACL によりフィルタリングされます。

mac access-list extended コマンドを **ip** キーワードとともに使用して作成された ACE は、変造されたり、無効であったり、故意に破壊されたりした EtherType 0x800 IP フレームだけをフィルタリングします。その他の IP トラフィックはフィルタリングしません。

例

次に、0000.4700.0001 から 0000.4700.0009 へのトラフィックを拒否する `mac_layer` という名前の MAC アクセス リストを作成する例を示します。その他のトラフィックはすべて許可されます。

```
Router(config)# mac access-list extended mac_layer
Router(config-ext-macl)# deny 0000.4700.0001 0.0.0 0000.4700.0009 0.0.0 dsm
Router(config-ext-macl)# permit any any
```

関連コマンド

コマンド	説明
show mac-address-table	MAC アドレス テーブルに関する情報を表示します。

mac-address-table aging-time

レイヤ 2 テーブルでエントリのエージング タイムを設定するには、**mac-address-table aging-time** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mac-address-table aging-time seconds [routed-mac | vlan vlan-id]

no mac-address-table aging-time seconds [routed-mac | vlan vlan-id]

シンタックスの説明	
<i>seconds</i>	エージング タイム。有効値は、0 および 5 ~ 1,000,000 秒です。
routed-mac	(任意) routed MAC (RM; ルーテッド MAC) エージング インターバルを指定します。
vlan vlan-id	(任意) 変更されたエージング タイムを適用させる VLAN を指定します。有効値は、1 ~ 4094 です。

コマンドのデフォルト **300 秒**

コマンド モード グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン VLAN を入力しない場合、変更はすべてのルーテッド ポート VLAN に適用されます。エージングをディセーブルにするには、**0** 秒を入力します。ルーテッド MAC (RM) ビットが設定されたトラフィックの MAC アドレスのエージング タイムを設定するには、**routed-mac** キーワードを入力します。

例 次に、エージング タイムを設定する例を示します。

```
Router(config)# mac-address-table aging-time 400
Router(config)#
```

次に、RM エージング タイムを変更する例を示します。

```
Router(config)# mac-address-table aging-time 500 routed-mac
Router(config)#
```

次に、エージングをディセーブルにする例を示します。

```
Router(config)# mac-address-table aging-time 0
Router(config)
```

■ mac-address-table aging-time

関連コマンド

コマンド	説明
show mac-address-table	MAC アドレス テーブルに関する情報を表示します。

mac-address-table learning

MAC アドレス ラーニングをイネーブルにするには、**mac-address-table learning** コマンドを使用します。学習をディセーブルにするには、このコマンドの **no** 形式を使用します。

[default] mac-address-table learning **{ {vlan vlan-id} | {vlans vlan-range} | {interface interface slot/port} }** **[module num]**

no mac-address-table learning **{ {vlan vlan-id} | {vlans vlan-range} | {interface interface slot/port} }** **[module num]**

シンタックスの説明

default	(任意) デフォルト設定に戻します。
vlan vlan-id	すべての MAC アドレスの VLAN 単位の学習を適用する VLAN を指定します。有効値は、1 ~ 4094 です。
vlans vlan-range	指定されたインスタンスにマッピングする VLAN の番号。有効値は 1 ~ 4094 です。
interface interface slot/port	すべての MAC アドレスのインターフェイス単位の学習を指定します。 インターフェイス タイプ、スロット番号、およびポート番号
module num	(任意) モジュール番号を指定します。

コマンドのデフォルト

モジュールのポート上で VLAN が設定されている場合は、Catalyst 6500 シリーズスイッチのすべてのスーパーバイザ エンジンおよび Distributed Forwarding Card (DFC) は、指定された VLAN のすべての MAC アドレスを学習するようイネーブル化されます。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。
12.(23)SXH	このコマンドは、VLAN の範囲を入力できるように変更されました。

使用上のガイドライン

スーパーバイザ エンジンまたは DFC だけを指定するのに、**module num** キーワードおよび引数が使用されます。

vlan vlan-id キーワードおよび引数は、スイッチ ポート VLAN だけで使用されます。**vlan vlan-id** キーワードおよび引数は、ルーテッド インターフェイスで学習を設定するには使用できません。

interface interface slot/port キーワードおよび引数は、ルーテッド インターフェイスおよびスーパーバイザ エンジンだけで使用できます。**interface interface slot/port** キーワードおよび引数は、スイッチ ポート インターフェイスで学習を設定するには使用できません。

Cisco IOS Release 12.(23)SXH よりあとのリリースでは、ハイフンで区切って VLAN の範囲を入力できます。

例

次に、すべてのモジュールのスイッチ ポート インターフェイス上で MAC アドレス ラーニングをイネーブルにする例を示します。

```
Router (config)# mac-address-table learning vlan 100
Router (config)#
```

次に、すべてのモジュールの VLAN 範囲で MAC アドレス ラーニングをイネーブルにする例を示します。

```
Router (config)# mac-address-table learning vlan 100-115,125
Router (config)#
```

次に、指定されたモジュールのスイッチ ポート インターフェイス上で MAC アドレス ラーニングをイネーブルにする例を示します。

```
Router (config)# mac-address-table learning vlan 100 module 4
Router (config)#
```

次に、すべてのモジュールの指定されたスイッチ ポート インターフェイス上で MAC アドレス ラーニングをディセーブルにする例を示します。

```
Router (config)# no mac-address-table learning vlan 100
Router (config)#
```

次に、すべてのモジュールのルーテッド インターフェイス上で MAC アドレス ラーニングをイネーブルにする例を示します。

```
Router (config)# mac-address-table learning vlan 100
Router (config)#
```

次に、特定のモジュールのルーテッド インターフェイス上で MAC アドレス ラーニングをイネーブルにする例を示します。

```
Router (config)# mac-address-table learning interface FastEthernet 3/48 module 4
Router (config)#
```

次に、特定のルーテッド インターフェイス上のすべてのモジュールで MAC アドレス ラーニングをディセーブルにする例を示します。

```
Router (config)# no mac-address-table learning interface FastEthernet 3/48
Router (config)#
```

関連コマンド

コマンド	説明
show mac-address-table learning	MAC アドレス ラーニング状態を表示します。

mac-address-table limit

MAC 制限をイネーブルにするには、**mac-address-table limit** コマンドを使用します。MAC 制限をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
mac-address-table limit [maximum num] [action {warning | limit | shutdown}]
[notification {syslog | trap | both}]
```

```
mac-address-table limit [{vlan vlan} | {interface type mod/port}] [maximum num]
[action {warning | limit | shutdown}] [flood]
```

```
no mac-address-table limit [vlan vlan] [maximum | action]
```

シンタックスの説明

maximum num	(任意) EARL ごとに許容される VLAN 単位の MAC エントリ最大数を指定します。有効値は、5 ~ 32,000 の MAC アドレス エントリです。
action	(任意) 違反が生じた場合にとるアクションのタイプを指定します。
warning	違反が生じた場合に、Syslog メッセージを 1 つ送信し、それ以上のアクションはとらないように指定します。
limit	違反が生じた場合に、Syslog メッセージの送信または MAC 制限に対応するトラップの生成のいずれか（またはその両方）を行うように指定します。
shutdown	違反が生じた場合に、Syslog メッセージの送信または VLAN のブロック ステートへの移行のいずれか（またはその両方）を行うように指定します。
notification	(任意) 違反が生じた場合に送信される通知のタイプを指定します。
syslog	違反が生じた場合に、Syslog メッセージを送信します。
trap	違反が生じた場合に、トラップ通知を送信します。
both	違反が生じた場合に、Syslog およびトラップ通知を送信します。
vlan vlan	(任意) VLAN 単位で MAC 制限をイネーブルにします。
interface type mod/port	(任意) ポート単位で MAC 制限をイネーブルにします。
flood	(任意) VLAN で不明なユニキャスト フラッドイングをイネーブルにします。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- **maximum num** は 500MAC アドレス エントリです。
- **action** は **warning** です。
- **notification** は **syslog** です。

コマンドモード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

MAC 制限をグローバルにイネーブルにするには、この構文を使用します。

```
mac-address-table limit [maximum num] [action {warning | limit | shutdown}]
[notification {syslog | trap | both}]
```

VLAN 単位の MAC 制限をイネーブルにするには、この構文を使用します。

```
mac-address-table limit [vlan vlan] [maximum num] [action {warning | limit |
shutdown}] [flood]
```

ポート単位の MAC 制限をイネーブルにするには、この構文を使用します。

```
mac-address-table limit [interface type mod/port] [maximum num] [action {warning |
limit | shutdown}] [flood]
```

VLAN 単位の MAC 制限をイネーブルにした場合は、VLAN 単位の MAC 制限が MAC 制限をグローバルにイネーブルにする **mac-address-table limit** コマンドよりも優先します。

MAC エントリの最大数は、VLAN 単位および EARL 単位です。

最大数、アクション、または通知を指定しない場合、デフォルト設定が使用されます。

VLAN 単位の MAC 制限をイネーブルにした場合、MAC 制限は指定された VLAN だけでイネーブルになります。

flood キーワードがサポートされるのは、VLAN インターフェイス上だけです。

limit アクションが設定され、違反が生じた場合にだけ、**flood** アクションが実行されます。

shutdown ステートでは、VLAN は CLI を使用して再度イネーブルにするまでブロック ステートのままになります。

例

次に、MAC 制限をグローバルにイネーブルにする例を示します。

```
Router(config)# mac-address-table limit
Router(config)#
```

次に、VLAN 単位の MAC 制限をイネーブルにする例を示します。

```
Router(config)# mac-address-table limit vlan 501 maximum 50 action shutdown
Router(config)#
```

関連コマンド

コマンド	説明
show mac-address-table limit	MAC アドレス テーブルに関する情報を表示します。

mac-address-table notification mac-move

MAC 移動通知をイネーブルにするには、**mac-address-table notification mac-move** コマンドを使用します。MAC 移動通知をディセーブルにするには、このコマンドの **no** 形式を使用します。

mac-address-table notification mac-move

no mac-address-table notification mac-move

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン MAC アドレスまたはホストが異なるスイッチ ポート間で移動した場合、MAC 移動通知は Syslog メッセージを生成します。

新しい MAC アドレスが content-addressable memory (CAM; 連想メモリ) に追加された場合または MAC アドレスが CAM から削除された場合には、MAC 移動通知は通知を行いません。

MAC 移動通知は、スイッチ ポート上だけでサポートされます。

例 次に、MAC 移動通知をイネーブルにする例を示します。

```
Router(config)# mac-address-table notification mac-move
Router(config)#
```

次に、MAC 移動通知をディセーブルにする例を示します。

```
Router(config)# no mac-address-table notification mac-move
Router(config)#
```

関連コマンド	コマンド	説明
	show mac-address-table notification mac-move	MAC アドレス テーブルに関する情報を表示します。

mac-address-table notification threshold

CAM テーブル使用状況モニタリング通知をイネーブルにするには、**mac-address-table notification threshold** コマンドを使用します。CAM テーブル使用状況モニタリング通知をディセーブルにするには、このコマンドの **no** 形式を使用します。

mac-address-table notification threshold {*limit percentage*} {*interval time*}

no mac-address-table notification threshold

シンタックスの説明

limit percentage	CAM の利用率（パーセンテージ）を指定します。有効値は、1 ～ 100% です。
interval time	通知間隔を指定します。有効値は、120 秒以上です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- ディセーブル
- *percentage* は、**50%** です。
- *time* は **120** 秒です。

コマンドモード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

CAM テーブル使用状況モニタリングをイネーブルにすると、CAM テーブル内の有効エン트리数がカウントされ、CAM の利用率（パーセンテージ）が指定されたしきい値以上になった場合に、メッセージが表示されます。

例

次に、CAM テーブル使用状況モニタリング通知をイネーブルにして、デフォルト設定を使用する例を示します。

```
Router(config)# mac-address-table notification threshold
Router(config)#
```

次に、CAM テーブル使用状況モニタリング通知をイネーブルにして、しきい値および間隔を設定する例を示します。

```
Router(config)# mac-address-table notification threshold limit 20 interval 200
Router(config)#
```

次に、CAM テーブル使用状況モニタリング通知をディセーブルにする例を示します。

```
Router(config)# no mac-address-table notification threshold
Router(config)#
```

関連コマンド

コマンド	説明
show mac-address-table notification threshold	MAC アドレス テーブルに関する情報を表示します。

mac-address-table static

スタティック エントリを MAC アドレス テーブルに追加する、または IGMP スヌーピングをアドレスに対してディセーブルにしてスタティック MAC アドレスを設定するには、**mac-address-table static** コマンドを使用します。このコマンドの **no** 形式の使用法については、「使用上のガイドライン」を参照してください。

```
mac-address-table static mac-addr vlan vlan-id {interface type | drop
[disable-snooping]}
[dlci dlci | pvc vpi/vci] [auto-learn | disable-snooping] [protocol {ip | ipv6 | ipx |
assigned}]

no mac-address-table static mac-addr {vlan vlan-id} {interface type} [disable-snooping]
[dlci dlci | pvc vpi/vci]
```

シンタックスの説明

mac-addr	MAC アドレス テーブルに追加するアドレス
vlan vlan-id	変更されたエージング タイムを適用させる VLAN を指定します。有効値は、1 ~ 4094 です。
interface type	インターフェイス タイプおよびモジュール/ポート番号を指定します。
drop	指定された VLAN 内で設定された MAC アドレスに送受信されるトラフィックをすべて廃棄します。
disable-snooping	(任意) マルチキャスト MAC アドレスの IGMP スヌーピングをディセーブルにします。
dlci dlci	(任意) この MAC アドレスへの DLCI のマッピングを指定します。有効値は、16 ~ 1007 です。
pvc vpi/vci	(任意) この MAC アドレスへの PVC のマッピングを指定します。
auto-learn	(任意) 新規ポートにエントリを更新させます。詳細については、「使用上のガイドライン」を参照してください。
protocol	(任意) エントリに関連付けられたプロトコルを指定します。
ip	IP プロトコルを指定します。
ipv6	IPv6 プロトコルを指定します。
ipx	IPX プロトコルを指定します。
assigned	DECnet、Banyan VINES、および AppleTalk などの割り当てられたプロトコルのパケット アカウントを指定します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドの **no** 形式は、次の場合に使用します。

- 指定したエントリ情報の組み合わせによって作成されたエントリを削除します。
- 指定したアドレスに対して、IGMP スヌーピングはディセーブルになりません。
- MAC アドレスのフレーム リレー DLCI または ATM PVC へのマッピングを削除します。

dlci dlci キーワードおよび引数は、指定されたインターフェイス上でフレーム リレーカプセル化がイネーブルの場合にだけ有効です。

pvc vpi/vci キーワードおよび引数は、ATM インターフェイスだけでサポートされます。

pvc vpi/vci を指定する場合、VPI 値および VCI 値の両方をスラッシュで区切って指定する必要があります。

スタティック MAC アドレスをインストールする場合、スタティック MAC アドレスはポートに関連付けられます。同じ MAC アドレスが異なるポートにある場合、**auto-learn** キーワードを入力すると、エントリが新しいポートに更新されます。

指定する出力インターフェイスは、SVI ではなく、レイヤ 2 IDB である必要があります。

ipx キーワードはサポートされていません。

1 つの入力コマンドで入力できるインターフェイス数は最大 15 個ですが、コマンドを繰り返すことによりさらに多くのインターフェイスを入力できます。

プロトコル タイプを入力しない場合、4 つのプロトコル タイプのそれぞれについてエントリが自動的に作成されます。

このコマンドの **no** 形式を入力しても、システム MAC アドレスは削除されません。

MAC アドレスを削除するときには、**interface type** の入力は省略できます。ユニキャスト エントリの場合、エントリは自動的に削除されます。マルチキャスト エントリの場合、インターフェイスを指定しないとエントリ全体が削除されます。インターフェイスを指定することにより、削除する選択ポートを指定できます。

mac-address-table static mac-addr {vlan vlan-id} {interface type} disable-snooping コマンドは、指定されたスタティックな MAC エントリ /VLAN ペアのスヌーピングだけをディセーブルにします。スヌーピングを再びイネーブルにするには、まず MAC アドレスを削除し、次に **mac-address-table static mac-addr {vlan vlan-id} {interface type}** コマンドを **disable-snooping** キーワードを入力せずに使用して、再インストールします。

mac-address-table static mac-addr {vlan vlan-id} drop コマンドをマルチキャスト MAC アドレスに適用することはできません。

マルチポイント ブリッジングおよびその他の機能をサポートするには、次のようにフレーム リレー インターフェイスに対しては **dlci dlc**i キーワードおよび引数、ATM インターフェイスに対しては **pvc vpi/vci** キーワードおよび引数も指定する必要があります。

```
Router (config) # mac-address-table static 000C.0203.0405 vlan 101 interface ATM6/1 pvc6/101
Router (config) #
```



(注)

フレーム リレー インターフェイスに対して **dlci dlc**i キーワードおよび引数を省略すると、MAC アドレスはこのインターフェイス上の指定の VLAN に設定された最初の DLCI 回線にマッピングされます。ATM インターフェイスに対して **pvc vpi/vci** キーワードおよび引数を省略すると、MAC アドレスはこのインターフェイス上の指定の VLAN に設定された最初の PVC 回線にマッピングされます。MAC アドレスが正しく設定されていることを確認するために、該当するインターフェイス上で常に **dlci dlc**i および **pvc vpi/vci** のキーワードと引数を使用することを推奨します。

■ mac-address-table static

例

次に、MAC アドレス テーブルへスタティック エントリを追加する例を示します。

```
Router(config)# mac-address-table static 0050.3e8d.6400 vlan 100 interface fastethernet5/7
Router(config)#
```

次に、指定されたアドレスに対して IGMP スヌーピングをディセーブルにしてスタティック MAC アドレスを設定する例を示します。

```
Router(config)# mac-address-table static 0050.3e8d.6400 vlan 100 interface fastethernet5/7 disable-snooping
Router(config)#
```

次に、ATM PVC 回線およびフレーム リレー DLCI 回線の MAC アドレス テーブルにスタティック エントリを追加する例を示します。

```
Router(config)# mac-address-table static 0C01.0203.0405 vlan 101 interface ATM6/1 pvc 6/101
Router(config)# mac-address-table static 0C01.0203.0406 vlan 202 interface POS4/2 dlci 200
Router(config)#
```

関連コマンド

コマンド	説明
show mac-address-table	MAC アドレス テーブルに関する情報を表示します。

mac-address-table synchronize

PFC およびすべての DFC にわたってレイヤ 2 MAC アドレス テーブル エントリを同期化するには、**mac-address-table synchronize** コマンドを使用します。MAC アドレス テーブルの同期化をディセーブルにするか、アクティビティ タイマーをリセットするには、このコマンドの **no** 形式を使用します。

mac-address-table synchronize [*activity-time seconds*]

no mac-address-table synchronize [*activity-time seconds*]

シンタックスの説明	activity-time seconds (任意) アクティビティ タイマーのインターバルを指定します。有効値は 160 秒、320 秒、640 秒 です。
------------------	---

コマンドのデフォルト デフォルト設定は次のとおりです。

- ディセーブル
- WS-X6708-10GE の場合はイネーブル
- **activity-time** は 160 秒

コマンド モード グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン 最低 2 個のアクティビティ タイムが通常のレイヤ 2 エージング タイム内 (この機能が分散型 EtherChannel 専用で使用される場合は、分散型 EtherChannel の VLAN に使用されるエージング タイム内) に存在するように、アクティビティ タイムを設定することを推奨します。最低 2 個のアクティビティ タイムがエージング タイム内に存在しない場合は、エラー メッセージが表示されます。

例 次に、アクティビティ タイマー インターバルを指定する例を示します。

```
Router(config)# mac-address-table synchronize activity-time 320
Router(config)#
```

関連コマンド	コマンド	説明
	show mac-address-table synchronize statistics	MAC アドレス テーブルに関する情報を表示します。

mac packet-classify

レイヤ 3 パケットをレイヤ 2 パケットとして分類するには、**mac packet-classify** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mac packet-classify

no mac packet-classify

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

PFC3BXL および PFC3B モードは、プロトコルに依存しない MAC ACL フィルタリングをサポートします。プロトコルに依存しない MAC ACL フィルタリングでは、すべての入力トラフィック タイプ (MAC レイヤ トラフィックのほか、IPv4 トラフィック、IPv6 トラフィック、MPLS トラフィックなど) に MAC ACL が適用されます。

マルチレイヤ MAC ACL QoS フィルタリングには、次のインターフェイス タイプを設定できます。

- レイヤ 3 アドレスが設定されていない VLAN インターフェイス
- Ethernet over Multiprotocol Label Switching (EoMPLS) をサポートするよう設定された物理 LAN ポート
- EoMPLS をサポートするよう設定された論理 LAN サブインターフェイス

マルチレイヤ MAC ACL QoS のフィルタリングを設定されたインターフェイス上で、MAC ACL により許可または拒否された入力トラフィックは、出力インターフェイスにより MAC レイヤ トラフィックとして処理されます。マルチレイヤ MAC ACL QoS のフィルタリングを設定されたインターフェイス上で、MAC ACL により許可または拒否されたトラフィックに、出力 IP ACL を適用することはできません。

マイクロフロー ポリシングは、**mac packet-classify** コマンドがイネーブルに設定されたインターフェイスでは機能しません。

mac packet-classify コマンドにより、レイヤ 3 パケットはレイヤ 2 パケットとして分類され、IP 分類はディセーブルになります。

トラフィックは、802.1Q CoS、トランク VLAN、EtherType、および MAC アドレスに基づいて分類されます。

例

次に、着信および送信レイヤ 3 パケットをレイヤ 2 パケットとして分類する例を示します。

```
Router(config-if)# mac packet-classify
Router(config-if)#
```

次に、着信および送信レイヤ 3 パケットのレイヤ 2 パケットとしての分類をディセーブルにする例を示します。

```
Router(config-if)# no mac packet-classify
Router(config-if)#
```

関連コマンド

コマンド	説明
mac packet-classify use vlan	VLAN ベースの QoS フィルタリングを MAC ACL でイネーブルにします。

mac packet-classify use vlan

MAC ACL で VLAN ベースの QoS フィルタリングをイネーブルにするには、**mac packet-classify use vlan** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mac packet-classify use vlan

no mac packet-classify use vlan

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

PFC3BXL および PFC3B モードは、プロトコルに依存しない MAC ACL フィルタリングをサポートします。プロトコルに依存しない MAC ACL フィルタリングでは、すべての入力トラフィック タイプ (MAC レイヤ トラフィックのほか、IPv4 トラフィック、IPv6 トラフィック、MPLS トラフィックなど) に MAC ACL が適用されます。

レイヤ 2 の service access point (SAP; サービス アクセス ポイント) で符号化されたパケット (Intermediate System-to-Intermediate System Intradomain Routing Protocol (IS-IS) および IPX など) に QoS を適用する場合、レイヤ 2 のキーで VLAN フィールドをディセーブルにするには、**no mac packet-classify use vlan** コマンドを使用する必要があります。

VLAN フィールドがイネーブルの場合、QoS は非 ARPA レイヤ 2 パケット (IS-IS および IPX など) のポリシングを許可しません。

例

次に、VLAN ベースの QoS フィルタリングを MAC ACL でイネーブルにする例を示します。

```
Router(config)# mac packet-classify use vlan
Router(config)
```

次に、VLAN ベースの QoS フィルタリングを MAC ACL でディセーブルにする例を示します。

```
Router(config)# no mac packet-classify use vlan
Router(config)
```

関連コマンド

コマンド	説明
mac packet-classify	レイヤ 2 パケットとしてレイヤ 3 パケットを分類します。

match

VLAN アクセス マップ シーケンスの 1 つまたは複数の ACL を選択することにより **match** 句を指定するには、**match** サブコマンドを使用します。**match** 句は、トラフィック フィルタリングに IP、IPX、または MAC ACL を指定します。**match** 句を削除するには、このコマンドの **no** 形式を使用します。

```
match {ip address {acl-number | acl-name}} | {ipx address {acl-number | acl-name}} |
{mac address acl-name}}
```

```
no match {ip address {acl-number | acl-name}} | {ipx address {acl-number | acl-name}} |
{mac address acl-name}}
```

シンタックスの説明

ip address <i>acl-number</i>	VLAN アクセス マップ シーケンスの IP ACL を 1 つまたは複数選択します。有効値は、1 ~ 199 および 1300 ~ 2699 です。
ip address <i>acl-name</i>	IP ACL を名前選択します。
ipx address <i>acl-number</i>	VLAN アクセス マップ シーケンスの IPX ACL を 1 つまたは複数選択します。有効値は、800 ~ 999 です。
ipx address <i>acl-name</i>	IPX ACL を名前選択します。
mac address <i>acl-name</i>	VLAN アクセス マップ シーケンスの MAC ACL を 1 つまたは複数選択します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

VLAN アクセス マップ サブモード

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

match ipx address および **match mac address** コマンドは、WAN インターフェイス上の VACL ではサポートされません。

VACL で使用される IPX ACL は、IPX プロトコル タイプ、送信元ネットワーク、宛先ネットワークおよび宛先ホスト アドレスだけを指定できます。

MAC シーケンスは、IP または IPX パケットに作用しません。IP パケットおよび IPX パケットは、IP および IPX の **match** 句によってアクセス制御が行われる必要があります。

VACL をセカンダリ VLAN で設定できません。セカンダリ VLAN は、プライマリ VLAN によって設定されたすべての機能を継承します。

次のサブコマンドは、CLI ヘルプに表示されますが、PFC QoS にはサポートされません。

- **match cos**
- **match any**
- **match class-map**
- **match destination-address**

- **match input-interface**
- **match qos-group**
- **match source-address**

設定に関する注意事項および制限については、『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*』を参照してください。

match コマンドの詳細については、『*Cisco IOS Release 12.2 Command Reference*』を参照してください。

例 次に、VLAN アクセス マップの **match** 句を定義する例を示します。

```
Router(config)# vlan access-map ganymede 10
Router(config-access-map)# match ip address 13
Router(config-access-map)#
```

関連コマンド

コマンド	説明
action	パケットの action 句を設定します。
port access-map	ポート アクセス マップを作成するか、ポート アクセス マップ コマンド モードを開始します。
show vlan access-map	VLAN アクセス マップの内容を表示します。
vlan access-map	VLAN アクセス マップを作成するか、VLAN アクセス マップ コマンド モードを開始します。

match protocol

指定されたプロトコル単位でのクラス マップの一致基準を設定するには、**match protocol** コマンドを使用します。プロトコルベースの一致基準をクラス マップから削除するには、このコマンドの **no** 形式を使用します。

```
match protocol {ip | ipv6}
```

```
no match protocol {ip | ipv6}
```

シンタックスの説明

ip	IP パケットのプロトコル一致を指定します。
ipv6	IPv6 パケットのプロトコル一致を指定します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

クラスマップ サブモード

コマンドの履歴

12.2(18)ZY このコマンドのサポートが追加されました。

使用上のガイドライン

match protocol クラス マップ サブコマンドは NBAR を設定し、入力ポートおよび出力ポート上のトラフィックをすべて送信して、PISA のソフトウェアで処理されるようにします。

クラスベース均等化キューイングの場合、一致基準（プロトコル、ACL、入力インターフェイス、QoS ラベル、および EXP フィールド値など）に基づいてトラフィック クラスを定義します。クラスの一貫基準を満たすパケットが、クラスのトラフィックを構成します。

match protocol コマンドは、パケットがクラス マップで指定されたクラスに属するかどうかを判別するのに照合される一致基準として使用されるプロトコル名を指定します。

match protocol コマンドを使用する場合は、まず **class-map** コマンドを入力して一致基準を確立するクラス名を指定する必要があります。

クラス マップで複数のコマンドを指定すると、最後に入力されたコマンドだけが適用されます。最新のコマンドは、以前に入力したコマンドを上書きします。

このコマンドは、NBAR 機能が認知するプロトコルを照合するのに使用されます。NBAR が現在サポートするプロトコルの一覧については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Classification」を参照してください。

例

次に、**ip** という名前のクラス マップを指定し、これに対する一致基準として **IP** を設定する例を示します。

```
Router(config)# class-map ip  
Router(config-cmap)# match protocol ip
```

maxconns (real server configuration submode)

実サーバへのアクティブ接続数を制限するには、**maxconns** コマンドを使用します。接続の最大数をデフォルト設定に変更するには、このコマンドの **no** 形式を使用します。

maxconns *number-conns*

no maxconns

シンタックスの説明

number-conns 任意の時点における実サーバのアクティブ接続最大数。有効値は、0 ~ 4,294,967,295 です。

コマンドのデフォルト

0

コマンド モード

実サーバ コンフィギュレーション サブモード

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

number-conns 値を指定しない場合、デフォルト値は **0** です。つまり、実サーバへの最大接続数はモニタされません。

例

次に、実サーバへのアクティブ接続数を制限する例を示します。

```
Router(config-if)# maxconns 49672
Router(config-if)#
```

次に、デフォルトの設定に戻す例を示します。

```
Router(config-if)# no maxconns
Router(config-if)#
```

関連コマンド

コマンド	説明
faildetect numconns	サーバ障害を示す条件を指定します。
inservice (実サーバ)	Cisco IOS Server Load Balancing (SLB) 機能が使用する実サーバをイネーブルにします。
reassign	別の実サーバへの接続を試す前に未応答になる、新規接続の連続 SYN の最大数を定義します。
retry	障害のあるサーバに接続を試みるまでの待機時間を定義します。

maximum-paths

IP ルーティング プロトコルがサポートできる最大パラレル ルート数を制御するには、**maximum-paths** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

maximum-paths *maximum*

no maximum-paths

シンタックスの説明

<i>maximum</i>	IP ルーティング プロトコルがルーティング テーブルにインストールする最大パラレル ルート数。有効値は、1 ~ 8 です。
----------------	--

コマンドのデフォルト

デフォルト設定は次のとおりです。

- BGP のパスは 1 つです。
- その他すべての IP ルーティング プロトコルのパスは 4 つです。

コマンド モード

ルーティング プロトコル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、宛先に最大 2 つのパスを許可する例を示します。

```
Router(config-router)# maximum-paths 2
Router(config-router)
```

mdix auto

自動 media-dependent interface crossover (MDIX; メディア依存型インターフェイス クロスオーバー) 検出をイネーブルにするには、**mdix auto** コマンドを使用します。自動検出をオフにするには、このコマンドの **no** 形式を使用します。

mdix auto

no mdix auto

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト イネーブル

コマンド モード EXEC

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドは、次のモジュールだけでサポートされています。

- WS-X6748-GE-TX
- WS-SUP720 (銅のポートのみ)
- WS-SUP720-10G (銅のポートのみ)
- WS-SUP32 (銅のポートのみ)
- WS-X6148A-RJ45
- WS-X6148A-GE-TX
- WS-X6548-RJ45
- WS-X6548-RJ21
- WS-X6548-GE-TX
- WS-X6516-GE-TX
- WS-X6148-GE-TX
- WS-X6148X2-RJ45
- WS-X6196-RJ21
- 銅の SFP (GLC-T) および GBIC (WS-G5483) は、これらのトランシーバをサポートするモジュールのいずれかで使用される場合に、自動 MDIX もサポートします。

例

次に、自動 MDIX 検出をイネーブルにする例を示します。

```
Router# mdix auto  
Router#
```

次に、自動 MDIX 検出をディセーブルにする例を示します。

```
Router# no mdix auto  
Router#
```

mdt data

データ Multicast Distribution Tree (MDT; マルチキャスト配信ツリー) グループ用にマルチキャストグループのアドレス範囲を設定するには、**mdt data** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

mdt data group-address-range wildcard-bits [threshold threshold-value] [list access-list]

no mdt data group-address-range wildcard-bits [threshold threshold-value] [list access-list]

シンタックスの説明

<i>group-address-range</i>	マルチキャストグループのアドレス範囲。有効値は 224.0.0.1 ~ 239.255.255.255 です。
<i>wildcard-bits</i>	マルチキャストグループのアドレス範囲に適用されるワイルドカードビット。
threshold threshold-value	(任意) 帯域幅のしきい値を定義します。有効値は 1 ~ 4,294,967 です。
list access-list	(任意) アクセスリストの名前または番号を定義します。

コマンドのデフォルト

ディセーブル

コマンドモード

VRF コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

データ MDT グループには、VPN ごとに最大 256 のマルチキャストグループを含められます。データ MDT グループの作成に使用されるマルチキャストグループは、設定済み IP アドレスのプールからダイナミックに選択されます。

このコマンドにより、トンネルヘッダー用に選択できるマルチキャスト宛先アドレスの範囲を設定できます。選択される宛先アドレスはトラフィックプロファイルにより異なります (送信元および宛先は指定されたアクセスリストに一致し、トラフィックレートは帯域幅しきい値を超過していません)。

例

次に、データ MDT グループ用にマルチキャストグループのアドレス範囲を設定する例を示します。

```
Router(config-vrf)# mdt data 232.0.1.0 0.0.0.255 threshold 500 list 101
Router(config-vrf)#
```

関連コマンド

コマンド	説明
mdt default	VRF インスタンスにデフォルト MDT グループを設定します。

mdt default

VRF インスタンスにデフォルト MDT グループを設定するには、VRF コンフィギュレーション モードで **mdt default** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

mdt default group-address

no mdt default group-address

シンタックスの説明	<i>group-address</i>	デフォルト MDT グループの IP アドレス
-----------	----------------------	-------------------------

コマンドのデフォルト	ディセーブル
------------	--------

コマンド モード	VRF コンフィギュレーション
----------	-----------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン デフォルト MDT グループは、同じ VPN に属するすべてのプロバイダーエッジルータに設定されたグループと同じである必要があります。

同じグループアドレスで設定されるプロバイダーエッジルータはグループのメンバーになるため、*group-address* はコミュニティの ID として機能し、これによってプロバイダーエッジルータ間で相互にパケットを送受信できるようになります。

デフォルト MDT に SSM プロトコルを使用する場合、送信元 IP アドレスは BGP セッションの送信元として使用されます。

このコマンドを入力すると、トンネル インターフェイスが作成されます。デフォルトでは、トンネル ヘッダーの宛先アドレスは *group-address* 引数です。

例 次に、VRF インスタンスにデフォルト MDT グループを設定する例を示します。

```
Router (config-vrf) # mdt default 232.0.0.1
Router (config-vrf) #
```

関連コマンド	コマンド	説明
	mdt data	データ MDT グループ用にマルチキャスト グループのアドレス範囲を設定します。

mdt log-reuse

データ MDT の再利用の記録をイネーブルにするには、VRF コンフィギュレーション モードで **mdt log-reuse** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

mdt log-reuse

no mdt log-reuse

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

ディセーブル

コマンド モード

VRF コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

mdt log-reuse コマンドは、データ MDT が再利用されるたびに Syslog メッセージを生成します。

次に、MDT ログ再利用機能をイネーブルにする例を示します。

```
Router(config-vrf)# mdt log-reuse
Router(config-vrf)#
```

関連コマンド

コマンド	説明
mdt data	データ MDT グループ用にマルチキャスト グループのアドレス範囲を設定します。
mdt default	VRF インスタンスにデフォルト MDT グループを設定します。

media-type

デュアルモード アップリンク ポートに使用するコネクタを選択するには、**media-type** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
media-type {rj45 | sfp}
```

```
no media-type
```

シンタックスの説明	コマンド	説明
	rj45	RJ-45 コネクタを使用します。
	sfp	SFP コネクタを使用します。

コマンドのデフォルト **sfp**

コマンドモード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン ポート 1 には、着脱可能小型フォーム ファクタ (SFP) コネクタが 1 つあります。ポート 2 には、RJ-45 コネクタと SFP コネクタが 1 つずつあります。ポートでどちらのコネクタを使用するか設定する必要があります。

例 次に、スロット 5 にポート 2 を設定して RJ-45 コネクタを使用する例を示します。

```
Router(config)# interface gigabitethernet 5/2  
Router(config-if)# media-type rj45
```

mkdir disk0:

フラッシュ ファイル システムに新しいディレクトリを作成するには、**mkdir disk0:** コマンドを使用します。

mkdir disk0:

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、フラッシュ ファイル システムだけで有効です。

mkdir disk0: コマンドを入力したあと、新しいディレクトリ ファイル名を入力するようにプロンプトが表示されます。

エントリをチェックするには、**dir** コマンドを入力します。

ディレクトリを削除するには、**rmdir** コマンドを入力します。

例

次に、**newdir** という名前のディレクトリを作成する例を示します。

```
Router# mkdir disk0:
Create directory filename [ ]? newdir
Created dir disk0: newdir
Router#
```

関連コマンド

コマンド	説明
cd	デフォルトのディレクトリまたはファイル システムを変更します。
dir	ファイル システムのファイル リストを表示します。
rmdir	クラス C フラッシュ ファイル システムで既存のディレクトリを削除します。

mls aclmerge algorithm

使用する ACL マージ方式のタイプを選択するには、**mls aclmerge algorithm** コマンドを使用します。

mls aclmerge algorithm {bdd | odm}

シンタックスの説明	bdd	odm
	binary decision diagrams (BDD) ベースのアルゴリズムを指定します。	order dependent merge (ODM) ベースのアルゴリズムを指定します。

コマンドのデフォルト **bdd**

コマンド モード グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン BDD ベースの ACL マージは、ブール関数を使用して、TCAM にプログラムできる TCAM エントリを結合した単一のリストを形成します。

Catalyst 6500 シリーズスイッチの ODM ベースの ACL マージをディセーブルにすることはできません。

ODM ベースの ACL マージは、ODM アルゴリズムを使用して、TCAM にプログラムできるエントリを処理します。



(注) ODM ベースの ACL マージは、セキュリティ ACL および QoS フィルタリングに使用される ACL の両方をサポートします。

アルゴリズム方式を変更しても、その変更は以前のものには適用されません。たとえば、マージがすでに適用された ACL には作用しません。マージの変更は、以降のマージに対してだけ適用されます。

現在のマージ方式のステータスを確認するには、**show fm summary** コマンドを使用します。

例 次に、BDD ベースの ACL を選択して、ACL を処理する例を示します。

```
Router(config)# mls aclmerge algorithm bdd
The algorithm chosen will take effect for new ACLs which are being applied, not
for already applied ACLs.
Router(config)
```

次に、ODM ベースの ACL マージを選択して、ACL を処理する例を示します。

```
Router(config)# mls aclmerge algorithm odm
The algorithm chosen will take effect for new ACLs which are being applied, not
for already applied ACLs.
Router(config)#
```

■ mls aclmerge algorithm

関連コマンド

コマンド	説明
show fm summary	機能マネージャ情報の概要を表示します。

mls acl tcam default-result

ACL TCAM 更新中のデフォルト動作を設定するには、**mls acl tcam default-result** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls acl tcam default-result {permit | deny | bridge}

no mls acl tcam default-result

シンタックスの説明

permit	すべてのトラフィックを許可します。
deny	すべてのトラフィックを拒否します。
bridge	すべてのレイヤ 3 トラフィックを、MSFC、RP またはソフトウェアにブリッジします。

コマンドのデフォルト

deny

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

既存の ACL を消去して新規の ACL を適用するまでの移行期間中は、デフォルトの **deny** がハードウェアに組み込まれています。新規の ACL がすべてハードウェアに適用されると、デフォルトの **deny** は削除されます。

移行期間中にハードウェア内のすべてのトラフィックを許可、またはすべてのトラフィックをソフトウェアにブリッジするには、**mls acl tcam default-result permit** コマンドを使用します。

例

次に、ACL TCAM の更新中にすべてのトラフィックの送受信を許可する例を示します。

```
Router(config)# mls acl tcam default-result permit
Router(config)#
```

次に、ACL TCAM の更新中にすべてのトラフィックを拒否する例を示します。

```
Router(config)# mls acl tcam default-result deny
Router(config)#
```

次に、ACL TCAM の更新中にすべてのトラフィックをブリッジする例を示します。

```
Router(config)# mls acl tcam default-result bridge
Router(config)#
```

mls acl tcam share-global

グローバルなデフォルト ACL の共有をイネーブルにするには、**mls acl tcam share-global** コマンドを使用します。グローバルなデフォルトの共有をオフに切り替えるには、このコマンドの **no** 形式を使用します。

mls acl tcam share-global

no mls acl tcam share-global

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト イネーブル

コマンド モード グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、グローバルなデフォルト ACL の共有をイネーブルにする例を示します。

```
Router(config)# mls acl tcam share-global  
Router(config)#
```

mls aging fast

レイヤ 3 テーブルでユニキャスト エントリの fast エージング タイムを設定するには、**mls aging fast** コマンドを使用します。MLS の fast エージング タイムをデフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

```
mls aging fast [ {threshold packet-count} [ {time seconds} ] ]
```

```
mls aging fast [ {time seconds} [ {threshold packet-count} ] ]
```

```
no mls aging fast
```

シンタックスの説明

threshold	(任意) レイヤ 3 fast エージングの fast エージングしきい値の <i>packet-count</i> 数を指定します。有効値は、1 ~ 128 です。
time seconds	(任意) エントリがチェックされる頻度を指定します。有効値は、1 ~ 128 秒です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- fast エージングはディセーブルです。
- fast エージングがイネーブルの場合、*packet-count* のデフォルト値は 100 パケットで、*seconds* のデフォルト値は 32 秒です。

コマンドモード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

サンプリング済み NetFlow を設定している場合、このコマンドは無効です。このコマンドを有効にするには、サンプリングした NetFlow をディセーブルにする必要があります。

例

次に、MLS fast エージングしきい値を設定する例を示します。

```
Router (config) # mls aging fast threshold 50
Router (config) #
```

関連コマンド

コマンド	説明
show mls netflow	NetFlow ハードウェアに関する設定情報を表示します。

mls aging long

レイヤ 3 テーブルでユニキャスト エントリの long エージング タイムを設定するには、**mls aging long** コマンドを使用します。MLS の long エージング タイムをデフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

mls aging long seconds

no mls aging long

シンタックスの説明	<i>seconds</i> レイヤ 3 の long エージング タイムアウト。有効値は、64 ~ 1920 秒です。
------------------	--

コマンドのデフォルト	1920 秒
-------------------	--------

コマンド モード	グローバル コンフィギュレーション (config) (config)
-----------------	-------------------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン	サンプリング済み NetFlow を設定している場合、このコマンドは無効です。このコマンドを有効にするには、サンプリングした NetFlow をディセーブルにする必要があります。
-------------------	---

例	次に、MLS long エージングしきい値を設定する例を示します。
----------	-----------------------------------

```
Router(config)# mls aging long 800
Router(config)#
```

関連コマンド	コマンド	説明
	show mls netflow	NetFlow ハードウェアに関する設定情報を表示します。

mls aging normal

レイヤ 3 テーブルでユニキャスト エントリの normal エージング タイムを設定するには、**mls aging normal** コマンドを使用します。MLS の normal エージング タイムをデフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

mls aging normal seconds

no mls aging normal

シンタックスの説明	<i>seconds</i>	レイヤ 3 の normal エージング タイムアウト。有効値は、32 ~ 4092 秒です。
-----------	----------------	---

コマンドのデフォルト	300 秒
------------	-------

コマンド モード	グローバル コンフィギュレーション (config) (config)
----------	-------------------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン	サンプリング済み NetFlow を設定している場合、このコマンドは無効です。このコマンドを有効にするには、サンプリングした NetFlow をディセーブルにする必要があります。
------------	---

例	次に、MLS normal エージングしきい値を設定する例を示します。
---	-------------------------------------

```
Router(config)# mls aging normal 200
Router(config)#
```

関連コマンド	コマンド	説明
	show mls netflow	NetFlow ハードウェアに関する設定情報を表示します。

mls cef maximum-routes

プロトコル単位でハードウェアにプログラミング可能な最大ルート数を制限するには、**mls cef maximum-routes** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
mls cef maximum-routes {ip maximum-routes} | {ip-multicast maximum-routes} |
{ipv6 maximum-routes} | {mpls maximum-routes}
```

```
no mls cef maximum-routes {ip | ip-multicast | ipv6 | mpls}
```

シンタックスの説明

ip	IP ルートの最大数を指定します。
<i>maximum-routes</i>	プロトコル単位でハードウェアにプログラミング可能な最大ルート数。有効な値については、「使用上のガイドライン」を参照してください。
ip-multicast	マルチキャスト ルートの最大数を指定します。
ipv6	IPv6 ルートの最大数を指定します。
mpls	MPLS ラベルの最大数を指定します。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- XL モード システム
 - IPv4 ユニキャストおよび MPLS : 512,000 ルート
 - IPv6 マルチキャスト/ユニキャストおよび IPv4 マルチキャスト : 256,000 ルート
- 非 XL モード システム
 - IPv4 ユニキャストおよび MPLS : 192,000 ルート
 - IPv6 マルチキャスト/ユニキャストおよび IPv4 マルチキャスト : 32,000 ルート



(注)

グローバル インターネット ルーティング テーブルとローカル ルートのサイズは、非 XL モードのデフォルトのパーティション サイズを超えることがあります。詳細については、「使用上のガイドライン」を参照してください。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



(注) MLS CEF 最大ルートを含むコンフィギュレーション ファイルをスタートアップ コンフィギュレーション ファイルにコピーして、Catalyst 6500 シリーズスイッチをリロードする場合、Catalyst 6500 シリーズスイッチは再起動後にリロードされます。

mls cef maximum-routes コマンドは、ハードウェアにプログラミング可能な最大ルート数を制限します。ルート数とそのプロトコルでの制限を超えたことが検出された場合、例外条件が生成されます。

XL および非 XL モードは、システムに搭載された PFC モジュールのタイプに基づきます。搭載されたハードウェアによってだけ、モードを設定できます。Supervisor Engine 32 PISA には、PFC3B が搭載されており、非 XL モードシステムと見なされます。

max-routes の有効値は次のとおりです。

- IP および MPLS : 最大 239,000 ルート
- IP マルチキャストおよび IPv6 マルチキャスト/ユニキャスト : 最大 119,000 ルート



(注) 設定可能な最大値は固定されておらず、他のプロトコルに割り当てられた値によって変化します。

次に、最大ルート引数を入力する例を示します。

```
Router(config)# mls cef maximum-routes ip 4
```

ここで、4 は 4096 IP ルート (1024 × 4 = 4096) を示します。

システム リロード後にだけ新しい設定が適用され、スイッチオーバーが発生した場合には有効になりません。

Route Processor Redundancy (RPR) モードでは、最大ルートの設定を変更して保存した場合、スイッチオーバーまたはシステム リロードからアクティブになる際に冗長スーパーバイザ エンジンがリロードします。スーパーバイザ エンジンがアクティブになった 5 分後にリロードが発生します。

現在の最大ルートのシステム コンフィギュレーションを表示するには、**show mls cef maximum-routes** コマンドを使用します。

例

次に、プロトコル単位で許可されている最大ルート数を設定する例を示します。

```
Router(config)# mls cef maximum-routes ip 100  
Router(config)#
```

次に、特定のプロトコルについてデフォルト設定に戻す例を示します。

```
Router(config)# no mls cef maximum-routes ip  
Router(config)#
```

関連コマンド

コマンド	説明
show mls cef maximum-routes	現在の最大ルートのシステム コンフィギュレーションを表示します。

mls cef tunnel fragment

トンネル フラグメンテーションを許可するには、**mls cef tunnel fragment** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls cef tunnel fragment

no mls cef tunnel fragment

コマンドのデフォルト デイセーブル

コマンド モード グローバル コンフィギュレーション (config) (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン トンネル フラグメンテーションをイネーブルにすると、トンネル インターフェイスに入るパケットのサイズが MTU を超える場合、パケットはフラグメントされます。フラグメントされたパケットは、宛先で再構成されます。

例 次に、トンネル フラグメンテーションを許可する例を示します。

```
Router(config)# mls cef tunnel fragment
Router(config)#
```

次に、デフォルト設定に戻す例を示します。

```
Router(config)# no mls cef tunnel fragment
Router(config)#
```

関連コマンド	コマンド	説明
	show mls cef tunnel fragment	トンネル フラグメンテーションの動作ステータスを表示します。

mls erm priority

プロトコルが例外ステータスからの回復を試行する順番を定義するプライオリティを割り当てるには、**mls erm priority** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
mls erm priority {ipv4 value} {ipv6 value} {mpls value}
```

```
no mls erm priority {ipv4} {ipv6} {mpls}
```

シンタックスの説明

ipv4	IPv4 プロトコルのプライオリティを設定します。
<i>value</i>	プライオリティ値。有効値は 1 ~ 3 です。
ipv6	IPv6 プロトコルのプライオリティを設定します。
mpls	MPLS プロトコルのプライオリティを設定します。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- **ipv4** は 1 です。
- **ipv6** は 2 です。
- **mpls** は 3 です。

コマンドモード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

value の値が小さいほどプライオリティは高くなります。

プロトコルが FIB テーブル例外を検出すると、プロトコルは FIB Exception Recovery Manager (ERM) マネージャに通知します。FIB ERM マネージャは、定期的に FIB テーブル例外ステータスをポーリングして、複数のプロトコルがその例外状態で稼働している場合にプロトコル間のプライオリティを決定します。同時に例外状態からの回復試行が可能なプロトコルは 1 つだけです。

FIB スペースが十分にある場合、プライオリティの最も高いプロトコルが最初に回復試行されます。例外状態にあるその他のプロトコルは、前のプロトコルが適切な FIB テーブルをリロードして回復プロセスを完了させるまで、回復を開始しません。

■ **mls erm priority**

例 次に、ERM 例外回復プライオリティを設定する例を示します。

```
Router(config)# mls erm priority ipv4 1 ipv6 2 mpls 3  
Router(config)#
```

次に、デフォルト設定に戻す例を示します。

```
Router(config)# no mls erm priority ipv4 ipv6 mpls  
Router(config)#
```

関連コマンド

コマンド	説明
show mls cef exception	CEF 例外に関する情報を表示します。

mls exclude protocol

ショートカットから除外するインターフェイス プロトコルを指定するには、**mls exclude protocol** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

```
mls exclude protocol {{both | tcp | udp}} {port port-number}}
```

```
no mls exclude
```

シンタックスの説明

both	UDP と TCP を両方指定します。
tcp	ショートカットから TCP インターフェイスを除外します。
udp	ショートカットから UDP インターフェイスを除外します。
port <i>port-number</i>	ポート番号を指定します。有効値は 1 ~ 65,535 です。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション (config) (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、ポート 69 上で UDP を除外するように MLS を設定する例を示します。

```
Router(config)# mls exclude protocol udp port 69
Router(config)#
```

関連コマンド

コマンド	説明
show mls ip multicast	MLS IP 情報を表示します。

■ mls exclude protocol

mls flow

NDE のフロー マスクを設定するには、**mls flow** コマンドを使用します。フロー マスクをデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
mls flow {{ip | ipv6} {destination | destination-source | full |
interface-destination-source | interface-full | source}}
```

```
no mls flow {ip | ipv6}
```

シンタックスの説明	
ip	MLS IP パケットのフロー マスクをイネーブルにします。
ipv6	MLS IPv6 パケットのフロー マスクをイネーブルにします。
destination	レイヤ 3 テーブルのキーとして、宛先 IP アドレスを使用します。
destination-source	レイヤ 3 テーブルのキーとして、宛先および送信元 IP アドレスを使用します。
full	レイヤ 3 テーブルのキーとして、送信元および宛先 IP アドレス、IP プロトコル (UDP または TCP)、送信元および宛先ポート番号を使用します。
interface-destination-source	レイヤ 3 テーブルのキーとして、宛先および送信元フロー マスク内のすべての情報と、送信元 VLAN 番号を使用します。
interface-full	レイヤ 3 テーブルのキーとして、フルフロー マスク内のすべての情報、および送信元 VLAN 番号を使用します。
source	送信元フロー マスクだけのすべての情報を使用します。

コマンドのデフォルト NDE フロー マスクはヌルです。

コマンド モード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドは、スーパーバイザ エンジンの統計情報を収集します。

例 次に、MLS IP の拡張アクセス リストに最小限のフロー マスクを設定する例を示します。

```
Router(config)# mls flow ip full
Router(config)#
```

関連コマンド	コマンド	説明
	show mls netflow	NetFlow ハードウェアに関する設定情報を表示します。

mls ip

インターフェイス上で内部ルータの MLS IP をイネーブルにするには、**mls ip** コマンドを使用します。MLS IP をインターフェイスでディセーブルにするには、このコマンドの **no** 形式を使用します。

mls ip

no mls ip

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

マルチキャストはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、MLS IP のショートカットをイネーブルにする例を示します。

```
Router(config-if)# mls ip  
Router(config-if)#
```

関連コマンド

コマンド	説明
mls rp ip (interface configuration mode)	外部システムが指定インターフェイスで MLS IP をイネーブルにすることができます。
show mls ip multicast	MLS IP 情報を表示します。

mls ip acl port expand

レイヤ 4 に対する ACL 固有機能をイネーブルにするには、**mls ip acl port expand** コマンドを使用します。ACL 固有のレイヤ 4 機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

mls ip acl port expand

no mls ip acl port expand

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード グローバル コンフィギュレーション (config)

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、レイヤ 4 ポート上での ACL の論理動作の拡張をイネーブルにする例を示します。

```
Router(config)# mls ip acl port expand  
Router(config)#
```

mls ip cef accounting per-prefix

MLS のプレフィクス単位のアカウンティングをイネーブルにするには、**mls ip cef accounting per-prefix** コマンドを使用します。MLS のプレフィクス単位のアカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

mls ip cef accounting per-prefix *prefix-entry prefix-entry-mask* [*instance-name*]

no mls ip cef accounting per-prefix

シンタックスの説明

<i>prefix</i>	A.B.C.D のフォーマットのプレフィクス エントリ
<i>prefix-entry-mask</i>	A.B.C.D のフォーマットのプレフィクス エントリ マスク
<i>instance-name</i>	(任意) VPN ルーティング / 転送インスタンス名

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

プレフィクス単位のアカウンティングでは、プレフィクスが使用する隣接カウンタが収集されます。プレフィクスをアカウンティングに使用する場合は、その他のプレフィクスと隣接を共有できません。特定宛先に送信されるパケットのアカウンティングを行うには、プレフィクス単位のアカウンティングを使用します。

例

次の例は、MLS のプレフィクス単位のアカウンティングをイネーブルにする方法を示しています。

```
Router(config)# mls ip cef accounting per-prefix 172.20.52.18 255.255.255.255
Router(config)#
```

次の例は、MLS のプレフィクス単位のアカウンティングをディセーブルにする方法を示しています。

```
Router(config)# no mls ip cef accounting per-prefix
Router(config)#
```

関連コマンド

コマンド	説明
show mls cef ip accounting per-prefix	統計情報の収集のために設定されたプレフィクスをすべて表示します。

mls ip cef load-sharing

CEF ロードバランスを設定するには、**mls ip cef load-sharing** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls ip cef load-sharing [full [exclude-port {destination | source}]] [simple]

no mls ip cef load-sharing

シンタックスの説明	full
	(任意) 送信元/宛先レイヤ 4 ポートおよび送信元 IP/宛先 IP アドレス (レイヤ 3) を含めるように CEF ロードバランスを設定します。
	exclude-port destination (任意) ロードバランス アルゴリズムから宛先レイヤ 4 ポートおよび送信元 IP/宛先 IP アドレス (レイヤ 3) を除外します。
	exclude-port source (任意) ロードバランス アルゴリズムから送信元レイヤ 4 ポートおよび送信元 IP/宛先 IP アドレス (レイヤ 3) を除外します。
	simple (任意) 単一ステージのロードシェアリングに対して CEF ロード バランスを設定します。

コマンドのデフォルト 送信元および宛先 IP アドレスおよびユニバーサル ID

コマンド モード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン **mls ip cef load-sharing** コマンドは、IPv4、IPv6、および MPLS 転送に影響します。

mls ip cef load-sharing コマンドの構造は、次のとおりです。

- **mls ip cef load-sharing full** : 複数の隣接関係とともにレイヤ 3 およびレイヤ 4 情報を使用します。
- **mls ip cef load-sharing full simple** : 複数の隣接関係なしでレイヤ 3 およびレイヤ 4 情報を使用します。
- **mls ip cef load-sharing simple** : 複数の隣接関係なしでレイヤ 3 情報を使用します。

その他の注意事項については、『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide Release 12.2ZY*』を参照してください。

例 次に、複数の隣接関係とともにレイヤ 3 およびレイヤ 4 ポートを含めるようにロードバランスを設定する例を示します。

```
Router (config) # mls ip cef load-sharing full
Router (config) #
```

■ mls ip cef load-sharing

次に、ロードバランス アルゴリズムから宛先レイヤ 4 ポートおよび送信元/宛先 IP アドレス (レイヤ 3) を除外するようロード バランスを設定する例を示します。

```
Router(config)# mls ip cef load-sharing full exclude-port destination
Router(config)#
```

次に、ロードバランス アルゴリズムから送信元レイヤ 4 ポートおよび送信元/宛先 IP アドレス (レイヤ 3) を除外するようロード バランスを設定する例を示します。

```
Router(config)# mls ip cef load-sharing full exclude-port source
Router(config)#
```

次に、デフォルト設定に戻す例を示します。

```
Router(config)# no mls ip cef load-sharing
Router(config)#
```

関連コマンド

コマンド	説明
show mls cef ip	MLS ハードウェア レイヤ 3 スイッチング テーブルの IP エントリを表示します。

mls ip cef rate-limit

CEF によりパントされたデータ パケットのレートを制限するには、**mls ip cef rate-limit** コマンドを使用します。CEF によりパントされたデータ パケットのレート制限をディセーブルにするには、このコマンドの **no** 形式を使用します。

mls ip cef rate-limit pps

no mls ip cef rate-limit

シンタックスの説明

pps データ パケットの番号。有効値は 0 ~ 1,000,000 です。

コマンドのデフォルト

レート制限は設定されていません。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

特定の DoS 攻撃は、ルータのルート処理エンジンをターゲットにしています。PFC で転送できない特定のデータ パケットは、PISA に転送されて処理されます。DoS 攻撃が発生すると、ルート処理エンジンは過負荷になり、ダイナミックなルーティング プロトコルの稼働時にはルーティングが不安定になることがあります。**mls ip cef rate-limit** コマンドを使用すると、PISA に送信されるトラフィック量を制限し、ルート処理エンジンへの **denial-of-servic** 攻撃を防ぐことができます。

このコマンドは、次のデータ パケットを含めて、CEF によりパントされたすべてのデータ パケットのレートを制限します。

- ローカル インターフェイス IP アドレス宛のデータ パケット
- ARP を必要とするデータ パケット

低いレートを設定すると、ローカル インターフェイスの IP アドレス宛のデータ パケット、および ARP を必要とするデータ パケットに影響が及びます。このコマンドは、これらのデータ パケットを通常の標準レートに制限して、異常な着信レートを回避する場合に使用してください。

その他の注意事項については、『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide Release 12.2ZY*』を参照してください。

例

次に、レート制限のイネーブル化および設定を行う例を示します。

```
Router(config)# mls ip cef rate-limit 50000
Router(config)#
```

関連コマンド

コマンド	説明
<code>show mls cef ip</code>	MLS ハードウェア レイヤ 3 スイッチング テーブルの IP エントリを表示します。

mls ip cef rpf hw-enable-rpf-acl

uRPF ACL がイネーブルの場合に deny ace に一致するパケットのハードウェアの uRPF をイネーブルにするには、**mls ip cef rpf hw-enable-rpf-acl** コマンドを使用します。RPF と ACL がイネーブルの場合にハードウェアの uRPF をディセーブルにするには、このコマンドの **no** 形式を使用します。

mls ip cef rpf hw-enable-rpf-acl

no mls ip cef rpf hw-enable-rpf-acl

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード グローバル コンフィギュレーション (config)

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン **mls ip cef rpf hw-enable-rpf-acl** コマンドを入力しない場合、uRPF ACL を指定すると、uRPF ACL によって許可されたパケットはハードウェアに転送され、拒否されたパケットは PISA に送信されて、uRPF チェックが行われます。このコマンドは、uRPF ACL によって拒否されたパケットの uRPF チェックを伴うハードウェア転送をイネーブルにします。ただし、この場合、uRPF ACL によって許可されたパケットは PISA に送信されて、転送されます。

uRPF は、PVLAN ホスト ポートではサポートされていません。

例 次に、RPF と ACL がイネーブルの場合にハードウェアの uRPF をイネーブルにする例を示します。

```
Router(config)# mls ip cef rpf hw-enable-rpf-acl  
Router(config)#
```

次に、RPF と ACL がイネーブルの場合にハードウェアの uRPF をディセーブルにする例を示します。

```
Router(config)# no mls ip cef rpf hw-enable-rpf-acl  
Router(config)#
```

コマンド	説明
ip verify unicast source reachable-via {any rx}	RPF ACL チェックをイネーブルにし、設定します。

mls ip cef rpf interface-group

RPF_VLAN テーブルでインターフェイス グループを定義するには、**mls ip cef rpf interface-group** コマンドを使用します。インターフェイス グループを削除するには、このコマンドの **no** 形式を使用します。

```
mls ip cef rpf interface-group group-number interface1 interface2 interface3 [...]
```

```
no mls ip cef rpf interface-group group-number interface1 interface2 interface3 [...]
```

シンタックスの説明

<i>group-number</i>	インターフェイス グループ番号。有効値は 1 ~ 4 です。
<i>interface</i>	インターフェイス番号。フォーマットの注意事項については、「使用上のガイドライン」を参照してください。
...	(任意) インターフェイス番号を追加で指定します。詳細については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

グループは設定されていません。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

1 つのインターフェイス グループには、3 ~ 6 個のインターフェイスがあります。インターフェイス グループは最大 4 つまで設定できます。各インターフェイス グループについて、最初の 4 つのエントリはハードウェアの RPF_VLAN テーブルに組み込まれます。

interface は *interface-typemod/port* の形式で入力します。

各インターフェイスは、スペースで区切って入力してください。 *interface-type* 引数と *mod/port* 引数の間には、スペースは不要です。入力例については、「例」を参照してください。

例

次に、インターフェイス グループを定義する例を示します。

```
Router(config)# mls ip cef rpf interface-group 0 F2/1 F2/2 F2/3 F2/4 F2/5 F2/6
Router(config)#
```

mls ip cef rpf multipath

RPF モードを設定するには、**mls ip cef rpf multipath** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls ip cef rpf multipath {interface-group | punt | pass}

シンタックスの説明

interface-group	複数パス ルートから着信するパケットの RPF チェックをディセーブルにします。詳しくは、「使用上のガイドライン」を参照してください。
punt	RPF に失敗したパケットをルート プロセッサにリダイレクトして、複数パスのプレフィクスに対応します。
pass	複数パス ルートから着信するパケットの RPF チェックをディセーブルにします。

コマンドのデフォルト

punt

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

interface-group モードは **pass** モードと類似していますが、RPF チェックに **RPF_VLAN** グローバル テーブルを使用します。その他の複数パス プレフィクスからのパケットは、常に RPF チェックを通過します。

RPF_VLAN テーブルのインターフェイス グループを定義するには、**mls ip cef rpf multipath interface-group** コマンドを使用します。1 つのインターフェイス グループには、3 ~ 6 個のインターフェイスがあり、最大 4 つのインターフェイス グループを設定できます。各インターフェイス グループについて、最初の 4 つのエントリはハードウェアの **RPF_VLAN** テーブルに組み込まれます。4 つ以上の複数パスを持つプレフィクスの場合、2 つを除いてパスはすべてインターフェイス グループに属し、そのプレフィクスの FIB エントリはこの **RPF_VLAN** エントリを使用します。

例

次に、RPF に失敗したパケットをルート プロセッサにリダイレクトして、複数パスのプレフィクスに対応する例を示します。

```
Router(config)# mls ip cef rpf multipath interface-group
Router(config)#
```

関連コマンド

コマンド	説明
show mls cef ip	MLS ハードウェア レイヤ 3 スイッチング テーブルの IP エントリを表示します。

mls ip delete-threshold

設定済みの ACL しきい値を削除するには、**mls ip delete-threshold** コマンドを使用します。

mls ip delete-threshold *acl-num*

シンタックスの説明

<i>acl-num</i>	再帰 ACL 番号。有効値は 1 ~ 10,000 です。
----------------	-------------------------------

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドのデフォルト

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

mls ip delete-threshold コマンドは、**mls ip reflexive ndr-entry tcam** コマンドをイネーブルに設定した場合にだけアクティブになります。

例

次に、ACL しきい値を削除する例を示します。

```
Router(config)# mls ip delete-threshold 223
Router(config)#
```

関連コマンド

コマンド	説明
mls ip install-threshold	設定済み ACL しきい値を組み込みます。
mls ip reflexive ndr-entry tcam	No Drop Rate (NDR) によって組み込まれた再帰 TCP/UDP エントリに対して TCAM 内のショートカットをイネーブルにします。

mls ip directed-broadcast

IP 転送ブロードキャストのハードウェア スイッチングをイネーブルにするには、**mls ip directed-broadcast** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls ip directed-broadcast {exclude-router | include-router}

no mls ip directed-broadcast

シンタックスの説明	説明
exclude-router	IP 転送ブロードキャスト パケットを、ルータを除く VLAN 内のすべてのホストに、ハードウェア転送します。
include-router	IP 転送ブロードキャスト パケットを、ルータを含む VLAN 内のすべてのホストに、ハードウェア転送します。

コマンド モード ディセーブル

コマンドのデフォルト インターフェイス コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン **exclude-router** および **include-router** キーワードは両方ともハードウェア スイッチングをサポートします。ただし、**exclude-router** の場合は、ハードウェアによりスイッチングされたパケットのコピーをルータに送信しません。**include-router** キーワードを入力した場合、ルータは IP 転送ブロードキャスト パケットを再転送しません。

デフォルト モードの場合、IP 転送ブロードキャスト パケットはハードウェアで転送されません。PISA によってプロセス レベルで処理されます。PISA がパケットを転送するかどうかは、**ip directed-broadcast** コマンド設定によって決まります。

ip directed-broadcast コマンドと **mls ip directed-broadcast** コマンドの間には連動関係がありません。**ip directed-broadcast** コマンドはソフトウェア転送に関係し、**mls ip directed-broadcast** コマンドはハードウェア転送に関係します。

MLS IP 転送ブロードキャストは、セカンダリ インターフェイス アドレスをサポートします。

ip directed-broadcast コマンドを同じインターフェイスに追加しないかぎり、CPU に到達したパケットは転送されません。

ポートチャネル インターフェイスには MLS IP 転送ブロードキャストを設定できますが、ポートチャネル インターフェイスの物理インターフェイスには設定できません。物理インターフェイスに MLS IP 転送ブロードキャストを設定したまま、ポートチャネル グループに物理インターフェイスを追加することはできません。まず、設定を手動で削除してから、チャネル グループに物理インターフェイスを追加する必要があります。物理インターフェイスがすでにチャネルグループに含まれている場合、CLI はこの物理インターフェイス上で **mls ip directed-broadcast** コンフィギュレーション コマンドを受け入れません。

■ mls ip directed-broadcast

例

次に、IP 転送ブロードキャスト パケットを、ルータを除く VLAN 内のすべてのホストにハードウェア転送する例を示します。

```
Router(config-if)# mls ip directed-broadcast exclude-router  
Router(config-if)#
```

次に、IP 転送ブロードキャスト パケットを、VLAN 内のすべてのホストにハードウェア転送する例を示します。

```
Router(config-if)# mls ip directed-broadcast include-router  
Router(config-if)#
```

関連コマンド

コマンド	説明
show mls cef adjacency	ハードウェアによりスイッチングされる IP 転送ブロードキャスト情報を表示します。

mls ip inspect

他のインターフェイス経由のトラフィックを拒否する任意の ACL を使用してトラフィックを許可するには、**mls ip inspect** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls ip inspect *acl-name*

no mls ip inspect *acl-name*

シンタックスの説明	<i>acl-name</i>	ACL 名
-----------	-----------------	-------

コマンドモード	ディセーブル
---------	--------

コマンドのデフォルト	グローバル コンフィギュレーション (config)
------------	----------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン Catalyst 6500 シリーズスイッチ上で、トラフィックを拒否するようにインターフェイスが設定されている場合、context based access control (CBAC; コンテキストベースのアクセス制御) が双方向のトラフィックフローを許可するのは、**ip inspect** コマンドで設定されたインターフェイスだけです。

例 次に、特定の ACL (deny_ftp_c) を使用してトラフィックを許可する例を示します。

```
Router(config)# mls ip inspect deny_ftp_c
Router(config)#
```

関連コマンド	コマンド	説明
	ip inspect	検査規則のセットをインターフェイスに適用します。

mls ip install-threshold

設定済みの ACL しきい値を組み込むには、**mls ip install-threshold** コマンドを使用します。

mls ip install-threshold *acl-num*

シンタックスの説明

<i>acl-num</i>	再帰 ACL 番号。有効値は 1 ~ 10,000 です。
----------------	-------------------------------

コマンドモード

このコマンドにはデフォルト設定がありません。

コマンドのデフォルト

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

mls ip install-threshold コマンドは、**mls ip reflexive ndr-entry tcam** コマンドをイネーブルに設定した場合にだけアクティブになります。

例

次に、ACL しきい値を組み込む例を示します。

```
Router(config)# mls ip install-threshold 123
Router(config)#
```

関連コマンド

コマンド	説明
mls ip delete-threshold	設定済み ACL しきい値を削除します。
mls ip reflexive ndr-entry tcam	NDR によって組み込まれた再帰 TCP/UDP エントリに対して TCAM 内のショートカットをイネーブルにします。

mls ip multicast (global configuration mode)

MLS IP をイネーブルにして、ハードウェア スイッチングをグローバルに設定するには、**mls ip multicast** コマンドを使用します。MLS IP をディセーブルにするには、このコマンドの **no** 形式を使用します。

mls ip multicast [capability]

mls ip multicast [vrf name] [connected | egress local | mfd | refresh-state | shared-tree-mfd | threshold ppsec]

no mls ip multicast [vrf]

シンタックスの説明

capability	(任意) スイッチ プロセッサからルート プロセッサに出力機能情報をエクスポートします。
vrf name	(任意) VRF 名を指定します。
connected	(任意) 直接接続されている送信元を内部ルータにブリッジングするために、インターフェイスまたはマスク エントリを組み込みます。
egress local	(任意) ローカル レイヤ 3 ルーテッド インターフェイスをマルチキャスト拡張テーブルに入力します。
mfd	(任意) 完全なハードウェア スイッチングをイネーブルにします。
refresh-state	(任意) (S,G) エントリまたは Outgoing interface of a multicast {*,G} or {source, group} flow (OIF; マルチキャスト {*,G} または {S,G} フローの Outgoing Interface) がヌルの (*,G) エントリの期限切れ時間をリフレッシュします。
shared-tree-mfd	(任意) (*,G) フローのすべてのショートカットをイネーブルにします。
threshold ppsec	(任意) 最小トラフィック レートを設定します。このレートを下回る場合、フローはハードウェアでスイッチングされずにソフトウェアでスイッチングされます。有効値は、10 ~ 10,000 秒です。

コマンド モード

デフォルト設定は次のとおりです。

- マルチキャストはディセーブルです。
- ハードウェア スイッチングは、すべての適格なマルチキャスト ルートに対して許可されます。
- **connected** はイネーブルです。
- **egress local** はディセーブルです。
- **mfd** はイネーブルです。
- **refresh-state** はイネーブルです。
- **shared-tree-mfd** はイネーブルです。

コマンドのデフォルト

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



(注)

mls ip multicast egress local コマンドの入力後、システムをリセットして設定を有効にする必要があります。

mls ip multicast egress local コマンドを入力するとき、IPv6 マルチキャストがイネーブルでないことを確認してください。出力マルチキャスト レプリケーション パフォーマンス拡張機能は、IPv4 および IPv6 のオンまたはオフを個別に実行できないので、この機能をオンに切り替えるとき、IPv4 および IPv6 のマルチキャストをイネーブルにすることはできません。

次のオプションのキーワードがサポートされています。

- **threshold**
- **connected**
- **refresh-state**
- **shared-tree-mfd**
- **mfd**

オプションの **threshold** *ppsec* キーワードおよび引数は、ハードウェア キャッシュにすでに存在しているフローには影響しません。

フロー統計情報を Catalyst 6500 シリーズ スイッチが受信すると（トラフィックが RPF インターフェイスから受信されることを示します）、期限切れ時間のリフレッシュが更新されます。

例 次に、MLS IP ショートカットをイネーブルにする例を示します。

```
Router(config)# mls ip multicast
Router(config)#
```

次に、特定のマルチキャスト ルートのハードウェア スイッチングをイネーブルにする例を示します。

```
Router(config)# mls ip multicast vrf test1
Router(config)#
```

次に、スイッチ プロセッサからルート プロセッサに出力機能情報をエクスポートする例を示します。

```
Router(config)# mls ip multicast capability
Router(config)#
```

次に、ローカル レイヤ 3 ルーテッド インターフェイスをマルチキャスト拡張テーブルに入力する例を示します。

```
Router(config)# mls ip multicast egress local
Router(config)#
```

関連コマンド

コマンド	説明
mls rp ip (global configuration mode)	外部システムが PISA への IP ショートカットを確立できるようにします。
show mls ip multicast	MLS IP 情報を表示します。

mls ip multicast (interface configuration mode)

インターフェイス上で MLS IP ショートカットをイネーブルにするには、**mls ip multicast** コマンドを使用します。MLS IP ショートカットをインターフェイスでディセーブルにするには、このコマンドの **no** 形式を使用します。

mls ip multicast

no mls ip multicast

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドモード マルチキャストはディセーブルです。

コマンドのデフォルト インターフェイス コンフィギュレーション

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、MLS IP ショートカットをイネーブルにする例を示します。

```
Router(config-if)# mls ip multicast
Router(config-if)#
```

コマンド	説明
show mls ip multicast	MLS IP 情報を表示します。

mls ip multicast bidir gm-scan-interval

Bidir ランデブーポイントの RPF スキャン インターバルを設定するには、**mls ip multicast bidir gm-scan-interval** コマンドを使用します。Bidir RP の RPF スキャン インターバルをディセーブルにするには、このコマンドの **no** 形式を使用します。

mls ip multicast bidir gm-scan-interval *interval*

no mls ip multicast bidir gm-scan-interval

シンタックスの説明	<i>interval</i>	Bidir RP の RPF スキャン インターバル。有効値は、1 ~ 1000 秒です。
------------------	-----------------	---

コマンド モード	10 秒
-----------------	------

コマンド モード	グローバル コンフィギュレーション (config)
-----------------	----------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン	Bidir ランデブーポイントの RPF スキャン インターバルを設定する場合、ハードウェアのすべての Bidir ランデブーポイントの DF テーブルで、定期スキャン タイマーが RPF を更新する時間を設定します。
-------------------	---

例	次に、Bidir ランデブーポイントの RPF スキャン インターバルを設定する例を示します。
----------	---

```
Router(config)# mls ip multicast bidir gm-scan-interval 30
Router(config)#
```

関連コマンド	コマンド	説明
	show mls ip multicast bidir	Bidir ハードウェアでスイッチングされるエントリを表示します。

mls ip multicast connected

直接接続されているサブネットのダウンロードをグローバルにイネーブルにするには、**mls ip multicast connected** コマンドを使用します。直接接続されているサブネットのダウンロードをグローバルにディセーブルにするには、このコマンドの **no** 形式を使用します。

mls ip multicast connected

no mls ip multicast connected

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドモード ディセーブル

コマンドモード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン 次の場合には、直接接続されたサブネットを作成しないでください。

- FIB TCAM で利用できる空間を増やす場合
- スイッチが送信元の最初のホップ ルータである場合
- エントリが双方向、SSM、および DM モードのグループの場合

これらの場合、直接接続されたサブネットのダウンロードをイネーブルにすると、直接接続された送信元は **multicast multilayer switching (MMLS; マルチキャスト マルチレイヤ スイッチング) (*,G)** エントリに到達し、**MMLS (*,G)** エントリを使用してスイッチングされます。レジスタはルート プロセッサに送信されず (PIM-SM の場合)、また、最初のホップで (S,G) ステートは作成されません (PIM-DM の場合)。

直接接続された送信元がこれらのエントリに到達する前に、直接接続された送信元を捕捉するために、マスクを短くしてサブネット エントリを TCAM エントリに組み込みます。直接接続された送信元から PISA にトラフィックをパントできます。PISA がこのトラフィックを確認すると、PISA はこの送信元の **MMLS (S,G)** エントリを組み込みます。MMLS (S,G) エントリは、TCAM のサブネット エントリよりも前に組み込まれます。これで、この送信元からのパケットは (S,G) エントリを使用してスイッチングされます。

例 次に、直接接続されたサブネットのダウンロードをイネーブルにする例を示します。

```
Router(config)# mls ip multicast connected
Router(config)#
```

関連コマンド

コマンド	説明
mls ip multicast (global configuration mode)	MLS IP をイネーブルにして、ハードウェア スイッチングをグローバルに設定します。
show mls ip multicast	MLS IP 情報を表示します。

mls ip multicast consistency-check

ハードウェアによるショートカットの一貫性チェッカーのイネーブル化および設定を行うには、**mls ip multicast consistency-check** コマンドを使用します。一貫性チェッカーをディセーブルにするには、このコマンドの **no** 形式を使用します。

mls ip multicast consistency-check [**settle-time** *seconds*] | **{type scan-mroute**
[count *count-number*] | **{settle-time** *seconds*} | **{period** *seconds*}]

no mls ip multicast consistency-check

シンタックスの説明	
settle-time <i>seconds</i>	(任意) 一貫性チェッカーに対するエントリ/OIF の処理時間を指定します。有効値は、2 ~ 3600 秒です。
type scan-mroute	(任意) 一貫性チェックのタイプをマルチキャスト ルート テーブルのスキャン チェックに指定します。
count <i>count-number</i>	(任意) 各スキャンでチェックする最大プレフィクス数を指定します。有効値は 2 ~ 500 です。
period <i>seconds</i>	(任意) スキャン間隔を指定します。有効値は 2 ~ 3600 秒です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- 一貫性チェックはイネーブルです。
- **count** *count-number* は **20** です。
- **period** *seconds* は **2** 秒です。
- **settle-time** *seconds* は **60** 秒です。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

oif エントリは、マルチキャスト **{*,G}** または **{S,G}** フローの Outgoing Interface です。

一貫性チェッカーはマルチキャスト ルート テーブルをスキャンし、マルチキャスト ハードウェア エントリとマルチキャスト ルート テーブルの一貫性を保証します。不一致が検出されると、その不一致は自動的に訂正されます。

不一致エラーを表示するには、**show mls ip multicast consistency-check** コマンドを使用します。

■ mls ip multicast consistency-check

例

次に、ハードウェアによるショートカットの一貫性チェッカーをイネーブルにする例を示します。

```
Router (config)# mls ip multicast consistency-check
Router (config)#
```

次に、ハードウェアによるショートカットの一貫性チェッカーをイネーブルにし、マルチキャストルートテーブルのスキャン チェックを設定する例を示します。

```
Router (config)# mls ip multicast consistency-check type scan-mroute count 20 period 35
Router (config)#
```

次に、ハードウェアによるショートカットの一貫性チェッカーをイネーブルにし、スキャン間隔を指定する例を示します。

```
Router (config)# mls ip multicast consistency-check type scan-mroute period 35
Router (config)#
```

関連コマンド

コマンド	説明
<code>show mls ip multicast consistency-check</code>	MLS IP 情報を表示します。

mls ip multicast flow-stat-timer

スイッチ プロセッサからルート プロセッサへのフロー統計情報メッセージのバッチ間隔を設定するには、**mls ip multicast flow-stat-timer** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls ip multicast flow-stat-timer *num*

no mls ip multicast flow-stat-timer

シンタックスの説明	<i>num</i>	スイッチ プロセッサからルート プロセッサへのフロー統計情報メッセージのバッチ間隔
------------------	------------	---

コマンドのデフォルト	25 秒
-------------------	------

コマンド モード	グローバル コンフィギュレーション (config)
-----------------	----------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、スイッチ プロセッサからルート プロセッサへのフロー統計情報メッセージのバッチ間隔を指定する例を示します。

```
Router (config)# mls ip multicast flow-stat-timer 10
Router (config)#
```

関連コマンド	コマンド	説明
	show mls ip multicast	MLS IP 情報を表示します。

mls ip multicast replication-mode

レプリケーション モードのイネーブル化および指定を行うには、**mls ip multicast replication-mode** コマンドを使用します。システムを自動検出モードに戻すには、このコマンドの **no** 形式を使用します。

mls ip multicast replication-mode {egress | ingress}

no mls ip multicast replication-mode {egress | ingress}

シンタックスの説明

egress	システムをレプリケーションの出力モードに強制します。
ingress	システムをレプリケーションの入力モードに強制します。

コマンドのデフォルト

ingress

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

Supervisor Engine 32 PISA は、**egress** キーワードをサポートしていません。



(注)

出力から入力レプリケーション モードに移行中、ショートカットが削除され、再インストールされるために、トラフィックが分断される可能性があります。トラフィック転送中の分断を防ぐには、**mls ip multicast replication-mode ingress** コマンドを入力します。

no mls ip multicast replication-mode ingress コマンドを入力すると、強制入力モードだけがリセットされます。

例

次に、入力レプリケーション モードをイネーブルにする例を示します。

```
Router (config)# mls ip multicast replication-mode ingress
Router (config)#
```

関連コマンド

コマンド	説明
show mls ip multicast capability	MLS IP 情報を表示します。

mls ip multicast sso

Stateful Switch Over (SSO) パラメータを設定するには、**mls ip multicast sso** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
mls ip multicast sso {{convergence-time time} | {leak interval} | {leak percentage}}
```

シンタックスの説明

convergence-time time	プロトコル コンバージェンスまでの最大待機時間を指定します。有効値は、0 ～ 3600 秒です。
leak interval	パケット リークのインターバルを指定します。有効値は、0 ～ 3600 秒です。
leak percentage	プロトコル コンバージェンスを実行するよう、スイッチオーバー中にルータにリークされるマルチキャスト パケットのパーセンテージを指定します。有効値は、1 ～ 100% です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- **convergence-time time** : 20 秒
- **leak interval** : 60 秒
- **leak percentage** : 10%

コマンドモード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、プロトコル コンバージェンスまでの最大待機時間を設定する例を示します。

```
Router (config)# mls ip multicast sso convergence-time 300
Router (config)#
```

次に、パケット リークのインターバルを設定する例を示します。

```
Router (config)# mls ip multicast sso leak 200
Router (config)#
```

次に、パケット リークのパーセンテージを設定する例を示します。

```
Router (config)# mls ip multicast sso leak 55
Router (config)#
```

関連コマンド

コマンド	説明
show mls ip multicast sso	マルチキャスト ハイ アベイラビリティ SSO に関する情報を表示します。

mls ip multicast stub

PIM sparse (疎) モードのスタブ ネットワークに対して、非 RPF トラフィック廃棄のサポートをイネーブルにするには、**mls ip multicast stub** コマンドを使用します。PIM sparse (疎) モードのスタブ ネットワークに対して、非 RPF トラフィック廃棄のサポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

mls ip multicast stub

no mls ip multicast stub

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

マルチキャストはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

mls ip multicast stub コマンドでは、ルーテッド インターフェイスまたは VLAN で次のフィルタが作成されます。

- インターフェイスに接続されているすべてのアドレスからすべての IP 宛先への IP パケットを許可します。**ip address addr mask [secondary]** コマンドで設定した IP アドレス プレフィクス内にアドレスが収まる場合、アドレスはインターフェイスに接続されています。

このフィルタでは、直接接続されている送信元からのユニキャスト パケットおよびマルチキャスト パケットが許可されます。

- すべての送信元アドレスからマルチキャスト グループ プレフィクス 224.0.0.0/24 および 224.0.1.0/24 への IP マルチキャスト パケットを許可します。

このフィルタでは、すべての送信元アドレスから well-known マルチキャスト アドレスへパケットを送信できます。224.0.0.0/24 は、PIM、open shortest path first (OSPF)、EIGRP、Network Time Protocol (NTP) などのプロトコルによって使用されます。224.0.1.0/24 のアドレスは、AutoRP などのプロトコルによって使用されます (224.0.1.39、224.0.1.40)。

- その他すべての IP マルチキャスト パケットを拒否します。

この拒否フィルタは、直接接続されていない送信元からのマルチキャスト パケットを禁止し、このインターフェイスまたは VLAN で受信したパケットに適用されます。

IP マルチキャスト パケットを許可するフィルタ、およびその他すべての IP マルチキャスト パケットを拒否するフィルタは、**mls ip multicast stub** コマンドを設定したすべてのインターフェイスまたは VLAN で同じです。インターフェイスに接続されているすべてのアドレスからすべての IP 宛先への IP パケットを許可するフィルタは、インターフェイスまたは VLAN ごとに異なります。

例 次に、PIM sparse (疎) モードのスタブ ネットワークに対して、非 RPF トラフィック廃棄のサポートをイネーブルにする例を示します。

```
Router(config-if)# mls ip multicast stub
Router(config-if)#
```

関連コマンド

コマンド	説明
show mls ip multicast	MLS IP 情報を表示します。

mls ip multicast threshold

ハードウェアによるショートカットを組み込むために、しきい値レートを設定するには、**mls ip multicast threshold** コマンドを使用します。しきい値の設定を解除するには、このコマンドの **no** 形式を使用します。

mls ip multicast threshold *ppsec*

no mls ip multicast threshold

シンタックスの説明

ppsec しきい値 (パケット/秒)。有効値は 10 ~ 10,000 パケット/秒です。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、join 要求など、存続期間の短いマルチキャストフローに対して MLS エントリの作成を禁止する場合に使用します。

マルチキャストトラフィックが設定されたマルチキャストレートのしきい値を下回ると、マルチキャストトラフィックはすべて PISA でルーティングされます。

このコマンドは組み込み済みのルートには影響しません。たとえば、ショートカットがすでに組み込まれている場合に、このコマンドを入力しても、それらのショートカットは不適格な場合でも削除されません。既存のルートにしきい値を適用するには、ルートをいったん消去して、再確立します。

例

次に、IP MLS しきい値を 10 パケット/秒に設定する例を示します。

```
Router (config)# mls ip multicast threshold 10
Router (config)#
```

関連コマンド

コマンド	説明
mls rp ip (global configuration mode)	外部システムが PISA への IP ショートカットを確立できるようにします。
show mls ip multicast	MLS IP 情報を表示します。

mls ip nat netflow-frag-l4-zero

フラグメントされたパケットに関する NetFlow 検索テーブルのレイヤ 4 情報を消去するには、**mls ip nat netflow-frag-l4-zero** コマンドを使用します。

mls ip nat netflow-frag-l4-zero

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドは、PFC3BXL または PFC3B モードだけでサポートされます。ソフトウェアに送信される最初のフラグメントを NetFlow ショートカットと照合する（通常の処理）のを回避するには、**mls ip nat netflow-frag-l4-zero** コマンドを使用します。ソフトウェアに送信される次のフラグメントは、最初のフラグメントからのレイヤ 4 ポート情報に基づいて変換されます。最初のフラグメントからのレイヤ 4 ポート情報に基づく変換は、NetFlow キーに照合用のフラグメントビットがないために実行されます。

TCAM でプログラムされる ACL TCAM エントリ/マスクを多数必要とする大規模の機能設定がインターフェイス上にある場合、インターフェイスが network address translation (NAT; ネットワークアドレス変換) 内部インターフェイスとして設定されていると、この機能設定が ACL TCAM に適合せず、インターフェイス上のトラフィックはソフトウェアでスイッチングされることがあります。

例 次に、フラグメントされたパケットに関する NetFlow 検索テーブルのレイヤ 4 情報を消去する例を示します。

```
Router (config)# mls ip nat netflow-frag-l4-zero
Router (config)#
```

mls ip pbr

ポリシー ルーティング パケットの MLS サポートをイネーブルにするには、**mls ip pbr** コマンドを使用します。ポリシー ルーティング パケットの MLS サポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

mls ip pbr [null0]

no mls ip pbr

シンタックスの説明

null0	(任意) ルート マップのインターフェイス null0 へのハードウェア サポートをイネーブルにします。
--------------	--

コマンドのデフォルト

ポリシー ルーティング パケットへの MLS サポートはディセーブルです。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



(注) 同じインターフェイス上で **policy-based routing** (PBR; ポリシー ベース ルーティング) と **SLB** をイネーブルにしないでください。PBR ベースのパケットが正しく転送されなくなります。

mls ip pbr コマンドを入力してハードウェア ポリシー ルーティングをイネーブルにすると、ハードウェアですべてのポリシー ルーティングが行われ、ポリシー ルーティングにインターフェイスが設定されているかどうかに関係なく、すべてのインターフェイスに適用されます。

ルートマップの **set interface null0** のハードウェア サポートをイネーブルにするためだけにルーテッドトラフィックがある場合は、**null0** キーワードを使用します。

例

次に、ポリシー ルーティング パケットの MLS サポートをイネーブルにする例を示します。

```
Router(config)# mls ip pbr
Router(config)#
```

関連コマンド

コマンド	説明
show team interface	インターフェイスベースの TCAM に関する情報を表示します。
vlan acl	

mls ip reflexive ndr-entry tcam

NDR によって組み込まれた再帰 TCP/UDP エントリに対して TCAM 内のショートカットをイネーブルにするには、**mls ip reflexive ndr-entry tcam** コマンドを使用します。NDR によって組み込まれた再帰 TCP/UDP エントリに対して TCAM 内のショートカットをディセーブルにするには、このコマンドの **no** 形式を使用します。

mls ip reflexive ndr-entry tcam

no mls ip reflexive ndr-entry tcam

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト ディセーブル

コマンド モード グローバル コンフィギュレーション (config)

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン **mls ip reflexive ndr-entry tcam** コマンドを入力すると、再帰 ACL ダイナミック エントリは NetFlow ではなく TCAM に組み込まれます。

例 次に、NDR によって組み込まれた再帰 TCP/UDP エントリに対して TCAM 内のショートカットをイネーブルにする例を示します。

```
Router(config)# mls ip reflexive ndr-entry tcam
Router(config)#
```

次に、NDR によって組み込まれた再帰 TCP/UDP エントリに対して TCAM 内のショートカットをディセーブルにする例を示します。

```
Router(config)# no mls ip reflexive ndr-entry tcam
Router(config)#
```

コマンド	説明
mls ip delete-threshold	設定済み ACL しきい値を削除します。
mls ip install-threshold	設定済み ACL しきい値を組み込みます。

mls ipv6 acl compress address unicast

IPv6 のアドレスの圧縮をオンにするには、**mls ipv6 acl compress address unicast** コマンドを使用します。IPv6 アドレスの圧縮をオフに切り替えるには、このコマンドの **no** 形式を使用します。

mls ipv6 acl compress address unicast

no mls ipv6 acl compress address unicast

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト デイセーブル

コマンド モード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



注意

ネットワーク内に非圧縮アドレス タイプがある場合は、圧縮モードをイネーブルにしないでください。表 2-15 に、圧縮アドレスのタイプおよびアドレス圧縮方式の一覧を示します。

表 2-15 圧縮アドレスのタイプおよび方式

アドレス タイプ	圧縮方式
MAC アドレスに基づく EUI-64	このアドレスは、ビット ロケーション [39:24] から 16 ビットを削除することにより圧縮されます。ハードウェアがこれらのアドレスを圧縮する際、情報は損失しません。
組み込み型 IPv4 アドレス	このアドレスは、上位 16 ビットを削除することにより圧縮されます。ハードウェアがこれらのアドレスを圧縮する際、情報は損失しません。

表 2-15 圧縮アドレスのタイプおよび方式 (続き)

アドレス タイプ	圧縮方式
リンク ローカル	これらのアドレスは、ビット [95:80] のゼロを削除することにより圧縮され、組み込み型 IPv4 アドレスと同じパケットタイプを使用して識別されます。ハードウェアがこれらのアドレスを圧縮する際、情報は損失しません。
その他	<p>上記のカテゴリに該当しない IPv6 アドレスは、その他に分類されます。IPv6 アドレスがその他に分類される場合、次のようになります。</p> <ul style="list-style-type: none"> 圧縮モードがオンの場合、IPv6 アドレスは EUI-64 圧縮方式 (ビット [39:24] の削除) と同様に圧縮され、レイヤ 4 情報を QoS TCAM を検索するのに使用されるキーの一部として使用できるが、レイヤ 3 情報は損失されます。 グローバル圧縮モードがオフの場合、IPv6 アドレスの 128 ビット全体が使用されます。レイヤ 4 のポート情報は IPv6 検索キーのサイズ制限のため、QoS TCAM を検索するためのキーに含まれません。

例

次に、IPv6 の非圧縮アドレスの圧縮をオンにする例を示します。

```
Router(config)# mls ipv6 acl compress address unicast
Router(config)#
```

次に、IPv6 の非圧縮アドレスの圧縮をオフにする例を示します。

```
Router(config)# no mls ipv6 acl compress address unicast
Router(config)#
```

関連コマンド

コマンド	説明
show fm ipv6 traffic-filter	IPv6 情報を表示します。
show mls netflow ipv6	NetFlow ハードウェアに関する設定情報を表示します。

mls ipv6 acl source

送信元特定アドレスからのすべての IPv6 パケットを拒否するには、**mls ipv6 acl source** コマンドを使用します。送信元特定アドレスからのすべての IPv6 パケットを受け入れるには、このコマンドの **no** 形式を使用します。

```
mls ipv6 acl source {loopback | multicast}
```

```
no mls ipv6 acl source {loopback | multicast}
```

シンタックスの説明

loopback	送信元ループバック アドレスを含むすべての IPv6 パケットを拒否します。
multicast	送信元マルチキャスト アドレスを含むすべての IPv6 パケットを拒否します。

コマンドのデフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、送信元ループバック アドレスを含むすべての IPv6 パケットを拒否する例を示します。

```
Router(config)# mls ipv6 acl source loopback
Router(config)#
```

次に、送信元マルチキャスト アドレスを含むすべての IPv6 パケットを拒否する例を示します。

```
Router(config)# no mls ipv6 acl source multicast
Router(config)#
```

関連コマンド

コマンド	説明
show mls netflow ipv6	NetFlow ハードウェアに関する設定情報を表示します。

mls mpls (recirculation)

MPLS 再循環をイネーブルにするには、**mls mpls** コマンドを使用します。MPLS 再循環をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
mls mpls {recir-agg | tunnel-recir}
```

```
no mls mpls {recir-agg | tunnel-recir}
```

シンタックスの説明	recir-agg	MPLS 集約ラベル パケットを再循環します（新規の集約ラベルは、影響されるだけです）。
	tunnel-recir	トンネル MPLS パケットを再循環します。

コマンドのデフォルト ディセーブル

コマンド モード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン トンネル MPLS 再循環をイネーブルにしない場合、ラベリングされる必要のある IPv4 および IPv4 トンネル パケット（MPLS ヘッダーでカプセル化されたパケット等）は、Catalyst 6500 シリーズスイッチから転送される際に破壊されます。

IPv4、IPv6、および MPLS プロトコルの FIB TCAM 例外ステータスを表示するには、**show erm statistics** コマンドを使用します。

例 次に、集約ラベル MPLS 再循環をイネーブルにする例を示します。

```
Router(config)# mls mpls recir-agg
Router(config)#
```

次に、トンネル MPLS 再循環をイネーブルにする例を示します。

```
Router(config)# mls mpls tunnel-recir
Router(config)#
```

次に、集約ラベル MPLS 再循環をディセーブルにする例を示します。

```
Router(config)# no mls mpls recir-agg
Router(config)#
```

次に、トンネル MPLS 再循環をディセーブルにする例を示します。

```
Router(config)# no mls mpls tunnel-recir
Router(config)#
```

関連コマンド

コマンド	説明
show erm statistics	IPv4、IPv6、MPLS プロトコルの FIB TCAM 例外ステータスを表示します。

mls mpls (guaranteed bandwidth traffic engineering)

guaranteed bandwidth traffic engineering (GBTE; 保証帯域幅トラフィック エンジニアリング) のフロー パラメータをグローバルに設定するには、**mls mpls** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
mls mpls {{gb-te-burst burst}} | {{gb-te-cir-ratio ratio}} | {{gb-te-dscp dscp-value
[markdown]}} | {{gb-te-enable [global-pool]}}
```

```
no mls mpls {{gb-te-burst burst}} | {{gb-te-cir-ratio ratio}} | {{gb-te-dscp dscp-value
[markdown]}} | {{gb-te-enable [global-pool]}}
```

シンタックスの説明

gb-te-burst <i>burst</i>	保証帯域幅トラフィック エンジニアリングのフローのバースト期間を指定します。有効値は、100 ~ 30000 ミリ秒です。
gb-te-cir-ratio <i>ratio</i>	Committed Information Rate (CIR; 認定情報レート) のポリシングの比率を指定します。有効値は 1 ~ 100% です。
gb-te-dscp <i>dscp-value</i>	保証帯域幅トラフィック エンジニアリングのフローの DSCP マップを指定します。有効値は、0 ~ 63 です。
markdown	(任意) 不適合フローをマークダウンまたは廃棄します。
gb-te-enable	保証帯域幅トラフィック エンジニアリングのフロー ポリシングをイネーブルにします。
global-pool	(任意) グローバル プールからポリシング トラフィック エンジニアリング フローに割り当てられたリソースの使用を指定します。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- *burst* は 1000 ミリ秒です。
- *ratio* は、1% です。
- *dscp-value* は 40 です。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ラベルなしの packets が交換された場合に MPLS packets の EXP 値をリセットするには、**mls qos map dscp-exp** コマンドを使用します。

トンネル MPLS 再循環をイネーブルにしない場合、ラベリングされる必要のある IPv4 および IPv4 トンネル packets (MPLS ヘッダーでカプセル化された packets 等) は、Catalyst 6500 シリーズスイッチから転送される際に破壊されます。

■ **mls mpls (guaranteed bandwidth traffic engineering)**

IPv4、IPv6、および MPLS プロトコルの FIB TCAM 例外ステータスを表示するには、**show erm statistics** コマンドを使用します。

例

次に、保証帯域幅トラフィック エンジニアリング フローのバースト期間を指定する例を示します。

```
Router(config)# mls mpls gb-te-burst 2000
Router(config)#
```

次に、CIR ポリシングの比率を指定する例を示します。

```
Router(config)# mls mpls gb-te-ratio 30
Router(config)#
```

次に、保証帯域幅トラフィック エンジニアリング フローの DSCP マップを指定し、不適合なフローを廃棄する例を示します。

```
Router(config)# mls mpls gb-te-dscp 25 markdown
Router(config)#
```

次に、保証帯域幅トラフィック エンジニアリング フローのポリシングをイネーブルにする例を示します。

```
Router(config)# mls mpls gb-te-enable
Router(config)#
```

関連コマンド

コマンド	説明
show erm statistics	IPv4、IPv6、MPLS プロトコルの FIB TCAM 例外ステータスを表示します。

mls nde flow

NDE のフィルタ オプションを指定するには、**mls nde flow** コマンドを使用します。NDE フロー フィルタをクリアし、フィルタをリセットしてデフォルト設定に戻す場合は、このコマンドの **no** 形式を使用します。

```
mls nde flow {include | exclude} {{dest-port port-num} | {destination ip-addr ip-mask} |
{protocol {tcp | udp}} | {source ip-addr ip-mask} | {src-port port-num}}
```

```
no mls nde flow {include | exclude}
```

シンタックスの説明

include	指定したフィルタと一致するフローを除くすべてのフローのインポートを許可します。
exclude	指定したフィルタと一致するすべてのフローのエクスポートを許可します。
dest-port port-num	フィルタする宛先ポートを指定します。有効値は 1 ~ 100 です。
destination ip-addr ip-mask	フィルタする宛先 IP アドレスおよびマスクを指定します。
protocol	追加または除外対象のプロトコルを指定します。
tcp	TCP を追加または除外対象にします。
udp	UDP を追加または除外対象にします。
source ip-addr ip-mask	フィルタする送信元 IP アドレスおよびサブネット マスクビットを指定します。
src-port port-num	フィルタする送信元ポートを指定します。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- すべての期限切れフローはインポートされます。
- インターフェイスのエクスポートはディセーブルです (**no mls nde interface**)。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

mls nde flow コマンドは、NDE にフィルタリングを追加します。指定された基準と一致する期限切れフローがエクスポートされます。これらの値は NVRAM に保存され、NDE をディセーブルにしてもクリアされません。このコマンドにオプションを指定しなかった場合は、ワイルドカードとして処理されます。NVRAM 内の NDE フィルタは、NDE をディセーブルにしてもクリアされません。

同時にアクティブにできるフィルタは、1 つだけです。**exclude** または **include** キーワードを入力しなかった場合は、フィルタは包含フィルタとして使用されます。

包含および排除フィルタは NVRAM に保存され、NDE をディセーブルにしても削除されません。

ip-addr/maskbits は、サブネットアドレスの簡易ロングフォーマットです。マスクビットは、ネットワークマスクのビット数を指定します。たとえば、172.25.2.1/22 は、22 ビットサブネットアドレスを示します。*ip-addr* は、193.22.253.1/22 のような完全ホストアドレスです。

例

次に、宛先ポート 23 への期限切れフローだけがエクスポートされるように、インターフェイスフローフィルタを指定する例を示します（フローマスクは *ip-flow* に設定されているものと想定します）。

```
Router(config)# mls nde flow include dest-port 23
Router(config)#
```

関連コマンド

コマンド	説明
show mls netflow	NetFlow ハードウェアに関する設定情報を表示します。

mls nde interface

NDE パケットに追加フィールドを入力するには、**mls nde interface** コマンドを使用します。追加フィールドの入力をディセーブルにするには、このコマンドの **no** 形式を使用します。

mls nde interface

no mls nde interface

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト イネーブル

コマンド モード インターフェイス コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン NDE パケットに次の追加フィールドを入力するように、NDE を設定できます。

- 出力インターフェイス SNMP インデックス
- 送信元自律システム番号
- 宛先自律システム番号
- ネクスト ホップ ルータの IP アドレス

フロー マスクが **interface-full** または **interface-src-dst** の場合、入力インターフェイス SNMP インデックスは必ず入力されます。

詳細については、『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide Release 12.2ZY*』の「Configuring NDE」の章を参照してください。

例 次に、NDE パケットに追加フィールドを入力する例を示します。

```
Router(config)# mls nde interface
Router(config)#
```

次に、追加フィールドの入力をディセーブルにする例を示します。

```
Router(config)# no mls nde interface
Router(config)#
```

関連コマンド	コマンド	説明
	mls netflow	NetFlow で統計収集を可能にします。
	mls netflow sampling	インターフェイス上でサンプリング済み NetFlow をイネーブルにします。

mls nde sender

MLS NDE エクスポートをイネーブルにするには、**mls nde sender** コマンドを使用します。MLS NDE エクスポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

mls nde sender [*version version*]

no mls nde sender

シンタックスの説明

version version (任意) NDE を指定します。有効値は **5** および **7** です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- MLS NDE エクスポートはディセーブルです。
- *version* は **7** です。

コマンドモード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、MLS NDE エクスポートをイネーブルにする例を示します。

```
Router(config)# mls nde sender
Router(config)#
```

次に、MLS NDE エクスポートをディセーブルにする例を示します。

```
Router(config)# no mls nde sender
Router(config)#
```

関連コマンド

コマンド	説明
show mls nde	NDE ハードウェアによってスイッチングされるフローに関する情報を表示します。

mls netflow

統計情報を収集する NetFlow をイネーブルにするには、**mls netflow** コマンドを使用します。NetFlow による統計収集をディセーブルにするには、このコマンドの **no** 形式を使用します。

mls netflow

no mls netflow

シンタックスの説明	interface (任意) インターフェイス単位の統計情報収集を指定します。
-----------	--

コマンドのデフォルト	イネーブル
------------	-------

コマンド モード	グローバル コンフィギュレーション (config)
----------	----------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン NetFlow は、Catalyst 6500 シリーズ スイッチを流れるトラフィックから統計情報を収集し、その統計情報を NetFlow テーブルに保存します。プロトコルに基づいてグローバルに、またはインターフェイス単位 (任意) で統計情報を収集できます。

NDE、またはハードウェア NetFlow テーブルを使用する Cisco IOS 機能 (micro-flow QoS、WCCP、TCP Intercept、または再帰 ACL) を使用していない場合は、グローバル コンフィギュレーション モードで **no mls netflow** コマンドを使用して、ハードウェア NetFlow テーブルの使用およびメンテナンスを安全にディセーブルにできます。

例 次に、統計情報を収集する例を示します。

```
Router(config)# mls netflow
Router(config)#
```

次に、統計情報収集の NetFlow をディセーブルにする例を示します。

```
Router(config)# no mls netflow
Disabling MLS netflow entry creation.
Router(config)#
```

関連コマンド	コマンド	説明
	show mls netflow	NetFlow ハードウェアに関する設定情報を表示します。

mls netflow maximum-flows

NetFlow テーブルの最大フロー割り当てを設定するには、**mls netflow maximum-flows** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls netflow maximum-flows [*maximum-flows*]

no mls netflow maximum-flows

シンタックスの説明

maximum-flows (任意) フローの最大数。有効値は、**16、32、64、80、96**、および **128** です。詳細については、「[使用上のガイドライン](#)」を参照してください。

コマンドのデフォルト

128

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

フローの最大数に指定する値は、その 1000 倍の値になります。たとえば、32 を入力すると、許可されたフローの最大数は 32000 に指定されます。

例

次に、NetFlow テーブルの最大フロー割り当てを設定する例を示します。

```
Router(config)# mls netflow maximum-flows 96
Router(config)#
```

次に、デフォルト設定に戻す例を示します。

```
Router(config)# no mls netflow maximum-flows
Router(config)#
```

関連コマンド

コマンド	説明
show mls netflow table-contention	NetFlow ハードウェアの table contention level (TCL; テーブル コンテンション レベル) の設定情報を表示します。

mls netflow sampling

インターフェイス上でサンプリング済み NetFlow をイネーブルにするには、**mls netflow sampling** コマンドを使用します。サンプリング済み NetFlow をディセーブルにするには、このコマンドの **no** 形式を使用します。

mls netflow sampling

no mls netflow sampling

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト ディセーブル

コマンド モード インターフェイス コンフィギュレーション

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン サンプリングをイネーブルにするには、**mls sampling** コマンドおよび **mls netflow sampling** コマンドを適切なインターフェイスで入力する必要があります。**mls netflow sampling** コマンドを入力しないと、NDE はフローをエクスポートしません。

現在のフロー マスクに応じて、サンプリング済み NetFlow をグローバルに、またはインターフェイス単位で設定できます。**Interface-Full** および **Interface-Src-Dest** フロー マスクの場合、サンプリング済み NetFlow はインターフェイス単位でイネーブル化されます。その他のすべてのフロー マスクの場合、サンプリング済み NetFlow は常にグローバルであり、すべてのインターフェイスに対して一括でイネーブルまたはディセーブルになります。

サンプリング済み NetFlow をグローバルにイネーブルにするには、**mls sampling** コマンドを入力します。

例 次に、インターフェイス上でサンプリング済み NetFlow をイネーブルにする例を示します。

```
Router(config-if)# mls netflow sampling
Router(config-if)#
```

次に、インターフェイス上でサンプリング済み NetFlow をディセーブルにする例を示します。

```
Router(config-if)# no mls netflow sampling
Router(config-if)#
```

■ mls netflow sampling

関連コマンド

コマンド	説明
mls sampling	サンプリング済み NetFlow のイネーブル化およびサンプリング方式の指定を行います。
show mls sampling	サンプリング済み NDE ステータスに関する情報を表示します。

mls netflow usage notify

スイッチ プロセッサ上での NetFlow テーブル使用率をモニタするには、**mls netflow usage notify** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls netflow usage notify {*threshold interval*}

no mls netflow usage notify

シンタックスの説明	threshold	超過した場合に警告メッセージを表示するしきい値パーセンテージ。有効値は、20 ~ 100% です。
	interval	NetFlow テーブル使用率が確認される頻度。有効値は、120 ~ 1,000,000 秒です。

コマンドのデフォルト ディセーブル

コマンドモード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン NetFlow テーブル使用のモニタリングがイネーブルで、NetFlow テーブル使用がしきい値パーセンテージを超えると、警告メッセージが表示されます。

NetFlow は、Catalyst 6500 シリーズスイッチを流れるトラフィックから統計情報を収集し、その統計情報を NetFlow テーブルに保存します。プロトコルに基づいてグローバルに、またはインターフェイス単位 (任意) で統計情報を収集できます。

NDE、またはハードウェア NetFlow テーブルを使用する Cisco IOS 機能 (micro-flow QoS、WCCP、TCP Intercept、または再帰 ACL) を使用していない場合は、グローバル コンフィギュレーション モードで **no mls netflow** コマンドを使用して、ハードウェア NetFlow テーブルの使用およびメンテナンスを安全にディセーブルにできます。

例 次に、スイッチ プロセッサに NetFlow テーブル使用率のモニタを設定する例を示します。

```
Router (config)# mls netflow usage notify 80 300
Router (config)#
```

関連コマンド	コマンド	説明
	show mls netflow usage	NetFlow ハードウェアに関する設定情報を表示します。

mls qos (global configuration mode)

QoS 機能をグローバルにイネーブルにするには、**mls qos** コマンドを使用します。QoS 機能をグローバルにディセーブルにするには、このコマンドの **no** 形式を使用します。

mls qos

no mls qos

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

QoS はグローバルにディセーブルです。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

QoS がグローバルにイネーブルの場合は、QoS がディセーブル化されているインターフェイスを除いて、すべてのインターフェイスで QoS がイネーブルになります。QoS がグローバルにディセーブルの場合は、すべてのトラフィックが QoS パススルー モードで渡されます。

ポートキューイング モードでは、PFC QoS (マーキングおよびポリシング) はディセーブルであり、パケットの Type of Service (ToS; サービス タイプ) および CoS は PFC で変更されません。受信および送信に関するすべてのキューイングは、着信パケットの QoS タグに基づいて行われます。この QoS タグは、着信 CoS に基づきます。

802.1Q または ISL カプセル化ポート リンクでは、キューイングはパケット 802.1Q または ISL CoS に基づいて行われます。

ルータのメイン インターフェイスまたはアクセス ポートでは、キューイングは設定されたポート単位の CoS (デフォルト CoS は 0) に基づいて行われます。

このコマンドは、オフの状態のすべてのインターフェイス上で TCAM QoS をイネーブルまたはディセーブルにできます。

例

次に、QoS をグローバルにイネーブルにする例を示します。

```
Router(config)# mls qos  
Router(config)#
```

次に、Catalyst 6500 シリーズスイッチで QoS をグローバルにディセーブルにする例を示します。

```
Router(config)# no mls qos  
Router(config)#
```

関連コマンド

コマンド	説明
mls qos (interface configuration mode)	インターフェイス上の QoS 機能をイネーブルにします。
show mls qos	MLS QoS 情報を表示します。

mls qos (interface configuration mode)

インターフェイス上で QoS 機能をイネーブルにするには、**mls qos** コマンドを使用します。QoS 機能をインターフェイスでディセーブルにするには、このコマンドの **no** 形式を使用します。

mls qos

no mls qos

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

イネーブル

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

CLI を使用すると、OC-12 ATM OSM の WAN ポートおよびチャネライズド OSM の WAN ポートに PFC ベースの QoS を設定できますが、PFC ベースの QoS はこれらの OSM の WAN ポートではサポートされていません。

QoS をグローバルにディセーブルにすると、すべてのインターフェイスでディセーブルになります。

このコマンドは、インターフェイスの TCAM QoS (分類、マーキング、およびポリシング) をイネーブルまたはディセーブルにします。

例

次に、インターフェイス上で QoS をイネーブルにする例を示します。

```
Router(config-if)# mls qos
Router(config-if)#
```

関連コマンド

コマンド	説明
mls qos (global configuration mode)	QoS 機能をグローバルにイネーブルにします。
show mls qos	MLS QoS 情報を表示します。

mls qos aggregate-policer

ポリシー マップで使用する名前付き集約ポリサーを定義するには、**mls qos aggregate-policer** コマンドを使用します。このポリサーは、異なったポリシー マップ クラスおよび異なったインターフェイスで共有できます。名前付き集約ポリサーを削除するには、このコマンドの **no** 形式を使用します。

mls qos aggregate-policer name rate-bps

mls qos aggregate-policer name rate-bps burst-bytes maximum-burst-bytes

mls qos aggregate-policer name rate-bps [**conform-action** {**drop** [**exceed-action** *action*]}] | **set-dscp-transmit** [*new-dscp*] | **set-prec-transmit** [*new-precedence*] | **transmit** [**exceed-action** *action*] | **violate-action** *action*]]]

mls qos aggregate-policer aggregate-name rate-bps {**pir peak-rate-bps** [**conform-action** {**drop** [**exceed-action** *action*]}] | **set-dscp-transmit** [*new-dscp*] | **set-prec-transmit** [*new-precedence*] | **transmit** [**exceed-action** *action*] | **violate-action** *action*]]]}

no mls qos aggregate-policer name

シンタックスの説明

<i>name</i>	集約ポリサー名
<i>rate-bps</i>	最大 bps。有効値は、32000 ~ 10,000,000,000 です。
<i>burst-bytes</i>	バースト バイト。有効値は 1000 ~ 31,250,000 です。
<i>maximum-burst-bytes</i>	最大バースト バイト。有効値は 1000 ~ 31,250,000 です (入力する場合は、標準バースト バイトと同じ値に設定する必要があります)。
conform-action	(任意) レートが超えない場合に実行するアクションを指定します。
drop	(任意) パケットを廃棄します。
exceed-action <i>action</i>	(任意) QoS 値を超えた場合に実行するアクションを指定します。有効値については、「使用上のガイドライン」を参照してください。
set-dscp-transmit	DSCP 値を設定し、パケットを送信します。
<i>new-dscp</i>	(任意) 新しい DSCP 値。有効値は 0 ~ 63 です。
set-prec-transmit	パケットの優先順位を書き換えて、パケットを送信します。
<i>new-precedence</i>	(任意) 新しい優先順位値。有効値は 0 ~ 7 です。
violate-action <i>action</i>	(任意) QoS 値に違反した場合に実行するアクションを指定します。有効値については、「使用上のガイドライン」を参照してください。
pir peak-rate-bps	Peak Information Rate (PIR; 最大情報レート) ピーク レートを設定します。有効値は 32000 ~ 10,000,000,000 です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- *extended-burst-bytes* は *burst-bytes* と同じです。
- **conform-action** は **transmit** です。
- **exceed-action** は **drop** です。
- **violate-action** は、**exceed-action** と同じです。
- **pir peak-rate-bps** は標準の (**cir**) レートと同じです。

コマンド モード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン *action* の有効値は次のとおりです。

- **drop** : パケットを廃棄します。
- **policed-dscp-transmit** : ポリシング済み DSCP マップごとに DSCP を変更して、送信します。
- **transmit** : パケットを伝送します。

Catalyst 6500 シリーズ スイッチでは、1023 までの集約規則および 1023 までのポリシング規則がサポートされます。

mls qos aggregate-policer コマンドを使用すると、集約フローおよびその集約のポリシング規則を設定できます。レートおよびバースト パラメータを入力すると、平均レートの範囲は 32 Kbps ~ 4 Gbps (それぞれ 32000、4000000000 と入力) となり、バースト サイズの範囲は 1 KB (1000 と入力) ~ 512 MB (512000000 と入力) となります。既存の集約レート制限エントリを変更すると、そのエントリが使用中の場合には、NVRAM および Catalyst 6500 シリーズ スイッチのエントリが変更されます。



(注) ハードウェア粒度のため、レート値が制限されます。そのため、設定したバースト値が使用されない場合があります。

既存のマイクロフローまたは集約レート制限を変更すると、使用中の場合には NVRAM および Catalyst 6500 シリーズ スイッチのエントリが変更されます。

集約ポリサー名を入力する場合、次の命名規則に従います。

- 最大 31 文字で、a ~ z、A ~ Z、0 ~ 9、ダッシュ文字 (-)、アンダースコア (_)、ピリオド文字 (.) を含むことができます。
- 英文字で始まり、すべてのタイプのすべての ACL で一意である必要があります。
- 大文字と小文字を区別します。
- 番号は使用できません。
- キーワードは使用できません。避けるべきキーワードは、**all**、**default-action**、**map**、**help**、および **editbuffer** です。

例 次に、QoS 集約ポリサーが最大 100,000 bps および 10,000 バイトの標準バースト サイズを許可し、これらのレートを超過しない場合には DSCP を 48 に設定し、これらのレートを超過した場合にはパケットを廃棄するよう設定する例を示します。

```
Router(config)# mls qos aggregate-policer micro-one 100000 10000 conform-action set-dscp
48 exceed action drop
Router(config)#
```

関連コマンド	コマンド	説明
	set ip dscp (policy-map configuration)	ToS バイトの IP DSCP を設定してパケットにマーキングします。

mls qos bridged

レイヤ 3 の LAN インターフェイス上でブリッジドトラフィックのマイクロフローポリシーをイネーブルにするには、**mls qos bridged** コマンドを使用します。ブリッジドトラフィックのマイクロフローポリシーをディセーブルにするには、このコマンドの **no** 形式を使用します。

mls qos bridged

no mls qos bridged

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト ディセーブル

コマンドモード インターフェイス コンフィギュレーション

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドをサポートするのは、SVI だけです。

例 次に、VLAN インターフェイスのブリッジドトラフィックに対してマイクロフローポリシーをイネーブルにする例を示します。

```
Router(config-if)# mls qos bridged
Router(config-if)#
```

コマンド	説明
show mls qos	MLS QoS 情報を表示します。

mls qos channel-consistency

EtherChannel バンドリングに関する QoS ポート属性チェックをイネーブルにするには、**mls qos channel-consistency** コマンドを使用します。EtherChannel バンドリングに関する QoS ポート属性チェックをディセーブルにするには、このコマンドの **no** 形式を使用します。

mls qos channel-consistency

no mls qos channel-consistency

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

イネーブル

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

mls qos channel-consistency コマンドは、ポート チャネルだけでサポートされています。

例

次に、EtherChannel バンドリングに関する QoS ポート属性チェックをイネーブルにする例を示します。

```
Router(config-if)# mls qos channel-consistency
Router(config-if)#
```

次に、EtherChannel バンドリングに関する QoS ポート属性チェックをディセーブルにする例を示します。

```
Router(config-if)# no mls qos channel-consistency
Router(config-if)#
```

mls qos cos

インターフェイスのデフォルトの CoS 値を定義するには、**mls qos cos** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

mls qos cos *cos-value*

no mls qos cos *cos-value*

シンタックスの説明	<i>cos-value</i> インターフェイスのデフォルト CoS 値。有効値は 0 ~ 7 です。
-----------	--

コマンドのデフォルト	デフォルト設定は次のとおりです。
------------	------------------

- *cos-value* は **0** です。
- CoS の上書きは設定されていません。

コマンドのデフォルト	インターフェイス コンフィギュレーション
------------	----------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン	CoS 値は、物理 LAN ポートだけで設定できます。
------------	-----------------------------

例	次に、デフォルト QoS CoS 値を 6 に設定する例を示します。
---	------------------------------------

```
Router(config-if)# mls qos cos 6
Router(config-if)#
```

関連コマンド	コマンド	説明
	show mls qos	MLS QoS 情報を表示します。

mls qos cos-mutation

入力 CoS 変換マップをインターフェイスに付加するには、**mls qos cos-mutation** コマンドを使用します。インターフェイスから入力 CoS 変換マップを削除するには、このコマンドの **no** 形式を使用します。

mls qos cos-mutation *cos-mutation-table-name*

no mls qos cos-mutation

シンタックスの説明

cos-mutation-table-name 入力 CoS 変換テーブル名

コマンド モード

テーブルは定義されていません。

コマンドのデフォルト

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、入力 CoS 変換マップ (mutemap2) を付加する例を示します。

```
Router(config-if)# mls qos cos-mutation mutemap2
Router(config-if)#
```

関連コマンド

コマンド	説明
mls qos map cos-mutation	パケットの CoS を新しい CoS 値にマッピングします。
show mls qos	MLS QoS 情報を表示します。

mls qos dscp-mutation

出力 DSCP 変換マップをインターフェイスに付加するには、**mls qos dscp-mutation** コマンドを使用します。インターフェイスから出力 DSCP 変換マップを削除するには、このコマンドの **no** 形式を使用します。

mls qos dscp-mutation *dscp-mutation-table-name*

no mls qos dscp-mutation

シンタックスの説明	<i>dscp-mutation-table-name</i> 出力 DSCP 変換テーブル名
------------------	---

コマンド モード	テーブルは定義されていません。
-----------------	-----------------

コマンドのデフォルト	インターフェイス コンフィギュレーション
-------------------	----------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例	次に、出力 DSCP 変換マップ（mutemap1）を付加する例を示します。 <pre>Router(config-if)# mls qos dscp-mutation mutemap1 Router(config-if)#</pre>
----------	---

関連コマンド	コマンド	説明
	mls qos map dscp-mutation	指定した DSCP 変換マップを定義します。
	show mls qos	MLS QoS 情報を表示します。

mls qos exp-mutation

出力 EXP 変換マップをインターフェイスに付加するには、**mls qos exp-mutation** コマンドを使用します。インターフェイスから出力 EXP 変換マップを削除するには、このコマンドの **no** 形式を使用します。

mls qos exp-mutation *exp-mutation-table-name*

no mls qos exp-mutation

シンタックスの説明

<i>exp-mutation-table-name</i>	出力 EXP 変換テーブル名
--------------------------------	----------------

コマンドのデフォルト

テーブルは定義されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、出力 EXP 変換マップ (mutemap2) を付加する例を示します。

```
Router(config-if)# mls qos exp-mutation mutemap2
Router(config-if)#
```

関連コマンド

コマンド	説明
mls qos map dscp-mutation	指定した DSCP 変換マップを定義します。
show mls qos mpls	ポリシー マップの MPLS QoS クラスのインターフェイス概要を表示します。

mls qos loopback

ループバック ケーブルを介した VLAN の SVI フラッドからルータ ポートを削除するには、**mls qos loopback** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos loopback

no mls qos loopback

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト デイセーブル

コマンドのデフォルト インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

インターフェイスに **mls qos loopback** コマンドを適用すると、パケットはそのインターフェイスに対して転送されなくなります。

mls qos loopback コマンドを入力する前に、OSM インターフェイスの MAC アドレスを指定する必要があります。MAC アドレスは、PFC2 ハードウェア スイッチングに使用される LAN ルータの MAC アドレスとは異なるものを設定します。

例

次に、パケットをそのインターフェイスに対して転送しないようにする例を示します。

```
Router (config-if)# mls qos loopback  
Router (config-if)#
```

mls qos map cos-dscp

信頼されたインターフェイスに入力 CoS/DSCP マップを定義するには、**mls qos map cos-dscp** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

mls qos map cos-dscp values

no mls qos map cos-dscp

シンタックスの説明

values スペースで区切った、CoS 値に対応する 8 つの DSCP 値。有効値は 0 ~ 63 です。

コマンド モード

表 2-16 に、デフォルトの CoS/DSCP 設定を示します。

表 2-16 デフォルトの CoS/DSCP マッピング

CoS	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

コマンドのデフォルト

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

CoS/DSCP マップは、信頼されたインターフェイス（またはフロー）に着信したパケットの CoS を、信頼タイプが **trust-cos** である DSCP にマッピングする場合に使用します。このマップは、8 つの CoS 値（0 ~ 7）およびこれに対応する DSCP 値のテーブルです。Catalyst 6500 シリーズ スイッチには 1 つのマップがあります。

例

次に、信頼されたインターフェイスに入力 CoS/DSCP マッピングを設定する例を示します。

```
Router(config)# mls qos map cos-dscp 20 30 1 43 63 12 13 8
Router(config)#
```

関連コマンド

コマンド	説明
mls qos map dscp-cos	出力 DSCP/CoS マップを定義します。
mls qos map ip-prec-dscp	信頼されたインターフェイスに入力 IP precedence/DSCP マップを定義します。
mls qos map policed-dscp	ポリシング済み DSCP 値とマーキング済み DSCP 値のマップを設定します。
show mls qos maps	QoS マップ設定およびランタイム バージョンに関する情報を表示します。

mls qos map cos-mutation

パケットの CoS を新しい CoS 値にマッピングするには、**mls qos map cos-mutation** コマンドを使用します。マップを削除するには、このコマンドの **no** 形式を使用します。

```
mls qos map cos-mutation name mutated_cos1 mutated_cos2 mutated_cos3 mutated_cos4
mutated_cos5 mutated_cos6 mutated_cos7 mutated_cos8
```

```
no mls qos map cos-mutation name
```

シンタックスの説明

<i>name</i>	CoS マップ名
<i>mutated_cos1</i> ... <i>mutated_cos8</i>	スペースで区切った、8 つの CoS 出力値。有効値は 0 ~ 7 です。詳細については、「使用上のガイドライン」を参照してください。

コマンドモード

表 2-17 に、CoS/CoS 変換マップが設定されていない場合のデフォルトの CoS/CoS 変換マッピングを示します。

表 2-17 デフォルトの CoS/CoS マッピング

CoS 入力	0	1	2	3	4	5	6	7
CoS 出力	0	1	2	3	4	5	6	7

コマンドのデフォルト

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

次のモジュールを搭載した Catalyst 6500 シリーズスイッチだけで、このコマンドはサポートされません。

- WS-X6704-10GE
- WS-X6724-SFP
- WS-X6748-GE-TX

CoS 変換は非 802.1Q トンネルポートではサポートされません。

mls qos map cos-mutation コマンドを入力すると、変換 CoS 値は、シーケンス番号にマッピングされます。たとえば、**mls qos map cos-mutation 2 3 4 5 6 7 0 1** コマンドを入力すると、次のようなマップが設定されます。

CoS 入力	0	1	2	3	4	5	6	7
CoS 出力	2	3	4	5	6	7	0	1

8 つの CoS 値はスペースで区切ります。

マップをグローバル コンフィギュレーション モードで定義したあと、マップをポートに付加できます。

QoS がディセーブルにされていると、ポートは CoS 信頼モードおよび 802.1Q トンネリング モードになりません。ポートを CoS 信頼モードにし、ポートが 802.1Q トンネル ポートとして設定されれば、変更されます。

802.1Q トンネル ポートでの入力 CoS 変換をサポートしますが、ポート グループ単位ベースだけです。

入力 CoS 変換コンフィギュレーションを失敗しないようにするには、すべてのメンバー ポートが入力 CoS 変換をサポートする EtherChannel だけを作成するか、またはどのメンバーも入力 CoS 変換をサポートしない EtherChannel だけを作成します。入力 CoS 変換のサポートと非サポートが混在するような EtherChannel を作成しないでください。

EtherChannel のメンバーであるポートに入力 CoS 変換を設定する場合、入力 CoS 変換はポートチャンネル インターフェイスに適用されます。

入力 CoS 変換をポートチャンネル インターフェイスに設定できます。

例

次に、CoS/CoS マップを定義する例を示します。

```
Router(config)# mls qos map cos-mutation test-map 5 4 3 to 1
Router(config)#
```

関連コマンド

コマンド	説明
show mls qos maps	QoS マップ設定およびランタイム バージョンに関する情報を表示します。

mls qos map dscp-cos

出力 DSCP/CoS マップを定義するには、**mls qos map dscp-cos** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

mls qos map dscp-cos dscp-values to cos-values

no mls qos map dscp-cos

シンタックスの説明

<i>dscp-values</i>	DSCP 値。有効値は、0 ~ 63 です。
to	マッピングを定義します。
<i>cos-values</i>	CoS 値。有効値は、0 ~ 63 です。

コマンド モード

表 2-18 に、デフォルトの DSCP/CoS マップを示します。

表 2-18 デフォルトの DSCP/CoS マップ

DSCP	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
CoS	0	1	2	3	4	5	6	7

コマンドのデフォルト

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

DSCP/CoS マップは、最終 DSCP 分類を最終 CoS にマッピングする場合に使用します。この最終マップにより、パケットが割り当てられる出力キューおよびしきい値が決まります。CoS マップは、リンク インターフェイス上の送信済みパケットの ISL ヘッダーまたは 802.1Q タグに書き込まれます。CoS マップには、64 個の DSCP 値およびこれに対応する CoS 値のテーブルが含まれます。Catalyst 6500 シリーズスイッチには 1 つのマップがあります。

スペースで区切ることにより最大 8 つの DSCP 値を入力できます。スペースで区切ることにより最大 8 つの CoS 値を入力できます。

例

次に、信頼されたインターフェイスに出力 DSCP/CoS マップを設定する例を示します。

```
Router(config)# mls qos map dscp-cos 20 25 to 3
Router(config)#
```

関連コマンド

コマンド	説明
mls qos map cos-dscp	信頼されたインターフェイスに入力 CoS/DSCP マップを定義します。
show mls qos maps	QoS マップ設定およびランタイム バージョンに関する情報を表示します。

mls qos map dscp-exp

最終 DSCP 分類を最終 EXP 値に定義するには、**mls qos map dscp-exp** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

mls qos map dscp-exp dscp-values to exp-values

no mls qos map dscp-exp

シンタックスの説明

dscp-values DSCP 値。有効値は、0 ~ 63 です。

to マッピングを定義します。

exp-values EXP 値。有効値は、0 ~ 7 です。

コマンドモード

表 2-19 に、デフォルトの DSCP/EXP マップを示します。

表 2-19 デフォルトの DSCP/EXP マップ

DSCP	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
EXP	0	1	2	3	4	5	6	7

コマンドのデフォルト

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

DSCP/EXP マップは、最終 DSCP 分類を最終 EXP にマッピングする場合に使用します。この最終マップにより、パケットが割り当てられる出力キューおよびしきい値が決まります。EXP マップには、64 個の DSCP 値およびこれに対応する EXP 値のテーブルが含まれます。Catalyst 6500 シリーズスイッチには 1 つのマップがあります。

スペースで区切ることで最大 8 つの DSCP 値を入力できます。スペースで区切ることで最大 8 つの EXP 値を入力できます。

例 次に、最終 DSCP 分類を最終 EXP 値に設定する例を示します。

```
Router(config)# mls qos map dscp-exp 20 25 to 3
Router(config)#
```

関連コマンド

コマンド	説明
show mls qos maps	QoS マップ設定およびランタイムバージョンに関する情報を表示します。

mls qos map dscp-mutation

名前付き DSCP 変換マップを定義するには、**mls qos map dscp-mutation** コマンドを使用します。デフォルト マッピングに戻すには、このコマンドの **no** 形式を使用します。

```
mls qos map dscp-mutation map-name input-dscp1 [input-dscp2 [input-dscp3 [input-dscp4 [input-dscp5 [input-dscp6 [input-dscp7 [input-dscp8]]]]]]] to output-dscp
```

```
no mls qos map dscp-mutation map-name
```

シンタックスの説明

<i>map-name</i>	DSCP 変換マップ名
<i>input-dscp#</i>	内部 DSCP 値。有効値は 0～63 です。詳細については、「使用上のガイドライン」を参照してください。
to	マッピングを定義します。
<i>output-dscp</i>	出力 DSCP 値。有効値は 0～63 です。

コマンドのデフォルト

output-dscp は *input-dscp* と同じです。

コマンドモード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

名前付き DSCP 変換マップを設定する場合、次のことに注意してください。

- 変換された DSCP 値にマッピングする入力 DSCP 値を、最大 8 つ入力できます。
- コマンドを複数入力して、変換された DSCP 値にマッピングする DSCP 値を追加できます。
- 個々の変換された DSCP 値に対して、個別のコマンドを入力できます。

出力 DSCP 値として書き込まれる前に内部 DSCP 値を変換するために、15 個の出力 DSCP 変換マップを設定できます。PFC QoS が対応する任意のインターフェイスに対して、出力 DSCP 変換マップを付加できます。

PFC QoS は、内部 DSCP 値から出力 CoS 値を取得します。出力 DSCP 変換を設定した場合は、PFC QoS は変換された DSCP 値から出力 CoS 値を取得しません。

例

次に、DSCP 30 を変換された DSCP 値 8 にマッピングする例を示します。

```
Router (config) # mls qos map dscp-mutation mutemap1 30 to 8
Router (config) #
```

関連コマンド

コマンド	説明
show mls qos maps	QoS マップ設定およびランタイム バージョンに関する情報を表示します。

mls qos map exp-dscp

内部 DSCP マップに入力 EXP 値を定義するには、**mls qos map exp-dscp** コマンドを使用します。デフォルト マップに戻すには、このコマンドの **no** 形式を使用します。

mls qos map exp-dscp dscp-values

no mls qos map exp-dscp

シンタックスの説明

dscp-values 内部 DSCP 値を指定。有効値は、0 ～ 63 です。

コマンドのデフォルト

表 2-20 に、デフォルトの EXP/DSCP マップを示します。

表 2-20 デフォルトの EXP/DSCP マップ

EXP	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

これらのマップの DSCP とは、パケット DSCP ではなく内部 DSCP を意味します。

EXP/DSCP マップは、受信された EXP 値を内部 DSCP マップにマッピングする場合に使用します。この最終マップにより、パケットが割り当てられる出力キューおよびしきい値が決まります。EXP マップには、64 個の DSCP 値およびこれに対応する EXP 値のテーブルが含まれます。Catalyst 6500 シリーズ スイッチには 1 つのマップがあります。

スペースで区切ることで最大 8 つの DSCP 値を入力できます。

例

次に、受信された EXP を内部 DSCP 値に設定する例を示します。

```
Router(config)# mls qos map exp-dscp 20 25 30 31 32 32 33 34
Router(config)#
```

関連コマンド

コマンド	説明
mls qos map exp-mutation	パケットの EXP を新しい EXP 値にマッピングします。
show mls qos mpls	ポリシー マップの MPLS QoS クラスのインターフェイス概要を表示します。

mls qos map exp-mutation

パケットの EXP を新しい EXP 値にマッピングするには、**mls qos map exp-mutation** コマンドを使用します。デフォルト マップに戻すには、このコマンドの **no** 形式を使用します。

```
mls qos map exp-mutation map-name mutated-exp1 mutated-exp2 mutated-exp3
mutated-exp4 mutated-exp5 mutated-exp6 mutated-exp7 mutated-exp8
```

```
no mls qos map exp-mutation map-name
```

シンタックスの説明

<i>map-name</i>	EXP 変換マップ名
<i>mutated-exp#</i>	スペースで区切った、8 つの EXP 値。有効値は 0 ~ 7 です。詳細については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

表 2-21 に、EXP/EXP 変換マップが設定されていない場合のデフォルトの EXP/EXP 変換マッピングを示します。

表 2-21 デフォルトの EXP/EXP マップ

EXP 入力	0	1	2	3	4	5	6	7
EXP 出力	0	1	2	3	4	5	6	7

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

mls qos map exp-mutation コマンドを入力すると、変換された EXP 値は一連の EXP シーケンス番号にマッピングされます。たとえば、**mls qos map exp-mutation 2 3 4 5 6 7 0 1** コマンドを入力すると、次のようなマップが設定されます。

EXP 入力	0	1	2	3	4	5	6	7
EXP 出力	2	3	4	5	6	7	0	1

8 つの EXP 値はスペースで区切ります。

マップをグローバル コンフィギュレーション モードで定義したあと、マップをポートに付加できます。

入力 EXP 値として書き込まれる前に内部 EXP 値を変換するために、15 個の入力 EXP 変換マップを設定できます。PFC QoS が対応する任意のインターフェイスに対して、入力 EXP 変換マップを付加できます。

PFC QoS は、内部 DSCP 値から出力 EXP 値を取得します。入力 EXP 変換を設定した場合は、PFC QoS は変換された EXP 値から入力 EXP 値を取得しません。

■ mls qos map exp-mutation

例

次に、パケットの EXP を新しい EXP 値にマッピングする例を示します。

```
Router(config)# mls qos map exp-mutation mutemap1 1 2 3 4 5 6 7 0
Router(config)#
```

関連コマンド

コマンド	説明
mls qos map exp-dscp	内部 DSCP マップに入力 EXP 値を定義します。
show mls qos mpls	ポリシー マップの MPLS QoS クラスのインターフェイス概要を表示します。

mls qos map ip-prec-dscp

信頼されたインターフェイスに入力 IP precedence/DSCP マップを定義するには、**mls qos map ip-prec-dscp** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

mls qos map ip-prec-dscp *dscp-values*

no mls qos map ip-prec-dscp

シンタックスの説明 *dscp-values* IP precedence 値 0 ~ 7 に対応する DSCP 値。有効値は 0 ~ 63 です。

コマンドのデフォルト 表 2-22 に、デフォルトの IP precedence/DSCP 設定を示します。

表 2-22 デフォルトの IP precedence/DSCP マップ

IP precedence	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

コマンドのデフォルト グローバル コンフィギュレーション (config)

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドは、信頼されたインターフェイス（またはフロー）に着信した IP パケットの IP precedence を、信頼タイプが trust-ipprec である DSCP にマッピングする場合に使用します。スペースで区切るにより最大 8 つの DSCP 値を入力できます。

このマップは、8 つの優先順位値（0 ~ 7）およびこれに対応する DSCP 値のテーブルです。Catalyst 6500 シリーズスイッチには 1 つのマップがあります。IP precedence 値は次のとおりです。

- network 7
- internet 6
- critical 5
- flash-override 4
- flash 3
- immediate 2
- priority 1
- routine 0

例 次に、信頼されたインターフェイスに入力 IP precedence/DSCP マッピングを設定する例を示します。

■ mls qos map ip-prec-dscp

```
Router(config)# mls qos map ip-prec-dscp 20 30 1 43 63 12 13 8
Router(config)#
```

関連コマンド

コマンド	説明
mls qos map cos-dscp	信頼されたインターフェイスに入力 CoS/DSCP マップを定義します。
mls qos map dscp-cos	出力 DSCP/CoS マップを定義します。
mls qos map policed-dscp	ポリシング済み DSCP 値とマーキング済み DSCP 値のマップを設定します。
show mls qos maps	QoS マップ設定およびランタイム バージョンに関する情報を表示します。

mls qos map policed-dscp

DSCP マークダウン マップを設定するには、**mls qos map policed-dscp** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

```
mls qos map policed-dscp {normal-burst | max-burst} dscp1 [dscp2 [dscp3 [dscp4 [dscp5
[dscp6 [dscp7 [dscp8]]]]]]] to policed-dscp
```

```
no mls qos map policed-dscp
```

シンタックスの説明	normal-burst	exceed-action policed-dscp-transmit	キーワードによって使用されるマークダウン マップを設定します。
	max-burst	violate-action policed-dscp-transmit	キーワードによって使用されるマークダウン マップを設定します。
	dscp1	DSCP 値。有効値は、0 ~ 63 です。	
	dscp2 ~ dscp8	(任意) DSCP 値。有効値は、0 ~ 63 です。	
	to	マッピングを定義します。	
	policed-dscp	ポリシング済み DSCP 値を指定します。有効値は、0 ~ 63 です。	

コマンドのデフォルト マーキング済みの値は設定されていません。

コマンド モード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン DSCP/ポリシング済み DSCP マップにより、不適合なフローに適用されるマーキング済み DSCP 値が決定します。Catalyst 6500 シリーズ スイッチには 1 つのマップがあります。

スペースで区切るにより最大 8 つの DSCP 値を入力できます。

スペースで区切るにより最大 8 つのポリシング済み DSCP 値を入力できます。



(注) シーケンス外パケットを避けるため、DSCP/ポリシング済み DSCP マップを設定して、マーキング済みパケットが適合トラフィックと同じキューに留まるようにします。

例 次に、複数の DSCP を単一のポリシング済み DSCP 値にマッピングする例を示します。

```
Router (config)# mls qos map policed-dscp normal-burst 20 25 43 to 4
Router (config)#
```

関連コマンド

コマンド	説明
mls qos map cos-dscp	信頼されたインターフェイスに入力 CoS/DSCP マップを定義します。
mls qos map dscp-cos	出力 DSCP/CoS マップを定義します。
mls qos map ip-prec-dscp	信頼されたインターフェイスに入力 IP precedence/DSCP マップを定義します。
show mls qos	MLS QoS 情報を表示します。

mls qos marking ignore port-trust

インターフェイスが信頼されていてもパケットをマークするには、**mls qos marking ignore port-trust** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos marking ignore port-trust

no mls qos marking ignore port-trust

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト ポート信頼はイネーブルです。

コマンドのデフォルト グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン インターフェイスが信頼されていてもパケットをマークするには、**mls qos marking ignore port-trust** コマンドを使用します。

例 次に、インターフェイスが信頼されていてもパケットをマークする例を示します。

```
Router(config)# mls qos marking ignore port-trust  
Router(config)#
```

次に、ポート信頼をイネーブルにする例を示します。

```
Router(config)# no mls qos marking ignore port-trust  
Router(config)#
```

関連コマンド [mls qos trust](#)

mls qos marking statistics

ポリサー トラフィック クラス ID の設定済みアクションへの割り当てをディセーブルにするには、**mls qos marking statistics** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos marking statistics

no mls qos marking statistics

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

イネーブル

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ポリシー マップ統計情報を表示するには、**show policy-map interface** コマンドを使用します。

例

次に、ポリサー トラフィック クラス ID の設定済みアクションへの割り当てをディセーブルにする例を示します。

```
Router(config)# mls qos marking statistics
Router(config)#
```

次に、ポリサー トラフィック クラス ID の設定済みアクションへの割り当てを許可する例を示します。

```
Router(config)# no mls qos marking statistics
Router(config)#
```

関連コマンド

コマンド	説明
show policy-map interface	インターフェイスに対応付けられた入力および出力ポリシーの統計情報およびコンフィギュレーションを表示します。

mls qos mpls trust exp

MPLS パケットだけの信頼状態を設定するには、**mls qos mpls trust exp** コマンドを使用します。MPLS パケットの信頼状態を信頼不可に設定するには、このコマンドの **no** 形式を使用します。

mls qos mpls trust exp

no qos mpls trust exp

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト 信頼状態がイネーブルである場合、デフォルトは次のとおりです。

- 信頼不可：パケットは 0 に、またはポリシーによってマークされます。
- trust-cos

信頼状態がディセーブルである場合、デフォルトは次のとおりです。

- trust-exp：ポート/ポリシー信頼状態は無視されます。
- パケットはポリシーによってマークされます。

コマンド モード インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

CoS および出力キューイングのため（たとえば、ポートまたはポリシーの信頼を適用）、MPLS パケットを別のレイヤ 2 パケットとして扱うには、**mls qos mpls trust exp** コマンドを入力できます。すべて信頼される場合（CoS/IP/DSCP を信頼）は、trust-cos として扱われます。

例

次に、MPLS パケットの信頼状態を trust-cos に設定する例を示します。

```
Router(config-if)# mls qos mpls trust exp
Router(config-if)#
```

次に、MPLS パケットの信頼状態を信頼不可に設定する例を示します。

```
Router(config-if)# no mls qos mpls trust exp
Router(config-if)#
```

関連コマンド

コマンド	説明
show mls qos mpls	ポリシー マップの MPLS QoS クラスのインターフェイス概要を表示します。

mls qos police redirected

ACL リダイレクト パケットのポリシングをオンにするには、**mls qos police redirected** コマンドを使用します。ACL リダイレクト パケットのポリシングをオフに切り替えるには、このコマンドの **no** 形式を使用します。

mls qos police redirected

no mls qos police redirected

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

イネーブル

コマンドのデフォルト

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

(QoS リダイレクト パケットを必要としない代わりに) NDE の精度を必要とする場合、**no mls qos police redirected** コマンドを使用します。

例

次に、ACL リダイレクト パケットのポリシングをオンにする例を示します。

```
Router(config)# mls qos police redirected
Router(config)#
```

次に、ACL リダイレクト パケットのポリシングをオフにする例を示します。

```
Router(config)# no mls qos police redirected
Router(config)#
```

関連コマンド

コマンド	説明
show platform earl-mode	プラットフォーム情報を表示します。

mls qos protocol

ルーティング プロトコル パケットのポリシングを定義するには、**mls qos protocol** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
mls qos protocol protocol-name {pass-through | {police rate burst} | {precedence value
[police rate burst]}}
```

```
no mls qos protocol
```

シンタックスの説明	
<i>protocol-name</i>	プロトコル名。有効値は、 arp 、 bgp 、 eigrp 、 igrp 、 isis 、 ldp 、 nd 、 ospf 、および rip です。
pass-through	パススルー モードを指定します。
police rate	ポリシングする最大のビット/秒 (bps) を指定します。有効値は、32,000 ~ 10,000,000,000 bps です。
<i>burst</i>	標準バースト バイト。有効値は 1000 ~ 31,250,000 バイトです。
precedence value	プロトコル パケットの書き換え後の IP precedence 値を指定します。有効値は、0 ~ 7 です。

コマンド モード

デフォルト設定は次のとおりです。

- *burst* は、1000 bps です。
- QoS がイネーブルの場合、DSCP は 0 に書き換えられます。
- QoS がディセーブルの場合、ポートはパススルー モード (マーキングまたはポリシングなし) になります。

コマンドのデフォルト

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

precedence value キーワードおよび引数を **police rate burst** キーワードおよび引数なしで入力すると、信頼できないポートからのパケットだけがマーキングされます。

police rate、**pass-through**、または **precedence value** キーワードおよび引数を入力すると、プロトコル パケットがインターフェイス単位のポリシー マップを回避するようにできます。

mls qos protocol コマンドにより、次のようにルーティング プロトコル パケット ポリシングを定義できます。

- **pass-through** モードを指定すると、DSCP 値は変更せず、ポリシングされません。
- **police rate** を設定すると、DSCP 値は変更せず、ポリシングされます。
- **precedence value** を指定すると、信頼できないポートからのパケットの DSCP 値は変更し、DSCP/CoS マップに基づく CoS 値は変更し、トラフィックはポリシングされません。

- **precedence value** および **police rate** を指定すると、DSCP 値は変更し、DSCP/CoS マップに基づく CoS 値は変更し、DSCP 値はポリシングされます。この場合、DSCP 値の変更は、ポートの信頼状態に基づきます。DSCP 値が変更されるのは、信頼できないポートからのパケットに対してだけです。
- **precedence value** を入力しない場合、DSCP 値は MLS QoS がイネーブルであるかどうかに基づきます。詳細は、次のとおりです。
 - MLS QoS がイネーブルでポートが信頼できない場合、内部 DSCP 値は 0 に書き込まれます。
 - MLS QoS がイネーブルでポートが信頼できる場合、着信 DSCP 値は維持されます。

パススルー モードを選択した場合、プロトコル パケットが完全にポリシングを避けるようにできます。ポリス モードが選択された場合、指定された CIR がすべての指定プロトコルのパケット (Catalyst 6500 シリーズ スイッチに着信または発信の両方) をポリシングするのに使用されるレートになります。

ARP ブロードキャストからシステムを保護するには、**mls qos protocol arp police bps** コマンドを入力します。

例

次に、ルーティング プロトコル パケットのポリシングを定義する例を示します。

```
Router(config)# mls qos protocol arp police 43000  
Router(config)#
```

次に、ポリシングを完全に避けるようにする例を示します。

```
Router(config)# mls qos protocol arp pass-through 43000  
Router(config)#
```

次に、プロトコル パケットの書き換え後の IP precedence 値を定義する例を示します。

```
Router(config)# mls qos protocol bgp precedence 4  
Router(config)#
```

次に、プロトコル パケットの書き換え後の IP-precedence 値を定義し、DSCP 値をポリシングする例を示します。

```
Router(config)# mls qos protocol bgp precedence 4 police 32000
Router(config)#
```

関連コマンド

コマンド	説明
show mls qos protocol	プロトコル パススルー情報を表示します。

mls qos queueing-only

ポートキューイング モードをイネーブルにするには、**mls qos queueing-only** コマンドを使用します。ポートキューイング モードをディセーブルにするには、このコマンドの **no** 形式を使用します。

mls qos queueing-only

no mls qos queueing-only

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

QoS はグローバルにディセーブルです。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ポートキューイング モードでは、PFC QoS (マーキングおよびポリシング) はディセーブルであり、パケットの ToS および CoS は PFC で変更されません。受信および送信に関するすべてのキューイングは、着信パケットの QoS タグに基づいて行われます。この QoS タグは、着信 CoS に基づきます。

802.1Q または ISL カプセル化ポート リンクでは、キューイングはパケット 802.1Q または ISL CoS に基づいて行われます。

ルータのメイン インターフェイスまたはアクセス ポートでは、キューイングは設定されたポート単位の CoS (デフォルト CoS は 0) に基づいて行われます。

例

次に、ポートキューイング モードをグローバルにイネーブルにする例を示します。

```
Router(config)# mls qos queueing-only
Router(config)#
```

次に、ポートキューイング モードをグローバルにディセーブルにする例を示します。

```
Router(config)# no mls qos queueing-only
Router(config)#
```

関連コマンド

コマンド	説明
mls qos (global configuration mode)	QoS 機能をグローバルにイネーブルにします。
show mls qos	MLS QoS 情報を表示します。

mls qos queue-mode mode-dscp

インターフェイスでキューイング モードを DSCP に設定するには、**mls qos queue-mode mode-dscp** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos queue-mode mode-dscp

no mls qos queue-mode mode-dscp

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト CoS モード

コマンド モード インターフェイス コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドは、10 ギガビット イーサネット ポートだけでサポートされます。

有効なレイヤ 3 DSCP を運ぶトラフィックを受信する場合にだけ DSCP を信頼するようにポートを設定する必要があります。

DSCP ベースの入力キューおよびしきい値を WS-X6708-10GE ポートでイネーブルにして、輻輳を回避できます。

信頼された DSCP ポートからのトラフィックの場合、PFC QoS は、受信した DSCP 値を初期内部 DSCP 値として使用します。PFC QoS は、受信 DSCP を信頼するように設定された入力ポートのトラフィックをマークしません。

例 次の例は、インターフェイスでキューイング モードを DSCP に設定する方法を示しています。

```
Router(config-if)# mls qos queue-mode mode-dscp
Router(config-if)#
```

関連コマンド	コマンド	説明
	priority-queue queue-limit	使用可能バッファ スペースをキューに割り当てます。
	show mls qos	MLS QoS 情報を表示します。

mls qos rewrite ip dscp

ToS から DSCP への書き換えをイネーブルにするには、**mls qos rewrite ip dscp** コマンドを使用します。ToS から DSCP への書き換えをディセーブルにするには、このコマンドの **no** 形式を使用します。

mls qos rewrite ip dscp

no mls qos rewrite ip dscp

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

QoS はグローバルにディセーブルです。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ToS から DSCP への書き換えをディセーブルにして、QoS をグローバルにイネーブルした場合、次のようになります。

- 最終 ToS から DSCP への書き換えがディセーブルになり、ToS から DSCP へのパケットはそのまま保持されます。
- ポリシングおよびマーキングは、QoS 設定に従って動作します。
- キューイングにはマーキングされた CoS が使用されます。
- QoS ディセーブル モードでは、ToS および CoS はそのまま保持されます。

no mls qos rewrite ip dscp コマンドは、MPLS との互換性がありません。デフォルトの **mls qos rewrite ip dscp** コマンドは、PFC3BXL または PFC3B が賦課するラベルの正しい EXP 値を割り当てるように、イネーブルのままにする必要があります。

例

次に、ToS から DSCP への書き換えをディセーブルにする例を示します。

```
Router(config)# mls qos rewrite ip dscp
Router(config)#
```

次に、ポートキューイング モードをグローバルにディセーブルにする例を示します。

```
Router(config)# no mls qos rewrite ip dscp
Router(config)#
```

関連コマンド

コマンド	説明
mls qos (global configuration mode)	QoS 機能をグローバルにイネーブルにします。
show mls qos	MLS QoS 情報を表示します。

mls qos statistics-export (global configuration mode)

QoS 統計データのエクスポートをグローバルにイネーブルにするには、**mls qos statistics-export** コマンドを使用します。QoS 統計データのエクスポートをグローバルにディセーブルにするには、このコマンドの **no** 形式を使用します。

mls qos statistics-export

no mls qos statistics-export

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

ディセーブル

コマンドのデフォルト

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

Catalyst 6500 シリーズ スイッチにデータ エクスポートを設定するには、データ エクスポートをグローバルにイネーブルにする必要があります。

QoS 統計データのエクスポートは、OSM インターフェイスではサポートされていません。

QoS 統計データのエクスポートを正常に実行するには、エクスポートの宛先ホスト名または IP アドレス、および UDP ポート番号を設定する必要があります。

例

次に、データ エクスポートをグローバルにイネーブルにする例を示します。

```
Router(config)# mls qos statistics-export
Router(config)#
```

次に、データ エクスポートをグローバルにディセーブルにする例を示します。

```
Router(config)# no mls qos statistics-export
Router(config)#
```

関連コマンド

コマンド	説明
show mls qos statistics-export info	MLS 統計データ エクスポート ステータスおよび設定に関する情報を表示します。

mls qos statistics-export (interface configuration mode)

ポート単位の QoS 統計データのエクスポートをイネーブルにするには、**mls qos statistics-export** コマンドを使用します。ポート単位の QoS 統計データのエクスポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

mls qos statistics-export

no mls qos statistics-export

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンド モード ディセーブル

コマンドのデフォルト インターフェイス コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン QoS 統計データのエクスポートは、OSM インターフェイスではサポートされていません。Catalyst 6500 シリーズスイッチにデータ エクスポートを設定するには、ポートで、グローバルにデータ エクスポートをイネーブルにする必要があります。

QoS 統計データのエクスポートを正常に実行するには、エクスポートの宛先ホスト名または IP アドレス、および UDP ポート番号を設定する必要があります。

QoS 統計データは、デリミタ区切りフィールドを使用してエクスポートされます。デリミタを設定するには、**mls qos statistics-export delimiter** コマンドを使用します。

ポートの統計情報はエクスポートされますが、ポートの QoS 統計情報はエクスポートされません。データ エクスポートがイネーブルであるポートでは、次の情報がエクスポートされます。

- タイプ (1 はポート タイプを意味します)
- モジュール/ポート
- 着信パケット数 (ハードウェアの累積カウンタ値)
- 着信バイト数 (ハードウェアの累積カウンタ値)
- 発信パケット数 (ハードウェアの累積カウンタ値)
- 発信バイト数 (ハードウェアの累積カウンタ値)
- タイム スタンプ (1970 年 1 月 1 日 Coordinated Universal Time (UTC; 協定世界時) を起点とする秒数)

たとえば、FastEthernet4/5 で QoS 統計データのエクスポートがイネーブルの場合、エクスポートされたレコードは次のようになります (この例では、デリミタは | (パイプ))。

■ mls qos statistics-export (interface configuration mode)

```
|1|4/5|123|80|12500|6800|982361894|
```

例

次に、QoS 統計データ エクスポートをイネーブルにする例を示します。

```
Router(config-if)# mls qos statistics-export
Router(config-if)#
```

次に、QoS 統計データ エクスポートをディセーブルにする例を示します。

```
Router(config-if)# no mls qos statistics-export
Router(config-if)#
```

関連コマンド

コマンド	説明
mls qos statistics-export delimiter	QoS 統計データのエクスポート フィールドのデリミタを設定します。
show mls qos statistics-export info	MLS 統計データ エクスポート ステータスおよび設定に関する情報を表示します。

mls qos statistics-export aggregate-policer

名前付き集約ポリサー上で QoS 統計データのエクスポートをイネーブルにするには、**mls qos statistics-export aggregate-policer** コマンドを使用します。名前付き集約ポリサー上で QoS 統計データのエクスポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

mls qos statistics-export aggregate-policer policer-name

no mls qos statistics-export aggregate-policer policer-name

シンタックスの説明	<i>policer-name</i> ポリサー名
-----------	---------------------------

コマンド モード	共有集約ポリサーの場合はすべてディセーブル
----------	-----------------------

コマンドのデフォルト	グローバル コンフィギュレーション (config)
------------	----------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

QoS 統計データのエクスポートは、OSM インターフェイスではサポートされていません。

Catalyst 6500 シリーズスイッチにデータ エクスポートを設定するには、共有集約ポリサーで、グローバルにデータ エクスポートをイネーブルにする必要があります。

QoS 統計データは、デリミタ区切りフィールドを使用してエクスポートされます。デリミタを設定するには、**mls qos statistics-export delimiter** コマンドを使用します。

データ エクスポートがイネーブルである共有集約ポリサーまたは名前付きポリサーごとに、統計データがポリサー単位、および EARL 単位でエクスポートされます。データ エクスポートがイネーブルである共有集約ポリサーまたは名前付きポリサーでは、次の情報がエクスポートされます。

- タイプ (3 は集約ポリサーのエクスポート タイプを意味します)
- 集約名
- 方向 (着信または発信)
- EARL 識別情報
- 受け入れパケット数 (ハードウェアの累積カウンタ値)
- 拒否標準レート パケット数 (ハードウェアの累積カウンタ値)
- 拒否超過レート パケット数 (ハードウェアの累積カウンタ値)
- タイム スタンプ (1970 年 1 月 1 日 UTC を起点とする秒数)

共有集約ポリサーがポリシーの両方の方向に付加されている場合、2 つのレコードがエクスポートされます (各方向に 1 つずつ)。各レコードには、受け入れパケット、拒否標準レート パケット、および拒否超過レート パケットに関する同じカウンタ値が格納されます。

たとえばエクスポート レコードは次のようになります (この例では、デリミタは | (パイプ))。

■ **mls qos statistics-export aggregate-policer**

```
|3|agg_1|in|1|45543|2345|982361894|
|3|agg_1|in|3|45543|2345|982361894|
```

上記の例は、以下の情報を示しています。

- 共有集約ポリサー「agg_1」上で QoS 統計データのエクスポートがイネーブル
- スロット 1 に装着されたスーパーバイザ エンジンに EARL が搭載
- スロット 3 に EARL が搭載

例

次に、共有集約ポリサー単位、または名前付きポリサー単位でデータ エクスポートをイネーブルにする例を示します。

```
Router(config)# mls qos statistics-export aggregate-policer aggr1M
Router(config)#
```

関連コマンド

コマンド	説明
mls qos statistics-export delimiter	QoS 統計データのエクスポート フィールドのデリミタを設定します。
show mls qos statistics-export info	MLS 統計データ エクスポート ステータスおよび設定に関する情報を表示します。

mls qos statistics-export class-map

クラス マップの QoS 統計データ エクスポートをイネーブルにするには、**mls qos statistics-export class-map** コマンドを使用します。QoS 統計データのエクスポートをクラス マップでディセーブルにするには、このコマンドの **no** 形式を使用します。

mls qos statistics-export class-map *classmap-name*

no mls qos statistics-export class-map *classmap-name*

シンタックスの説明

classmap-name クラス マップ名

コマンドのデフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

QoS 統計データのエクスポートは、OSM インターフェイスではサポートされていません。

Catalyst 6500 シリーズスイッチにデータ エクスポートを設定するには、クラス マップで、グローバルにデータ エクスポートをイネーブルにする必要があります。

QoS 統計データは、デリミタ区切りフィールドを使用してエクスポートされます。デリミタを設定するには、**mls qos statistics-export delimiter** コマンドを使用します。

データ エクスポートがイネーブルであるクラス マップごとに、統計データがポリサー単位、およびインターフェイス単位でエクスポートされます。インターフェイスが物理インターフェイスの場合、次の情報がエクスポートされます。

- タイプ (4 はクラス マップ物理エクスポートを意味します)
- クラスマップ名
- 方向 (着信または発信)
- モジュール/ポート
- 受け入れパケット数 (ハードウェアの累積カウンタ値)
- 拒否標準レート パケット数 (ハードウェアの累積カウンタ値)
- 拒否超過レート パケット数 (ハードウェアの累積カウンタ値)
- タイム スタンプ (1970 年 1 月 1 日 UTC を起点とする秒数)

インターフェイスが Catalyst 6500 シリーズスイッチ VLAN である場合は、次の情報がエクスポートされます。

- タイプ (5 はクラス マップ VLAN エクスポートを意味します)
- クラスマップ名

- 方向 (着信または発信)
- EARL 識別情報 (EARL が搭載されたスロット番号)
- VLAN 番号
- 受け入れパケット数 (ハードウェアの累積カウンタ値)
- 拒否標準レート パケット数 (ハードウェアの累積カウンタ値)
- 拒否超過レート パケット数 (ハードウェアの累積カウンタ値)
- タイム スタンプ (1970 年 1 月 1 日 UTC を起点とする秒数)

インターフェイスが Catalyst 6500 シリーズ スイッチ ポート チャネルである場合は、次の情報がエクスポートされます。

- タイプ (6 はクラス マップ ポート チャネル エクスポートを意味します)
- クラスマップ名
- 方向 (着信または発信)
- EARL 識別情報 (EARL が搭載されたスロット番号)
- ポート チャネル番号
- 受け入れパケット数 (ハードウェアの累積カウンタ値)
- 拒否標準レート パケット数 (ハードウェアの累積カウンタ値)
- 拒否超過レート パケット数 (ハードウェアの累積カウンタ値)
- タイム スタンプ (1970 年 1 月 1 日 UTC を起点とする秒数)

たとえば、次のように設定されているとします。

- クラス マップ「class_1」上で QoS 統計データ エクスポートがイネーブル
- スロット 1 に装着されたスーパーバイザ エンジンに EARL が搭載
- スロット 3 に EARL が搭載
- Catalyst 6500 シリーズ スイッチは、「policy_1」というポリシー マップ内に存在
- policy_1 は、次のインターフェイスの入力方向に付加
 - FastEthernet4/5
 - VLAN 100
 - ポート チャネル 24

エクスポートされたレコードは、次のようになります (この例では、デリミタは | (パイプ))。

```
|4|class_1|in|4/5|45543|2345|2345|982361894| |
|5|class_1|in|1|100|44000|3554|36678|982361894|
|5|class_1|in|3|100|30234|1575|1575|982361894|
```

例 次に、クラス マップの QoS 統計データ エクスポートをイネーブルにする例を示します。

```
Router(config)# mls qos statistics-export class-map class3  
Router(config)#
```

関連コマンド

コマンド	説明
mls qos statistics-export delimiter	QoS 統計データのエクスポート フィールドのデリミタを設定します。
show mls qos statistics-export info	MLS 統計データ エクスポート ステータスおよび設定に関する情報を表示します。

mls qos statistics-export delimiter

QoS 統計データ エクスポート フィールドのデリミタを設定するには、**mls qos statistics-export delimiter** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos statistics-export delimiter

no mls qos statistics-export delimiter

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

デフォルトのデリミタはパイプ記号 (|) です。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

QoS 統計データのエクスポートは、OSM インターフェイスではサポートされていません。

Catalyst 6500 シリーズ スイッチにデータ エクスポートを設定するには、データ エクスポートをグローバルにイネーブルにする必要があります。

例

次に、QoS 統計データ エクスポート フィールドのデリミタ (カンマ) を設定し、設定を確認する例を示します。

```
Router(config)# mls qos statistics-export delimiter ,  
Router(config)#
```

関連コマンド

コマンド	説明
show mls qos statistics-export info	MLS 統計データ エクスポート ステータスおよび設定に関する情報を表示します。

mls qos statistics-export destination

QoS 統計データ エクスポートの宛先ホストおよび UDP ポート番号を設定するには、**mls qos statistics-export destination** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos statistics-export destination {*host-name* | *host-ip-address*} [{**port** *port-number*] | **syslog**] [**facility** *facility-name*] [**severity** *severity-value*]

シンタックスの説明

<i>host-name</i>	ホスト名
<i>host-ip-address</i>	ホストの IP アドレス
port <i>port-number</i>	UDP ポート番号を指定します。
syslog	Syslog ポートを指定します。
facility <i>facility-name</i>	(任意) エクスポートするファシリティタイプを指定します。有効値については「使用上のガイドライン」を参照してください。
severity <i>severity-value</i>	(任意) エクスポートする重大度を指定します。有効値については「使用上のガイドライン」を参照してください。

コマンドのデフォルト

syslog を指定しないかぎり、デフォルトでは何も設定されません。**syslog** を指定した場合、デフォルトは次のとおりです。

- *port* は **514** です。
- *facility* は **local6** です。
- *severity* は **debug** です。

コマンドモード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

QoS 統計データのエクスポートは、OSM インターフェイスではサポートされていません。有効な *facility* 値は次のとおりです。

- **authorization** : セキュリティ / 認証メッセージ
- **cron** : クロック デーモン
- **daemon** : システム デーモン
- **kernel** : カーネル メッセージ
- **local0** : ローカル使用 0
- **local1** : ローカル使用 1
- **local2** : ローカル使用 2

■ `mls qos statistics-export destination`

- **local3** : ローカル使用 3
- **local4** : ローカル使用 4
- **local5** : ローカル使用 5
- **local6** : ローカル使用 6
- **local7** : ローカル使用 7
- **lpr** : ライン プリンタ サブシステム
- **mail** : メール システム
- **news** : ネットワーク ニュース サブシステム
- **syslog** : syslogd により内部で生成されるメッセージ
- **user** : ユーザレベル メッセージ
- **uucp** : UUCP サブシステム

有効な *severity* レベルは次のとおりです。

- **alert** : ただちに対処が必要
- **critical** : クリティカルな状況
- **debug** : デバッグレベル メッセージ
- **emergency** : システムが使用不可
- **error** : エラー
- **informational** : 情報提供
- **notice** : 正常だが特異な状況
- **warning** : 警告

例

次に、宛先ホスト アドレス、および UDP ポート番号として Syslog を指定する例を示します。

```
Router(config)# mls qos statistics-export destination 172.20.52.3 syslog
Router(config)#
```

関連コマンド

コマンド	説明
show mls qos statistics-export info	MLS 統計データ エクスポート ステータスおよび設定に関する情報を表示します。

mls qos statistics-export interval

ポートまたは集約ポリサー QoS 統計データの読み込み頻度およびエクスポート頻度を指定するには、**mls qos statistics-export interval** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos statistics-export interval *interval*

no mls qos statistics-export interval

シンタックスの説明 *interval* エクスポート時間。有効値は 30 ~ 65,535 秒です。

コマンドのデフォルト 300 秒

コマンド モード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン QoS 統計データのエクスポートは、OSM インターフェイスではサポートされていません。
interval は、設定内のアクティビティによるカウンタ ラップアラウンドを防止できるように、十分短い値を設定する必要があります。



注意

QoS 統計をエクスポートすると、Catalyst 6500 シリーズスイッチでトラフィックが増加するので、インターバルを短縮する場合は注意してください。

例 次に、QoS 統計データ エクスポートのインターバルを設定する例を示します。

```
Router (config) # mls qos statistics-export interval 250
Router (config) #
```

関連コマンド	コマンド	説明
	show mls qos statistics-export info	MLS 統計データ エクスポート ステータスおよび設定に関する情報を表示します。

mls qos trust

インターフェイスの信頼状態を設定するには、**mls qos trust** コマンドを使用します。インターフェイスを信頼しない状態に設定するには、このコマンドの **no** 形式を使用します。

mls qos trust [cos | dscp | ip-precedence]

no mls qos trust

シンタックスの説明

cos	(任意) 着信フレームの CoS ビットを信頼し、CoS ビットから内部 DSCP 値を取得することを指定します。
dscp	(任意) 着信パケットの ToS ビットに DSCP 値が含まれることを指定します。
ip-precedence	(任意) 着信パケットの ToS ビットに IP precedence 値が含まれていて、IP precedence ビットから内部 DSCP 値を取得することを指定します。

コマンドのデフォルト

OSM 上の LAN インターフェイスおよび WAN インターフェイスのデフォルトは、次のとおりです。

- グローバル QoS がイネーブルの場合、ポートは信頼できない状態です。
- グローバル QoS がディセーブルの場合、デフォルトは **dscp** です。
- 引数を入力しない場合は、**trust dscp** が使用されます。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

mls qos trust コマンドを使用して、インターフェイスの信頼状態を設定できます。たとえば、特定のインターフェイスに着信するパケットの CoS、ToS、および DSCP の分類が正しいものであると信頼するかどうかを設定できます。

cos キーワードは、**pos** または **atm** インターフェイス タイプではサポートされません。

FlexWAN モジュールに信頼状態を設定できません。

ギガビット イーサネット ポートを除く 1q4t LAN ポートには、信頼状態を設定できません。

4 ポートギガビット イーサネット WAN モジュールに **mls qos trust cos** コマンドを入力した場合、入力キュー廃棄しきい値は実装されません。

レイヤ 2 WAN インターフェイスの信頼状態を設定するには、**set qos-group** コマンドを使用します。

例

次に、インターフェイスの信頼状態を IP precedence に設定する例を示します。

```
Router(config-if)# mls qos trust ip-precedence
Router(config-if)#
```

関連コマンド

コマンド	説明
mls qos bridged	レイヤ 3 LAN インターフェイスのブリッジドトラフィックにマイクロフロー ポリシングをイネーブルにします。
mls qos cos	インターフェイスのデフォルト CoS 値を定義します。
mls qos vlan-based	VLAN のデフォルト CoS 値を定義します。
show queueing interface	キューイング情報を表示します。

mls qos trust extend

電話の信頼モードを設定するには、**mls qos trust extend** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos trust extend [cos value]

no mls qos trust extend

シンタックスの説明

cos value	(任意) PC からのパケットに設定するために使用される CoS 値を指定します。有効値は 0 ~ 7 です。
------------------	---

コマンドのデフォルト

デフォルト設定は次のとおりです。

- モードは **untrusted** です。
- **cos value** は 0 です。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、WAN モジュールではサポートされません。

電話が信頼モードに設定されている場合、PC から着信したすべてのパケットはそのまま電話を経由して Catalyst 6500 シリーズ スイッチに直接送信されます。電話が非信頼モードに設定されている場合、PC から着信したすべてのトラフィックは、所定の CoS 値に設定されてから、Catalyst 6500 シリーズ スイッチに送信されます。

mls qos trust extend コマンドを入力するたびに、モードが変わります。たとえば、モードが信頼に設定されている場合にコマンドを入力すると、モードは非信頼に変わります。現在設定されている信頼モードを表示するには、**show queuing interface** コマンドを入力します。

例

次に、スイッチ ポートに接続された電話を信頼モードで設定する例を示します。

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# mls qos trust extend
Router(config-if)#
```

次に、モードを非信頼に変更して、CoS 値を 3 に設定する例を示します。

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# mls qos trust extend cos 3
Router(config-if)#
```

次に、設定をデフォルト モードに設定する例を示します。

```
Router(config-if)# interface fastethernet5/1  
Router(config-if)# no mls qos trust extend  
Router(config-if)#
```

関連コマンド

コマンド	説明
show queueing interface	キューイング情報を表示します。

mls qos vlan-based

レイヤ 2 インターフェイスの VLAN 単位の QoS をイネーブルにするには、**mls qos vlan-based** コマンドを使用します。レイヤ 2 インターフェイスの VLAN 単位の QoS をディセーブルにするには、このコマンドの **no** 形式を使用します。

mls qos vlan-based

no mls qos vlan-based

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、スイッチポートおよびポートチャネル インターフェイスだけでサポートされます。VLAN ベース モードでは、レイヤ 2 インターフェイスに対応付けられたポリシー マップは無視され、QoS は対応する VLAN インターフェイスに対応付けられたポリシー マップによって実行されます。VLAN 単位の QoS は、レイヤ 2 インターフェイス上だけで設定できます。



(注)

レイヤ 3 インターフェイスは常にインターフェイスベース モードです。レイヤ 3 VLAN インターフェイスは常に VLAN ベース モードです。

例

次に、レイヤ 2 インターフェイスの VLAN 単位の QoS をイネーブルにする例を示します。

```
Router(config-if)# mls qos vlan-based
Router(config-if)#
```

関連コマンド

コマンド	説明
mls qos bridged	レイヤ 3 LAN インターフェイスのブリッジド トラフィックにマイクロフロー ポリシングをイネーブルにします。
mls qos cos	インターフェイスのデフォルト CoS 値を定義します。
show queuing interface	キューイング情報を表示します。

mls rate-limit all

ユニキャスト パケットとマルチキャスト パケットに共通のレート リミッタのイネーブル化および設定を行うには、**mls rate-limit all** コマンドを使用します。レート リミッタをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
mls rate-limit all {mtu-failure | ttl-failure} pps [packets-in-burst]
```

```
no mls rate-limit all {mtu-failure | ttl-failure}
```

シンタックスの説明

all	ユニキャストおよびマルチキャスト パケットのレート制限を指定します。
mtu-failure	MTU 障害パケットに対するレート リミッタのイネーブル化および設定を行います。
ttl-failure	TTL 障害パケットに対するレート リミッタのイネーブル化および設定を行います。
<i>pps</i>	パケット/秒。有効値は 10 ~ 1,000,000 パケット/秒です。
<i>packets-in-burst</i>	(任意) バースト状態のパケット。有効値は 1 ~ 255 です。

コマンドのデフォルト

デフォルトでは、レイヤ 2 レート リミッタはオフです。レート リミッタのイネーブル化および設定を行う場合、*packets-in-burst* は、デフォルトで **10** になります。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

レート リミッタ機能は、ハードウェアのデータ パスからソフトウェアのデータ パスにパントされたパケットをレート制限できます。レート リミッタ機能は、設定したレートを超えるトラフィックを廃棄することにより、ソフトウェアの制御パスが輻輳しないようにします。

例

次に、ユニキャストおよびマルチキャスト パケットに対する TTL 障害リミッタ機能を設定する例を示します。

```
Router(config)# mls rate-limit all ttl-failure 15
Router(config)#
```

関連コマンド

コマンド	説明
show mls rate-limit	MLS レート リミッタに関する情報を表示します。

mls rate-limit layer2

レイヤ 2 の制御パケットのイネーブル化およびレート制限を行うには、**mls rate-limit layer2** コマンドを使用します。ハードウェアでレートリミッタをディセーブルにするには、このコマンドの **no** 形式を使用します。

mls rate-limit layer2 {pdu | l2pt | port-security} pps [*packets-in-burst*]

no mls rate-limit layer2 [pdu | l2pt | port-security]

シンタックスの説明

pdu pps	BPDU、CDP、PDU、および VTP PDU のレイヤ 2 制御パケットのレート制限を指定します。有効値は、10 ~ 1,000,000 パケット/秒です。
l2pt pps	レイヤ 2 プロトコル トンネリングのマルチキャスト MAC アドレスを使用して、レイヤ 2 制御パケットのレート制限を指定します。有効値は、10 ~ 1,000,000 パケット/秒です。
port-security pps	ポートセキュリティトラフィックのレート制限を指定します。有効値は 10 ~ 1,000,000 パケット/秒です。
packets-in-burst	(任意) バースト状態のパケット。有効値は 1 ~ 255 です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- デフォルトでは、レイヤ 2 レートリミッタはオフです。
- レートリミッタのイネーブル化および設定を行う場合、*packets-in-burst* のデフォルト設定は **10** であり、*pps* にはデフォルト設定がありません。

コマンドモード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

グローバル スイッチング モードが **truncated** モードに設定されている場合は、レイヤ 2 レートリミッタを設定できません。

port-security pps キーワードおよび引数については、次の注意事項に従ってください。

- PFC2 ではポートセキュリティ レートリミッタがサポートされません。
- truncated** スイッチング モードでは、ポートセキュリティ レートリミッタがサポートされません。
- 値を下げると、CPU はより効果的に保護されます。

レートリミッタは、次のようにパケットを制限します。

- フレームは、宛先 MAC アドレスによってレイヤ 2 制御フレームとして分類されます。宛先 MAC アドレスは、次のように使用されます。
 - IEEE BPDU には、0180.C200.0000
 - CDP には、0100.0CCC.CCCC

– PVST/SSTP BPDU には、0100.0CCC.CCCD

- ソフトウェアは、フレームに Local Target Logic (LTL) インデックスを割り当てます。
- LTL インデックスは、すべての関連付けられたフレームの集約レート制限のために転送エンジンへ送られます。

レイヤ 2 制御パケットは、次のとおりです。

- GARP VLAN Registration Protocol (GVRP)
- BPDU
- CDP/DTP/PAgP/UDLD/LACP/VTP PDU
- PVST/SSTP PDU

トラフィック レートが設定したレートを超えると、超過したパケットはハードウェアで廃棄されます。

pdu および **l2pt** のレートリミッタは、特定のハードウェアのレートリミッタ番号 (9 ~ 12 など) だけを使用します。使用可能なレートリミッタ番号を表示するには、**show mls rate-limit usage** コマンドを入力します。使用可能な番号に対しては、出力フィールドに **[Free]** と表示されます。他の機能でレートリミッタ機能が 4 つとも使用されている場合、レイヤ 2 制御パケットのレート制限を行うには他の機能をオフにする必要があるというシステムメッセージが表示されます。

MAC 移動が発生して 1 つのパケットが 2 つのポートで認識された場合、そのパケットはソフトウェアにリダイレクトされます。いずれかのポートで違反モードが制限または保護に設定されている場合、パケットはソフトウェアで廃棄されます。このようなパケットがソフトウェアにリダイレクトされる量を抑制するには、ポートセキュリティ レートリミッタを使用できます。これにより、高トラフィック レートからソフトウェアを保護できます。

例

次に、レイヤ 2 プロトコル トネリング パケットのレートリミッタ機能のイネーブル化および設定を行う例を示します。

```
Router(config)# mls rate-limit layer2 l2pt 3000
Router(config)#
```

次に、ポートセキュリティ レートリミッタを設定する例を示します。

```
Router(config)# mls rate-limit layer2 port-security 500
Router(config)# end
```

関連コマンド

コマンド	説明
show mls rate-limit	MLS レートリミッタに関する情報を表示します。

mls rate-limit multicast ipv4

IPv4 マルチキャスト パケットのレート リミッタのイネーブル化および設定を行うには、**mls rate-limit multicast ipv4** コマンドを使用します。レート リミッタをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
mls rate-limit multicast ipv4 {connected | fib-miss | igmp | ip-option | partial | non-rpf}
pps [packets-in-burst]
```

```
no mls rate-limit multicast ipv4 {connected | fib-miss | igmp | ip-option | partial |
non-rpf}
```

シンタックスの説明

connected	直接接続された送信元からのマルチキャスト パケットに対するレート リミッタのイネーブル化および設定を行います。
fib-miss	FIB 不一致マルチキャスト パケットに対するレート リミッタのイネーブル化および設定を行います。
igmp	IGMP パケットに対するレート リミッタのイネーブル化および設定を行います。
ip-option	IP オプションを持つマルチキャスト パケットに対するレート リミッタのイネーブル化および設定を行います。
partial	パーシャル SC 状態時のマルチキャスト パケットに対するレート リミッタのイネーブル化および設定を行います。
non-rpf	RPF チェックに失敗したマルチキャスト パケットに対するレート リミッタのイネーブル化および設定を行います。
<i>pps</i>	パケット/秒。有効値は 10 ~ 1,000,000 パケット/秒です。
<i>packets-in-burst</i>	(任意) バースト状態のパケット。有効値は 1 ~ 255 です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- *packets-in-burst* を設定しないと、マルチキャストの場合はデフォルトの **100** が適用されます。
- **fib-miss** : イネーブル (**100,000 pps**) で、*packet-in-burst* は **100** に設定されています。
- **ip-option** : ディセーブル
- **partial** : イネーブル (**100,000 pps**) で、*packet-in-burst* は **100** に設定されています。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

グローバル スイッチング モードが **truncated** モードに設定されている場合は、IPv4 レート リミッタを設定できません。

レートリミッタ機能は、ハードウェアのデータパスからソフトウェアのデータパスにパントされたパケットをレート制限できます。レートリミッタ機能は、ソフトウェアの制御パスが輻輳しないようにし、設定したレートを超えるトラフィックを廃棄します。

ip-option キーワードは、PFC3BXL または PFC3B モードだけでサポートされます。

例

次に、RPF チェックに失敗したマルチキャストパケットに対するレートリミッタを設定する例を示します。

```
Router(config)# mls rate-limit multicast ipv4 non-rpf 100
Router(config)#
```

次に、パーシャル SC 状態時のマルチキャストパケットに対するレートリミッタを設定する例を示します。

```
Router(config)# mls rate-limit multicast ipv4 partial 250
Router(config)#
```

次に、FIB 不一致マルチキャストパケットに対するレートリミッタを設定する例を示します。

```
Router(config)# mls rate-limit multicast ipv4 fib-miss 15
Router(config)#
```

関連コマンド

コマンド	説明
show mls rate-limit	MLS レートリミッタに関する情報を表示します。

mls rate-limit multicast ipv6

IPv6 マルチキャスト レート リミッタを設定するには、**mls rate-limit multicast ipv6** コマンドを使用します。レート リミッタをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
mls rate-limit multicast ipv6 {connected pps [packets-in-burst]} | {rate-limiter-name
{share {auto | target-rate-limiter}}}
```

```
no mls rate-limit multicast ipv6 {connected | rate-limiter-type}
```

シンタックスの説明

connected pps	直接接続された送信元からの IPv6 マルチキャスト パケットのレート リミッタをイネーブル化および設定します。有効値は、10 ~ 1,000,000 パケット/秒です。
packets-in-burst	(任意) バースト状態のパケット。有効値は 1 ~ 255 です。
rate-limiter-name	レート リミッタ名。有効値は、 default-drop 、 route-ctrl 、 secondary-drop 、 sg 、 starg-bridge 、および starg-m-bridge です。詳細については、「使用上のガイドライン」を参照してください。
share	IPv6 レート リミッタの共有ポリシーを指定します。詳細については、「使用上のガイドライン」を参照してください。
auto	共有ポリシーを自動的に決定します。
target-rate-limiter	このグループ用にハードウェアでプログラムされた最初のレート リミッタ名です。有効値は、 default-drop 、 route-ctrl 、 secondary-drop 、 sg 、 starg-bridge 、および starg-m-bridge です。詳細については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

バースト値を設定しないと、マルチキャストの場合はデフォルトの **100** が適用されます。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

rate-limiter-name 引数は、現在プログラムされていないレート リミッタである必要があります。

target-rate-limiter 引数は、ハードウェアでプログラムされているレート リミッタで、そのグループ用にプログラムされた最初のレート リミッタである必要があります。

表 2-23 に、IPv6 レート リミッタおよび各レート リミッタの対象トラフィック クラスを示します。

表 2-23 IPv6 レートリミッタ

レートリミッタ ID	レート制限されるトラフィック クラス
Connected	直接接続された送信元トラフィック
Default-drop	* (*, G/m)SSM * (*, G/m)SSM 非 rpf
Route-control	* (*, FF02::X/128)
Secondary-drop	* (*, G/128) SPT しきい値は無限
SG	* (S, G)RP-RPF ポスト スイッチオーバー * (*, FFx2/16)
Starg-bridge	* (*, G/128) SM (* , G) が存在する場合の * SM 非 rpf トラフィック
Starg-M-bridge	* (*, G/m) SM * (*, FF/8) * (*, G) が存在しない場合の SM 非 rpf トラフィック

次の方式のいずれかを使用して、IPv6 マルチキャストトラフィックのレートリミッタを設定できます。

- トラフィッククラス用のレートリミッタの直接アソシエーション：レートを選択して、レートリミッタとレートを関連付けます。次に、**1000 pps** および **20** パケット/バーストのレートを選択し、**default-drop** レートリミッタとレートを関連付ける例を示します。

```
Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
```

- レートリミッタと事前設定された他のレートリミッタとのスタティックな共有：隣接ベースの使用可能なレートリミッタが十分でない場合は、すでに設定済みのレートリミッタ（ターゲットレートリミッタ）と、レートリミッタを共有できます。次に、**route-cntl** レートリミッタを **default-drop** ターゲットレートリミッタと共有する例を示します。

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop
```

ターゲットレートリミッタが設定されていない場合は、ターゲットレートリミッタを他のレートリミッタと共有できるように設定する必要があるというメッセージが表示されます。

- レートリミッタのダイナミックな共有：共有するレートリミッタがいずれか不明な場合、**share auto** キーワードを使用してダイナミックな共有をイネーブルにします。ダイナミックな共有をイネーブルにすると、システムは事前設定されたレートリミッタを選択し、所定のレートリミッタとこの事前設定されたレートリミッタを共有します。次に、**route-cntl** レートリミッタ用にダイナミックな共有を選択する例を示します。

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share auto
```

例

次に、直接接続された送信元からの IPv6 マルチキャストパケットにレートリミッタを設定する例を示します。

```
Router(config)# mls rate-limit multicast ipv6 connected 1500 20
Router(config)#
```

次に、トラフィッククラスのレートリミッタの直接アソシエーションを設定する例を示します。

```
Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
```

■ **mls rate-limit multicast ipv6**

```
Router(config)#
```

次に、任意のレート リミッタと他の事前設定されたレート リミッタとのスタティックな共有を設定する例を示します。

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop  
Router(config)#
```

次に、**route-cntrl** レート リミッタ用にダイナミックな共有をイネーブルにする例を示します。

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share auto  
Router(config)#
```

関連コマンド

コマンド	説明
show mls rate-limit	MLS レート リミッタに関する情報を表示します。

mls rate-limit unicast acl

ACL ブリッジド レート リミッタ機能のイネーブル化および設定を行うには、**mls rate-limit unicast acl** コマンドを使用します。レート リミッタをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
mls rate-limit unicast acl {input | output | vcl-log} {pps [packets-in-burst]}
```

```
no mls rate-limit unicast acl {input | output | vcl-log}
```

シンタックスの説明

input	入力 ACL ブリッジドユニキャストパケットに対するレートリミッタ機能を指定します。
output	出力 ACL ブリッジドユニキャストパケットに対するレートリミッタ機能を指定します。
vcl-log	VACL ログに対するレートリミッタ機能を指定します。
<i>pps</i>	パケット/秒。有効値については、「使用上のガイドライン」を参照してください。
<i>packets-in-burst</i>	(任意) バースト状態のパケット。有効値は 1 ~ 255 です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- **input** : ディセーブル
- **output** : ディセーブル
- **vcl-log** : イネーブル (2000 pps) で、*packet-in-burst* は 1 に設定されています。
- *packets-in-burst* を設定しないと、ユニキャストの場合は 10 が適用されます。

コマンドモード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

レートリミッタ機能は、ハードウェアのデータパスからソフトウェアのデータパスにパントされたパケットをレート制限できます。レートリミッタ機能は、ソフトウェアの制御パスが輻輳しないようにし、設定したレートを超えるトラフィックを廃棄します。

pps を設定する場合、有効値は次のとおりです。

- ACL 入力および出力の場合 : 10 ~ 1,000,000 pps
- VACL ログの場合 : 10 ~ 5000 pps

vcl-log packets-in-burst キーワードおよび引数を変更することはできず、デフォルトで 1 に設定されます。

同じハードウェア レジスタが共有される場合もあります。これは次の 2 つのグループに分けられます。

- グループ 1 :
 - 出力 ACL ブリッジド パケット
 - 入力 ACL ブリッジド パケット
- グループ 2 :
 - RPF 障害
 - ACL 廃棄に対する ICMP 到達不能
 - ルートなしに対する ICMP 到達不能
 - IP エラー

各グループのすべてのコンポーネントは、同じハードウェア レジスタを使用または共有します。たとえば、ACL ブリッジド入力および出力パケットはレジスタ A を使用します。一方、ICMP 到達不能、ルートなし、および RPF 障害はレジスタ B を使用します。

ほとんどの場合、グループのコンポーネントを変更すると、最初のコンポーネントが変更されたときに、グループ内のコンポーネントはすべて同じハードウェア レジスタを使用するように上書きされます。上書きが行われるたびに、警告メッセージが出力されますが、サービス内部モードをイネーブルにしておく必要があります。次の場合には、上書きは行われません。

- 特別な場合で、*pps* の値が **0** (ゼロ) に設定されている場合
- 入力および出力 ACL ブリッジド パケットがディセーブルの場合、これらを再度イネーブルにするまで上書きは行われません。一方がディセーブルの場合、もう一方はイネーブルであるかぎり影響を受けません。たとえば、入力 ACL ブリッジド パケットを **100 pps** に設定したあとに、出力 ACL ブリッジド パケットを **200 pps** に設定すると、入力 ACL ブリッジド パケットの値は **200 pps** に上書きされ、入力および出力 ACL ブリッジド パケットは両方とも **200 pps** になります。

例

次に、ユニキャスト パケットに対する入力 ACL ブリッジド パケット リミッタ機能を設定する例を示します。

```
Router(config)# mls rate-limit unicast acl ingress 100
Router(config)#
```

次に、ユニキャスト パケットに対する入力 ACL ブリッジド パケット リミッタ機能をディセーブルにする例を示します。

```
Router(config)# no mls rate-limit unicast acl ingress
Router(config)#
```

関連コマンド

コマンド	説明
show mls rate-limit	MLS レート リミッタに関する情報を表示します。

mls rate-limit unicast cef

CEF レート リミッタ機能のイネーブル化および設定を行うには、**mls rate-limit unicast cef** コマンドを使用します。レート リミッタをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
mls rate-limit unicast cef {receive | glean} pps [packets-in-burst]
```

```
no mls rate-limit unicast cef {receive | glean}
```

シンタックスの説明

receive	受信パケットに対するレート リミッタのイネーブル化と設定を行います。
glean	ARP 解決パケットに対するレート リミッタのイネーブル化と設定を行います。
<i>pps</i>	パケット/秒。有効値は 10 ~ 1,000,000 パケット/秒です。
<i>packets-in-burst</i>	(任意) バースト状態のパケット。有効値は 1 ~ 255 です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- **receive** : ディセーブル
- **glean** : ディセーブル

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

CEF レート リミッタ機能をイネーブルにする場合、次の状況が発生します（これらの状況が望ましくない場合は、CEF レート リミッタをディセーブルにしてください）。

- パケットが **glean/receive** 隣接関係にヒットする場合、パケットはソフトウェアに送信されず、廃棄される可能性があります（入力 VLAN に出力 ACL があり、一致したエントリの結果が **deny**（拒否）である場合）。
- 一致した ACL エントリの結果が **bridge**（ブリッジ）である場合、パケットは **glean/receive** レート制限ではなく、出力 ACL ブリッジ レート制限（オンの場合）の制約を受けます。
- **glean/receive** 隣接レート制限は、出力 ACL 検索の結果が **permit**（許可）、または入力 VLAN に出力 ACL がない場合にだけ適用されます。

例

次に、ユニキャストパケットに対する CEF の **glean** リミッタ機能を設定する例を示します。

```
Router(config)# mls rate-limit unicast cef glean 5000
Router(config)#
```

次に、ユニキャストパケットに対する CEF の **glean** リミッタ機能をディセーブルにする例を示します。

```
Router(config)# no mls rate-limit unicast cef glean
Router(config)#
```

関連コマンド

コマンド	説明
show mls rate-limit	MLS レートリミッタに関する情報を表示します。

mls rate-limit unicast ip

ユニキャストパケットのレートリミッタ機能のイネーブル化および設定を行うには、**mls rate-limit unicast ip** コマンドを使用します。レートリミッタをディセーブルにするには、このコマンドの **no** 形式を使用します。

mls rate-limit unicast ip {errors | features | options | rpf-failure} pps [packets-in-burst]

mls rate-limit unicast ip icmp {redirect | unreachable {acl-drop pps} | no-route pps} [packets-in-burst]

no mls rate-limit unicast ip {errors | features | {icmp {redirect | unreachable {acl-drop | no-route}}}} | options | rpf-failure} pps [packets-in-burst]

シンタックスの説明

errors	IP チェックサム エラーおよび IP 長エラーのユニキャストパケットのレート制限を指定します。
features	レイヤ 3 のソフトウェアセキュリティ機能（認証プロキシ、IPSec、および検査など）を使用したユニキャストパケットのレート制限を指定します。
options	オプションを持つユニキャスト IPv4 パケットのレート制限を指定します。
rpf-failure	RPF 障害のユニキャストパケットのレート制限を指定します。
pps	パケット/秒。有効値については、「使用上のガイドライン」を参照してください。
packets-in-burst	(任意) バースト状態のパケット。有効値は 1 ~ 255 です。
icmp redirect	ICMP リダイレクトを必要とするユニキャストパケットのレート制限を指定します。
icmp unreachable acl-drop pps	ACL 廃棄パケットに対する ICMP 到達不能のレートリミッタのイネーブル化および設定を行います。
icmp unreachable no-route pps	FIB 不一致パケットに対する ICMP 到達不能のレートリミッタのイネーブル化および設定を行います。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- **packets-in-burst** を設定しないと、ユニキャストのバーストとしてデフォルトの **10** が設定されます。
- **errors** : イネーブル (**100 pps**) で、**packets-in-burst** は **10** に設定されています。
- **rpf-failure** : イネーブル (**100 pps**) で、**packets-in-burst** は **10** に設定されています。
- **icmp unreachable acl-drop** : イネーブル (**100 pps**) で、**packets-in-burst** は **10** に設定されています。
- **icmp unreachable no-route** : イネーブル (**100 pps**) で、**packets-in-burst** は **10** に設定されています。
- **icmp redirect** : ディセーブル

コマンドモード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

拒否されたパケットに対して OAL サポートを提供するには、**mls rate-limit unicast ip icmp unreachable acl-drop 0** コマンドを入力します。

OAL キャプチャと VACL キャプチャは、互換性がありません。スイッチに両方の機能を設定しないでください。OAL を設定した場合は、SPAN を使用してトラフィックをキャプチャします。

レートリミッタ機能は、ハードウェアのデータパスからソフトウェアのデータパスにパントされたパケットをレート制限できます。レートリミッタ機能は、ソフトウェアの制御パスが輻輳しないようにし、設定したレートを超えるトラフィックを廃棄します。



(注)

ICMP レートリミッタを設定して ICMP リダイレクトが発生する場合、既存のデータトラフィックが廃棄されますが、同じインターフェイス上の残りのトラフィックは転送されます。

pps を設定する場合、有効値は **0** および 10 ~ 1,000,000 です。*pps* をグローバルに **0** に設定すると、ルートプロセッサへのパケットのリダイレクトがディセーブルになります。**0** の値は、次のレートリミッタでサポートされます。

- icmp unreachable acl-drop
- icmp unreachable no-route
- icmp redirect
- ip rpf failure

同じハードウェアレジスタが共有される場合もあります。これは次の 2 つのグループに分けられます。

- グループ 1 :
 - 出力 ACL ブリッジド パケット
 - 入力 ACL ブリッジド パケット
- グループ 2 :
 - RPF 障害
 - ACL 廃棄に対する ICMP 到達不能
 - ルートなしに対する ICMP 到達不能
 - IP エラー

各グループのすべてのコンポーネントは、同じハードウェアレジスタを使用または共有します。たとえば、ACL ブリッジド入力および出力パケットはレジスタ A を使用します。一方、ICMP 到達不能、ルートなし、および RPF 障害はレジスタ B を使用します。

ほとんどの場合、グループのコンポーネントを変更すると、最初のコンポーネントが変更されたときに、グループ内のコンポーネントはすべて同じハードウェアレジスタを使用するように上書きされます。上書きが行われるたびに、警告メッセージが出力されますが、サービス内部モードをイネーブルにしておく必要があります。次の場合には、上書きは行われません。

- 特別な場合で、*pps* の値が **0** (ゼロ) に設定されている場合

- 入力および出力 ACL ブリッジドパケットがディセーブルの場合、これらを再度イネーブルにするまで上書きは行われません。一方がディセーブルの場合、もう一方はイネーブルであるかぎり影響を受けません。たとえば、入力 ACL ブリッジドパケットを 100 pps に設定したあとに、出力 ACL ブリッジドパケットを 200 pps に設定すると、入力 ACL ブリッジドパケットの値は 200 pps に上書きされ、入力および出力 ACL ブリッジドパケットは両方とも 200 pps になります。

例 次に、ユニキャストパケットに対する ICMP リダイレクトのリミッタ機能を設定する例を示します。

```
Router(config)# mls rate-limit unicast ip icmp redirect 250
Router(config)#
```

関連コマンド

コマンド	説明
show mls rate-limit	MLS レートリミッタに関する情報を表示します。

mls rate-limit unicast l3-features

ユニキャストパケットのレイヤ 3 セキュリティ レート リミッタ機能のイネーブル化および設定を行うには、**mls rate-limit unicast l3-features** コマンドを使用します。レート リミッタをディセーブルにするには、このコマンドの **no** 形式を使用します。

mls rate-limit unicast l3-features pps [*packets-in-burst*]

no mls rate-limit unicast l3-features pps [*packets-in-burst*]

シンタックスの説明

<i>pps</i>	パケット/秒。有効値については、「使用上のガイドライン」を参照してください。
<i>packets-in-burst</i>	(任意) バースト状態のパケット。有効値は 1 ~ 255 です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- イネーブル (**2000 pps**) で、*packet-in-burst* は **1** に設定されています。
- *packets-in-burst* を設定しないと、ユニキャストの場合は **10** が適用されます。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、ユニキャストパケットにレイヤ 3 セキュリティ レート リミッタを設定する例を示します。

```
Router(config)# mls rate-limit unicast l3-features 5000
Router(config)#
```

関連コマンド

コマンド	説明
show mls rate-limit	MLS レート リミッタに関する情報を表示します。

mls rate-limit unicast vacl-log

VACL ログ レート リミッタ機能のイネーブル化および設定を行うには、**mls rate-limit unicast vacl-log** コマンドを使用します。レート リミッタをディセーブルにするには、このコマンドの **no** 形式を使用します。

mls rate-limit unicast vacl-log {pps [packets-in-burst]}

no mls rate-limit unicast vacl-log

シンタックスの説明	
<i>pps</i>	パケット/秒。有効値については、「使用上のガイドライン」を参照してください。
<i>packets-in-burst</i>	(任意) バースト状態のパケット。有効値は 1 ~ 255 です。

コマンドのデフォルト デフォルト設定は次のとおりです。

- イネーブル (2000 pps) で、*packet-in-burst* は 1 に設定されています。
- *packets-in-burst* を設定しないと、ユニキャストの場合は 10 が適用されます。

コマンド モード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン レート リミッタ機能は、ハードウェアのデータ パスからソフトウェアのデータ パスにパントされたパケットをレート制限できます。レート リミッタ機能は、ソフトウェアの制御パスが輻輳しないようにし、設定したレートを超えるトラフィックを廃棄します。

pps を設定する場合、有効値は次のとおりです。

- ACL 入力および出力の場合 : 10 ~ 1,000,000 pps
- VACL ログの場合 : 10 ~ 5000 pps

pps をグローバルに 0 に設定すると、ルート プロセッサへのパケットのリダイレクトがディセーブルになります。

vacl-log *packets-in-burst* キーワードおよび引数を変更することはできず、デフォルトで 1 に設定されます。

同じハードウェア レジスタが共有される場合もあります。これは次の 2 つのグループに分けられます。

- グループ 1 :
 - 出力 ACL ブリッジド パケット
 - 入力 ACL ブリッジド パケット
- グループ 2 :
 - RPF 障害

- ACL 廃棄に対する ICMP 到達不能
- ルートなしに対する ICMP 到達不能
- IP エラー

各グループのすべてのコンポーネントは、同じハードウェア レジスタを使用または共有します。たとえば、ACL ブリッジド入力および出力パケットはレジスタ A を使用します。一方、ICMP 到達不能、ルートなし、および RPF 障害はレジスタ B を使用します。

ほとんどの場合、グループのコンポーネントを変更すると、最初のコンポーネントが変更されたときに、グループ内のコンポーネントはすべて同じハードウェア レジスタを使用するように上書きされます。上書きが行われるたびに、警告メッセージが出力されますが、サービス内部モードをイネーブルにしておく必要があります。次の場合には、上書きは行われません。

- 特別な場合で、*pps* の値が **0** (ゼロ) に設定されている場合。
- 入力および出力 ACL ブリッジド パケットがディセーブルの場合、これらを再度イネーブルにするまで上書きは行われません。一方がディセーブルの場合、もう一方はイネーブルであるかぎり影響を受けません。たとえば、入力 ACL ブリッジド パケットを 100 pps に設定したあとに、出力 ACL ブリッジド パケットを 200 pps に設定すると、入力 ACL ブリッジド パケットの値は 200 pps に上書きされ、入力および出力 ACL ブリッジド パケットは両方とも 200 pps になります。

例

次に、ユニキャスト パケットに対する VACL ログ パケット リミッタ機能を設定する例を示します。

```
Router(config)# mls rate-limit unicast vacl-log 100
Router(config)#
```

次に、レート リミッタをディセーブルにする例を示します。

```
Router(config)# no mls rate-limit unicast vacl-log 100
Router(config)#
```

関連コマンド

コマンド	説明
show mls rate-limit	MLS レート リミッタに関する情報を表示します。

mls rp ip (global configuration mode)

外部システムが PISA への IP ショートカットを確立できるようにするには、**mls rp ip** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

mls rp ip [input-acl | route-map]

no mls rp ip

シンタックスの説明	
input-acl	(任意) IP 入力アクセス リストをイネーブルにします。
route-map	(任意) IP ルート マップをイネーブルにします。

コマンドのデフォルト ショートカットは設定されていません。

コマンドモード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、外部システムが IP 入力アクセス リストを使用して IP ショートカットを確立できるようにする例を示します。

```
Router(config)# mls rp ip input-acl
Router(config)#
```

関連コマンド	コマンド	説明
	mls ip	インターフェイス上で内部ルータの MLS IP をイネーブルにします。
	show mls ip multicast	MLS IP 情報を表示します。

mls rp ip (interface configuration mode)

外部システムが指定のインターフェイス上で MLS IP をイネーブルにできるようにするには、**mls rp ip** コマンドを使用します。MLS IP をディセーブルにするには、このコマンドの **no** 形式を使用します。

mls rp ip

no mls rp ip

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード インターフェイス コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、外部システムがインターフェイス上で MLS IP をイネーブルにできるようにする例を示します。

```
Router(config-if)# mls rp ip  
Router(config-if)
```

関連コマンド	コマンド	説明
	mls rp ip (global configuration mode)	外部システムが PISA への IP ショートカットを確立できるようにします。
	show mls ip multicast	MLS IP 情報を表示します。

mls rp ipx (global configuration mode)

外部システムが PISA への MLS IPX をイネーブルにできるようにするには、**mls rp ipx** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

mls rp ipx [input-acl]

no mls rp ipx

シンタックスの説明	input-acl (任意) MLS IPX をイネーブルにして、ACL を上書きします。
-----------	--

コマンドのデフォルト	このコマンドにはデフォルト設定がありません。
------------	------------------------

コマンド モード	グローバル コンフィギュレーション (config)
----------	----------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例	次に、外部システムが PISA への MLS IPX をイネーブルにして、ACL を上書きできるようにする例を示します。
---	--

```
Router(config)# mls rp ipx input-acl
Router(config)#
```

関連コマンド	コマンド	説明
	mls rp ipx (interface configuration mode)	外部システムがインターフェイスで MLS IPX をイネーブルにすることができます。
	show mls rp ipx	IPX MLS ルータにおけるすべての IPX MLS インターフェイスの詳細を表示します。

mls rp ipx (interface configuration mode)

外部システムがインターフェイス上で MLS IPX をイネーブルにできるようにするには、**mls rp ipx** コマンドを使用します。MLS IPX をインターフェイスでディセーブルにするには、このコマンドの **no** 形式を使用します。

mls rp ipx

no mls rp ipx

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、外部システムがインターフェイス上で MLS IPX をイネーブルにできるようにする例を示します。

```
Router(config-if)# mls rp ipx
Router(config-if)#
```

関連コマンド

コマンド	説明
mls rp ipx (global configuration mode)	外部システムが PISA で MLS IPX をイネーブルにできるようにします。
show mls rp ipx	IPX MLS ルータにおけるすべての IPX MLS インターフェイスの詳細を表示します。

mls rp management-interface

インターフェイスを管理インターフェイスとしてイネーブルにするには、**mls rp management-interface** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

mls rp management-interface

no mls rp management-interface

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード インターフェイス コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、インターフェイスを管理インターフェイスとしてイネーブルにする例を示します。

```
Router(config-if)# mls rp management-interface  
Router(config-if)#
```

関連コマンド	コマンド	説明
	show mls rp	MLS 詳細を表示します。

mls rp nde-address

NDE アドレスを指定するには、**mls rp nde-address** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

mls rp nde-address ip-address

no mls rp nde-address ip-address

シンタックスの説明

<i>ip-address</i>	NDE IP アドレス
-------------------	-------------

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

IP サブネット アドレスを指定するには、次の構文を使用します。

- *ip-subnet-addr* : サブネットアドレスのショートフォーマット。IP アドレス YY.YY.YY.00 の末尾の 10 進数 00 は、IP サブネットアドレスの境界を指定します。たとえば、172.22.36.00 は 24 ビット サブネットアドレス (サブネットマスク 172.22.36.00/255.255.255.0) を示し、173.24.00.00 は 16 ビット サブネットアドレス (サブネットマスク 173.24.00.00/255.255.0.0) を示します。ただし、このフォーマットで識別できるのは、8、16、または 24 ビットのサブネットアドレスだけです。
- *ip-addr/subnet-mask* : サブネットアドレスのロングフォーマット。たとえば、172.22.252.00/255.255.252.00 は、22 ビット サブネットアドレスを示します。このフォーマットは、任意のビット数のサブネットアドレスを指定できます。より柔軟に指定するには、*ip-addr* に 172.22.253.1/255.255.252.00 のような完全ホストアドレスを指定します。
- *ip-addr/maskbits* : サブネットアドレスの簡易ロングフォーマット。マスクビットは、ネットワーク マスクのビット数を指定します。たとえば、172.22.252.00/22 は、22 ビット サブネットアドレスを示します。*ip-addr* は、193.22.253.1/22 のような完全ホストアドレスです。このアドレスのサブネットアドレスは、*ip-subnet-addr* と同じです。

例

次に、NDE アドレスを 170.25.2.1 に設定する例を示します。

```
Router(config)# mls rp nde-address 170.25.2.1
Router(config)#
```

関連コマンド

コマンド	説明
show mls rp	MLS 詳細を表示します。

mls rp vlan-id

インターフェイスに VLAN ID を割り当てるには、**mls rp vlan-id** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

```
mls rp vlan-id {vlan-id}
```

```
no mls rp vlan-id
```

シンタックスの説明	<i>vlan-id</i> VLAN ID 番号。有効値は 1 ~ 4094 です。
-----------	---

コマンドのデフォルト	このコマンドにはデフォルト設定がありません。
------------	------------------------

コマンドモード	インターフェイス コンフィギュレーション
---------	----------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、インターフェイスに VLAN ID を割り当てる例を示します。

```
Router(config-if)# mls rp vlan-id 4  
Router(config-if)#
```

関連コマンド	コマンド	説明
	show mls rp	MLS 詳細を表示します。

mls rp vtp-domain

インターフェイスを VTP ドメインにリンクするには、**mls rp vtp-domain** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

mls rp vtp-domain name

no mls rp vtp-domain name

シンタックスの説明

<i>name</i>	VLAN ドメイン名
-------------	------------

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、インターフェイスを VTP ドメインにリンクする例を示します。

```
Router(config-if)# mls rp vtp-domain EverQuest
Router(config-if)#
```

関連コマンド

コマンド	説明
show mls rp	MLS 詳細を表示します。
vtp	グローバル VTP ステートを設定します。

mls sampling

サンプリング済み NetFlow のイネーブル化およびサンプリング方式の指定を行うには、**mls sampling** コマンドを使用します。サンプリング済み NetFlow をディセーブルにするには、このコマンドの **no** 形式を使用します。

mls sampling **{{time-based rate}** | **{packet-based rate [interval]}**

no mls sampling

シンタックスの説明	time-based rate	packet-based rate interval
	時間ベースのサンプリング レートを指定します。有効値は 64、128、256、512、1024、2046、4096 、および 8192 です。詳細については、「使用上のガイドライン」を参照してください。	パケットベースのサンプリング レートを指定します。有効値は 64、128、256、512、1024、2046、4096 、および 8192 です。
		(任意) サンプリング インターバル。有効値は 8000 ~ 16,000 ミリ秒です。

コマンドのデフォルト ディセーブル

コマンド モード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン PFC3 でサンプリングをイネーブルにするには、**mls sampling** コマンドおよび **mls netflow sampling** コマンドを適切なインターフェイスで入力する必要があります。**mls netflow sampling** コマンドを入力しないと、NDE はフローをエクスポートしません。

サンプリング済み NetFlow がサポートされるのは、レイヤ 3 インターフェイスだけです。

NDE がディセーブルの場合も、サンプリング済み NetFlow をイネーブルにできますが、フローはエクスポートされません。

パケットベース サンプリングの場合、パケット数が n のフローは n/m 回サンプリングされます (m はサンプリング レート)。

時間ベース サンプリングは、各サンプリング レートに事前設定されたインターバルに基づいて実行されます。表 2-24 に、各レートおよび期間におけるサンプル インターバルを示します。

表 2-24 時間ベース サンプリングのインターバル

サンプリング レート	サンプリング時間 (ミリ秒)	エクスポート インターバル (ミリ秒)
1/64	128	8192
1/128	64	8192
1/256	32	8192

表 2-24 時間ベース サンプリングのインターバル (続き)

サンプリング レート	サンプリング時間 (ミリ秒)	エクスポート インターバル (ミリ秒)
1/512	16	8192
1/1024	8	8192
1/2048	4	8192
1/4096	4	16384
1/8192	4	32768

例

次に、時間ベース NetFlow サンプリングをイネーブルにして、サンプリング レートを設定する例を示します。

```
Router(config)# mls sampling time-based 1024
Router(config)#
```

次に、パケットベース NetFlow サンプリングをイネーブルにして、サンプリング レートおよびインターバルを設定する例を示します。

```
Router(config)# mls sampling packet-based 1024 8192
Router(config)#
```

関連コマンド

コマンド	説明
mls netflow sampling	インターフェイス上でサンプリング済み NetFlow をイネーブルにします。
show mls sampling	サンプリング済み NDE ステータスに関する情報を表示します。

mls switching

ハードウェア スイッチングをイネーブルにするには、**mls switching** コマンドを使用します。ハードウェア スイッチングをディセーブルにするには、このコマンドの **no** 形式を使用します。

mls switching

no mls switching

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、ハードウェア スイッチングをイネーブルにする例を示します。

```
Router(config)# mls switching
Router(config)#
```

次に、ハードウェア スイッチングをディセーブルにする例を示します。

```
Router(config)# no mls switching
Router(config)#
```

関連コマンド	コマンド	説明
	mls switching unicast	ユニキャスト トラフィックのハードウェア スイッチングをインターフェイスでイネーブルにします。

mls switching unicast

インターフェイスに対するユニキャスト トラフィックのハードウェア スイッチングをイネーブルにするには、**mls switching unicast** コマンドを使用します。インターフェイスに対するユニキャスト トラフィックのハードウェア スイッチングをディセーブルにするには、このコマンドの **no** 形式を使用します。

mls switching unicast

no mls switching unicast

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード インターフェイス コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、インターフェイスのハードウェア スイッチングをイネーブルにする例を示します。

```
Router(config-if)# mls switching unicast
Router(config-if)#
```

次に、インターフェイスのハードウェア スイッチングをディセーブルにする例を示します。

```
Router(config-if)# no mls switching unicast
Router(config-if)#
```

関連コマンド	コマンド	説明
	mls switching	ハードウェア スイッチングをイネーブルにします。

mls verify

ハードウェア パケット解析エラー チェックをイネーブルにするには、**mls verify** コマンドを使用します。ハードウェアでレイヤ 3 エラー チェックをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
mls verify {ip | ipx} {checksum | {length {consistent | minimum}}} | same-address |
syslog
```

```
no mls verify {ip | ipx} {checksum | {length {consistent | minimum}}} same-address |
syslog
```

シンタックスの説明

ip	IP チェックサム エラーを指定します。
ipx	IPX チェックサム エラーを指定します。
checksum	チェックサムのエラー チェックを指定します。
length	物理フレーム長と比較してヘッダーの長さをチェックします。
consistent	
length	最小パケット長をチェックします。
minimum	
same-address	送信元 IP アドレスと宛先 IP アドレスが同一であるパケットをチェックします。
syslog	Syslog パケット解析エラー トラップを指定します。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- **checksum**
- **same-address** はディセーブルです。
- **syslog** はディセーブルです。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

短すぎる IP パケットとは、IP ヘッダーの長さの IP パケット、または IP の全長フィールドが 20 バイト未満のパケットのことです。

mls verify ip length minimum コマンドを入力すると、IP プロトコル フィールドが次のうちいずれかのタイプと同じである場合に限り、有効な IPv4 パケットがハードウェアでスイッチングされます。

- ICMP (1)
- IGMP (2)
- IP (4)
- TCP (6)

- UDP (17)
- IPv6 (41)
- generic routing encapsulation (GRE; 総称ルーティングカプセル化) (47)
- SIPP-ESP (50)

no mls verify ip length minimum コマンドを入力すると、短すぎるパケットはハードウェアでスイッチングされず、IP プロトコルが 6 (TCP) の短すぎるパケットはソフトウェアに送信されます。

送信元と宛先の IP アドレスが同じであるパケットがハードウェアでスイッチングされることを防ぐには、**mls verify ip same-address** コマンドを使用します。

例

次に、ハードウェアでのレイヤ 3 エラー チェックをイネーブルにする例を示します。

```
Router(config)# mls verify ip checksum
Router(config)#
```

次に、ハードウェアでのレイヤ 3 エラー チェックをディセーブルにする例を示します。

```
Router(config)# no mls verify ip checksum
Router(config)#
```

次に、送信元と宛先の IP アドレスが同じであるパケットがハードウェアでスイッチングされることを防止する例を示します。

```
Router(config)# mls verify ip same-address
Router(config)#
```

mobility

ワイヤレス multipoint generic routing encapsulation (mGRE; マルチポイント総称ルーティングカプセル化) トンネルを設定するには、**mobility** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mobility {network-id *id*} | {tcp adjust-mss}

mobility [trust | broadcast]

シンタックスの説明

network-id <i>id</i>	mGRE トンネル用のワイヤレス ネットワーク ID を指定します。有効値は、1 ~ 4095 です。
tcp adjust-mss	アクセス ポイント上の TCP SYN および TCP ACK の maximum segment size (MSS; 最大セグメント サイズ) 値を自動調整します。
trust	(任意) 信頼されるネットワークを指定します。
broadcast	(任意) mGRE トンネルが nonbroadcast multiaccess (NBMA; 非ブロードキャスト マルチアクセス) から broadcast multiaccess (BMA; ブロードキャスト マルチアクセス) へ変換するよう指定します。

コマンドのデフォルト

信頼されないネットワーク

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、WLSM が搭載された Catalyst 6500 シリーズ スイッチだけでサポートされます。

tcp adjust-mss キーワードは、mGRE トンネル インターフェイス上だけでサポートされます。

TCC MSS を小さい値に変更する場合、**ip tcp adjust-mss *value*** コマンドを入力できます。

信頼されるネットワークは、DHCP またはスタティックな IP アドレスを使用できます。信頼されないネットワークは、DHCP クライアントだけをサポートします。

例

次に、mGRE トンネルのネットワーク識別番号を指定する例を示します。

```
Router (config-if)# mobility network-id 200
Router (config-if)#
```

次に、信頼されるネットワークを指定する例を示します。

```
Router (config-if)# mobility trust
Router (config-if)#
```

次に、mGRE トンネルが NBMA から BMA へと変換するよう指定する例を示します。

```
Router (config-if)# mobility broadcast
Router (config-if)#
```

次に、アクセス ポイント上の TCP SYN および TCP ACK の MSS 値を自動調整する例を示します。

```
Router (config-if)# mobility tcp adjust-mss
Router (config-if)#
```

関連コマンド

コマンド	説明
<code>ip tcp adjust-mss</code>	ルータを通過する TCP SYN パケットの MSS 値を調整します。
<code>show mobility</code>	レイヤ 3 モビリティおよびワイヤレス ネットワークに関する情報を表示します。

mode

冗長モードを設定するには、**mode** コマンドを使用します。

```
mode {rpr | rpr-plus | sso}
```

シンタックスの説明

rpr	RPR モードを指定します。
rpr-plus	RPR+ モードを指定します。
sso	SSO モードを指定します。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- システムが冗長モードに設定されておらず、アクティブおよびスタンバイ スーパーバイザ エンジンに同じイメージがある場合は **SSO** モードになります。
- 異なるバージョンがインストールされている場合は **RPR** モードになります。
- 冗長機能がイネーブルの場合、デフォルトは設定されたモードになります。

コマンドモード

冗長コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

rpr-plus キーワードは、Supervisor Engine 32 PISA ではサポートされていません。

Non-Stop Forwarding (NSF) /SSO 冗長モードは IPv4 をサポートします。NSF/SSO 冗長モードは、IPv6、IPX、および MPLS をサポートしません。

冗長スーパーバイザ エンジンが搭載された Catalyst 6500 シリーズ スイッチで MPLS を設定する場合は、Catalyst 6500 シリーズ スイッチを RPR モードで設定する必要があります。スイッチは、SSO のデフォルト モードで稼働しないでください。

冗長コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **redundancy** コマンドを入力します。冗長コンフィギュレーション モードで、**mode** コマンドを入力できます。

スタンバイ スーパーバイザ エンジンはモードが変更されると必ずリロードを行い、現在のモードで処理を開始します。

例

次に、冗長モードを SSO に設定する例を示します。

```
Router(config)# redundancy
Router(config-red)# mode sso
Router(config-red)#
```

関連コマンド

コマンド	説明
redundancy	冗長コンフィギュレーション モードを開始します。
redundancy force-switchover	アクティブ スーパーバイザ エンジンからスタンバイ スーパーバイザ エンジンへのスイッチオーバーを強制します。
route-converge-interval	古い FIB エントリの消去を開始する間隔を設定します。
show redundancy	Redundancy Facility (RF) 情報を表示します。
show running-config	モジュールまたはレイヤ 2 VLAN のステータスおよび設定を表示します。

mode dot1q-in-dot1q access-gateway

ギガビットイーサネット WAN インターフェイスをイネーブルにして、QinQ VLAN 変換に関してゲートウェイとして動作させるには、**mode dot1q-in-dot1q access-gateway** コマンドを使用します。QinQ VLAN 変換をインターフェイスでディセーブルにするには、このコマンドの **no** 形式を使用します。

mode dot1q-in-dot1q access-gateway

no mode dot1q-in-dot1q access-gateway

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト ディセーブル

コマンド モード インターフェイス コンフィギュレーション

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドは、OSM-2+4GE-WAN+ OSM モジュールが搭載された Catalyst 6500 シリーズスイッチのギガビットイーサネット WAN インターフェイスだけでサポートされます。

802.1Q は、パケットに 2 つの VLAN タグでタグ付けするトランッキング オプションを提供して、複数の VLAN が中間ネットワークで同時にトランッキングできるようにします。二重タグ付きトンネルのこの使用方法もまた、QinQ トンネリングといえます。

mode dot1q-in-dot1q access-gateway コマンドは、2 つの VLAN タグでパケットにタグ付けすることにより QinQ トンネリングを拡張し、中間ネットワークで複数の VLAN を同時にトランッキングできるようにします。二重タグ付きトンネルでは次の機能が実行されます。

- 2 つの 802.1Q VLAN タグでタグ付けされたパケットを、VLAN タグの組み合わせに基づく宛先サービスにスイッチングします。
- VLAN タグに基づくトラフィック シェーピングをサポートします。
- 802.1P prioritization bit (P bit; 優先順位ビット) を内部 (カスタマー) VLAN タグから外部 (サービス プロバイダー) VLAN タグにコピーします。

複数の GE-WAN インターフェイスを 1 つの仮想ポートチャネル インターフェイスに統合して、QinQ リンク バンドルを有効にすることもできます。インターフェイスの統合は設定を簡略化するだけではなく、GE-WAN OSM がバンドルのメンバーである物理インターフェイス間の PE VLAN をロード バランシングできるようになります。また、リンク バンドルのインターフェイス メンバーの 1 つがダウンした場合、PE VLAN は自動的に他のバンドル メンバーへと再割り当てされます。



(注) **mode dot1q-in-dot1q access-gateway** コマンドを使用する前に、インターフェイス上で設定されたすべての IP アドレスを削除する必要があります。

mode dot1q-in-dot1q access-gateway コマンドを設定したあと、各サブインターフェイス上で使用される VLAN マッピングを設定するには、**bridge-domain** (サブインターフェイス コンフィギュレーション) コマンドを使用します。



注意

インターフェイス上で **mode dot1q-in-dot1q access-gateway** コマンドを使用することにより、インターフェイスで設定された可能性のあるすべてのサブインターフェイスは自動的に削除されます。また、インターフェイスおよびそのサブインターフェイス上で事前に使用された可能性のあるすべての内部 VLAN が解放され、QinQ 変換で再利用できるようになります。このコマンドの **no** 形式を使用すると、すべてのサブインターフェイスが削除され、そのインターフェイスおよびサブインターフェイスによって現在使用されているすべての VLAN が解放されます。**mode dot1q-in-dot1q access-gateway** コマンドを入力する前に、インターフェイスのコンフィギュレーションを保存しておくことを推奨します。



(注)

ポートチャネル インターフェイス カウンタは (**show counters interface port-channel** コマンドおよび **show interface port-channel counters** コマンドにより表示される)、QinQ リンク バンドルに GE-WAN インターフェイスを使用するチャネル グループではサポートされません。ただし、**show interface port-channel {number | number.subif}** コマンド (**counters** キーワードなし) は、サポートされます。



ヒント

mls qos trust コマンドは、**mode dot1q-in-dot1q access-gateway** コマンドで設定された GE-WAN インターフェイスまたはポートチャネル グループには影響しません。これらのインターフェイスおよびポートチャネルは常に、この設定における VLAN CoS ビットを信頼します。

例

次に、**mode dot1q-in-dot1q access-gateway** コマンドの一般的な設定例を示します。

```
Router# configure terminal
Router(config)# interface GE-WAN 4/1
Router(config-if)# mode dot1q-in-dot1q access-gateway
Router(config-if)#
```

次に、IP アドレスの設定を最初に削除せずに **mode dot1q-in-dot1q access-gateway** コマンドを設定しようとした場合に表示されるシステム メッセージの例を示します。

```
Router# configure terminal
Router(config)# interface GE-WAN 3/0
Router(config-if)# mode dot1q-in-dot1q access-gateway

% interface GE-WAN3/0 has IP address 192.168.100.101
configured. Please remove the IP address before configuring
'mode dot1q-in-dot1q access-gateway' on this interface.

Router(config-if)# no ip address 192.168.100.101 255.255.255
Router(config-if)# mode dot1q-in-dot1q access-gateway
Router(config-if)#
```

次に、**mode dot1q-in-dot1q access-gateway** コマンドの **no** 形式を使用してインターフェイス上の QinQ マッピングをディセーブルにする例を示します。さらに、このコマンドはインターフェイス上のすべてのサブインターフェイス、およびサブインターフェイス QinQ マッピング (**bridge-domain** (サブインターフェイス コンフィギュレーション) コマンドで設定される) とサービス ポリシーのすべてを自動的に削除します。

```
Router# configure terminal
```

```
Router(config)# interface GE-WAN 3/0
Router(config-if)# no mode dot1q-in-dot1q access-gateway
Router(config-if)#
```

次に、2つの GE-WAN インターフェイスで作成され割り当てられた仮想ポートチャンネル インターフェイスの例を示します。 **mode dot1q-in-dot1q access-gateway** コマンドはポートチャンネル インターフェイス上でイネーブルとなり、ポートチャンネル インターフェイスが QinQ リンク バンドルとして動作できるようにになります。

```
Router(config)# interface port-channel 20
Router(config-if)# interface GE-WAN 3/0
Router(config-if)# port-channel 20 mode on
Router(config-if)# interface GE-WAN 3/1
Router(config-if)# port-channel 20 mode on
Router(config-if)# interface port-channel 20
Router(config-if)# no ip address
Router(config-if)# mode dot1q-in-dot1q access-gateway
Router(config-if)#
```

次に、1つまたは複数の無効なインターフェイスを含むポートチャンネル インターフェイス上で QinQ 変換をイネーブルにしようとした場合に表示されるエラー メッセージの例を示します。

```
Router# configure terminal
Router(config)# interface port-channel 30
7600-2(config-if)# mode dot1q-in-dot1q access-gateway

% 'mode dot1q-in-dot1q access-gateway' is not supported on Port-channel30
% Port-channel30 contains 2 Layer 2 Gigabit Ethernet interface(s)

Router(config-if)#
```

関連コマンド

コマンド	説明
bridge-domain (サブ インターフェイス コン フィギュレーション)	PVC を指定された <i>vlan-id</i> にバインドします。
class-map	QoS クラス マップを設定するための QoS クラス マップ コンフィギュレーション モードにアクセスします。
policy-map	QoS ポリシー マップを設定するための QoS ポリシー マップ コンフィギュレーション モードにアクセスします。
service-policy	インターフェイスにポリシー マップを対応付けます。
set cos cos-inner (policy-map configuration)	QinQ 変換された送信パケットのトランク VLAN タグの 802.1Q 優先順位ビットを、内部カスタマー エッジの VLAN タグからのプライオリティ値で設定します。

monitor event-trace (EXEC)

指定された Cisco IOS ソフトウェア サブシステム コンポーネントのイベント トレース機能を制御するには、**monitor event-trace** コマンドを使用します。

monitor event-trace all-traces **{continuous [cancel]}** | **{dump [merged] [pretty]}**

monitor event-trace l3 **{clear | {continuous [cancel]} | disable | {dump [pretty]} | enable**
| {interface type mod/port} | one-shot

monitor event-trace spa **{clear | {continuous [cancel]} | disable | {dump [pretty]} | enable | one-shot**

monitor event-trace subsys **{clear | {continuous [cancel]} | disable | {dump [pretty]} | enable | one-shot**

シンタックスの説明

all-traces	設定された統合イベント トレースを表示します。
continuous	最新のイベント トレース エントリを連続的に表示します。
cancel	(任意) 最新のトレース エントリの連続表示をキャンセルします。
dump	monitor event-trace (global configuration) コマンドにより設定されたファイルにイベント トレース結果を書き込みます。
merged	(任意) 時間でソートされたすべてのイベント トレースのエントリをダンプします。
pretty	(任意) イベント トレース メッセージを ASCII 形式で保存します。
l3	レイヤ 3 トレースに関する情報を表示します。
clear	トレースをクリアします。
disable	指定されたコンポーネントのイベント トレーシングをオフにします。
enable	指定されたコンポーネントのイベント トレーシングをオンにします。
interface type mod/port	記録されるインターフェイスを指定します。
one-shot	メモリからすべての既存トレース情報をクリアし、イベント トレーシングを再開し、トレースが monitor event-trace (global configuration) コマンドで指定されたサイズに到達するとトレースをディセーブルにします。
spa	SPA トレースに関する情報を表示します。
subsys	サブシステムの初期トレースに関する情報を表示します。

コマンドのデフォルト

トレース情報は、バイナリ形式で保存されます。

コマンド モード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

収集されるイベント トレース データの種類、収集時期、および方法を制御するには、**monitor event-trace (EXEC)** コマンドを使用します。このコマンドは、**monitor event-trace (global configuration)** コマンドによりネットワーク デバイス上でイベント トレース機能を設定してから使用してください。

トレース メッセージは、バイナリ形式で保存されます。



(注)

トレースから収集されるデータ量は、トレース インスタンスごとの **monitor event-trace (global configuration)** コマンドで設定されたトレース メッセージ サイズに応じて異なります。

Cisco IOS ソフトウェアにより、サブシステム コンポーネントはブート時のイベント トレーシングのサポートがイネーブルかディセーブルかを定義できるようになります。イベント トレーシングをイネーブルまたはディセーブルにするには、2 つの方法があります。**monitor event-trace (EXEC)** コマンド、または **monitor event-trace (global configuration)** コマンドの使用です。イベント トレーシングを再度イネーブルにするには、このコマンドのいずれかから **enable** を入力します。

サブシステムがイベント トレーシングをイネーブルまたはディセーブルにしたかどうかを判別するには、**monitor event-trace?** コマンドを使用して、イベント トレーシングをサポートするソフトウェア コンポーネントのリストを取得します。サブシステムのデフォルトでイベント トレーシングがイネーブルかどうかを判別するには、**show monitor event-trace** コマンドを使用してトレース メッセージを表示します。

トレース メッセージは、**show monitor event-trace** コマンドを使用して表示します。

単一イベントのトレース メッセージ情報を保存するには、**monitor event-trace component dump** コマンドを使用します。デフォルトでは、トレース情報はバイナリ形式で保存されます。トレース メッセージを ASCII 形式で保存するには（おそらくは追加のアプリケーション処理用に）、**monitor event-trace component dump pretty** コマンドを使用します。

ネットワーク デバイス上で現在イネーブルなすべてのイベントのトレース メッセージをファイルに書き込むには、**monitor event-trace dump-file** (グローバル コンフィギュレーション) コマンドを入力します。

トレース情報を保存するファイルを設定するには、**monitor event-trace (global configuration)** コマンドを使用します。

例

次に、イベント トレーシングを停止して、現在のメモリをクリアし、SPA コンポーネント用にトレース機能を再度イネーブルにする例を示します。次の例では、トレーシング機能がネットワーク デバイス上で設定され、イネーブルにされていると仮定します。

```
Router# monitor event-trace spa disable
Router# monitor event-trace spa clear
Router# monitor event-trace spa enable
```

次に、**one-shot** キーワードを使用して、それほど多くのコマンドを入力せずに前出の例と同じ機能を実現する例を示します。トレース メッセージ ファイルのサイズが超過すると、トレースは終了します。

```
Router# monitor event-trace spa one-shot
Router#
```

次に、あるイベントのトレース メッセージをバイナリ形式で書き込む例を示します。interprocessor communication (IPC; プロセッサ間通信) コンポーネント用のトレース メッセージは、次のようにファイルに書き込まれます。

```
Router# monitor event-trace ipc dump
Router#
```

■ monitor event-trace (EXEC)

次に、あるイベントのトレース メッセージを ASCII 形式で書き込む例を示します。この例では、MBUS コンポーネント用のトレース メッセージがファイルに書き込まれます。

```
Router# monitor event-trace mbus dump pretty
Router#
```

関連コマンド

コマンド	説明
monitor event-trace (global configuration)	指定 Cisco IOS ソフトウェア サブシステム コンポーネントのイベント トレーシングを設定します。
show monitor event-trace	CiscoIOS ソフトウェア サブシステム コンポーネントのイベント トレーシング メッセージを表示します。

monitor event-trace (global configuration)

指定した Cisco IOS ソフトウェア サブシステム コンポーネントのイベント トレース機能を設定するには、**monitor event-trace** (グローバル) コマンドを使用します。デフォルト設定を変更してイベント トレーシングをイネーブルまたはディセーブルにするには、このコマンドの「使用上のガイドライン」を参照してください。

monitor event-trace all-traces dump-file *filename*

monitor event-trace l3 {disable | dump-file *filename* | enable | size *number* | {stacktrace [*depth*]}}

monitor event-trace sequence-number

monitor event-trace spa {disable | dump-file *filename* | enable | size *number* | {stacktrace [*depth*]}}

monitor event-trace stacktrace

monitor event-trace subsys {disable | dump-file *filename* | enable | size *number* | {stacktrace [*depth*]}}

monitor event-trace timestamps [{datetime [*localtime*] [*msec*] [*show-timezone*]} | uptime]

シンタクスの説明

dump-file <i>filename</i>	統合トレースを含むダンプ ファイルを保存する URL を指定します。
l3	レイヤ 3 トレースに関する情報を表示します。
disable	イベント トレーシングをオフにします。
enable	イベント トレーシングをオンにします。
size <i>number</i>	トレースの単一インスタンス用にメモリに書き込めるメッセージ数を設定します。有効値は、1 ~ 65,536 メッセージです。
stacktrace	イベント トレース エントリとともに保存されるスタック トレースを表示します。
<i>depth</i>	(任意) トレースポイントでのトレース コール スタック。有効値は、1 ~ 16 です。
sequence-number	イベント トレース エントリをシーケンス番号とともに表示します。
spa	SPA トレースに関する情報を表示します。
subsys	サブシステムの初期トレースに関する情報を表示します。
timestamps	イベント トレース タイム スタンプの形式に関する情報を表示します。
datetime	(任意) イベント トレース タイム スタンプの形式に関する情報を表示します。
localtime	(任意) イベント トレース タイム スタンプの形式に関する情報を表示し、日時を含めます。
msec	(任意) タイム スタンプにミリ秒を含めます。
show-timezone	(任意) イベント トレース タイム スタンプの形式に関する情報を表示し、タイムゾーン情報を含めます。
uptime	(任意) システム アップタイムに関するタイプ スタンプ情報を表示します。

コマンドのデフォルト ソフトウェア コンポーネントに応じてイネーブルまたはディセーブルです。

コマンド モード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



(注) イベント トレーシングは、ソフトウェア診断ツールとしての使用を目的としているため TAC 代理店の指導の下だけで設定する必要があります。イベント トレース機能のサブシステムのサポートを提供しない Cisco IOS ソフトウェア イメージでは、**monitor event-trace (global configuration)** コマンドは使用できません。

Cisco IOS ソフトウェアにより、サブシステム コンポーネントはデフォルトのイベント トレーシングのサポートがイネーブルかディセーブルかを定義できるようになります。イベント トレーシングのコマンド インターフェイスにより、ユーザはデフォルトの 2 つの方法を変更できます。**monitor event-trace (EXEC)** コマンドまたは **monitor event-trace (global configuration)** コマンドの使用です。

さらに、デフォルト設定はコンフィギュレーション ファイルに表示されません。サブシステム ソフトウェアがデフォルトでイベント トレーシングをイネーブルにする場合、**monitor event-trace component enable** コマンドはネットワーク デバイスのコンフィギュレーション ファイルに表示されません。ただし、サブシステムによりデフォルトでイネーブルになったイベント トレーシングをディセーブルにすると、コンフィギュレーション ファイル内に 1 行作成されます。



(注) トレースから収集されるデータ量は、トレース インスタンスごとの **monitor event-trace (global configuration)** コマンドで設定されたトレース メッセージ サイズに応じて異なります。

メモリ内のイベント トレース メッセージ数がサイズを超過した場合、新規メッセージはファイル内の古いメッセージを上書きします。

filename 長の最大数 (パスおよびファイル名) は 100 文字で、パスはネットワーク デバイス上のフラッシュ メモリ、または TFTP サーバか FTP サーバにすることができます。

サブシステムがイベント トレーシングをイネーブルまたはディセーブルにしたかどうかを判別するには、**monitor event-trace?** コマンドを使用して、イベント トレーシングをサポートするソフトウェア コンポーネントのリストを取得します。

サブシステムのデフォルトでイベント トレーシングがイネーブルかどうかを判別するには、**show monitor event-trace** コマンドを使用してトレース メッセージを表示します。

トレースポイントのトレース コール スタックを指定するには、まずトレース バッファをクリアする必要があります。

例 次に、イベント トレーシングを停止して、現在のメモリをクリアし、SPA コンポーネント用にトレース機能を再度イネーブルにする例を示します。次の例では、トレーシング機能がネットワーク デバイス上で設定され、イネーブルにされていると仮定します。

```
Router(config)# monitor event-trace spa disable  
Router(config)# monitor event-trace spa clear  
Router(config)# monitor event-trace spa enable
```

関連コマンド

コマンド	説明
monitor event-trace (EXEC)	指定 Cisco IOS ソフトウェア サブシステム コンポーネントのイベント トレース機能を制御します。
show monitor event-trace	CiscoIOS ソフトウェア サブシステム コンポーネントのイベント トレース メッセージを表示します。

monitor permit-list

宛先ポート許可リストを設定し、既存の宛先ポート許可リストに追加するには、**monitor permit-list** コマンドを使用します。既存の宛先ポート許可リストから削除またはクリアするには、このコマンドの **no** 形式を使用します。

monitor permit-list

monitor permit-list destination {interface type} {slot/port[-port] [, type slot/port - port]}

no monitor permit-list

no monitor permit-list destination {interface type} {slot/port[-port] [, type slot/port - port]}

シンタックスの説明

destination	宛先ポートを指定します。
interface type	インターフェイスタイプを指定します。有効値は、 ethernet 、 fastethernet 、 gigabitethernet 、または tengigabitethernet です。
slot/port	スロット番号およびポート番号
-port	(任意) ポート範囲
,	(任意) その他のインターフェイスタイプおよびポート範囲

コマンドのデフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ポートが宛先として予想外に設定されるのを回避するために、宛先として使用できるポートの許可リストを作成できます。宛先ポート許可リストを設定した場合、宛先として設定できるのは許可リスト内のポートだけです。

例

次に、ギガビットイーサネットポート 5/1 ~ 5/4 および 6/1 を含む宛先ポート許可リストを設定する例を示します。

```
Router# configure terminal
Router(config)# monitor permit-list
Router(config)# monitor permit-list destination interface gigabitethernet 5/1-4,
gigabitethernet 6/1
```

関連コマンド

コマンド	説明
show monitor permit-list	許可リストの状態、および設定されているインターフェイスを表示します。

monitor session

新規 Encapsulated remote SPAN (ERSPAN)、SPAN または remote SPAN (RSPAN) セッションの開始、既存セッションに対するインターフェイスまたは VLAN の追加や削除、特定の VLAN への ERSPAN、SPAN、または RSPAN トラフィックのフィルタリング、またはセッションの削除を行うには、**monitor session** コマンドを使用します。セッションから送信元または宛先インターフェイスを 1 つまたは複数削除したり、セッションから送信元 VLAN を削除したり、セッションを削除するには、このコマンドの **no** 形式を使用します。

```
monitor session session source {{interface type} | {{vlan vlan-id} [rx | tx | both]} |
  {remote vlan rspan-vlan-id}}
```

```
monitor session session destination {{interface type} | {vlan vlan-id} |
  {remote vlan vlan-id} | {analysis-module slot-number} | {data-port port-number}}
```

```
monitor session session-number filter vlan vlan-range
```

```
monitor session servicemodule mod-list
```

```
monitor session session-number type {erspan-source | erspan-destination}
```

```
no monitor session {{range session-range} | local | remote | all | session}
```

```
no monitor session session source {{interface type} | {{vlan vlan-id} [rx | tx | both]} |
  {remote vlan rspan-vlan-id}}
```

```
no monitor session session destination {{interface type} | {vlan vlan-id} |
  {remote vlan vlan-id} | {analysis-module slot-number} | {data-port port-number}}
```

シンタックスの説明

session	SPAN セッション番号。有効値は 1 ～ 66 です。
source	SPAN の始点を指定します。
interface type	インターフェイス タイプを指定します。フォーマットの詳細については、「使用上のガイドライン」を参照してください。
vlan vlan-id	VLAN ID を指定します。有効値は 1 ～ 4094 です。
rx	(任意) 受信トラフィックだけをモニタするように指定します。
tx	(任意) 送信トラフィックだけをモニタするように指定します。
both	(任意) 受信トラフィックおよび送信トラフィックをモニタするように指定します。
remote vlan rspan-vlan-id	宛先 VLAN として RSPAN VLAN を指定します。
destination	SPAN 宛先インターフェイスを指定します。
analysis-module slot-number	ネットワーク解析モジュール番号を指定します。詳細については、「使用上のガイドライン」を参照してください。
data-port port-number	データポート番号を指定します。詳細については、「使用上のガイドライン」を参照してください。
filter vlan vlan-range	SPAN 送信元トラフィックを特定の VLAN に限定します。
servicemodule mod-list	サービス モジュールを指定します。 (任意) サービス モジュール番号のリスト

type erspan-source	ERSPAN 送信元セッション コンフィギュレーション モードを開始します。詳細については、 monitor session type コマンドを参照してください。
type erspan-destination	ERSPAN 宛先セッション コンフィギュレーション モードを開始します。詳細については、 monitor session type コマンドを参照してください。
range session-range	セッション範囲を指定します。
local	ローカル セッションを指定します。
remote	リモートセッションを指定します。
all	すべてのセッションを指定します。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- **both**
- **servicemodule** : すべてのサービス モジュールが、SPAN サービスモジュール セッションの使用を許可されます。

コマンドのデフォルト

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



(注)

SPAN タイプ宛先ポートに関連付ける SPAN タイプ送信元ポートを設定するときは注意してください。高トラフィック インターフェイスでは SPAN を設定しません。高トラフィック インターフェイスで SPAN を設定すると、レプリケーション エンジンおよびインターフェイスを飽和させることがあります。SPAN タイプ宛先ポートに関連付ける SPAN タイプ送信元ポートを設定するには、**monitor session session source** `{{interface type} | {{vlan vlan-id} [rx | tx | both]} | {remote vlan rspan-vlan-id}}` コマンドを入力します。

モニタセッションを設定するには、フォーマットに関する次の注意事項に従ってください。

- *interface* および *single-interface* のフォーマットは、*type slot/port* です。*type* の有効値は **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** です。
- *interface-list* は、カンマで区切られたインターフェイス リストです。次の例のように、各カンマの前後にスペースを挿入します。

single-interface , *single-interface* , *single-interface* ...

- *interface-range* は、ダッシュで区切られたインターフェイスの範囲です。各ダッシュの前後にスペースを挿入します。複数の範囲を入力するには、次の例のように各範囲をカンマで区切ります。

type slot/first-port - last-port

- *mixed-interface-list* は、インターフェイス リストを組み合わせたものです。次の例のように、各ダッシュおよびカンマの前後にスペースを挿入します。

single-interface , *interface-range* , ... (任意の順番)

- *single-vlan* は、単一 VLAN の ID 番号です。有効値は 1 ~ 4094 です。
- *vlan-list* は、カンマで区切られた VLAN ID リストです。次に例を示します。

single-vlan , *single-vlan* , *single-vlan* ...

- *vlan-range* は、ダッシュで区切られた VLAN ID の範囲です。次に例を示します。

first-vlan-ID - last-vlan-ID

- *mixed-vlan-list* は、VLAN ID リストを組み合わせたものです。各ダッシュの前後にスペースを挿入します。複数の範囲を入力するには、次の例のように各 VLAN ID をカンマで区切ります。

single-vlan , *vlan-range* , ... (任意の順番)

analysis-module slot-number および **data-port port-number** キーワードおよび引数は、ネットワーク解析モジュールだけでサポートされています。

port-channel number の有効値は、1 ~ 256 の範囲の最大 64 個の値です。

SPAN セッション間で宛先インターフェイスを共有することはできません。たとえば、1 つの宛先インターフェイスは 1 つの SPAN セッションにだけ属することができ、別の SPAN セッションの宛先インターフェイスとして設定することはできません。

ローカル SPAN、RSPAN、および ERSPAN セッションの制限は次のとおりです。

総セッション	ローカル SPAN、RSPAN 送信元、または ERSPAN 送信元のセッション	RSPAN 宛先セッション	ERSPAN 宛先セッション
66	2 (入力、出力、または両方)	64	23

ローカル SPAN、RSPAN、および ERSPAN の送信元および宛先の制限は次のとおりです。

	各ローカル SPAN セッション内	各 RSPAN 送信元セッション内	各 ERSPAN 送信元セッション内	各 RSPAN 宛先セッション内	各 ERSPAN 宛先セッション内
出力または入力/出力送信元				—	—
	128	128	128		
入力送信元				—	—
	128	128	128		
RSPAN および ERSPAN 宛先セッション送信元	—	—	—	RSPAN VLAN × 1	IP アドレス × 1
セッション単位の宛先	64	RSPAN VLAN × 1	IP アドレス × 1	64	64

特定の SPAN セッションは VLAN または各インターフェイスをモニタできます。特定のインターフェイスと特定の VLAN を両方ともモニタする SPAN セッションを設定することはできません。SPAN セッションを送信元インターフェイスで設定し、送信元 VLAN を同じ SPAN セッションに追加しようとした場合は、エラーとなります。送信元 VLAN で SPAN セッションを設定し、送信元インターフェイスをそのセッションに追加しようとした場合も、エラーとなります。別のタイプの送信元に切り替える前に、SPAN セッションのあらゆる送信元をクリアしてください。

モニタされたトランク インターフェイス上で **filter** キーワードを入力した場合、指定された VLAN セット上のトラフィックだけがモニタされます。

ポート チャネル インターフェイスを設定した場合、これらは、**interface** オプションのリスト上に表示されます。VLAN インターフェイスはサポートされません。ただし、**monitor session session source vlan vlan-id** コマンドを入力することにより、特定の VLAN にまたがることができます。

show monitor コマンドにより、SPAN サービスモジュール セッションが表示されます（割り当てられている場合だけ）。また、許可モジュールのリストおよびサービスモジュール セッションを使用できるアクティブ モジュールのリストも表示されます。

show running-config コマンドを入力すると、**monitor session servicemodule** コマンドの **no** 形式だけが表示されます。

モジュールでサービスモジュール セッションの使用が許可されない場合、サービスモジュール セッションの割り当ては自動的に解除されます。少なくとも 1 つのモジュールでサービスモジュール セッションの使用が許可され、少なくとも 1 つのモジュールがオンラインである場合、サービスモジュール セッションは自動的に割り当てられます。

サービス モジュールではないモジュールのリストによるサービスモジュール セッションの使用を許可する場合も許可しない場合でも、サービスモジュール セッションの割り当てまたは割り当ての解除には影響しません。モジュールのリストだけが、設定に保存されます。

no monitor session servicemodule コマンドにより SPAN サービスモジュール セッションをディセーブルにした場合、モジュールのリストによるサービスモジュール セッションの使用を許可するか許可しないかは、サービスモジュール セッションの割り当てまたは割り当て解除に影響しません。モジュールのリストだけが、設定に保存されます。

monitor session servicemodule コマンドは、スロットにモジュールが物理的に挿入されていない場合でも受け入れられます。

例

次に、セッションに複数の送信元を設定する方法を示します。

```
Router(config)# monitor session 2 source interface fastethernet 5/15 , 7/3 rx
Router(config)# monitor session 2 source interface gigabitethernet 1/2 tx
Router(config)# monitor session 2 source interface port-channel 102
Router(config)# monitor session 2 source filter vlan 2 - 3
Router(config)# monitor session 2 destination remote vlan 901
```

次に、最終スイッチに RSPAN 宛先を設定する例を示します (RSPAN 宛先セッション)。

```
Router(config)# monitor session 8 source remote vlan 901
Router(config)# monitor session 8 destination interface fastethernet 1/2 , 2/3
```

次に、セッション 1 および 2 の設定を削除する例を示します。

```
Router(config)# no monitor session 1 - 2
Router(config)#
```

次に、すべてのセッションの設定を削除する例を示します。

```
Router(config)# no monitor session all
Router(config)#
```

次に、すべてのリモートセッションの設定を削除する例を示します。

```
Router(config)# no monitor session remote
Router(config)#
```

次に、モジュールのリストによる SPAN サービスモジュールセッションの使用を許可する例を示します。

```
Router(config)# monitor session servicemodule module 1-2
Router(config)#
```

次に、モジュールのリストによる SPAN サービスモジュールセッションの使用を許可しない例を示します。

```
Router(config)# no monitor session servicemodule module 1-2
Router(config)#
```

関連コマンド

コマンド	説明
remote-span	VLAN を RSPAN VLAN として設定します。
show monitor session	ERSPAN、SPAN、RSPAN のセッションに関する情報を表示します。

monitor session type

ERSPAN 送信元セッション番号を作成するか、またはセッションに対して ERSPAN セッション コンフィギュレーション モードを開始するには、**monitor session type** コマンドを使用します。ERSPAN セッションから 1 つまたは複数の送信元/宛先インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

```
monitor session erspan-session-number type {erspan-destination | erspan-source}
```

```
no monitor session erspan-session-number type {erspan-destination | erspan-source}
```

シンタックスの説明

<i>erspan-session-number</i>	SPAN セッション番号。有効値は 1 ~ 66 です。
type <i>erspan-destination</i>	ERSPAN 宛先セッション コンフィギュレーション モードを指定します。
type <i>erspan-source</i>	ERSPAN 送信元セッション コンフィギュレーション モードを指定します。

コマンドモード

このコマンドにはデフォルト設定がありません。

コマンドのデフォルト

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ERSPAN は、ハードウェア リビジョン 3.2 以上でサポートされています。ハードウェア リビジョンを表示するには、**show module version | include WS-SUP720-BASE** コマンドを入力します。

ERSPAN トラフィックは、GRE カプセル化された SPAN トラフィックで、ERSPAN 宛先セッションによってだけ処理されます。

スイッチ上のすべての ERSPAN 送信元セッションは、同じ送信元 IP アドレスを使用する必要があります。ERSPAN 送信元セッションに IP アドレスを設定するには、**origin ip address** コマンドを入力します。

スイッチ上のすべての ERSPAN 宛先セッションは、同じ IP アドレスを使用する必要があります。ERSPAN 宛先セッションに IP アドレスを設定するには、**ip address** コマンドを入力します。ERSPAN 宛先 IP アドレスが Supervisor Engine 32 PISA ではない場合 (ネットワーク スニファの場合など)、トラフィックは GRE および RSPAN ヘッダー/カプセル化とともにそのまま着信します。

ERSPAN 送信元セッションの宛先 IP アドレスが (宛先スイッチ上のインターフェイスで設定される必要がある)、ERSPAN 宛先セッションが宛先ポートに送信するトラフィックの送信元です。**ip address** コマンドを使用して、送信元および宛先セッションの両方で同じアドレスを設定します。

ERSPAN ID により、同じ宛先 IP アドレスに着信する ERSPAN トラフィックと異なる ERSPAN 送信元セッションとが区別されます。

monitor session type

ローカル ERSPAN セッションの制限は次のとおりです。

- 総セッション：66
- 送信元セッション：2（入力、出力、または両方）
- 宛先セッション：23

monitor session type コマンドにより、新しい ERSPAN セッションが作成されるか、または ERSPAN セッション コンフィギュレーション モードが開始されます。ERSPAN は別々の送信元および宛先セッションを使用します。送信元セッションと宛先セッションは、異なるスイッチに設定します。

ERSPAN セッション コンフィギュレーション モードのプロンプトは、次のとおりです。

- Router(config-mon-erspan-src) : ERSPAN 送信元セッション コンフィギュレーション モードを示します。
- Router(config-mon-erspan-src-dst) : ERSPAN 送信元セッション宛先コンフィギュレーション モードを示します。
- Router(config-mon-erspan-dst) : ERSPAN 宛先セッション コンフィギュレーション モードを示します。
- Router(config-mon-erspan-dst-src) : ERSPAN 宛先セッション送信元コンフィギュレーション モードを示します。

表 2-25 に、ERSPAN 宛先セッション コンフィギュレーション モードの構文を示します。

表 2-25 ERSPAN 宛先セッション コンフィギュレーション モードの構文

構文	説明
グローバル コンフィギュレーション モード	
monitor session <i>erspan-destination-session-number type erspan-destination</i>	ERSPAN 宛先セッション コンフィギュレーション モードを開始して、プロンプトを次のように変更します。 Router (config-mon-erspan-dst) #
宛先セッション コンフィギュレーション モード	
description <i>session-description</i>	(任意) ERSPAN 宛先セッションを説明します。
shutdown	(任意) (デフォルト) ERSPAN 宛先セッションを終了します。
no shutdown	ERSPAN 宛先セッションを始動します。
destination { <i>single-interface interface-list interface-range mixed-interface-list</i> }	ERSPAN 宛先セッション数を宛先ポートに関連付けます。
source	ERSPAN 宛先セッション送信元コンフィギュレーション モードを開始して、プロンプトを次のように変更します。 Router (config-mon-erspan-dst-src) #
宛先セッション送信元コンフィギュレーション モード	
ip address <i>ip-address</i> [force]	ERSPAN フローの宛先 IP アドレスを設定します。これは、宛先スイッチ上のインターフェイスでも設定される必要があり、ERSPAN 宛先セッション コンフィギュレーション で入力されます。
erspan-id <i>erspan-flow-id</i>	ERSPAN トラフィックを識別するために、宛先および宛先セッションで使用される ID 番号を設定します。
vrf <i>vrf-name</i>	(任意) ERSPAN トラフィックのパケットの VRF 名を設定します。

表 2-26 に、ERSPAN 送信元セッション コンフィギュレーション モードの構文を示します。

表 2-26 ERSPAN 送信元セッション コンフィギュレーション モードの構文

構文	説明
グローバル コンフィギュレーション モード	
monitor session <i>erspan-source-session-number</i> type erspan-source	ERSPAN 送信元セッション コンフィギュレーション モードを開始して、プロンプトを次のように変更します。 Router(config-mon-erspan-src)#
送信元セッション コンフィギュレーション モード	
description <i>session-description</i>	(任意) ERSPAN 送信元セッションを説明します。
shutdown	(任意) (デフォルト) ERSPAN 送信元セッションを終了します。
no shutdown	ERSPAN 送信元セッションを始動します。
source {{ <i>single-interface</i> <i>interface-list</i> <i>interface-range</i> <i>mixed-interface-list</i> <i>single-vlan</i> <i>vlan-list</i> <i>vlan-range</i> <i>mixed-vlan-list</i> } [rx tx both]}	ERSPAN 送信元セッション番号を送信元ポートまたは VLAN に関連付け、モニタされるトラフィック方向を選択します。
filter { <i>single-vlan</i> <i>vlan-list</i> <i>vlan-range</i> <i>mixed-vlan-list</i> }	(任意) ERSPAN 送信元がトランク ポートである場合に、送信元 VLAN フィルタリングを設定します。
destination	ERSPAN 送信元セッション宛先コンフィギュレーション モードを開始して、プロンプトを次のように変更します。 Router(config-mon-erspan-src-dst)#
送信元セッション宛先コンフィギュレーション モード	
ip address <i>ip-address</i>	ERSPAN フローの宛先 IP アドレスを設定します。これは、宛先スイッチ上のインターフェイスでも設定される必要があり、ERSPAN 宛先セッション コンフィギュレーション で入力されます。
erspan-id <i>erspan-flow-id</i>	ERSPAN トラフィックを識別するために、送信元および宛先セッションで使用される ID 番号を設定します。
origin ip address <i>ip-address</i>	ERSPAN トラフィックの送信元として使用される IP アドレスを設定します。
ip {{ ttl <i>ttl-value</i> } { prec <i>ipp-value</i> } { dscp <i>dscp-value</i> }}	(任意) 次の ERSPAN トラフィックのパケット値を設定します。 <ul style="list-style-type: none"> • ttl <i>ttl-value</i> : IP 存続可能時間 (TTL) 値 • prec <i>ipp-value</i> : IP precedence 値 • dscp <i>dscp-value</i> : IP precedence 値
vrf <i>vrf-name</i>	(任意) ERSPAN トラフィックのパケットの VRF 名を設定します。

モニタ セッションを設定する場合は、次の構文の注意事項に従ってください。

- *erspan-destination-span-session-number* の範囲は、1 ~ 66 です。
- *single-interface* は、**interface type slot/port** です。type は、**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** です。

- *interface-list* の形式は、*single-interface* , *single-interface* , *single-interface* です。



(注) リストでは、カンマの前後でスペースを入力してください。リストでは、ダッシュの前後でスペースを入力してください。

- *interface-range* の形式は、**interface type slot/first-port - last-port** です。
- *mixed-interface-list* の形式は、順不同で *single-interface* , *interface-range* です。
- *erspan-flow-id* の範囲は、1 ~ 1023 です。

モニタセッションをクリアする場合は、次の構文の注意事項に従ってください。

- **no monitor session session-number** コマンドを他のパラメータなしで入力すると、セッションの *session-number* をクリアします。
- *session-range* の形式は、*first-session-number-last-session-number* です。



(注) **no monitor session range** コマンドを入力する場合は、ダッシュの前後にスペースを入力しないでください。複数の範囲を入力する場合は、カンマの前後にスペースを入力しないでください。

例

次に、ERSPAN 送信元セッション番号を設定し、セッションに対して ERSPAN 送信元セッション コンフィギュレーション モードを開始する例を示します。

```
Router(config)# monitor session 55 type erspan-source
Router(config-mon-erspan-src)#
```

次に、ERSPAN 宛先セッション番号を設定し、セッションに対して ERSPAN 宛先セッション コンフィギュレーション モードを開始する例を示します。

```
Router(config)# monitor session 55 type erspan-destination
Router(config-mon-erspan-dst)#
```

次に、ERSPAN 宛先セッション番号を宛先ポートに関連付ける例を示します。

```
Router(config-mon-erspan-dst) destination interface fastethernet 1/2 , 2/3
```

次に、ERSPAN 宛先セッション送信元設定を開始する例を示します。

```
Router(config-mon-erspan-dst)# source
Router(config-mon-erspan-dst-src)#
```

次に、ERSPAN 宛先セッション送信元コンフィギュレーション モードを開始する例を示します。

```
Router(config-mon-erspan-dst)# source
Router(config-mon-erspan-dst-src)#
```

次に、セッションに複数の送信元を設定する方法を示します。

```
Router(config-mon-erspan-src)# source interface fastethernet 5/15 , 7/3 rx
Router(config-mon-erspan-src)# source interface gigabitethernet 1/2 tx
Router(config-mon-erspan-src)# source interface port-channel 102
Router(config-mon-erspan-src)# source filter vlan 2 - 3
Router(config-mon-erspan-src)#
```

次に、ERSPAN 送信元セッション宛先コンフィギュレーション モードを開始する例を示します。

```
Router(config-mon-erspan-src)# destination  
Router(config-mon-erspan-src-dst)#
```

次に、送信元および宛先セッションで使用される ID 番号を設定して、ERSPAN トラフィックを識別する例を示します。

```
Router(config-mon-erspan-src-dst)# erspan-id 1005  
Router(config-mon-erspan-src-dst)#
```

関連コマンド

コマンド	説明
show monitor session	ERSPAN、SPAN、RSPAN のセッションに関する情報を表示します。

mpls l2transport route

MPLS 上のレイヤ 2 パケットのルーティングをイネーブルにするには、**mpls l2transport route** コマンドを使用します。MPLS 上のルーティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

mpls l2transport route destination vc-id

no mpls l2transport route destination vc-id

シンタックスの説明

<i>destination</i>	仮想回線の宛先となるルータの IP アドレス
<i>vc-id</i>	ルータへの仮想回線識別子

コマンドモード

このコマンドにはデフォルト設定がありません。

コマンドのデフォルト

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

mpls l2transport route コマンドは、VLAN パケットをルーティングするのに使用される仮想回線をイネーブルにします。使用される仮想回線のタイプは次のとおりです。

- VC タイプ 4: VLAN 内のすべてのトラフィックが MPLS ネットワークで 1 つの VC を使用するようになります。
- VC タイプ 5: ポート上のすべてのトラフィックが MPLS ネットワークで 1 つの VC を共有するようになります。

VC 設定時は、VC タイプ 5 がアドバタイズされます。ピアが VC タイプ 4 をアドバタイズする場合、VC タイプがタイプ 4 に変更され、VC が再開します。変更はタイプ 5 からタイプ 4 だけが有効で、タイプ 4 からタイプ 5 には変更できません。

レイヤ 2 の MPLS VLAN 仮想回線は、MPLS クラウドを介して、2 つの PE ルータの VLAN インターフェイスを接続します。

MPLS クラウドを介して他の PE ルータの VLAN インターフェイスにレイヤ 2 の VLAN パケットをルーティングするには、各 PE ルータの VLAN インターフェイス上で **mpls l2transport route** コマンドを使用します。宛先パラメータには、他の PE ルータの IP アドレスを指定します。コマンドを発行しているルータの IP アドレスは指定しないでください。

仮想回線 ID は任意の値を選択できます。ただし、仮想回線 ID は仮想回線に対して一意でなければなりません。大規模ネットワークでは、同じ仮想回線 ID を 2 回割り当てることがないように、割り当てを管理する必要があります。

ルーテッド仮想回線はメイン インターフェイスではサポートされますが、サブインターフェイスではサポートされません。

仮想回線 ID は、仮想回線ごとに一意でなければなりません。

例

次に、MPLS 上のレイヤ 2 パケットのルーティングをイネーブルにする例を示します。

```
Router(config-if)# mpls l2transport route 192.16.0.1
Router(config-if)#
```

関連コマンド

コマンド	説明
show mpls l2transport vc	ルータの仮想回線の状態を表示します。

mpls load-balance per-label

タグ間のトラフィックのロードバランスをイネーブルにするには、**mpls load-balance per-label** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mpls load-balance per-label

no mpls load-balance per-label

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドモード

ディセーブル

コマンドのデフォルト

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

タグ間のトラフィックのロードバランスをイネーブルにする場合、トラフィックは MPLS インターフェイス間の着信ラベル（プレフィクスごと）に基づいて分散されます。各 MPLS インターフェイスは、同数の着信ラベルをサポートします。

show mpls ttfib コマンドを使用すれば、ロードバランサに含まれる着信ラベル（アスタリスク * で表示される）を表示できます。

例

次に、タグ間のトラフィックのロードバランスをイネーブルにする例を示します。

```
Router(config)# mpls load-balance per-label
Router(config)#
```

次に、タグ間のトラフィックのロードバランスをディセーブルにする例を示します。

```
Router(config)# no mpls load-balance per-label
Router(config)#
```

関連コマンド

コマンド	説明
show mpls ttfib	MPLS Toaster Tag FIB (TTFIB) テーブルに関する情報を表示します。

mpls ttl-dec

標準 MPLS タギングを指定するには、**mpls ttl-dec** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mpls ttl-dec

no mpls ttl-dec

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドモード 最適化された MPLS タギング (**no mpls ttl-dec**)

コマンドのデフォルト インターフェイス コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン MPLS ラベルがパケット ヘッダーに付加される前に、元のパケットの IP ToS および TTL 値が書き換えられるように、MPLS タギングが最適化されました。この変更により、特定のトラフィック タイプに関して少しパフォーマンスが落ちる場合があります。パケットの元の ToS/TTL 値が重要でない場合は、**mpls ttl-dec** コマンドで標準 MPLS タギングを指定してください。

例 次に、Catalyst 6500 シリーズスイッチが標準の MPLS タギング動作を使用するよう設定する例を示します。

```
Router(config)# mpls ttl-dec  
Router(config)#
```

次に、Catalyst 6500 シリーズスイッチが最適化 MPLS タギング動作を使用するよう設定する例を示します。

```
Router(config)# no mpls ttl-dec  
Router(config)#
```

関連コマンド	コマンド	説明
	mpls l2transport route	MPLS 上のレイヤ 2 パケットのルーティングをイネーブルにします。

mtu

最大パケット サイズまたは MTU サイズを調整するには、**mtu** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mtu bytes

no mtu

シンタックスの説明

bytes バイト サイズ。有効値は、SVI ポートでは 64 ～ 9216、GE-WAN+ ポートでは 1500 ～ 9170、その他のすべてのポートでは 1500 ～ 9216 です。

コマンド モード

表 2-27 に、ジャンボ フレームがディセーブルの場合のデフォルトの MTU 値を示します。

表 2-27 デフォルトの MTU 値

メディア タイプ	デフォルトの MTU (バイト)
イーサネット	1500
シリアル	1500
トークンリング	4464
ATM	4470
FDDI	4470
HSSI (HSA)	4470

ジャンボ フレームがイネーブルの場合、デフォルトは、SVI ポートでは 64、その他のすべてのポートでは 9216 です。デフォルトでは、ジャンボ フレームがディセーブルです。

コマンドのデフォルト

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

スイッチ ポートの場合、グローバルに使用できるのは、デフォルト値よりも大きい MTU が 1 つだけです。レイヤ 3 ポート (ルータ ポートや VLAN を含む) の場合、インターフェイスごとにデフォルト以外の MTU 値を設定できます。

ジャンボ フレームをサポートしていないモジュールのリストについては、『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide Release 12.2ZY*』を参照してください。

mtu コマンドで MTU 値を設定すると、プロトコル固有バージョンのコマンドの値に影響が及ぶことがあります (**ip mtu** コマンドなど)。**ip mtu** コマンドで指定された値が **mtu** コマンドで指定された値と同じである場合に、**mtu** コマンドの値を変更すると、**ip mtu** 値は新しい **mtu** コマンドの値と一致するように自動的に調整されます。ただし、**ip mtu** コマンドの値を変更しても、**mtu** コマンドの値には影響しません。

例

次に、1800 バイトの MTU を指定する例を示します。

```
Router(config)# interface fastethernet 5/1
Router(config-if)# mtu 1800
```

関連コマンド

コマンド	説明
ip mtu	インターフェイスで送信される IP パケットの MTU サイズを設定します。

name (MST configuration submode)

MST リージョン名を設定するには、**name** コマンドを使用します。デフォルト名に戻すには、このコマンドの **no** 形式を使用します。

name *name*

no *name name*

シンタックスの説明

<i>name</i>	MST リージョンに付ける名前を指定します。最大 32 文字の任意のストリングです。
-------------	--

コマンド モード

空のストリング

コマンドのデフォルト

MST コンフィギュレーション サブモード

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

同じ VLAN マッピングおよびコンフィギュレーション バージョン番号を持つ複数の Catalyst 6500 シリーズ スイッチは、リージョン名が異なっている場合は異なった MST リージョンにあると見なされません。



注意

name コマンドで MST リージョン名を設定する場合には注意してください。設定を間違えると、Catalyst 6500 シリーズ スイッチが別のリージョンに配置されます。コンフィギュレーション名は大文字と小文字の区別があります。

例

次に、リージョンに名前を付ける例を示します。

```
Router(config-mst)# name Cisco  
Router(config-mst)#
```

関連コマンド

コマンド	説明
instance	1 つまたは一連の VLAN を MST インスタンスにマッピングします。
revision	MST コンフィギュレーションのリビジョン番号を設定します。
show	MST の設定を確認します。
show spanning-tree mst	MST プロトコルに関する情報を表示します。
spanning-tree mst configuration	MST コンフィギュレーション サブモードを開始します。

neighbor

ピアごとにトンネル シグナリングおよびカプセル化メカニズムのタイプを指定するには、**neighbor** コマンドを使用します。スプリット ホライズンをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
neighbor remote-router-id {encapsulation encapsulation-type} | {pw-class pw-name}
[no-split-horizon]
```

```
no neighbor remote-router-id
```

シンタックスの説明

remote-router-id	リモート ピアリング ルータの ID
encapsulation encapsulation	トンネル カプセル化タイプを指定します。有効値は l2tpv3 および mpls です。
pw-class pw-name	エミュレート VC の設定に使用する擬似配線プロパティを指定します。
no-split-horizon	(任意) データ パスにおいてレイヤ 2 スプリット ホライズンをディセーブルにします。

コマンド モード

スプリット ホライズンはイネーブルです。

コマンドのデフォルト

レイヤ 2 VFI 手動コンフィギュレーション サブモード

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

ループを避けるには、完全にメッシュ化されている Virtual PVLAN service (VPLS) ネットワークでスプリット ホライズンをディセーブルにしないでください。

例

次に、トンネル カプセル化タイプの指定する例を示します。

```
Router(config-vfi)# neighbor 333 encapsulation mpls
Router(config-vfi)#
```

次に、レイヤ 2 スプリット ホライズンをデータ パスでディセーブルにする例を示します。

```
Router(config-vfi)# neighbor 333 no-split-horizon
Router(config-vfi)#
```

net

ルーティングプロセスに IS-IS network entity title (NET) を設定するには、**net** コマンドを使用します。NET を削除するには、このコマンドの **no** 形式を使用します。

```
net net1 {alt net2}
```

```
no net net
```

シンタックスの説明

<i>net1</i>	プライマリ スロットに搭載された PISA 上の IS-IS ルーティング プロセスの NET network service access point (NSAP; ネットワーク サービス アクセス ポイント) 名またはアドレス。詳細については、「使用上のガイドライン」を参照してください。
<i>alt net2</i>	代替スロットに搭載された PISA 上の IS-IS ルーティング プロセスの NET 名またはアドレスを指定します。詳細については、「使用上のガイドライン」を参照してください。
<i>net</i>	削除する NET NSAP 名またはアドレス

コマンドのデフォルト

デフォルト設定は次のとおりです。

- NET は設定されていません。
- IS-IS プロセスはディセーブルです。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

NET は、最終バイトが常に **n** セレクタであって常にゼロである NSAP です。NET のバイト数は 8 ～ 20 です。

ほとんどの場合、NET を 1 つだけ設定する必要があります。

net を入力する場合、次の点に注意してください。

- 3 スロット シャーシでは、スロット 1 がプライマリ スロットでスロット 2 が代替スロットです。
- 6 スロット シャーシでは、スロット 5 がプライマリ スロットでスロット 6 が代替スロットです。
- 9 スロット シャーシでは、スロット 5 がプライマリ スロットでスロット 6 が代替スロットです。
- 13 スロット シャーシでは、スロット 7 がプライマリ スロットでスロット 8 が代替スロットです。

IS-IS を使用して IP ルーティングだけを実行している (Connection-Less Network Service (CLNS) がイネーブルでない) 場合、ルータ ID およびエリア ID を定義するように NET を設定する必要があります。

ルータごとに複数の NET (最大 3 つの NET) を設定できます。まれに、2 つまたは 3 つの NET を設定できることがあります。このような場合、このルータが属するエリアは、1 つのエリアに対して 3 つのエリア アドレスを持ちます。

複数の NET があると、複数のエリアを結合したり、1 つのエリアを複数のエリアに分割するネットワーク再設定時に、一時的に便利です。複数のエリア アドレスがある場合は、必要に応じてエリアごとに番号を付け直すことができます。

例

次に、ルータのシステム ID を 0000.0c11.1110、エリア ID を 47.0004.004d.0001 に設定する例を示します。

```
router isis Pieinthesky
 net 47.0004.004d.0001.0001.0c11.1111.00
```

次に、3 つのエリアが設定された IS-IS ルーティング プロセスを示します。エリアごとに一意の ID がありますが、システム ID はすべてのエリアで同じです。

```
clns routing

...

interface Tunnel529
 ip address 10.0.0.5 255.255.255.0
 ip router isis BB
 clns router isis BB

interface Ethernet1
 ip address 10.1.1.5 255.255.255.0
 ip router isis A3253-01
 clns router isis A3253-01
!
interface Ethernet2
 ip address 10.2.2.5 255.255.255.0
 ip router isis A3253-02
 clns router isis A3253-02

...

router isis BB                                ! Defaults to "is-type level-1-2"
 net 49.2222.0000.0000.0005.00
!
router isis A3253-01
 net 49.0553.0001.0000.0000.0005.00
 is-type level-1
!
router isis A3253-02
 net 49.0553.0002.0000.0000.0005.00
 is-type level-1
```

関連コマンド

コマンド	説明
is-type	IS-IS ルーティング プロセスのインスタンスのルーティング レベルを設定します。
router isis	IS-IS ルーティング プロトコルをイネーブルにして、IS-IS プロセスを指定します。

nsf

Cisco NSF をイネーブルにし、設定するには、**nsf** コマンドを使用します。NSF をディセーブルにするには、このコマンドの **no** 形式を使用します。

nsf [enforce global]

nsf [{**cisco** | **ietf**}] | {**interface** {**wait seconds**}} | {**interval minutes**} | {**t3 [adjacency | manual seconds]**}}

no nsf

シンタックスの説明

enforce global	(任意) NSF 非対応ネイバが検出された場合、OSPF NSF の再開をキャンセルします。
cisco	(任意) アクティブな RP のフェールオーバーの場合に、シスコ独自の IS-IS NSF チェックポイント方式を指定します。
ietf	(任意) アクティブな RP のフェールオーバーの場合に、IETF IS-IS NSF プロトコル変更方式を指定します。
interface wait seconds	(任意) フェールオーバーのあと Cisco NSF プロセスを実行するまで、インターフェイスが動作するのを待機する時間を指定します。有効値は、1 ~ 60 秒です。
interval minutes	(任意) ルートプロセッサが安定したあと、再開するまで待機する時間を指定します。有効値は、0 ~ 1440 分です。
t3 adjacency	(任意) Label Switched Path (LSP; ラベル スイッチドパス) データベースが同期化するのを IETF NSF が待機する時間が、スイッチオーバーの前に、指定された RP のネイバにアダプタイズされる隣接の保持時間により決定されるよう指定します。
t3 manual seconds	(任意) NSF データベースの同期化のあと、再開ノードを中継として見なさないようその他のノードに知らせるまでの待機時間を指定します。有効値は、5 ~ 3600 秒です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- NSF はディセーブルです。
- **enforce global** : イネーブル
- **interval minutes** : 5 分
- **interface wait seconds** : 10 秒
- **t3 manual seconds** : 30 秒

コマンド モード

ルータ コンフィギュレーション IS-IS

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



(注)

nsf t3 マニュアル コマンドを使用して、シスコ独自の IS-IS NSF が設定されているかまたは Internet Engineering Task Force (IETF) IS-IS NSF がイネーブルの場合、**nsf interface wait** コマンドを使用できます。インターフェイスが動作するまで時間がかかる場合、このコマンドを使用できます。

Cisco NSF は、Catalyst 6500 シリーズ スイッチが再開時に Cisco NSF の実行が予想される場合だけ必要です。Catalyst 6500 シリーズ スイッチが、Cisco NSF の再開だけを実行するネイバと協力すると予想される場合、スイッチはデフォルト (Cisco NSF をサポートするバージョンのコードを実行) で NSF 対応である必要があります。

nsf コマンドは、**router** コマンドのサブセットで、指定されたプロセスの対象となるすべてのインターフェイスに影響します。Cisco NSF は、BGP、OSPF、IS-IS、および EIGRP プロトコルをサポートします。NSF 処理をイネーブルにするコンフィギュレーション コマンドは、次のとおりです。

- **nsf under the router ospf** コマンド
- **nsf ietf under the router isis** コマンド
- **bgp graceful-restart under the router bgp** コマンド

これらのコマンドは、ルータの実行コンフィギュレーションの一部として発行される必要があります。再開時にこれらのコマンドは、NSF 処理を作動させるよう復元されます。

`{[cisco | ietf]} | {interface {wait seconds}} | {interval minutes} | {t3 [adjacency | {manual seconds}]}`
キーワードおよび引数は、IS-IS だけに適応されます。

`{enforce global}` キーワードは、OSPF だけに適応されます。

BGP NSF に関するガイドライン

NSF の BGP サポートでは、ネイバ ネットワークのデバイスが NSF 対応デバイスである必要があります。つまり、これらのデバイスにはグレースフル リスタート機能があり、セッション確立中に OPEN メッセージでこの機能をアドバタイズする必要があります。NSF 対応ルータが、特定の BGP ネイバでグレースフル リスタート機能がイネーブルでないことを検出した場合、このネイバを使用した NSF 対応セッションは確立されません。他のすべてのネイバに、グレースフル リスタート機能が備わっている場合は、この NSF 対応ネットワーキング デバイスを使用して NSF 対応セッションを引き続き維持します。グレースフル リスタート機能をイネーブルにするには、**bgp graceful-restart** ルータ コンフィギュレーション コマンドを入力します。詳細については、『Cisco IOS Release 12.2 Command Reference』を参照してください。

EIRGP NSF に関するガイドライン

ルータは NSF 対応のルータである可能性がありますが、コールド スタートから動作するため、NSF 再開のネイバの援助には参加しない場合があります。

IS-IS NSF に関するガイドライン

ネットワーキング デバイス上で IETF は設定されていても、ネイバ ルータが IETF と互換性がない場合、NSF はスイッチオーバーのあとで打ち切られます。

IS-IS NSF を設定する場合、次の 2 つのキーワードを使用します。

- **ietf** : Internet Engineering Task Force IS-IS。スーパーバイザ エンジンのスイッチオーバー後に、NSF 対応のルータが隣接する NSF 対応デバイスに IS-IS NSF 再開要求を送信します。

- **cisco** : Cisco IS-IS。すべての隣接情報および LSP 情報が、スタンバイ スーパーバイザ エンジンに対して保存 (チェックポイント) されます。スイッチオーバー後、新しいアクティブ スーパーバイザ エンジンは、迅速にそのルーティング テーブルを再確立するために、チェックポイントされたデータを使用してその隣接を維持します。

OSPF NSF に関するガイドライン

OSPF NSF では、すべてのネイバ ネットワーキング デバイスが NSF 対応デバイスである必要があります。NSF 対応ルータが、特定のネットワーク セグメントに非 NSF アウェアのネイバが存在することを検出すると、このセグメントに対する NSF 機能はディセーブルになります。完全に NSF 可能または NSF 対応のルータだけで構成されているその他のネットワーク セグメントは、引き続き NSF 機能を提供します。

OSPF NSF は、IPv4 トラフィックに対してだけ NSF/SSO をサポートします。OSPFv3 は、NSF/SSO ではサポートされません。OSPFv2 だけが、NSF/SSO でサポートされます。

例

次に、すべての OSPF プロセス インターフェイスに関して NSF をイネーブルにする例を示します。

```
Router(config)# router ospf 109
Router(config-router)# nsf
Router(config-router)#
```

次に、すべての OSPF プロセス インターフェイスに関して NSF をディセーブルにする例を示します。

```
Router(config)# router ospf 109
Router(config-router)# no nsf
Router(config-router)#
```

関連コマンド

コマンド	説明
router	ルーティング プロセスをイネーブルにします。

pagp learn-method

着信パケットの入力インターフェイスを学習するには、**pagp learn-method** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

pagp learn-method {aggregation-port | physical-port}

no pagp learn-method

シンタックスの説明

aggregation-port	ポート チャネルでのアドレス学習を指定します。
physical-port	バンドル内の物理ポート上のアドレス学習を指定します。

コマンドのデフォルト

aggregation-port 方式

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、バンドル内の物理ポートのアドレス学習方式を設定する例を示します。

```
Router(config-if)# pagp learn-method physical-port
Router(config-if)#
```

次に、バンドル内のポートチャネルのアドレス学習方式を設定する例を示します。

```
Router(config-if)# pagp learn-method
Router(config-if)#
```

関連コマンド

コマンド	説明
show pagp	ポート チャネル情報を表示します。

pagp port-priority

ホット スタンバイ モードのポートを選択するには、**pagp port-priority** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

pagp port-priority *priority*

no pagp port-priority

シンタックスの説明

<i>priority</i>	プライオリティ番号。有効値は 1 ~ 255 です。
-----------------	----------------------------

コマンドのデフォルト

priority は **128** です。

コマンドのデフォルト

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

プライオリティが高いほど、ポートがホット スタンバイ モードで選択される可能性が高くなります。

例

次に、ポート プライオリティを設定する例を示します。

```
Router(config-if)# pagp port-priority 45
Router(config-if)#
```

関連コマンド

コマンド	説明
pagp learn-method	着信パケットの入力インターフェイスを学習します。
show pagp	ポート チャネル情報を表示します。

■ pagp port-priority

platform ip features pisa

PISA へのトラフィックをフィルタする Intelligent Traffic Redirect (ITR) 機能を設定するには、インターフェイス コンフィギュレーション モードで、**platform ip features pisa** コマンドを使用します。

platform ip features pisa access-group {*ip-acl-name* | *ip-acl-number*} {**input** | **output**}
 [**reverse-only**]

シンタックスの説明

access-group <i>ip-acl-name</i>	ITR ACL の名前を指定します。
access-group <i>ip-acl-number</i>	ITR ACL の番号を指定します。範囲は、1 ~ 199 および 1300 ~ 2699 です。
input	入力トラフィックに ITR ACL を適用します。
output	出力トラフィックに ITR ACL を適用します。
reverse-only	(任意) inspect direction トラフィックにだけ ITR ACL を適用することを指定します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZYA1	このコマンドのサポートが追加されました。

使用上のガイドライン

platform ip features pisa コマンドを設定しない場合、PISA アクセラレーション機能を設定したインターフェイス上のすべてのトラフィックが PISA に送信されます。

このコマンドは、レイヤ 2 およびレイヤ 3 ポート、レイヤ 2 およびレイヤ 3 トランク、レイヤ 2 およびレイヤ 3 ポートチャンネル インターフェイス、マルチ VLAN アクセス ポイント (MVAP)、レイヤ 3 サブインターフェイス、および、SVI だけに適用できます。このコマンドは他のタイプのインターフェイスに入力できません。他のタイプのインターフェイスに設定しようとすると、エラー メッセージが表示されます。

このコマンドをレイヤ 3 インターフェイスに入力すると、このパケットが PISA による双方向の送信を必要とする場合は、ソフトウェアは自動的にリバース ACL (ミラー ACL ともいう) を同一インターフェイスの反対方向にマッピングしようとします。

このコマンドをレイヤ 2 インターフェイスに入力すると、ハードウェア制限によってリバース ACL が出力方向にマップされることが防止されます。レイヤ 2 インターフェイスで、LTL コピーメカニズムがすべてのパケットをキャプチャします。

PISA アクセラレーション機能に必要な PISA アクション

機能	キーワード	入力トラフィックのアクション	出力トラフィックのアクション
NBAR Modular QoS CLI (MQC; モジュラ QoS CLI)	input, input reverse-only	修正	検査
	output, output reverse-only	検査	修正
NBAR プロトコル検出	input, input reverse-only	検査	検査
	output, output reverse-only	検査	検査
NBAR タギング	input, input reverse-only	なし	なし
	output, output reverse-only	なし	修正
フレキシブル パケット マッチング	input, input reverse-only	修正	なし
	output, output reverse-only	なし	修正
URL フィルタリング	input, input reverse-only	修正	修正
	output, output reverse-only	修正	修正

インターフェイスに PISA アクセラレーション機能が設定されている場合、ITR ACL は以下のように動作します。

- **input** : ITR ACL は PISA アクセラレーション機能に必要なアクションのために、ACL によって許可された入力 (modify-direction) トラフィックを PISA へリダイレクトします。許可されない入力トラフィックは PFC3 によって処理されます。

ITR 機能によって自動的に適用される場合は、リバース ITR ACL はリバース ACL によって許可された出力 (inspect-direction) トラフィックを PISA へリダイレクトし、統計情報、保有ステート、または、その他のタイプの情報を収集します。

- **input reverse-only** : PISA アクセラレーション機能に必要なアクションのために、すべての入力 (modify-direction) トラフィックは PISA へ送信されます。ITR ACL は、ACL によって許可された出力 (inspect-direction) トラフィックを PISA へリダイレクトし、統計情報、保有ステート、または、その他のタイプの情報を収集します。reverse-only キーワードを使用して、出力 (inspect-direction) トラフィックだけに対する ITR ACL を設定します。

- **output** : ITR ACL は PISA アクセラレーション機能に必要なアクションのために、ACL によって許可された出力 (modify-direction) トラフィックを PISA へリダイレクトします。許可されない出力トラフィックは PFC3 によって処理されます。

ITR 機能によって自動的に適用される場合は、リバース ITR ACL は PISA アクセラレーション機能に必要なアクションのために、リバース ACL によって許可された入力 (inspect-direction) トラフィックを PISA へリダイレクトします。

- **output reverse-only** : PISA アクセラレーション機能に必要なアクションのために、すべての出力 (modify-direction) トラフィックは PISA へ送信されます。ITR ACL は PISA アクセラレーション機能に必要なアクションのために、ACL によって許可された入力 (inspect-direction) トラフィックを PISA へリダイレクトします。reverse-only キーワードを使用して、入力 (inspect-direction) トラフィックだけに対して ITR ACL を設定します。

PFC QoS を適用するトラフィックを許可しないように ITR ACL を設定します。

過剰なトラフィックを PISA に送信することを避けるために、ITR が設定されている場合に、VACL キャプチャ、OAL、および、NAM および Intrusion Detection System (IDS) サービス モジュールのトラフィックなどの非 PISA キャプチャ ベース機能がイネーブルでないことを確認します。

ITR が設定されている場合、NetFlow ベースの機能 (たとえば、NAT および WCCP) によって処理されるトラフィックは PISA へ送信されない場合があります。

例

次に、出力トラフィックを PISA へリダイレクトする例を示します。

```
Router(config-if)# platform ip features pisa access-group pisa_egress_redirect out  
Router(config-if)#
```

関連コマンド

コマンド	説明
show platform software pisa fm interface	インターフェイス単位の Supervisor Engine 32 PISA 固有情報を表示します。
show platform pisa np	Supervisor Engine 32 PISA 固有情報を表示します。
show running-config interface	現在稼働中のコンフィギュレーションファイルの内容を表示します。

platform ip features sequential

IP precedence ベースまたは DSCP ベースの出力 QoS フィルタリングを有効にして、入力 PFC QoS によって加えられた IP precedence または DSCP ポリシングまたはマーキングの変更を適用するには、**platform ip features sequential** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

platform ip features sequential [**access-group** {*ip-acl-name* | *ip-acl-number*}]

no platform ip features sequential [**access-group** {*ip-acl-name* | *ip-acl-number*}]

シンタックスの説明

access-group <i>ip-acl-name</i>	(任意) 再循環パケットの一致条件を指定するために使用される ACL の名前を指定します。
access-group <i>ip-acl-number</i>	(任意) 再循環パケットの一致条件を指定するために使用される ACL の番号を指定します。有効値は 1 ~ 199 と 1300 ~ 2699 です。

コマンドのデフォルト

IP precedence ベースまたは DSCP ベースの出力 QoS フィルタリングは、受信した IP precedence または DSCP 値を使用し、ポリシングまたはマーキングの結果として入力 QoS によって加えられた IP precedence または DSCP の変更を使用しません。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

強化出力 QoS フィルタリングにより、IP precedence ベースまたは DSCP ベースの出力 QoS フィルタリングで入力 QoS によって加えられた IP precedence または DSCP ポリシング/マーキングの変更を使用することができます。

強化されていない出力 QoS フィルタリングの動作は、QoS がハードウェアで適用されたときの通常の Catalyst 6500 シリーズ スイッチ動作です。

PFC3 は、出力レイヤ 3 インターフェイス (レイヤ 3 インターフェイスとして設定された LAN ポートまたは VLAN インターフェイス) 上のレイヤ 3 スイッチドおよびルーテッドトラフィックについてだけ、出力 PFC QoS を提供します。

強化出力 QoS フィルタリングは、入力レイヤ 3 インターフェイス (レイヤ 3 インターフェイスとして設定された LAN ポートまたは VLAN インターフェイス) 上で設定します。

特定の標準、拡張名前付き、または拡張番号付き IP ACL によってフィルタされたトラフィックについてだけ強化出力 QoS フィルタリングをイネーブルにするには、IP ACL の名前または番号を入力します。

IP ACL の名前または番号を入力しなかった場合、強化出力 QoS フィルタリングはインターフェイス上のすべての IP 入力 IP トラフィックについてイネーブルになります。



(注)

- 強化出力 QoS フィルタリングを設定すると、PFC3 はトラフィックを処理して、入力 PFC QoS を適用します。PFC3 は入力 QoS フィルタリングと Catalyst 6500 シリーズスイッチ ハードウェア入力 QoS を適用します。PFC3 は、入力インターフェイス上で設定される出力 QoS フィルタリングおよび Catalyst 6500 シリーズスイッチ ハードウェア出力 QoS を誤って適用します。
- 入力 QoS マーキングによって変更された IP precedence または DSCP のマッチングを行うためにレイヤ 2 機能を使用するインターフェイス上で強化出力 QoS フィルタリングを設定した場合、パケットはリダイレクトまたは破棄されて、出力 QoS によって処理されません。
- 強化出力 QoS フィルタリングをイネーブルにした場合、再帰 ACL、NAT、TCP インターセプトなどの NetFlow ベース機能のハードウェア アクセラレーションはディセーブルになります。

設定を確認するには、**show running-config interface** コマンドを使用します。

例

次に、強化出力 QoS フィルタリングをイネーブルにする例を示します。

```
Router(config-if)# platform ip features sequential
Router(config-if)#
```

次に、強化出力 QoS フィルタリングをディセーブルにする例を示します。

```
Router(config-if)# no platform ip features sequential
Router(config-if)#
```

関連コマンド

コマンド	説明
show running-config interface	現在稼働中のコンフィギュレーション ファイルの内容を表示します。

platform ipv6 acl icmp optimize neighbor-discovery

IPv6 ACL の TCAM サポートを最適化するには、**platform ipv6 acl icmp optimize neighbor-discovery** コマンドを使用します。IPv6 ACL の TCAM サポートの最適化をディセーブルにするには、このコマンドの **no** 形式を使用します。

platform ipv6 acl icmp optimize neighbor-discovery

no platform ipv6 acl icmp optimize neighbor-discovery

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト ディセーブル

コマンド モード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



(注) Cisco TAC の指導を受けた場合にだけ、このコマンドを使用してください。

IPv6 ACL の TCAM サポートの最適化をイネーブルにすると、TCAM の上部にあるグローバル ICMPv6 neighbor-discovery ACL はすべての ICMP v 6 ネイバ検出パケットを許可するようにプログラムされます。最適化のイネーブル化によって、すべての IP v 6 セキュリティ ACL の末尾への ICMP v 6 ACE の追加が行われなくなり、使用される TCAM リソースの数が削減されます。このコマンドをイネーブルにすると、すべてのインターフェイス上の IP v 6 ACL が再プログラムされます。



(注) TCAM 上部の ICMPv6 neighbor-discovery ACL は、設定した ICMP ネイバ検出パケットについてセキュリティ ACL に優先しますが、グローバル ICMP ACL と重複する bridge/deny があつた場合は無効です。

例 次に、IP v 6 ACL の TCAM サポートを最適化する例を示します。

```
Router(config)# platform ipv6 acl icmp optimize neighbor-discovery  
Router(config)#
```

次に、IP v 6 ACL の TCAM サポートの最適化をディセーブルにする例を示します。

```
Router(config)# no platform ipv6 acl icmp optimize neighbor-discovery  
Router(config)#
```

platform scp retry interval

SCP の高速リトライをイネーブルにして、高速リトライのインターバルを設定するには、**platform scp retry interval** コマンドを使用します。SCP の高速リトライをディセーブルにするには、このコマンドの **no** 形式を使用します。

platform scp retry interval *timeout-value*

no platform scp retry interval

シンタックスの説明	<i>timeout-value</i>	高速リトライのインターバル。有効値は、200 ~ 2000 ミリ秒です。
-----------	----------------------	--------------------------------------

コマンドのデフォルト	2000 ミリ秒
------------	----------

コマンドモード	グローバル コンフィギュレーション (config)
---------	----------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



(注) Cisco TAC の指導を受けた場合にだけ、このコマンドを使用してください。

例	次に、SCP 高速リトライをイネーブルにして、高速リトライのインターバルを設定する例を示します。 Router(config)# platform scp retry interval 600 Router(config)#
---	---

platform vfi dot1q-transparency

802.1Q 透過性モードをイネーブルにするには、**platform vfi dot1q-transparency** コマンドを使用します。802.1Q 透過性をディセーブルにするには、このコマンドの **no** 形式を使用します。

platform vfi dot1q-transparency

no platform vfi dot1q-transparency

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドをサポートするのは、OSM モジュールだけです。

802.1Q 透過性により、サービス プロバイダーは、VPLS カスタマーの 802.1p ビットには変更を加えずに、コアベースの QoS ポリシーの MPLS EXP ビットを変更できるようになりました。

EoMPLS の dot1q 透過性機能では、VLAN に適用されたポリシーが Interior Gateway Protocol (IGP; 内部ゲートウェイ プロトコル) ラベル (コア QoS 用) にだけ影響し、VC ラベル EXP ビットと 802.1p ビットを同じにします。一方出力 PE では、802.1p ビットは受信した VC EXP ビットに基づいて書き換えられますが、EXP ビットは入力 802.1p ビットに一致しているため、VPLS カスタマーの 802.1p ビットは変更されません。

グローバル コンフィギュレーション (config) は、Cisco 7600 シリーズ ルータに設定されたすべての Virtual Forwarding Instance (VFI) およびスイッチ仮想インターフェイス (SVI) の EoMPLS VC に適用されます。

インターオペラビリティを実現するには、接続されているすべての PE ルータに EoMPLS の Dot1q 透過性を適用する必要があります。

例

次に、802.1Q 透過性をイネーブルにする例を示します。

```
Router (config)# platform vfi dot1q-transparency
Router (config)#
```

次に、802.1Q 透過性をディセーブルにする例を示します。

```
Router (config)# no platform vfi dot1q-transparency
Router (config)#
```

police (policy map)

インターフェイス単位のポリサーを作成して、それを使用するようにポリシーマップクラスを設定するには、**police** コマンドを使用します。ポリシーマップクラスからインターフェイス単位のポリサーを削除するには、このコマンドの **no** 形式を使用します。

```
police {bits-per-second [normal-burst-bytes] [maximum-burst-bytes] [pir peak-rate-bps]} |
[conform-action action] [exceed-action action] [violate-action action]
```

```
no police {bits-per-second [normal-burst-bytes] [extended-burst-bytes] [pir peak-rate-bps]} |
[conform-action action] [exceed-action action] [violate-action action]
```

シンタックスの説明

<i>bits-per-second</i>	CIR ビット/秒。有効値は、32,000 bps ~ 2 Gbps です。
<i>normal-burst-bytes</i>	(任意) CIR トークン バケット サイズ。有効値は 1000 ~ 512,000,000 バイトです。
<i>maximum-burst-bytes</i>	(任意) PIR トークン バケット サイズ。有効値は 1000 ~ 32,000,000 バイトです。
pir <i>peak-rate-bps</i>	(任意) PIR ピーク レートを設定します。有効値は 32,000 bps ~ 2 Gbps です。
conform-action <i>action</i>	(任意) <i>bits-per-second</i> レートを超えなかった場合に行うアクションを指定します。有効値については、「使用上のガイドライン」を参照してください。
exceed-action <i>action</i>	(任意) <i>bits-per-second</i> レートを超えた場合に行うアクションを指定します。有効値については、「使用上のガイドライン」を参照してください。
violate-action <i>action</i>	(任意) <i>bits-per-second</i> レートが <i>maximum-burst-bytes</i> レートより大きいときに行うアクションを指定します。有効値については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- *maximum-burst-bytes* は *normal-burst-bytes* と同じです。
- **conform-action** は **transmit** です。
- **exceed-action** は **drop** です。
- **violate-action** は、**exceed-action** と同じです。
- **pir** *peak-rate-bps* は、*normal-burst-bytes* レートと同じです。

コマンドモード

policy-map サブコマンド

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

Supervisor Engine 32 PISA では、ソフトウェアで **police** コマンドがサポートされています。

名前付き集約ポリサーとマイクロフロー ポリサーは、Supervisor Engine 32 PISA ではサポートされていません。

normal-burst-bytes 引数は、CIR トークン バケット サイズを設定します。

maximum-burst-bytes 引数は、PIR トークン バケット サイズを設定します (**flow** キーワードとの併用はサポートされません)。*maximum-burst-bytes* 引数は、*normal-burst-bytes* 設定と同じになるように設定する必要があります。

pir peak-rate-bps は、*extended-burst-bytes* に対応します。

action の有効値は次のとおりです。

- **drop** : *bits-per-second* レートを超えないパケットを廃棄します。
- **policed-dscp-transmit** : すべての不適合トラフィックに、マークダウン マップで指定されているとおりマーキングします。
- **set-dscp-transmit** {*dscp-value* | *dscp-bit-pattern* | **default** | **ef**} : 一致したトラフィックを新しい DSCP 値でマークします。有効値は次のとおりです。
 - *dscp-value* : DSCP 値を指定します。有効値は 0 ~ 63 です。
 - *dscp-bit-pattern* : DSCP ビット パターンを指定します。有効値は表 2-28 に列挙されています。
 - **default** : パケットとデフォルトの dscp (000000) とのマッチングを行います。
 - **ef** : パケットと EF dscp (101110) とのマッチングを行います。

表 2-28 有効な dscp-bit-pattern 値

キーワード	定義
af11	パケットと AF11 dscp (001010) とのマッチングを行います。
af12	パケットと AF12 dscp (001100) とのマッチングを行います。
af13	パケットと AF13 dscp (001110) とのマッチングを行います。
af21	パケットと AF21 dscp (010010) とのマッチングを行います。
af22	パケットと AF22 dscp (010100) とのマッチングを行います。
af23	パケットと AF23 dscp (010110) とのマッチングを行います。
af31	パケットと AF31 dscp (011010) とのマッチングを行います。
af32	パケットと AF32 dscp (011100) とのマッチングを行います。
af33	パケットと AF33 dscp (011110) とのマッチングを行います。
af41	パケットと AF41 dscp (100010) とのマッチングを行います。
af42	パケットと AF42 dscp (100100) とのマッチングを行います。
af43	パケットと AF43 dscp (100110) とのマッチングを行います。
cs1	パケットと CS1 (precedence 1) dscp (001000) とのマッチングを行います。
cs2	パケットと CS2 (precedence 2) dscp (010000) とのマッチングを行います。
cs3	パケットと CS3 (precedence 3) dscp (011000) とのマッチングを行います。

表 2-28 有効な dscp-bit-pattern 値

キーワード	定義
cs4	パケットと CS4 (precedence 4) dscp (10000) とのマッピングを行います。
cs5	パケットと CS5 (precedence 5) dscp (101000) とのマッピングを行います。
cs6	パケットと CS6 (precedence 6) dscp (110000) とのマッピングを行います。
cs7	パケットと CS7 (precedence 7) dscp (111000) とのマッピングを行います。

- **set-mpls-exp-imposition-transmit new-mpls-exp** : インポートされたラベル エントリの MPLS EXP ビットを書き換えて送信します。*new-mpls-exp* 引数は、ポリシー マップによって定義される MPLS EXP ビットを設定するために使用される値を指定します。*new-mpls-exp* の有効値は 0 ~ 7 です。
- **set-mpls-exp-topmost-transmit** : 最上部のラベル エントリの MPLS EXP ビットを書き換えて、送信します。*new-mpls-exp* 引数は、ポリシー マップによって定義される MPLS EXP ビットを設定するために使用される値を指定します。*new-mpls-exp* の有効値は 0 ~ 7 です。
- **set-prec-transmit new-precedence** : 一致したトラフィックを新しい IP precedence 値でマークして送信します。*new-precedence* の有効値は 0 ~ 7 です。
- **transmit** : *bits-per-second* レートを超えないパケットを送信します。

例

次に、ipp5 という名前のクラス マップを使用するポリシー マップ max-pol-ipp5 を作成する例を示します。この例では、受信した IP precedence 値を信頼するように設定し、最大容量に関する集約ポリサーを設定します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# policy-map max-pol-ipp5
Router(config-pmap)# class ipp5
Router(config-pmap-c)# trust ip-precedence
Router(config-pmap-c)# police 2000000000 2000000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)#
```

関連コマンド

コマンド	説明
class-map	QoS クラス マップを設定するための QoS クラス マップ コンフィギュレーション モードにアクセスします。
service-policy	インターフェイスにポリシー マップを対応付けます。
show class-map	クラス マップ情報を表示します。
show policy-map	ポリシー マップに関する情報を表示します。
show policy-map interface	インターフェイスに対応付けられた入力および出力ポリシーの統計情報およびコンフィギュレーションを表示します。

police rate

コントロール プレーン宛のトラフィックのトラフィック ポリシングを設定するには、**police rate** コマンドを使用します。設定からトラフィック ポリシングを削除するには、このコマンドの **no** 形式を使用します。

police rate units pps [burst burst-in-packets packets] [peak-rate peak-rate-in-pps pps] [peak-burst peak-burst-in-packets packets]

police rate units bps [burst burst-in-bytes bytes] [peak-rate peak-rate-in-bps bps] [peak-burst peak-burst-in-bytes bytes]

police rate percent percentage [burst ms ms] [peak-rate percent percentage] [peak-burst ms ms]

no police rate units pps [burst burst-in-packets packets] [peak-rate peak-rate-in-pps pps] [peak-burst peak-burst-in-packets packets]

no police rate units bps [burst burst-in-bytes bytes] [peak-rate peak-rate-in-bps bps] [peak-burst peak-burst-in-bytes bytes]

no police rate percent percentage [burst ms ms] [peak-rate percent percentage] [peak-burst ms ms]

シンタックスの説明

units	ポリス レート。有効値については、「使用上のガイドライン」を参照してください。
pps	トラフィックを規制するレートをパケット/秒で指定します。
burst burst-in-packets packets	(任意) トラフィックのポリシングに使用されるバースト レートを指定します。有効値は 1 ~ 512000 パケットです。
peak-rate peak-rate-in-pps pps	(任意) トラフィックのポリシングに使用される PIR を指定します。有効値は 1 ~ 512,000 パケットです。
peak-burst peak-burst-in-packets packets	(任意) トラフィックのポリシングに使用されるピーク バースト値を指定します。有効値は 1 ~ 512,000 パケットです。
bps	トラフィックを規制するレートをビット/秒で指定します。
burst burst-in-bytes bytes	(任意) トラフィックのポリシングに使用されるバースト レートを指定します。有効値は 1000 ~ 512,000,000 ビットです。
peak-rate peak-rate-in-bps bps	(任意) ピーク レートとして使用されるピーク バースト値を指定します。有効値は 1000 ~ 512,000,000 ビットです。
peak-burst peak-burst-in-bytes bytes	(任意) トラフィックのポリシングに使用されるピーク バースト値を指定します。有効値は 1000 ~ 512,000,000 ビットです。
percent percentage	(任意) トラフィックを規制するレートを決めるために使用されるインターフェイス帯域幅のパーセントを指定します。有効値は 1 ~ 100 です。
burst ms ms	(任意) トラフィックのポリシングに使用されるバースト レートを指定します。有効値は 1 ~ 2000 ミリ秒です。

peak-rate percent <i>percentage</i>	(任意) PIR を決めるために使用されるインターフェイス帯域幅のパーセン トを指定します。有効値は 1 ~ 100 です。
peak-burst ms ms	(任意) トラフィックのポリシングに使用されるピーク バースト レートを 指定します。有効値は 1 ~ 2000 ミリ秒です。

コマンドのデフォルト ディセーブル

コマンドモード ポリシーマップ クラス コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン *units* の有効値は次のとおりです。

- ポリス レートを **pps** で指定する場合、有効値は 1 ~ 2,000,000 pps です。
- ポリス レートを **bps** で指定する場合、有効値は 8000 ~ 10,000,000,000 bps です。

pps は、PIR *peak-rate-in-pps* を計算するために使用されます。

コントロールプレーン宛のトラフィックをパケット/秒 (pps)、バイト/秒 (bps)、またはインターフェイス帯域幅のパーセントで制限するには、**police rate** コマンドを使用します。

police rate コマンドを入力して、レートを指定しなかった場合、コントロールプレーン宛のトラフィックは bps 単位で規制されます。

例 次に、クラスのポリシングを設定して、トラフィックを平均レート 1,500,000 pps に制限する例を示します。

```
Router(config)# class-map telnet-class
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map control-plane-policy
Router(config-pmap)# class telnet-class
Router(config-pmap-c)# police rate 1500000 pps bc 500000 packets
Router(config-pmap-c)# exit
```

関連コマンド	コマンド	説明
	policy-map	QoS ポリシー マップを設定するための QoS ポリシー マップ コンフィギュレーション モードにアクセスします。
	show policy-map	ポリシー マップに関する情報を表示します。

policy-map

QoS ポリシー マップを設定するための QoS ポリシー マップ コンフィギュレーション モードにアクセスするには、**policy-map** コマンドを使用します。ポリシー マップを削除するには、このコマンドの **no** 形式を使用します。

policy-map *policy-map-name*

no policy-map *policy-map-name*

シンタックスの説明

<i>policy-map-name</i>	ポリシー マップ名。 policy-map サブコマンドの説明については、「使用上のガイドライン」を参照してください。
------------------------	--

コマンドのデフォルト

デフォルト設定は次のとおりです。

- *extended-burst-bytes* は *burst-bytes* と同じです。
- **conform-action** は transmit です。
- **exceed-action** は drop です。
- **violate-action** は、**exceed-action** と同じです。
- **pir peak-rate-bps** は標準の (**cir**) レートと同じです。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

QoS ポリシー マップ コンフィギュレーション モードでは、次のコンフィギュレーション コマンドが利用できます。

- **exit** : QoS クラス マップ コンフィギュレーション モードを終了します。
- **no** : 定義済みポリシー マップを削除します。
- **class class-map [name]** : QoS クラス マップ コンフィギュレーション モードにアクセスして、以前に作成したクラス マップがポリシー マップに含まれるよう指定したり、クラス マップを作成したりします (詳細については、**class-map** コマンドを参照してください)。
- **class {class-name | class-default}** は、クラス コンフィギュレーション モードにアクセスして、作成または変更するポリシーのクラス名を指定します (詳細については、**class (policy-map)** コマンドを参照してください)。
- **police [aggregate name]** サブコマンド : マイクロフローまたは集約ポリサーを定義します (詳細については、**police (policy map)** コマンドを参照してください)。構文は次のとおりです。
 - **police** {*aggregate name*}
 - **police flow** {*bits-per-second* [*normal-burst-bytes*] [*maximum-burst-bytes*] [**pir peak-rate-bps**]} | [**conform-action** *action*] [**exceed-action** *action*] [**violate-action** *action*]

– **police flow mask** {**dest-only** | **full-flow** | **src-only**} {*bits-per-second* [*normal-burst-bytes*] [*maximum-burst-bytes*]} [**conform-action** *action*] [**exceed-action** *action*]

- **trust** {**cos** | **dscp** | **ip-precedence**} : 指定されたクラス信頼値を設定します。このコマンドで設定された信頼値は、特定のインターフェイス上で設定された信頼値よりも優先します。

表 2-29 に、**class** の構文を示します。

表 2-29 class の構文

サブコマンド	説明
exit	(任意) QoS クラス アクション コンフィギュレーション モードを終了します。
police	(任意) フロー ポリシングを指定します。詳細については、 police (policy map) コマンドを参照してください。
trust state	(任意) ポリシー マップ クラスの信頼状態を設定します。信頼状態は cos 、 dscp 、および ip precedence です。
cos	(任意) 受信した CoS またはインターフェイスの CoS から、内部 DSCP 値を設定します。
dscp	(任意) 受信した DSCP 値を使用するように QoS を設定します。
ip-precedence	(任意) 受信した IP precedence から、DSCP 値を設定します。

policy-map で **exceed-action** を指定しなかった場合は、デフォルトの **drop** に設定され、**violate-action** が続きます。

ポリシー マップ クラスでは、PFC QoS は **bandwidth**、**priority**、**queue-limit**、**random-detect**、または **set** キーワードをサポートしません。

例

次に、設定済みのクラスマップ **ipp5** を使用するポリシー マップ **max-pol-ipp5** を作成する例、および信頼状態を受信された IP precedence 値に設定し、最大容量に関する集約ポリサーおよびマイクロフロー ポリサーを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# policy-map max-pol-ipp5
Router(config-pmap)# class ipp5
Router(config-pmap-c)# trust ip-precedence
Router(config-pmap-c)# police 2000000000 2000000 8000000 conform-action set-prec-transmit
6 exceed-action policed-dscp-transmit
Router(config-pmap-c)# police flow 10000000 10000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)# end
Router#
```

関連コマンド

コマンド	説明
class-map	QoS クラス マップを設定するための QoS クラス マップ コンフィギュレーション モードにアクセスします。
class (policy-map)	ポリシーを設定する前に、作成または変更するポリシーを持つクラス名を指定するか、デフォルトのクラス（一般に class-default クラスの呼び名で知られている）を指定します。
service-policy	インターフェイスにポリシー マップを対応付けます。

コマンド	説明
<code>show class-map</code>	クラス マップ情報を表示します。
<code>show policy-map</code>	ポリシー マップに関する情報を表示します。
<code>show policy-map interface</code>	インターフェイスに対応付けられた入力および出力ポリシーの統計情報およびコンフィギュレーションを表示します。

port access-map

ポート アクセス マップを作成するか、またはポート アクセス マップ コマンド モードを開始するには、**port access-map** コマンドを使用します。マッピング シーケンスまたはマップ全体を削除するには、このコマンドの **no** 形式を使用します。

port access-map *name* [*seq#*]

no port access-map *name* [*seq#*]

シンタックスの説明

<i>name</i>	ポート アクセスマップのタグです。
<i>seq#</i>	(任意) マップ シーケンス番号。有効値は 0 ~ 65,535 です。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

既存のマップ シーケンスのシーケンス番号を入力すると、ポート アクセスマップ モードが開始します。シーケンス番号を指定しないと、番号が自動的に割り当てられます。各マップ シーケンスには、**match** 句および **action** 句をそれぞれ 1 つずつ指定できます。

シーケンス番号を指定しないで **no port access-map name [seq#]** コマンドを入力すると、マップ全体が削除されます。

ポート アクセスマップ モードを開始すると、次のコマンドが使用可能になります。

- **action** : パケットの **action** 句を指定します。 **action** コマンドを参照してください。
- **default** : コマンドをデフォルトに設定します。
- **end** : コンフィギュレーション モードを終了します。
- **exit** : ポート アクセスマップ コンフィギュレーション モードを終了します。
- **match** : **match** 句を指定します。 **match** コマンドを参照してください。
- **no** : コマンドを否定するか、またはデフォルトを設定します。

例

次に、ポート アクセスマップ モードを開始する例を示します。

```
Router(config)# port access-map ted
Router(config-port-map)#
```

■ port access-map

関連コマンド

コマンド	説明
action	パケットの action 句を設定します。
match	VLAN アクセス マップ シーケンスの ACL を 1 つまたは複数選択して、match 句を指定します。

port-channel load-balance

バンドル内のポートの負荷分散方式を設定するには、**port-channel load-balance** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

port-channel load-balance *method*

no port-channel load-balance

シンタックスの説明	<i>method</i>	負荷分散方式。有効値の一覧については、「使用上のガイドライン」を参照してください。
-----------	---------------	---

コマンドのデフォルト	<i>method</i> は src-dst-ip です。
------------	---------------------------------------

コマンド モード	グローバル コンフィギュレーション (config)
----------	----------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン 有効な *method* 値は次のとおりです。

- **dst-ip** : 宛先 IP アドレス方式での負荷分散
- **dst-mac** : 宛先 MAC アドレス方式での負荷分散
- **dst-port** : 宛先ポート方式での負荷分散
- **src-dst-ip** : 送信元 XOR 宛先 IP アドレス方式での負荷分散
- **src-dst-mac** : 送信元 XOR 宛先 MAC アドレス方式での負荷分散
- **src-dst-port** : 送信元 XOR 宛先ポート方式での負荷分散
- **src-ip** : 送信元 IP アドレス方式での負荷分散
- **src-mac** : 送信元 MAC アドレス方式での負荷分散
- **src-port** : 送信元ポート方式での負荷分散

port-channel per-module load-balance コマンドを使用すると、モジュール単位でポート チャネルロードバランスをイネーブルまたはディセーブルにできます。

port-channel load-balance

次に負荷分散方式を **dst-ip** に設定する例を示します。

```
Router(config)# port-channel load-balance dst-ip
Router(config)#
```

次に特定のモジュールの負荷分散方式を設定する例を示します。

```
Router(config)# port-channel load-balance dst-ip module 2
Router(config)#
```

関連コマンド

コマンド	説明
interface port-channel	ポート チャネル仮想インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
port-channel per-module load-balance	モジュール単位で負荷分散をイネーブルにします。
show etherchannel	チャネルの EtherChannel 情報を表示します。

port-channel load-balance mpls

MPLS パケットに関してバンドル内のポートの負荷分散方式を設定するには、**port-channel load-balance mpls** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

port-channel load-balance mpls {label | label-ip}

no port-channel load-balance mpls

シンタックスの説明	label	label-ip
	パケットを分散するための MPLS ラベルの使用を指定します。詳細については、「使用上のガイドライン」を参照してください。	パケットを分散するための MPLS ラベルまたは IP アドレスの使用を指定します。詳細については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト **label-ip**

コマンドモード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

label を選択する場合、次の点に注意してください。

- MPLS ラベルが 1 つだけの場合、最後の MPLS ラベルが使用されます。
- MPLS ラベルが 2 つ以上ある場合、最後の 2 つの MPLS ラベル（5 つめのラベルまで）が使用されます。

label-ip を選択する場合、次の点に注意してください。

- IPv4 でラベルが 3 つ以下の場合、送信元 XOA または宛先 IP アドレスがパケットの分散に使用されます。
- MPLS ラベルが 4 つ以上ある場合、最後の 2 つの MPLS ラベル（5 つめのラベルまで）が使用されます。
- 非 IPv4 パケットの場合、負荷分散方式は **label** 方式と同じです。

例 次に、負荷分散方式を **label-ip** に設定する例を示します。

```
Router(config)# port-channel load-balance mpls label-ip
Router(config)#
```

関連コマンド

コマンド	説明
interface port-channel	ポート チャネル仮想インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
show etherchannel	チャネルの EtherChannel 情報を表示します。

port-channel min-links

チャンネルをアクティブにする前に、EtherChannel にバンドルされていなければならないポートの最小数を指定するには、**port-channel min-links** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

port-channel min-links *min-num*

no port-channel min-links

シンタックスの説明

min-num チャンネルをアクティブにする前に、チャンネルにバンドルしなければならないポートの最小数。有効値は 2 ~ 8 です。

コマンドのデフォルト

min-num は 1 です。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、LACP (802.3ad) ポートだけでサポートされます。複数の LACP セカンダリポートチャンネルを同一のチャンネル グループに含めることができます。このコマンドは、同一グループのすべてのポート チャンネルに適用されます。

使用可能なリンクが指定された数より少ない場合、ポート チャンネル インターフェイスがアクティブになりません。

show running-config コマンドを使用して、設定を確認します。

例

次に、チャンネルをアクティブにする前に、EtherChannel にバンドルしなければならないポートの最小数を指定する例を示します。

```
Router(config-if)# port-channel min-links 3
Router(config-if)#
```

関連コマンド

コマンド	説明
show running-config	モジュールまたはレイヤ 2 VLAN のステータスおよび設定を表示します。

port-channel per-module load-balance

モジュール単位で負荷分散をイネーブルにするには、**port-channel per-module load-balance** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

port-channel per-module load-balance

no port-channel per-module load-balance

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト ディセーブル

コマンド モード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン **port-channel load-balance method module slot** コマンドは、DFC システムだけでサポートされています。

port-channel per-module load-balance コマンドを使用すると、モジュール単位でポート チャネルロードバランスをイネーブルまたはディセーブルにできます。**port-channel per-module load-balance** コマンドを入力したあとに **port-channel load-balance method module slot** コマンドを入力して、特定のモジュールのロードバランス方式を指定できます。

例 次に、モジュール単位でロード バランスをイネーブルにする例を示します。

```
Router(config)# port-channel per-module load-balance
Router(config)#
```

関連コマンド	コマンド	説明
	interface port-channel	ポート チャネル仮想インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
	port-channel load-balance module	特定のモジュールで負荷分散をイネーブルにします。
	show etherchannel	チャネルの EtherChannel 情報を表示します。

power enable

モジュールに電源を投入するには、**power enable** コマンドを使用します。モジュールの電源を切断するには、このコマンドの **no** 形式を使用します。

power enable {module slot}

no power enable {module slot}

シンタックスの説明	module slot	モジュールのスロット番号を指定します。有効値については、「使用上のガイドライン」を参照してください。
------------------	--------------------	--

コマンドのデフォルト	イネーブル
-------------------	-------

コマンドモード	グローバル コンフィギュレーション (config)
----------------	----------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン **no power enable module slot** コマンドを入力してモジュールの電源を切断した場合、そのモジュールの設定は保存されません。

no power enable module slot コマンドを入力して空のスロットの電源を切断した場合、その設定は保存されます。

slot 引数はモジュール番号を指定します。*slot* の有効値は、使用するシャーシによって異なります。たとえば、13 スロット シャーシを使用している場合、モジュール番号の有効値は 1 ~ 13 です。

例 次に、電源が切断されているモジュールに電源を投入する例を示します。

```
Router(config)# power enable module 5
Router(config)#
```

次に、モジュールの電源を切断する例を示します。

```
Router(config)# no power enable module 5
Router(config)#
```

関連コマンド	コマンド	説明
	show power	パワー ステータスに関する情報を表示します。

power inline

インターフェイスのインライン パワーの管理モードを設定するには、**power inline** コマンドを使用します。

```
power inline {auto [max max-milliwatts]} | never | {static [max max-milliwatts]}
```

シンタックスの説明

auto	デバイス検出プロトコルをオンにして、検出されたデバイスに電力を供給します。
max <i>max-milliwatts</i>	(任意) ポートに接続されているデバイスが消費できる最大電力量を指定します。 有効値は、4000 ~ 16800 ミリワットです。
never	デバイス検出プロトコルをオフにして、デバイスへの電力供給を停止します。
static	システムの電力プールからポートに電力を割り当てます。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- **auto**
- *max-milli-watts* は、15,400 ミリワットです。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。
12.2(18)ZYA	このコマンドは、 <i>max-milliwatts</i> が 15400 から 16800 へ変更されました。

使用上のガイドライン

power inline コマンドを使用してインライン パワー サポートを設定する場合、次の点に注意してください。

- インライン パワー デバイスの自動検出およびポート インライン パワーの自動割り当てを設定するには、**auto** キーワードを入力します。
- インライン パワー デバイスの自動検出を設定し、固定インライン パワー割り当てを維持するには、**static** キーワードを入力します。
- ポートに割り当てる最大電力量を指定するには、**auto** または **static** キーワードのいずれかを入力し、そのあとに **max** キーワードおよび電力レベル (ミリワット) を入力します。
- **auto** キーワードが入力され、ポート上で CDP がイネーブルである場合、CDP をサポートするインライン パワー デバイスは、異なる電力レベルをネゴシエーションできます。
- インライン パワー デバイスの自動検出をディセーブルにするには、**never** キーワードを入力します。

例

次に、インターフェイスのインライン パワーをオフ モードに設定する例を示します。

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# switchport
Router(config-if)# power inline never
```

次に、システムの電力プールからポートに電力を割り当てる例を示します。

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# switchport
Router(config-if)# power inline static max 15000
```

関連コマンド

コマンド	説明
show power	パワー ステータスに関する情報を表示します。

power redundancy-mode

電源装置の冗長モードを設定するには、**power redundancy-mode** コマンドを使用します。

power redundancy-mode {combined | redundant}

シンタックスの説明

combined	非冗長モードを指定します（電源装置の出力が合計されます）。
redundant	冗長モードを指定します（いずれかの電源装置でシステムを稼働できます）。

コマンドのデフォルト

redundant

コマンドモード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、電源装置を非冗長モードに設定する例を示します。

```
Router(config)# power redundancy-mode combined
Router(config)#
```

次に、電源装置を冗長モードに設定する例を示します。

```
Router(config)# power redundancy-mode redundant
Router(config)#
```

関連コマンド

コマンド	説明
show power	パワー ステータスに関する情報を表示します。

priority-queue cos-map

受信および送信完全優先キューに CoS 値をマッピングするには、**priority-queue cos-map** コマンドを使用します。デフォルト マッピングに戻すには、このコマンドの **no** 形式を使用します。

```
priority-queue cos-map queue-id cos1 [cos2 [cos3 [cos4 [cos5 [cos6 [cos7 [cos8]]]]]]]
```

シンタックスの説明

<i>queue-id</i>	キュー番号。有効値は 1 です。
<i>cos1</i>	CoS 値。有効値は 0 ~ 7 です。
<i>...cos8</i>	(任意) CoS 値。有効値は、0 ~ 7 です。

コマンドのデフォルト

デフォルト マッピングはキュー 1 で、次の受信および送信完全優先キューで CoS 5 にマッピングされます。

- 1p1q4t 受信キュー
- 1p1q0t 受信キュー
- 1p1q8t 受信キュー
- 1p2q2t 送信キュー
- 1p3q8t 送信キュー
- 1p7q8t 送信キュー
- 1p3q1t 送信キュー
- 1p2q1t 送信キュー

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

完全優先キューに CoS 値をマッピングする場合、次の点に注意してください。

- キュー番号は、常に **1** です。
- キューにマッピングする、最大 8 つの CoS 値を入力できます。

例

次に、ギガビットイーサネットポート 1/1 の完全優先キューに、CoS 値 7 をマッピングする例を示します。

```
Router(config-if)# priority-queue cos-map 1 7
Router(config-if)#
```

関連コマンド

コマンド	説明
show queueing interface	キューイング情報を表示します。

priority-queue queue-limit

インターフェイス上にプライオリティ キュー サイズを設定するには、**priority-queue queue-limit** コマンドを使用します。

priority-queue queue-limit weight

シンタックスの説明	<i>weight</i> プライオリティ キュー サイズの重み。有効値は、1 ~ 100% です。
------------------	--

コマンドのデフォルト	デフォルト設定は次のとおりです。 <ul style="list-style-type: none"> • グローバル QoS がイネーブルの場合 : 15 • グローバル QoS がディセーブルの場合 : 0
-------------------	---

コマンド モード	インターフェイス コンフィギュレーション (config-if)
-----------------	----------------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン	このコマンドをサポートするモジュールのリストについては、『 <i>Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY</i> 』を参照してください。
-------------------	---

例	次に、プライオリティ キューに使用可能なバッファ スペースを割り当てる例を示します。 <pre>Router(config-if)# priority-queue queue-limit 15 Router(config-if)#</pre>
----------	--

関連コマンド	コマンド	説明
	show queueing interface	キューイング情報を表示します。

private-vlan

PVLAN、および PVLAN とセカンダリ VLAN のアソシエーションを設定するには、**private-vlan** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

private-vlan {isolated | community | primary}

private-vlan association secondary-vlan-list | {add secondary-vlan-list} |
{remove secondary-vlan-list}

no private-vlan {isolated | community | primary}

no private-vlan association

シンタックスの説明

isolated	VLAN を隔離 PVLAN として指定します。
community	VLAN をコミュニティ PVLAN として指定します。
primary	VLAN をプライマリ PVLAN として指定します。
association	セカンダリ VLAN とプライマリ VLAN とのアソシエーションを作成します。
<i>secondary-vlan-list</i>	セカンダリ VLAN の番号
add	セカンダリ VLAN をプライマリ VLAN に対応付けます。
remove	セカンダリ VLAN とプライマリ VLAN とのアソシエーションをクリアします。

コマンドのデフォルト

PVLAN は設定されていません。

コマンド モード

config-VLAN サブモード

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

PVLAN をポート セキュリティ ポートには設定できません。

ポートセキュリティが設定されたポートで **pvlan** コマンドを入力すると、次のエラー メッセージが表示されます。

```
Command rejected: Gix/y is Port Security enabled port.
```

12 個のポートからなるグループ (1 ~ 12、13 ~ 24、25 ~ 36、および 37 ~ 48) 内のポートの 1 つがトランクや SPAN の宛先、または混合モードプライベート VLAN ポートの場合は、ポートを隔離 VLAN ポートまたはコミュニティ VLAN ポートとして設定しないでください。1 つのポートがトランクや SPAN の宛先、または混合モードプライベート VLAN ポートの場合は、12 ポート中の他のポートの隔離 VLAN またはコミュニティ VLAN 設定は非アクティブになります。ポートを再度アクティブにするには、隔離 VLAN またはコミュニティ VLAN のポート設定を削除し、**shutdown** および **no shutdown** コマンドを入力します。

**注意**

PVLAN (プライマリまたはセカンダリ) 上の **config-vlan** モードで **shutdown** コマンドを入力して、次に **no shutdown** コマンドを入力すると、PVLAN タイプおよびアソシエーション情報が削除されます。VLAN が PVLAN になるよう再設定する必要があります。

**(注)**

この制限事項は WS-X6548-RJ-45 および WS-X6548-RJ-21 を除くイーサネット 10-Mb、10/100-Mb、および 100-Mb モジュールに適用されます。

VLAN 1 または VLAN 1001 ~ 1005 を PVLAN として設定することはできません。

VTP は PVLAN をサポートしません。PVLAN ポートを使用するデバイスごとに、PVLAN を設定する必要があります。

secondary-vlan-list 引数には、スペースを挿入できません。複数のカンマ区切り項目を含めることができます。各項目として入力できるのは、単一の PVLAN ID または PVLAN ID のハイフンで連結した範囲です。*secondary-vlan-list* パラメータには、複数のコミュニティ VLAN ID を含めることができます。

secondary-vlan-list 引数には、1 つの隔離 VLAN ID だけを含めることができます。PVLAN は、VLAN 番号ペアの共通のセットを特徴とするプライベートポートのセットです。各ペアは、少なくとも 2 つの特別単方向 VLAN で構成され、ルータと通信するために隔離ポートとポートのコミュニティの一方または両方によって使用されます。

隔離 VLAN は、混合モードポートと通信するために隔離ポートによって使用される VLAN です。隔離 VLAN のトラフィックは、同じ VLAN 内のその他のすべてのプライベートポート上でブロックされます。このトラフィックを受信できるのは、対応するプライマリ VLAN に割り当てられた標準トランクポートおよび混合モードポートだけです。

混合モードポートは、プライマリ VLAN に割り当てられたプライベートポートとして定義されます。

プライマリ VLAN は、トラフィックをルータからプライベートポート上のカスタマーエンドステーションへ伝送する VLAN として定義されます。

コミュニティ VLAN は、コミュニティポート間で、およびコミュニティポートから対応するプライマリ VLAN 上の混合モードポートに、トラフィックを伝送する VLAN として定義されます。

複数のコミュニティ VLAN が許可される場合、隔離された *vlan-id* は 1 つだけ指定できます。隔離 VLAN およびコミュニティ VLAN は、1 つの VLAN にだけ対応付けることができます。対応付けられた VLAN リストには、プライマリ VLAN が含まれてはなりません。同様に、すでにプライマリ VLAN に対応付けられた VLAN は、プライマリ VLAN として設定できません。

コンフィギュレーション VLAN サブモードを終了しないと、**private-vlan** コマンドは有効になりません。

プライマリまたはセカンダリ VLAN を削除する場合、VLAN と対応付けられるポートは非アクティブとなります。

設定に関する注意事項については、『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*』を参照してください。

例

次に、プライマリ VLAN 14、隔離 VLAN 19、およびコミュニティ VLAN 20 ~ 21 間の PVLAN 関係を作成する例を示します。

```
Router(config) # vlan 19
Router(config-vlan) # private-vlan isolated
Router(config) # vlan 20
Router(config-vlan) # private-vlan community
Router(config-vlan) # private-vlan community
Router(config) # vlan 14
Router(config-vlan) # private-vlan primary
Router(config-vlan) # private-vlan association 19-21
```

次に、隔離 VLAN およびコミュニティ VLAN 20 を PVLAN アソシエーションから削除する例を示します。

```
Router(config) # vlan 14
Router(config-vlan) # private-vlan association remove 18,20
Router(config-vlan) #
```

次に、PVLAN 関係を削除し、プライマリ VLAN を削除する例を示します。対応付けられたセカンダリ VLAN は削除されません。

```
Router(config-vlan) # no private-vlan 14
Router(config-vlan) #
```

関連コマンド

コマンド	説明
show vlan	VLAN 情報を表示します。
show vlan private-vlan	PVLAN 情報を表示します。

private-vlan mapping

プライマリ VLAN とセカンダリ VLAN のマッピングを作成して、両方の VLAN で同じプライマリ VLAN SVI を共有できるようにするには、**private-vlan mapping** コマンドを使用します。SVI からすべての PVLAN マッピングを削除するには、このコマンドの **no** 形式を使用します。

```
private-vlan mapping {[secondary-vlan-list | {add secondary-vlan-list} |
  {remove secondary-vlan-list}}}
```

```
no private-vlan mapping
```

シンタックスの説明	
<i>secondary-vlan-list</i>	(任意) プライマリ VLAN にマッピングするセカンダリ VLAN の VLAN ID
add	(任意) セカンダリ VLAN をプライマリ VLAN にマッピングします。
remove	(任意) セカンダリ VLAN とプライマリ VLAN との間のマッピングを削除します。

コマンドのデフォルト PVLAN SVI マッピングは設定されていません。

コマンド モード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン **private-vlan mapping** コマンドは、PISA 上のソフトウェアでスイッチングされるトラフィックに影響します。

secondary-vlan-list 引数にはスペースを挿入できません。複数のカンマ区切り項目を含めることができます。各項目として入力できるのは、単一の PVLAN ID または PVLAN ID のハイフンで連結した範囲です。

このコマンドは、プライマリ VLAN のインターフェイス コンフィギュレーション モードで有効です。

プライマリ VLAN の SVI はレイヤ 3 で作成されます。

セカンダリ VLAN で受信されたトラフィックは、プライマリ VLAN の SVI によってルーティングされます。

既存のセカンダリ VLAN の SVI は機能せず、このコマンドが入力されたあとはダウンしていると見なされます。

セカンダリ SVI は、1 つのプライマリ SVI にだけマッピングできます。プライマリ VLAN をセカンダリ VLAN として設定した場合、このコマンドで指定されたすべての SVI はダウン状態になります。

有効なレイヤ 2 アソシエーションのない 2 つの VLAN 間のマッピングを設定しても、マッピング設定は有効になりません。

例

次に、VLAN 20 のインターフェイスを VLAN 18 の SVI にマッピングする例を示します。

```
Router(config)# interface vlan 18
Router(config-if)# private-vlan mapping 18 20
Router(config-if)#
```

次に、PVLAN 303 ~ 307、309、および 440 からのセカンダリ VLAN 入力トラフィックのルーティングを許可して、設定を確認する例を示します。

```
Router# configure terminal
Router(config)# interface vlan 202
Router(config-if)# private-vlan mapping add 303-307,309,440
Router(config-if)# end
Router# show interfaces private-vlan mapping
Interface Secondary VLAN Type
-----
vlan202    303          community
vlan202    304          community
vlan202    305          community
vlan202    306          community
vlan202    307          community
vlan202    309          community
vlan202    440          isolated
Router#
```

次に、追加する VLAN がすでに VLAN 18 の SVI にマッピングされている場合に表示されるエラーメッセージの例を示します。まず、VLAN 18 の SVI からマッピングを削除する必要があります。

```
Router(config)# interface vlan 19
Router(config-if)# private-vlan mapping 19 add 21
Command rejected: The interface for VLAN 21 is already mapped as s secondary.
Router(config-if)#
```

次に、VLAN 19 の SVI からすべての PVLAN マッピングを削除する例を示します。

```
Router(config)# interface vlan 19
Router(config-if)# no private-vlan mapping
Router(config-if)#
```

関連コマンド

コマンド	説明
show interfaces private-vlan mapping	VLAN SVI の PVLAN マッピングに関する情報を表示します。
show vlan	VLAN 情報を表示します。
show vlan private-vlan	PVLAN 情報を表示します。

private-vlan synchronize

セカンダリ VLAN をプライマリ VLAN と同じインスタンスにマッピングするには、**private-vlan synchronize** コマンドを使用します。

private-vlan synchronize

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード MST コンフィギュレーション サブモード

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン MST コンフィギュレーション サブモードを終了するときに、対応付けられたプライマリ VLAN と同じインスタンスに VLAN をマッピングしていないと、警告メッセージにより、対応付けられたプライマリ VLAN と同じインスタンスにマッピングされていないセカンダリ VLAN のリストが表示されます。**private-vlan synchronize** コマンドは、すべてのセカンダリ VLAN を対応付けられたプライマリ VLAN と同じインスタンスに自動的にマッピングします。

例 次の例では、プライマリ VLAN 2 およびセカンダリ VLAN 3 が VLAN 2 に対応付けられ、すべての VLAN が CIST インスタンス 1 にマッピングされていると仮定します。また、プライマリ VLAN 2 だけのマッピングを変更しようとした場合の出力も示します。

```
Router(config)# spanning-tree mst configuration
Router(config-mst)# instance 1 vlan 2
Router(config-mst)# exit
These secondary vlans are not mapped to the same instance as their primary:
-> 3
```

次に、PVLAN 同期を初期化する例を示します。

```
Router(config-mst)# private-vlan synchronize
Router(config-mst)#
```

関連コマンド	コマンド	説明
	show	MST の設定を確認します。
	show spanning-tree mst	MST プロトコルに関する情報を表示します。

process-min-time percent

他のプロセスに対して CPU を解放する前に OSPF が必要とするプロセス時間の最小の割合を指定するには、**process-min-time percent** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

process-min-time percent *percent*

no process-min-time

シンタックスの説明

<i>percent</i>	他のプロセスに対して CPU を解放する前に使用される CPU プロセス時間の割合。有効値は、1 ~ 100 です。
----------------	--

コマンドのデフォルト

percent は、25 です。

コマンド モード

ルータ コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



(注) Cisco TAC の指導を受けた場合にだけ、このコマンドを使用してください。

このコマンドは、OSPFv2 および OSPFv3 でサポートされます。

process-min-time コマンドを使用して、プロセスの最大時間から起算する最小の割合を設定します。割合が超過すると、CPU 制御はプライオリティが高い方のプロセスに割り当てられる可能性があります。

process-max-time コマンドを使用して、プロセスの最大時間を設定します。**process-max-time** コマンドとともに **process-min-time** コマンドを使用してください。

例

次に、CPU を解放する前に使用される CPU プロセス時間の割合を設定する例を示します。

```
Router> configure terminal
Router(configure)# router ospf
Router(config-router)# process-min-time percent 35
Router(config-router)#
```

次に、デフォルト設定に戻す例を示します。

```
Router> configure terminal
Router(configure)# router rip
Router(config-router)# no process-min-time
Router(config-router)#
```

関連コマンド

コマンド	説明
process-max-time	プロセスが別のプロセスに自発的に移行する時間を設定します。

process-min-time percent

rcv-queue bandwidth

入力（受信）Weighted Round-Robin（WRR; 重み付けラウンドロビン）キューの帯域幅をスケジューリング重みにより定義するには、**rcv-queue bandwidth** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
rcv-queue bandwidth weight-1 ... weight-n
```

```
no rcv-queue bandwidth
```

シンタックスの説明

weight-1 ... weight-n WRR 重みを指定します。有効値は 0 ~ 255 です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- QoS がイネーブルの場合 - 4 : 255
- QoS がディセーブルの場合 - 255 : 1

コマンドモード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、Supervisor Engine2 が搭載された Catalyst 6500 シリーズスイッチではサポートされません。

このコマンドは、2q8t および 8q8t ポートだけでサポートされます。

設定できるキューの重みは最大で 7 つです。

例

次に、3 対 1 の帯域幅比率を割り当てる例を示します。

```
Router(config-if)# rcv-queue bandwidth 3 1
Router(config-if)#
```

関連コマンド

コマンド	説明
rcv-queue queue-limit	完全優先キューと標準受信キューの間のサイズ比を設定します。
show queueing interface	キューイング情報を表示します。

rcv-queue cos-map

CoS 値を標準受信キュー廃棄しきい値にマッピングするには、**rcv-queue cos-map** コマンドを使用します。マッピングを削除するには、このコマンドの **no** 形式を使用します。

```
rcv-queue cos-map queue-id threshold-id cos-1 ... cos-n
```

```
no rcv-queue cos-map queue-id threshold-id
```

シンタックスの説明

queue-id キュー ID。有効値は 1 です。

threshold-id しきい値 ID。有効値は 1 ~ 4 です。

cos-1 ... cos-n CoS 値。有効値は、0 ~ 7 です。

コマンドのデフォルト

表 2-30 に、デフォルト設定を示します。

表 2-30 デフォルトの CoS に対する標準受信キューマップ

キュー	しきい値	cos-map	キュー	しきい値	cos-map
QoS がディセーブルの場合			QoS がイネーブルの場合		
1	1	0,1, 2,3,4,5,6,7	1	1	0,1
1	2		1	2	2,3
1	3		1	3	4
1	4		1	4	6,7
2	1	5	2	1	5

コマンドモード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

cos-n 値は、モジュールおよびポート タイプによって定義されます。*cos-n* 値を入力する場合は、大きい値ほど高いプライオリティを示すことに注意してください。

このコマンドは、信頼されたポート上だけで使用してください。

受信キューのしきい値の設定方法については、『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide Release 12.2ZY*』の「QoS」の章を参照してください。

例

次に、標準受信キューのしきい値 1 に CoS 値 0 および 1 をマッピングする例を示します。

```
Router (config-if)# rcv-queue cos-map 1 1 0 1
  cos-map configured on: Gi1/1 Gi1/2
Router(config-if)#
```

関連コマンド

コマンド	説明
show queueing interface	キューイング情報を表示します。

rcv-queue queue-limit

完全優先キューと標準受信キューの間のサイズ比を設定するには、**rcv-queue queue-limit** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
rcv-queue queue-limit {q-limit-1} {q-limit-2}
```

```
no rcv-queue queue-limit
```

シンタックスの説明

<i>q-limit-1</i>	標準キューの重み。有効値は 1 ~ 100% です。
<i>q-limit-2</i>	完全優先キューの重み。有効値については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- 80 % (ロー プライオリティ)
- 20 % (完全優先)

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

1p1q8t 入力 LAN ポートを除き、有効な完全優先キューの重み値は 1 ~ 100% です。1p1q8t 入力 LAN ポートでは、完全優先キューの有効値は 3 ~ 100% です。

rcv-queue queue-limit コマンドは、ASIC 単位でポートを設定します。

ネットワークにおける完全優先トラフィックと標準トラフィックの配分（標準トラフィック 80%、完全優先トラフィック 20% など）を推定し、推定値をキューの重みに使用します。

例

次に、ギガビット イーサネット インターフェイス 1/2 に受信キュー サイズ比を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitethernet 1/2
Router(config-if)# rcv-queue queue-limit 75 15
Router(config-if)# end
Router#
```

関連コマンド

コマンド	説明
show queueing interface	キューイング情報を表示します。

rcv-queue random-detect

指定した受信キューについて最小および最大しきい値を指定するには、**rcv-queue random-detect** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
rcv-queue random-detect {max-threshold | min-threshold} queue-id threshold-percent-1
... threshold-percent-n
```

```
no rcv-queue random-detect {max-threshold | min-threshold} queue-id
```

シンタックスの説明

max-threshold	最大しきい値を指定します。
min-threshold	最小しきい値を指定します。
<i>queue-id</i>	キュー ID。有効値は 1 です。
<i>threshold-percent-1</i> <i>threshold-percent-n</i>	しきい値の重み。有効値は 1 ~ 100% です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- **min-threshold** : 80%
- **max-threshold** : 20%

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、1p1q8t および 8q8t ポートだけでサポートされます。

1p1q8t インターフェイスは、1 つの完全優先キューと、8 つのしきい値がある 1 つの標準キューを意味します。8q8t インターフェイスは、8 つのしきい値がある 8 つの標準キューを意味します。完全優先キューのしきい値は、設定できません。

しきい値には、それぞれ低および高しきい値があります。しきい値は受信キュー容量のパーセントです。

受信キューのしきい値の設定方法については、『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide Release 12.2ZY*』の「QoS」の章を参照してください。

例

次に、低プライオリティ受信キューのしきい値を設定する例を示します。

```
Router (config-if)# rcv-queue random-detect max-threshold 1 60 100
Router (config-if)#
```

関連コマンド

コマンド	説明
show queueing interface	キューイング情報を表示します。

rcv-queue threshold

1p1q4t および 1p1q0t インターフェイス上の標準受信キューに廃棄しきい値を設定するには、**rcv-queue threshold** コマンドを使用します。しきい値をデフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

rcv-queue threshold *queue-id* *threshold-percent-1* ... *threshold-percent-n*

no rcv-queue threshold

シンタックスの説明

<i>queue-id</i>	キュー ID。有効値は 1 です。
<i>threshold-percent-1</i> ...	しきい値。有効値は 1 ~ 100% です。
<i>threshold-percent-n</i>	

コマンドのデフォルト

1p1q4t および 1p1q0t のデフォルト設定は、次のとおりです。

- QoS は CoS が 5 のすべてのトラフィックを完全優先キューに割り当てます。
- QoS はその他のすべてのトラフィックを標準キューに割り当てます。

1q4t のデフォルト設定では、QoS はすべてのトラフィックを標準キューに割り当てます。

QoS がイネーブルの場合は、次のデフォルトのしきい値が適用されます。

- 1p1q4t インターフェイスの廃棄しきい値のデフォルト設定は、次のとおりです。
 - CoS 0、1、2、3、4、6、または 7 のフレームは、標準受信キューに送られます。
 - 標準受信キュー廃棄しきい値が 1 の場合、受信キュー バッファが 50% 以上満たされると、Catalyst 6500 シリーズスイッチは CoS 0 または 1 の着信フレームを廃棄します。
 - 標準受信キュー廃棄しきい値が 2 の場合、受信キュー バッファが 60% 以上満たされると、Catalyst 6500 シリーズスイッチは CoS 2 または 3 の着信フレームを廃棄します。
 - 標準受信キュー廃棄しきい値が 3 の場合、受信キュー バッファが 80% 以上満たされると、Catalyst 6500 シリーズスイッチは CoS 4 の着信フレームを廃棄します。
 - 標準受信キュー廃棄しきい値が 4 の場合、受信キュー バッファが 100% 満たされると、Catalyst 6500 シリーズスイッチは CoS 6 または 7 の着信フレームを廃棄します。
 - CoS 5 のフレームは、完全優先受信キュー（キュー 2）に送られます。完全優先受信キュー バッファが 100% 満たされた場合にだけ、Catalyst 6500 シリーズスイッチは着信フレームを廃棄します。
- 1p1q0t インターフェイスの廃棄しきい値のデフォルト設定は、次のとおりです。
 - CoS 0、1、2、3、4、6、または 7 のフレームは、標準受信キューに送られます。受信キュー バッファが 100% 満たされると、Catalyst 6500 シリーズスイッチは着信フレームを廃棄します。
 - CoS 5 のフレームは、完全優先受信キュー（キュー 2）に送られます。完全優先受信キュー バッファが 100% 満たされた場合にだけ、Catalyst 6500 シリーズスイッチは着信フレームを廃棄します。



(注)

100% のしきい値は、実際は、BPDU トラフィックを処理できるように、モジュールによって 98% に変更されます。BPDU しきい値は、出荷時に 100% に設定されています。

■ **rcv-queue threshold**

コマンド モード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン *queue-id* 値は、常に **1** です。

値 **10** は、バッファが 10% 満たされたときのしきい値を示します。

しきい値 **4** は常に 100% に設定してください。

受信しきい値が有効なのは、信頼状態が **trust cos** のポート上だけです。

1q4t の受信キュー テール廃棄しきい値を設定するには、**wrr-queue threshold** コマンドを使用します。

例 次に、ギガビット イーサネット インターフェイス 1/1 に受信キュー廃棄しきい値を設定する例を示します。

```
Router(config-if)# rcv-queue threshold 1 60 75 85 100
Router(config-if)#
```

関連コマンド	コマンド	説明
	show queueing interface	キューイング情報を表示します。
	wrr-queue threshold	1q4t および 2q2t インターフェイス上の標準受信キューおよび標準送信キューの廃棄しきい値パーセントを設定します。

reassign

別の実サーバへの接続を試みるまでに許容される、新規接続の未応答 SYN の最大数を定義するには、**reassign** コマンドを使用します。接続の最大数をデフォルト設定に変更するには、このコマンドの **no** 形式を使用します。

reassign threshold

no reassign

シンタックスの説明	<i>threshold</i>	別の実サーバに接続が割り当て直されるまでに、実サーバに送られる未応答 TCP SYN の数。有効値は 1 ~ 4 です。
------------------	------------------	--

コマンドのデフォルト *threshold* は 3 です。

コマンドモード 実サーバ コンフィギュレーション サブモード

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン *threshold* 値を指定しない場合は、再割り当てしきい値のデフォルト値が使用されます。

例 次に、再割り当てしきい値を定義する例を示します。

```
Router(config-if)# reassign 4
Router(config-if)#
```

次に、デフォルト値に戻す例を示します。

```
Router(config-if)# no reassign
Router(config-if)#
```

関連コマンド	コマンド	説明
	faildetect numconns	サーバ障害を示す条件を指定します。
	inservice (実サーバ)	Cisco IOS SLB 機能が使用する実サーバをイネーブルにします。
	retry	障害のあるサーバに接続を試みるまでの待機時間を定義します。
	maxconns (real server configuration submode)	実サーバへのアクティブ接続数を制限します。

redundancy

冗長コンフィギュレーション モードを開始するには、**redundancy** コマンドを使用します。このモードから、メイン CPU サブモードを開始して、2 つのスーパーバイザ エンジンで使用される設定を手動で同期化できます。

redundancy

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

冗長コンフィギュレーション モードを開始すると、次のオプションが使用可能になります。

- **exit** : 冗長コンフィギュレーション モードを終了します。
- **main-cpu** : メイン CPU サブモードを開始します。
- **no** : コマンドを否定するか、またはデフォルトを設定します。

メイン CPU サブモードから、**auto-sync** コマンドを使用して、メイン CPU に適用可能な冗長コマンドをすべて使用できます。

冗長モードのタイプを選択するには、**mode** コマンドを使用します。

NSF/SSO 冗長モードは IPv4 をサポートします。NSF/SSO 冗長モードは、IPv6、IPX、および MPLS をサポートしません。

例

次に、冗長モードを開始する例を示します。

```
Router (config)# redundancy
Router (config-r)#
```

次に、メイン CPU サブモードを開始する例を示します。

```
Router (config)# redundancy
Router (config-r)# main-cpu
Router (config-r-mc)#
```

関連コマンド

コマンド	説明
<code>auto-sync</code>	NVRAM 内のコンフィギュレーション ファイルの自動同期化をイネーブルにします。
<code>mode</code>	冗長モードを設定します。

redundancy force-switchover

アクティブからスタンバイへのスーパーバイザ エンジンのスイッチオーバーを強制するには、**redundancy force-switchover** コマンドを使用します。

redundancy force-switchover

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドを使用する前に、『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide Release 12.2ZY*』の「Performing a Fast Software Upgrade (FSU)」を参照して、さらに詳しい情報を入手してください。

redundancy force-switchover コマンドは、冗長スーパーバイザ エンジンの手動切り替えを行います。冗長スーパーバイザ エンジンが、新しい Cisco IOS イメージを稼働させる新しいアクティブ スーパーバイザ エンジンになります。モジュールがリセットされ、モジュール ソフトウェアが新しいアクティブ スーパーバイザ エンジンからダウンロードされます。

古いアクティブ スーパーバイザ エンジンが新しいイメージで再起動され、冗長スーパーバイザ エンジンになります。

例

次に、アクティブ スーパーバイザ エンジンからスタンバイ スーパーバイザ エンジンに手動で切り替える例を示します。

```
Router# redundancy force-switchover
Router#
```

関連コマンド

コマンド	説明
mode	冗長モードを設定します。
redundancy	冗長コンフィギュレーション モードを開始します。
show redundancy	RF 情報を表示します。

reload

Catalyst 6500 シリーズスイッチ全体をリロードするには、**reload** コマンドを使用します。

reload [*text* | **in** [*hh:mm*] [*text*] | **at** *hh:mm* [*month day* | *day month*] [*text*] | **cancel**]

シンタックスの説明

<i>text</i>	(任意) リロードの理由。1 ~ 255 文字のストリングを指定できます。
in [<i>hh:mm</i>]	(任意) 特定の期間、Catalyst 6500 シリーズスイッチのリロードを遅らせます。
at <i>hh:mm</i>	(任意) 指定された時刻 (24 時間方式のクロックを使用) で実行するように、Catalyst 6500 シリーズスイッチのリロードをスケジューリングします。
<i>month</i>	(任意) 月の名前。任意の文字数からなる一意のストリングです。
<i>day</i>	(任意) 日付の数字。有効値は 1 ~ 31 です。
cancel	(任意) スケジューリングされたリロードをキャンセルします。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

reload コマンドはシステムを停止します。エラー発生時に再起動するようにシステムが設定されている場合は、自動的に再起動します。**reload** コマンドは、設定情報をファイルに入力し、それをスタートアップ コンフィギュレーションに保存したあとに使用してください。

あとでリロードを実行するようにスケジュールする場合は (**in** キーワードを使用)、約 24 日以内にリロードを実行するようにする必要があります。

リロード時刻を指定するときに (**at** キーワードを使用) 月日を指定した場合は、指定された日時にリロードが実行されます。月日を指定しなかった場合、リロードは当日の指定された時刻 (指定された時刻が現在の時刻よりあとの場合) または翌日 (指定された時刻が現在の時刻よりも前の場合) に実行されます。00:00 を指定すると、リロードは午前 0 時にスケジューリングされます。リロードはおよそ 24 日以内に実行される必要があります。

コンフィギュレーションファイルを変更すると、Catalyst 6500 シリーズスイッチは、設定を保存するように要求します。存在しないスタートアップ コンフィギュレーションファイルを環境変数 CONFIG_FILE が示している場合は、保存動作中に、Catalyst 6500 シリーズスイッチによって保存を進めるかどうかの確認が要求されます。この状況で [yes] と応答すると、Catalyst 6500 シリーズスイッチはリロード時にセットアップモードを開始します。

at キーワードを使用するのは、(NTP、ハードウェアのカレンダー、または手動のいずれかで) Multilayer Switch Module (MSM) にシステムクロックが設定されている場合です。複数の MSM でリロードが同時に実行されるようスケジューリングするには、各 MSM の時刻を NTP によって同期化する必要があります。

スケジューリングされたリロードの情報を表示するには、**show reload** コマンドを使用します。

例

次に、Catalyst 6500 シリーズスイッチをただちにリロードする例を示します。

```
Router# reload
Router#
```

次に、Catalyst 6500 シリーズスイッチを 10 分後にリロードする例を示します。

```
Router# reload in 10
Router# Reload scheduled for 11:57:08 PDT Fri Apr 21 1996 (in 10 minutes)
Proceed with reload? [confirm]
Router#
```

次に、Catalyst 6500 シリーズスイッチを当日の午後 1 時にリロードする例を示します。

```
Router# reload at 13:00
Router# Reload scheduled for 13:00:00 PDT Fri Apr 21 1996 (in 1 hour and 2 minutes)
Proceed with reload? [confirm]
Router#
```

次に、Catalyst 6500 シリーズスイッチを 4 月 20 日の午前 2 時にリロードする例を示します。

```
Router# reload at 02:00 apr 20
Router# Reload scheduled for 02:00:00 PDT Sat Apr 20 1996 (in 38 hours and 9 minutes)
Proceed with reload? [confirm]
Router#
```

次に、リロードの保留をキャンセルする例を示します。

```
Router# reload cancel
%Reload cancelled.
Router#
```

関連コマンド

コマンド	説明
copy system:running-config nvram:startup-config	設定変更をスタートアップ コンフィギュレーションに保存します。
show reload	ルータのリロード ステータスを表示します。

remote command

Catalyst 6500 シリーズスイッチに最初にログインすることなく、スイッチ コンソールまたは指定したモジュール上で直接 Catalyst 6500 シリーズスイッチ コマンドを実行するには、**remote command** コマンドを使用します。

remote command **{{module num} | standby-rp | switch} command**

シンタックスの説明

module num	アクセスするモジュールを指定します。有効値については、「使用上のガイドライン」を参照してください。
standby-rp	スタンバイ ルート プロセッサを指定します。
switch	アクティブ スイッチ プロセッサを指定します。
command	実行するコマンド

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

module num キーワードおよび引数は、モジュール番号を指定します。有効値は、使用するシャーシによって異なります。たとえば、13 スロット シャーシを使用している場合、モジュール番号の有効値は 1 ~ 13 です。**module num** キーワードおよび引数はスタンバイ スーパーバイザ エンジン上だけでサポートされます。

remote command switch コマンドを実行すると、プロンプトは Switch-sp# に変更されます。

このコマンドは、スーパーバイザ エンジンだけでサポートされています。

このコマンドはコマンド補完機能をサポートしていませんが、コマンドの短縮形を使用できます (たとえば、**show** の代わりに **sh** を入力できます)。

例

次に、スタンバイ ルート プロセッサから **show calendar** コマンドを実行する例を示します。

```
Router# remote command standby-rp show calendar
Switch-sp#
09:52:50 UTC Mon Nov 12 2001
Router#
```

関連コマンド

コマンド	説明
remote login	Catalyst 6500 シリーズ スイッチ コンソールまたは特定のモジュールにアクセスします。

remote login

Catalyst 6500 シリーズ スイッチ コンソールまたは特定のモジュールにアクセスするには、**remote login** コマンドを使用します。

```
remote login {{module num} | standby-rp | switch}
```

シンタックスの説明

module num	アクセスするモジュールを指定します。有効値については、「使用上のガイドライン」を参照してください。
standby-rp	スタンバイ ルート プロセッサを指定します。
switch	アクティブ スイッチ プロセッサを指定します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



注意

attach または **remote login** コマンドを入力し、スイッチから別のコンソールにアクセスする場合、グローバルまたはインターフェイス コンフィギュレーション モードのコマンドを入力すると、スイッチがリセットすることがあります。

module num キーワードおよび引数は、モジュール番号を指定します。有効値は、使用するシャーシによって異なります。たとえば、13 スロット シャーシを使用している場合、モジュール番号の有効値は 1 ~ 13 です。**module num** キーワードおよび引数はスタンバイ スーパーバイザ エンジン上だけでサポートされます。

remote login module num コマンドを実行すると、接続しているモジュールのタイプに応じて、プロンプトは変更されます。

remote login standby-rp コマンドを実行すると、プロンプトは Router-sdby# に変更されます。

remote login switch コマンドを実行すると、プロンプトは Switch-sp# に変更されます。

remote login module num コマンドは、**attach** コマンドと同一です。

セッションは次の 2 つの方法で終了できます。

- 次のように、**exit** コマンドを入力します。

```
Switch-sp# exit
```

```
[Connection to Switch closed by foreign host]
Router#
```

- 次のように、**Ctrl-C** を 3 回押します。

```
Switch-sp# ^C
Switch-sp# ^C
Switch-sp# ^C
Terminate remote login session? [confirm] y
[Connection to Switch closed by local host]
Router#
```

例

次に、特定のモジュールにリモート ログインを実行する例を示します。

```
次に、Router# remote login module 1
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
```

```
Switch-sp#
```

Catalyst 6500 シリーズスイッチのプロセッサにリモート ログインを実行する例を示します。

```
次に、Router# remote login switch
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
Switch-sp#
```

スタンバイ ルート プロセッサにリモート ログインを実行する例を示します。

```
Router# remote login standby-rp
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
Router-sdby#
```

関連コマンド

コマンド	説明
attach	リモートから特定のモジュールに接続します。

remote-span

VLAN を RSPAN VLAN として設定するには、**remote-span** コマンドを使用します。RSPAN の指定を削除するには、このコマンドの **no** 形式を使用します。

remote-span

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

config-VLAN (config-vlan)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、VLAN データベース モードではサポートされません。

show vlan remote-span コマンドを入力すると、Catalyst 6500 シリーズ スイッチの RSPAN VLAN を表示できます。

例

次に、RSPAN VLAN として VLAN を設定する例を示します。

```
Router(config-vlan)# remote-span  
Router(config-vlan)
```

次に、RSPAN の指定を削除する例を示します。

```
Router(config-vlan)# no remote-span  
Router(config-vlan)
```

関連コマンド

接続	説明
show vlan remote-span	RSPAN VLAN のリストを表示します。

reset

提示された新しい VLAN データベースを放棄し、VLAN コンフィギュレーション モードのまま、提示された新しい VLAN データベースを現在の VLAN データベースにリセットするには、**reset** コマンドを使用します。

reset

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード VLAN コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、提示された新規 VLAN データベースを放棄して、現在の VLAN データベースにリセットする例を示します。

```
Router(vlan)# reset
RESET completed.
Router(vlan)#
```

retry

障害のあるサーバに接続を試みるまでの待機時間を定義するには、**retry** コマンドを使用します。接続の再割り当てしきい値およびクライアントしきい値をデフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

retry *retry-value*

no **retry**

シンタックスの説明	<i>retry-value</i>
	サーバ障害が検出されてからサーバへの新規接続を試みるまでの待機時間 (秒)。有効値は 1 ~ 3600 です

コマンドのデフォルト	<i>retry-value</i> は 60 です。
------------	------------------------------------

コマンド モード	実サーバ コンフィギュレーション サブモード
----------	------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、再試行タイマーを定義する例を示します。

```
Router(config-if)# retry 145
Router(config-if)#
```

次に、デフォルト値に戻す例を示します。

```
Router(config-if)# no retry
Router(config-if)#
```

関連コマンド	コマンド	説明
	faildetect numconns	サーバ障害を示す条件を指定します。
	inservice (実サーバ)	Cisco IOS SLB 機能が使用する実サーバをイネーブルにします。
	maxconns (real server configuration submode)	実サーバへのアクティブ接続数を制限します。

revision

MST コンフィギュレーションのリビジョン番号を設定するには、**revision** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

revision version

no revision

シンタックスの説明	<i>version</i> 設定のリビジョン番号を指定します。有効値は 0 ~ 65,535 です。
-----------	---

コマンドのデフォルト	<i>version</i> は 0 です。
------------	------------------------

コマンドのデフォルト	MST コンフィギュレーション サブモード
------------	-----------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン 設定が同じで、リビジョン番号が異なる 2 つの Catalyst 6500 シリーズスイッチは、2 つの異なるリージョンに属していると思なされます。



注意

MST コンフィギュレーションのリビジョン番号を設定するのに **revision** コマンドを使用する場合には注意が必要です。設定を間違えると、スイッチは異なるリージョンに置かれる可能性があります。

例 次に、MST コンフィギュレーションのリビジョン番号を設定する例を示します。

```
Router (config-mst) # revision 5
Router (config-mst) #
```

関連コマンド	コマンド	説明
	instance	1 つまたは一連の VLAN を MST インスタンスにマッピングします。
	name (MST configuration submode)	MST リージョン名を設定します。
	show	MST の設定を確認します。
	show spanning-tree	スパンニングツリー ステートに関する情報を表示します。
	spanning-tree mst configuration	MST コンフィギュレーション サブモードを開始します。

rmon alarm

アラームを任意の Management Information Base (MIB; 管理情報ベース) オブジェクトで設定するには、**rmon alarm** コマンドを使用します。アラームをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
rmon alarm number variable interval {delta | absolute} rising-threshold value
[event-number] falling-threshold value [event-number] [owner string]
```

```
no rmon alarm number
```

シンタックスの説明

<i>number</i>	remote network monitor (RMON; リモート ネットワーク モニタ) MIB の alarmTable 内の alarmIndex と同じアラーム番号。有効値は 1 ~ 65,535 です。
<i>variable</i>	モニタする MIB オブジェクト。この値は RMON MIB の alarmTable で使用される alarmVariable に変換されます。
<i>interval</i>	アラームが MIB 変数をモニタする秒数。この値は、RMON MIB の alarmTable で使用される alarmInterval と同じです。有効値は 1 ~ 4,294,967,295 です。
delta	MIB 変数間の変更を指定します。この値は、RMON MIB の alarmTable 内の alarmSampleType に影響します。
absolute	各 MIB 変数を直接指定します。この値は、RMON MIB の alarmTable 内の alarmSampleType に影響します。
rising-threshold <i>value</i>	アラームがトリガーされる値を指定します。有効値は -2,147,483,648 ~ 2,147,483,647 です。
<i>event-number</i>	(任意) 上限および下限しきい値の限度を超過したときにトリガーされるイベント番号。この値は、RMON MIB の alarmTable 内の alarmRisingEventIndex または alarmFallingEventIndex と同じです。有効値は 1 ~ 65,535 です。
falling-threshold <i>value</i>	アラームがリセットされる値を指定します。有効値は -2,147,483,648 ~ 2,147,483,647 です。
owner string	(任意) アラームの所有者を指定します。この値は、RMON MIB の alarmTable 内の alarmOwner と同じです。

コマンド モード

アラームは設定されていません。

コマンドのデフォルト

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

エン트리 シーケンスのあとで、MIB オブジェクトをドット付き 10 進数として指定する必要があります (ifEntry.10.1 など)。変数名やインスタンス (ifInOctets.1 など)、またはドット付き 10 進表記全体を指定することはできません。引数は、entry.integer.instance の形式で指定する必要があります。

RMON アラームをディセーブルにするには、設定されたアラームごとに、このコマンドの **no** 形式を入力する必要があります。たとえば、**no rmon alarm 1** コマンドを入力します。1 は削除するアラームを示します。

RMON アラーム グループの詳細については、RFC 1757 を参照してください。

例に示した設定では、アラームはディセーブルになるまで 20 秒に 1 回、MIB 変数 *ifEntry.20.1* をモニタし、この変数の上昇または下降の変化をチェックします。*ifEntry.20.1* 値が 15 以上の MIB カウンタの増加を示した場合は (たとえば 100000 から 100015)、アラームがトリガーされます。アラームはイベント番号 1 をトリガーします。イベントの設定には、**rmon event** コマンドを使用します。設定可能なイベントには、ログ エントリまたは SNMP トラップなどがあります。*ifEntry.20.1* 値の変化が 0 (下限しきい値が 0) の場合、アラームはリセットされ、再度トリガーできます。

例

次に、RMON アラームを設定する例を示します。

```
Router(config)# rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1
falling-threshold 0
owner jjohnson
```

関連コマンド

コマンド	説明
rmon	イーサネットインターフェイス上で RMON をイネーブルにします。
rmon event	RMON イベント番号に対応付けられた RMON イベントテーブルでイベントを追加または削除します。
show rmon	ルータの現在の RMON エージェント ステータスを表示します。

rmon event

RMON イベント番号に対応付けられた RMON イベント テーブルでイベントを追加または削除するには、**rmon event** コマンドを使用します。インターフェイス上で RMON をディセーブルにするには、このコマンドの **no** 形式を使用します。

rmon event *number* [**log**] [**trap community**] [**description string**] [**owner string**]

no rmon event *number*

シンタックスの説明

number	RMON MIB の eventTable 内の eventIndex と同じである、割り当て済みイベント番号を指定します。有効値は 1 ~ 65535 です。
log	(任意) イベントがトリガーされた場合に RMON ログ エントリを生成して、RMON MIB の eventType を log または log-and-trap に設定します。
trap community	(任意) このトラップに使用される SNMP コミュニティ スtring を指定します。
description string	(任意) RMON MIB の eventTable 内のイベント説明と同じイベント説明を指定します。
owner string	(任意) RMON MIB の eventTable 内の eventOwner と同じである、このイベントの所有者を指定します。

コマンドのデフォルト

アラームは設定されていません。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

RMON MIB の詳細については、RFC 1757 を参照してください。

この行の RMON MIB の eventType の設定を snmp-trap または log-and-trap に設定するには、**trap community** キーワードおよび引数を使用します。この値は、RMON MIB の eventTable 内の eventCommunityValue と同じです。

例

次に、イベントを RMON イベント テーブルに追加する例を示します。

```
Router(config)# rmon event 1 log trap eventtrap description "High ifOutErrors" owner
sdurham
```

この設定例では、High ifOutErrors として定義された RMON イベント番号 1 を作成し、アラームによるイベント トリガー時にログ エントリを生成します。ユーザ sdurham は、このコマンドによってイベント テーブルに作成された行を所有します。また、この設定では、イベント トリガー時に SNMP トラップが生成されます。

関連コマンド

コマンド	説明
<code>rmon</code>	イーサネットインターフェイス上で RMON をイネーブルにします。
<code>rmon alarm</code>	アラームを任意の MIB オブジェクトで設定します。
<code>show rmon</code>	ルータの現在の RMON エージェント ステータスを表示します。

route-converge-interval

古い FIB エントリの削除が開始するまでの間隔を設定するには、**route-converge-interval** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

route-converge-interval seconds

シンタックスの説明

seconds 古い FIB エントリの削除が開始するまでの間隔。有効値は 60 ~ 3600 秒です。

コマンドのデフォルト

seconds は **120** 秒 (2 分) です。

コマンドモード

メイン CPU サブモード

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ルート コンバージェンス遅延の間隔は、スイッチオーバー時にルーティング プロトコルを再始動する際に必要なルート コンバージェンス時間をシミュレートするのに必要です。

例

次に、ルート コンバージェンス遅延の間隔を設定する例を示します。

```
Router(config)# redundancy
Router(config-red)# main-cpu
Router(config-red-main)# route-converge-interval 90
Router(config-red-main)#
```

次に、ルート コンバージェンス遅延の間隔をデフォルトに戻す例を示します。

```
Router(config)# redundancy
Router(config-red)# main-cpu
Router(config-red-main)# no route-converge-interval
Router(config-red-main)#
```

関連コマンド

コマンド	説明
redundancy	冗長コンフィギュレーション モードを開始します。

router

ルーティングプロセスをイネーブルにするには、**router** コマンドを使用します。ルーティングプロセスを終了するには、このコマンドの **no** 形式を使用します。

```
router {bgp as-num} | {eigrp as-num} | {isis process-id} | {ospf process-id [vrf vrf-id]}
```

```
no router ospf process-id
```

シンタックスの説明

bgp as-num	自律 BGP システム番号を指定します。有効値は、1 ~ 65,535 です。
eigrp as-num	自律 EIGRP システム番号を指定します。有効値は、1 ~ 65,535 です。
isis routing-area-tag	International Organization of Standardization (ISO; 国際標準化機構) ルーティング エリア指定を指定します。
ospf process-id	ルーティングプロセス用に内部的に使用される ID パラメータを指定します。有効値は、1 ~ 65,535 です。
vrf vrf-id	(任意) VRF インスタンス名を指定します。

コマンドのデフォルト

定義済みまたはイネーブルの OSPF ルーティング プロセスはありません。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

process-id を指定した場合、値はローカルに割り当てられます。この値は任意の自然数です。各 OSPF ルーティングプロセスには、一意の値が割り当てられます。

各ルータでは、複数の OSPF ルーティングプロセスを指定できます。

例

次に、OSPF ルーティングプロセスを設定して、プロセス番号 109 を割り当てる例を示します。

```
Router(config)# router ospf 109
Router(config)#
```

次に、OSPF ルーティングプロセスを設定して、特定の VRF インスタンスにプロセス番号 109 を割り当てる例を示します。

```
Router(config)# router ospf 109 vrf 109
Router(config)#
```

関連コマンド

コマンド	説明
nsf	Cisco NSF をイネーブルにし、設定します。

scheduler allocate

プロセス タスク用に CPU 時間を保証するには、**scheduler allocate** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

scheduler allocate interrupt-time process-time

no scheduler allocate

シンタックスの説明

<i>interrupt-time</i>	1 つのネットワーク割り込みが発生している状況で、高速スイッチングの最大所要時間を制限する整数（マイクロ秒）を指定します。有効値は 400 ～ 60,000 マイクロ秒です。
<i>process-time</i>	ネットワーク割り込みがディセーブルの場合に、プロセス レベルにおける最小所要時間を保証する整数（マイクロ秒）を指定します。有効値は 100 ～ 4000 です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- *interrupt-time* は **4000** マイクロ秒です。
- *process-time* は **800** マイクロ秒です。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



注意

デフォルトの設定は変更しないことを推奨します。

scheduler allocate コマンドを引数なしで入力するのは、**no scheduler allocate** または **default scheduler allocate** コマンドを入力するのと同様です。

例

次に、CPU 時間の 20% をプロセス タスクで使用可能にする例を示します。

```
Router-config# scheduler allocate 2000 500
Router-config#
```

service counters max age

統計情報を取得する間隔を設定するには、**service counters max age** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

service counters max age seconds

no service counters max age

シンタックスの説明	<i>seconds</i>	CLI または SNMP から取得された統計情報の有効期限。有効値は、0 ~ 60 秒です。
------------------	----------------	--

コマンドのデフォルト *seconds* は、5 秒です。

コマンド モード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



(注) 統計情報を取得する間隔を、デフォルトの設定 (5 秒) より短縮する場合、トラフィック輻輳により SNMP (SNMP バルク) 取得が頻繁に行われる可能性があります。

6 ~ 9 秒の間で *seconds* 値を設定する場合、カウンタの更新はデフォルトの 10 秒で行われ、システムが統計情報の算出に関わりすぎないようにしています。統計情報の収集で 20% 以上の CPU 時間が使用されている場合、統計情報がカウンタの更新間のスリープを処理する時間はシステムによって自動的に増加されます。

0 ~ 5 秒の間で *seconds* 値を設定する場合、CPU ユーティリティが低いと、設定された遅延秒でカウンタの更新が行われ、システムのロードは 20% に保たれます。

たとえば、統計情報の計算時間が 4 秒の場合、サービスの最大時間を 5 秒にしていると、ユーザの設定に関係なく、統計情報の収集間の時間は 20 秒になり (収集時間は、5 の倍数の時間に相当します)、統計情報の収集で CPU ユーティリティを増加させません。

例 次に、統計情報を取得する間隔を設定する例を示します。

```
Router(config)# service counters max age 10
Router(config)#
```

次に、デフォルト設定に戻す例を示します。

```
Router(config)# no service counters max age
Router(config)#
```

service-policy

ポリシーマップをインターフェイスに付加するには、**service-policy** コマンドを使用します。インターフェイスからポリシー マップを削除するには、このコマンドの **no** 形式を使用します。

service-policy {input | output} *policy-map-name*

no service-policy {input | output} *policy-map-name*

シンタックスの説明

input *policy-map-name* 設定済みの入力ポリシーマップを指定します。

output *policy-map-name* 設定済みの出力ポリシーマップを指定します。

コマンドのデフォルト

ポリシーマップは対応付けられていません。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

EtherChannel のメンバーであるポートにサービス ポリシーを付加しないでください。

CLI を使用すると、OC-12 ATM OSM の WAN ポートおよびチャネライズド OSM の WAN ポートに PFC ベースの QoS を設定できますが、PFC ベースの QoS はこれらの OSM の WAN ポートではサポートされていません。OSM は、Supervisor Engine32 PISA が搭載された Catalyst 6500 シリーズ スイッチではサポートされません。

PFC QoS は、VLAN インターフェイス上だけで **output** キーワード (任意) をサポートします。VLAN インターフェイスには、入力ポリシーマップおよび出力ポリシーマップの両方を対応付けられます。

例

次に、ポリシーマップをファスト イーサネット インターフェイスに付加する例を示します。

```
Router(config)# interface fastethernet 5/20
Router(config-if)# service-policy input pmap1
Router(config-if)#
```

関連コマンド

コマンド	説明
class-map	QoS クラス マップを設定するための QoS クラス マップ コンフィギュレーション モードにアクセスします。
policy-map	QoS ポリシー マップを設定するための QoS ポリシー マップ コンフィギュレーション モードにアクセスします。

service-policy (control-plane)

集約コントロールプレーン サービスのコントロールプレーンにポリシーマップを付加するには、**service-policy** コマンドを使用します。コントロールプレーンからサービス ポリシーを削除するには、このコマンドの **no** 形式を使用します。

service-policy {input | output} *policy-map-name*

no service-policy {input | output} *policy-map-name*

シンタックスの説明	パラメータ	説明
	input	指定したサービス ポリシーをコントロールプレーンに入るパケットに適用します。
	output	指定したサービス ポリシーをコントロールプレーンを出るパケットに適用して、Catalyst 6500 シリーズ スイッチでパケットを自動的に廃棄できるようにします。
	<i>policy-map-name</i>	付加されるサービス ポリシーマップ (policy-map コマンドを使用して作成した) の名前

コマンドのデフォルト サービス ポリシーは指定されません。

コマンド モード コントロールプレーン コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン *policy-map-name* は最大 40 文字の英数字です。

control-plane コマンドを入力したあと、**service-policy** コマンドを使用して QoS ポリシーを設定してください。このポリシーは集約コントロールプレーン サービスのコントロールプレーン インターフェイスに付加されて、プロセス レベルに入るパケットの数やレートを制御します。

サイレント モードでは、Cisco IOS ソフトウェアを実行しているルータは、システム メッセージを送信せずに動作できます。ルータ宛のパケットが何らかの理由で廃棄された場合も、ユーザはエラー メッセージを受信しません。エラー メッセージを生成しないイベントは次のとおりです。

- ルータが監視していないポートに送信されるトラフィック
- 変造された要求なので拒否された正当なアドレスとポートへの接続

例 次に、送信元アドレス 10.1.1.1 および 10.1.1.2 の信頼できるホストが Telnet パケットを無制限にコントロールプレーンに転送し、残りのすべての Telnet パケットを指定したレートで規制できるように設定する例を示します。

```
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
! Allow 10.1.1.2 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
```

service-policy (control-plane)

```

! Rate limit all other Telnet traffic.
Router(config)# access-list 140 permit tcp any any eq telnet
! Define class-map "telnet-class."
Router(config)# class-map telnet-class
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map control-plane-policy
Router(config-pmap)# class telnet-class
Router(config-pmap-c)# police 80000 conform transmit exceed drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
! Define aggregate control plane service for the active Route Processor.
Router(config)# control-plane
Router(config-cp)# service-policy input control-plane-policy
Router(config-cp)# exit

```

次に、送信元アドレス 3.3.3.0 および 4.4.4.0 の信頼できるネットワークは Internet Control Message Protocol (ICMP) ポート到達不能応答を無制限に受信し、残りのすべての ICMP ポート到達不能を廃棄できるように設定する例を示します。

```

Router(config)# access-list 141 deny icmp host 3.3.3.0 0.0.0.255 any port-unreachable
! Allow 4.4.4.0 trusted network traffic.
Router(config)# access-list 141 deny icmp host 4.4.4.0 0.0.0.255 any port-unreachable
! Rate limit all other ICMP traffic.
Router(config)# access-list 141 permit icmp any any port-unreachable
Router(config)# class-map icmp-class
Router(config-cmap)# match access-group 141
Router(config-cmap)# exit
Router(config)# policy-map control-plane-out-policy
! Drop all traffic that matches the class "icmp-class."
Router(config-pmap)# class icmp-class
Router(config-pmap-c)# drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# control-plane
! Define aggregate control plane service for the active route processor.
Router(config-cp)# service-policy output control-plane-policy
Router(config-cp)# exit

```

関連コマンド

コマンド	説明
control-plane	ユーザが、装置のコントロールプレーンに関連付けられた属性またはパラメータ（サービス ポリシーなど）の関連付けおよび変更が許可されるコントロールプレーン コンフィギュレーション モードを開始します。
policy-map	QoS ポリシー マップを設定するための QoS ポリシー マップ コンフィギュレーション モードにアクセスします。
show policy-map control-plane	コントロールプレーンのポリシー マップの 1 つのクラスまたはすべてのクラスの設定を表示します。

session slot

モジュール (NAM など) とのセッションを開始するには、**session slot** コマンドを使用します。

```
session slot mod {processor processor-id}
```

シンタックスの説明

<i>mod</i>	スロット番号
processor <i>processor-id</i>	プロセッサ ID を指定します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

セッションを終了するには、**quit** コマンドを入力します。
このコマンドを使用すると、モジュール固有の CLI が使用可能になります。

例

次に、MSM (モジュール 4) とのセッションを開始する例を示します。

```
Router# session slot 4 processor 2  
Router#
```

set cos cos-inner (policy-map configuration)

QinQ 変換された送信パケットのトランク VLAN タグの 802.1Q 優先順位ビットを、内部カスタマー エッジの VLAN タグからのプライオリティ値で設定するには、**set cos cos-inner** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

set cos cos-inner

no set cos cos-inner

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

P bit は、外部プロバイダー エッジの VLAN タグからコピーされます。

コマンドのデフォルト

ポリシーマップ クラス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、OSM-2+4GE-WAN+ OSM モジュールが搭載された Catalyst 6500 シリーズ スイッチのギガビット イーサネット WAN インターフェイスだけでサポートされます。

OSM は、Supervisor Engine32 が搭載された Catalyst 6500 シリーズ スイッチではサポートされません。

802.1P 優先ビットは、QoS 処理の VLAN タグで使用されます。

ルータが二重タグ付き QinQ パケットを宛先インターフェイスにコピーする場合、デフォルトで外部 (プロバイダー) VLAN タグからの P bit を使用します。内部 (カスタマー) VLAN タグの P bit を保持するには、**set cos cos-inner** コマンドを使用します。

set cos cos-inner コマンドを有効にするには、**mls qos trust** コマンドを使用して、該当するインターフェイスまたはサブインターフェイスを信頼されるインターフェイスとして設定する必要があります。設定していない場合、インターフェイスまたはサブインターフェイスはデフォルトで信頼されない状態になり、**set cos cos-inner** コマンドにより外部 VLAN タグに着信パケットをコピーする前に、レイヤ 2 インターフェイスが着信パケットの P bit をゼロにします。

set cos cos-inner コマンドは、内部 (カスタマー) VLAN で設定されたサブインターフェイスに対してだけサポートされます。**set cos cos-inner** コマンドは、**bridge-domain** (サブインターフェイス コンフィギュレーション) コマンドで **out-range** キーワードを使用する、または **bridge-domain** (サブインターフェイス コンフィギュレーション) コマンドのいずれの形式でも設定されていないサブインターフェイスに対してサポートされません。

この動作は、メイン インターフェイスに適用されるポリシーで **set cos cos-inner** コマンドを設定する場合も保持されます。**set cos cos-inner** コマンドは、特定の内部 VLAN により設定されたサブインターフェイスには影響しますが、いずれの VLAN でも設定されていない、または **out-range** キーワードで設定されているサブインターフェイスには影響しません。

例 次に、内部 VLAN タグからの P bit を使用する音声トラフィック用のポリシーマップを設定する例を示します。

```
Router(config-pmap-c)# set cos cos-inner
Router(config-pmap-c)#
```

次に、デフォルトのポリシーマップ クラスを設定して、デフォルト値にリセットする例を示します。

```
Router(config-pmap-c)# no set cos cos-inner
Router(config-pmap-c)#
```

次に、**bridge-domain** (サブインターフェイス コンフィギュレーション) コマンドで設定されたサブインターフェイスにポリシーを適用する場合に表示されるシステム メッセージの例を示します。

```
Router(config-if)# bridge-vlan 32 dot1q-tunnel out-range
Router(config-if)# service-policy output cos1
```

```
%bridge-vlan 32 does not have any inner-vlan configured. 'set cos cos-inner' is not supported
```

```
Router(config-if)#
```

関連コマンド

コマンド	説明
bridge-domain (サブインターフェイス コンフィギュレーション)	PVC を指定された <i>vlan-id</i> にバインドします。
class-map	QoS クラス マップを設定するための QoS クラス マップ コンフィギュレーション モードにアクセスします。
mode dot1q-in-dot1q access-gateway	ギガビット イーサネット WAN インターフェイスをイネーブルにして、QinQ VLAN 変換に関してゲートウェイとして動作するようにします。
policy-map	QoS ポリシー マップを設定するための QoS ポリシー マップ コンフィギュレーション モードにアクセスします。
service-policy	インターフェイスにポリシー マップを対応付けます。
set ip dscp (policy-map configuration)	ToS バイトの IP DSCP を設定してパケットにマーキングします。
set ip precedence (policy-map configuration)	IP ヘッダーに優先順位を設定します。
show policy-map	ポリシー マップに関する情報を表示します。
show policy-map interface	インターフェイスに対応付けられた入力および出力ポリシーの統計情報およびコンフィギュレーションを表示します。

set ip dscp (policy-map configuration)

ToS バイトの IP DSCP を設定してパケットにマーキングするには、**set ip dscp** コマンドを使用します。設定済みの IP DSCP を削除するには、このコマンドの **no** 形式を使用します。

set ip dscp ip-dscp-value

no set ip dscp ip-dscp-value

シンタックスの説明

<i>ip-dscp-value</i>	出力 DSCP 値。有効値は 0～63 です。詳細については、「使用上のガイドライン」を参照してください。
----------------------	---

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

QoS ポリシーマップ コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ip-dscp-value の数値の代わりに、予約済みキーワード **EF** (緊急転送)、**AF11** (保証転送クラス AF11)、および **AF12** (保証転送クラス AF12) を入力できます。

IP DSCP ビットを設定すると、このビット設定で他の QoS サービスを稼働できます。

set ip precedence (policy-map configuration) コマンドを使用して IP precedence 別にパケットにマーキングしてから、**set ip dscp** コマンドを使用して同じパケットに IP DSCP 値でマーキングすることはできません。

マーキングされたトラフィックには、ネットワークによってプライオリティ (または緊急処理のタイプ) が設定されます。通常は、ネットワーク (または管理ドメイン) のエッジで IP precedence を設定します。データはこの優先順位に基づいてキューイングされます。Weighted Fair Queueing (WFQ; 均等化キューイング) は、輻輳ポイントにおいて、優先順位が高いトラフィックの処理を高速化できます。WRED を使用すると、トラフィック輻輳時における優先順位が高いトラフィックの損失率は、他のトラフィックよりも低くなります。

QoS ポリシーマップ コンフィギュレーション モードでサービス ポリシーを作成すると、**set ip precedence (policy-map configuration)** コマンドが適用されます。このサービス ポリシーはインターフェイスまたは ATM 仮想回線に対応付けられません。インターフェイスへのサービス ポリシーの対応付けについては、**service-policy** コマンドを参照してください。

ポリシー マップ クラスのアクションを設定する場合は、次の点に注意してください。

- ハードウェアでスイッチングされるトラフィックの場合、PFC QoS は **bandwidth**、**priority**、**queue-limit**、または **random-detect** ポリシーマップ クラス コマンドをサポートしません。ソフトウェアでスイッチングされるトラフィックの場合は、これらのコマンドは使用可能であるため、設定できます。
- PFC QoS は **set mpls** または **set qos-group** ポリシーマップ クラス コマンドをサポートしません。

- PFC QoS は **set ip dscp** および **set ip precedence** ポリシーマップ クラス コマンドをサポートします (『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide Release 12.2ZY*』の「Configuring Policy Map Class Marking」を参照)。
- ポリシーマップ クラス内で次の 3 つをすべて実行することはできません。
 - **set ip dscp** または **set ip precedence (policy-map configuration)** コマンドによるトラフィックのマーキング
 - 信頼状態の設定
 - ポリシングの設定

ポリシーマップ クラスでは、**set ip dscp** または **set ip precedence (policy-map configuration)** コマンドによるトラフィックのマーキング、あるいは次のいずれかまたは両方を実行できます。

- 信頼状態の設定
- ポリシングの設定

例

次に、ポリシーマップ `policy1` 内で IP DSCP ToS バイトを 8 に設定する例を示します。

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set ip dscp 8
```

`class1` の一致基準を満たすすべてのパケットには、IP DSCP 値 8 がマーキングされます。IP DSCP 値 8 がマーキングされたパケットの処理方法は、ネットワーク構成によって決まります。

次に、ネットワークのエッジで音声パケットに関する設定を行ったあと、音声パケットに対して低遅延処理を行うようにすべての中間ルータを設定する例を示します。

```
Router(config)# class-map voice
Router(config-cmap)# match ip dscp ef
Router(config)# policy qos-policy
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 24
```

関連コマンド

コマンド	説明
policy-map	QoS ポリシー マップを設定するための QoS ポリシー マップ コンフィギュレーション モードにアクセスします。
service-policy	インターフェイスにポリシー マップを対応付けます。
show policy-map	ポリシー マップに関する情報を表示します。
show policy-map interface	インターフェイスに対応付けられた入力および出力ポリシーの統計情報およびコンフィギュレーションを表示します。

set ip precedence (policy-map configuration)

IP ヘッダーに優先順位を設定するには、**set ip precedence** コマンドを使用します。現在の設定の優先順位値を放棄するには、このコマンドの **no** 形式を使用します。

set ip precedence ip-precedence-value

no set ip precedence

シンタックスの説明

ip-precedence-value IP ヘッダーの優先順位ビット値。有効値は 0 ~ 7 です。値の定義については、表 2-31 を参照してください。

コマンドのデフォルト

このコマンドは、デフォルトではディセーブルです。

コマンドのデフォルト

QoS ポリシーマップ コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

表 2-31 に、IP ヘッダー内の優先順位値の値定義を示します。重要性が低いものから高いものへ、順に示します。

表 2-31 IP precedence 値の定義

値	定義
0	routine
1	priority
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	network

IP precedence ビットを設定すると、このビット設定で、WFQ や WRED など他の QoS サービスが稼働します。

ネットワーク プライオリティ（または緊急処理のタイプ）によって、ネットワーク内のダウンストリーム ポイントに WFQ または WRED が適用され、トラフィックがマーキングされます。通常は、ネットワーク（または管理ドメイン）のエッジで IP precedence を設定します。データはこの優先順位

に基づいてキューイングされます。WFQ は、輻輳ポイントにおいて、特定の優先順位のトラフィックの処理を高速化できます。WRED を使用すると、トラフィック輻輳時における特定の優先順位値を持つトラフィックの損失率は、他のトラフィックよりも低くなります。

QoS ポリシーマップ コンフィギュレーション モードでサービス ポリシーを作成すると、**set ip precedence** コマンドが適用されます。このサービス ポリシーはインターフェイスまたは ATM 仮想回線に対応付けられません。インターフェイスへのサービス ポリシーの対応付けについては、**service-policy** コマンドを参照してください。

例

次に、クラス マップ `class1` の一致基準を満たすパケットに、IP precedence 値 5 を設定する例を示します。

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set ip precedence 5
```

`class1` の一致基準を満たすすべてのパケットには、IP precedence 値 5 がマーキングされます。IP precedence 値 5 がマーキングされたパケットの処理方法は、ネットワーク構成によって決まります。

関連コマンド

コマンド	説明
policy-map	QoS ポリシー マップを設定するための QoS ポリシー マップ コンフィギュレーション モードにアクセスします。
service-policy	インターフェイスにポリシー マップを対応付けます。
show policy-map	ポリシー マップに関する情報を表示します。
show policy-map interface	インターフェイスに対応付けられた入力および出力ポリシーの統計情報およびコンフィギュレーションを表示します。

set mpls experimental

試験値を設定するには、**set mpls experimental** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

set mpls experimental **{imposition | topmost}** *experimental-value*

シンタックスの説明

imposition	新しくインポートされたすべてのラベルの IP から MPLS または MPLS 入力の試験ビット値を指定します。
topmost	入力または出力フローの最上部のラベルの試験ビット値を指定します。
<i>experimental-value</i>	試験ビット値を指定します。有効値は 0 ~ 7 です。

コマンドのデフォルト

このコマンドは、デフォルトではディセーブルです。

コマンドモード

QoS ポリシーマップ コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、入力または出力の最上部ラベルの試験ビット値を設定する例を示します。

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set mpls experimental topmost 5
```

set qos-group

レイヤ 2 WAN インターフェイスの信頼状態を設定するには、**set qos-group** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
set qos-group group-value {cos | prec}
```

シンタックスの説明	group-value	QoS グループ値を指定します。有効値は 0 ~ 99 です。
	cos	着信フレームの CoS ビットを信頼し、CoS ビットから内部 DSCP 値を取得することを指定します。
	prec	着信パケットの ToS ビットに IP precedence 値が含まれていて、IP precedence ビットから内部 DSCP 値を取得することを指定します。

コマンドのデフォルト このコマンドは、デフォルトではディセーブルです。

コマンドモード QoS ポリシーマップ コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドは、MPLS 入力のパイプ モードで入力されて、出力キューを選択します。このコマンドは、WAN インターフェイスだけでサポートされます。LAN インターフェイスの信頼状態を設定するには、**mls qos trust** コマンドを使用します。

例 次に、インターフェイスの信頼状態を IP precedence に設定する例を示します。

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set qos-group 54 prec
Router(config-if)#
```

show

MST の設定を確認するには、**show** コマンドを使用します。

show [current | pending]

シンタックスの説明

current	(任意) MST の実行に使用される現在の設定を表示します。
pending	(任意) 現在の設定と置き換える編集済みの設定を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

MST コンフィギュレーション サブモード

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

show pending コマンドの出力は、**exit** コマンドを入力して MST コンフィギュレーション モードを終了した場合に、現在の設定と置き換えられる編集済みの設定です。

引数を指定しないで **show** コマンドを入力すると、保留中の設定が表示されます。

例

次に、編集済みの設定を表示する例を示します。

```
Router(config-mst)# show pending
Pending MST configuration
Name      [zorglub]
Version   31415
Instance  Vlans Mapped
-----
0         4001-4096
2         1010, 1020, 1030, 1040, 1050, 1060, 1070, 1080, 1090, 1100, 1110
          1120
3         1-1009, 1011-1019, 1021-1029, 1031-1039, 1041-1049, 1051-1059
          1061-1069, 1071-1079, 1081-1089, 1091-1099, 1101-1109, 1111-1119
          1121-4000
-----
Router(config-mst)#
```

次に、現在の設定を表示する例を示します。

```
Router(config-mst)# show current
Current MST configuration
Name []
Revision 0
Instance Vlans mapped
-----
0 1-4094
-----
```

関連コマンド

コマンド	説明
instance	1 つまたは一連の VLAN を MST インスタンスにマッピングします。
name (MST configuration submode)	MST リージョン名を設定します。
revision	MST コンフィギュレーションのリビジョン番号を設定します。
show spanning-tree mst	MST プロトコルに関する情報を表示します。
spanning-tree mst configuration	MST コンフィギュレーション サブモードを開始します。

show adjacency

ハードウェア レイヤ 3 スイッチング隣接テーブルに関する情報を表示するには、**show adjacency** コマンドを使用します。

```
show adjacency [{interface interface-number} | {null interface-number} | {port-channel
number} | {vlan vlan-id} | detail | internal | summary]
```

シンタックスの説明

<i>interface</i>	(任意) インターフェイス タイプ。有効値は、 ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 ge-wan 、および atm です。
<i>interface-number</i>	(任意) モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
null <i>interface-number</i>	(任意) ヌル インターフェイスを指定します。有効値は 0 です。
port-channel <i>number</i>	(任意) チャネル インターフェイスを指定します。有効値は 1 ~ 256 の範囲の最大 64 個の値です。
vlan <i>vlan-id</i>	(任意) VLAN を指定します。有効値は 1 ~ 4094 です。
detail	(任意) プロトコルの詳細およびタイマーに関する情報を表示します。
internal	(任意) 内部データ構造に関する情報を表示します。
summary	(任意) CEF 隣接情報のサマリーを表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

interface-number 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

ハードウェア レイヤ 3 スイッチング隣接統計情報は、60 秒間隔で更新されます。

show adjacency コマンドで表示される情報は、次のとおりです。

- プロトコル インターフェイス
- インターフェイスに設定されているルーティング プロトコルのタイプ
- インターフェイスのアドレス
- 隣接学習方式
- 隣接ルータの MAC アドレス

- 隣接ルータが隣接テーブルからロールアウトするまでの時間。ロールアウト後、パケットでは宛先方向に同じネクスト ホップを使用する必要があります。

例

次に、隣接情報を表示する例を示します。

```
Router# show adjacency
Protocol Interface          Address
IP        FastEthernet2/3         172.20.52.1 (3045)
IP        FastEthernet2/3         172.20.52.22 (11)
Router#
```

次に、隣接情報のサマリーを表示する例を示します。

```
Router# show adjacency summary
Adjacency Table has 2 adjacencies
Interface          Adjacency Count
FastEthernet2/3    2
Router#
```

次に、プロトコルの詳細およびタイマー情報を表示する例を示します。

```
Router# show adjacency detail
Protocol Interface          Address
IP        FastEthernet2/3         172.20.52.1 (3045)
0 packets, 0 bytes
000000000FF920000380000000000000
00000000000000000000000000000000
00605C865B2800D0BB0F980B0800
ARP        03:58:12
IP        FastEthernet2/3         172.20.52.22 (11)
0 packets, 0 bytes
000000000FF920000380000000000000
00000000000000000000000000000000
00801C93804000D0BB0F980B0800
ARP        03:58:06
Router#
```

次に、特定のインターフェイスの隣接情報を表示する例を示します。

```
Router# show adjacency fastethernet 2/3
Protocol Interface          Address
IP        FastEthernet2/3         172.20.52.1 (3045)
IP        FastEthernet2/3         172.20.52.22 (11)
Router#
```

関連コマンド

コマンド	説明
show mls cef adjacency	MLS ハードウェア レイヤ 3 スイッチング隣接ノードに関する情報を表示します。

show arp

ARP テーブルを表示するには、**show arp** コマンドを使用します。

show arp

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、ARP テーブルを表示する例を示します。

```
Router> show arp
Protocol Address           Age (min) Hardware Addr  Type   Interface
Internet 172.20.52.11        4         0090.2156.d800  ARPA   Vlan2
Internet 172.20.52.1         58        0060.5c86.5b28  ARPA   Vlan2
Internet 172.20.52.22       129       0080.1c93.8040  ARPA   Vlan2
Router>
```

show asic-version

特定のモジュールの ASIC バージョンを表示するには、**show asic-version** コマンドを使用します。

show asic-version slot number

シンタクスの説明	<i>number</i>	モジュール番号
----------	---------------	---------

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン **show asic-version** コマンド出力では、ASIC タイプは次のとおりです。

- Lyra : レイヤ 2 転送エンジン
- Hyperion : パケットの書き換え、マルチキャスト、および SPAN エンジン
- Polaris : レイヤ 3 CEF エンジン
- Pinnacle : 4 ポート ギガビットイーサネットインターフェイス
- R2D2 : ネットワーク インターフェイス (10/100/1000 Mbps および 10 Gbps の組み合わせ)、受信パケットのバッファ インターフェイス、送信パケットのバッファ インターフェイスのほか、さらにアップストリームの ASIC または FPGA に対するインターフェイス
- Titan : パケット リライトおよびレプリケーション エンジン
- Vela : コンステレーション バス インターフェイス

例 次に、特定のモジュールの ASIC タイプおよびバージョンを表示する例を示します。

```
Router# show asic-version slot 1
Module in slot 1 has 3 type(s) of ASICs
      ASIC Name      Count  Version
      PINNACLE       1      (2.0)
      MEDUSA         1      (2.0)
      TITAN          1      (0.1)
Router#
```

show bootflash:

bootflash ファイル システムに関する情報を表示するには、**show sup-bootflash** コマンドを使用します。

show bootflash: [all | chips | filesys]

シンタックスの説明

all	(任意) 使用可能なすべてのフラッシュの情報を表示します。
chips	(任意) フラッシュ チップに関する情報を表示します。
filesys	(任意) ファイル システムに関する情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、ファイル システム ステータスに関する情報を表示する例を示します。

```
Router> show bootflash: filesys

----- F I L E   S Y S T E M   S T A T U S -----
  Device Number = 0
DEVICE INFO BLOCK: bootflash
  Magic Number      = 6887635   File System Vers = 10000   (1.0)
  Length            = 1000000   Sector Size      = 40000
  Programming Algorithm = 39     Erased State     = FFFFFFFF
  File System Offset = 40000    Length = F40000
  MONLIB Offset     = 100      Length = C628
  Bad Sector Map Offset = 3FFF8  Length = 8
  Squeeze Log Offset = F80000   Length = 40000
  Squeeze Buffer Offset = FC0000  Length = 40000
  Num Spare Sectors = 0
  Spares:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  No Unrecovered Errors
  No Squeeze in progress
USAGE INFO:
  Bytes Used      = 917CE8   Bytes Available = 628318
  Bad Sectors    = 0        Spared Sectors  = 0
  OK Files       = 2        Bytes = 917BE8
  Deleted Files  = 0        Bytes = 0
  Files w/Errors = 0        Bytes = 0
Router>
```

次に、イメージ情報を表示する例を示します。

```
Router> show bootflash:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
1  .. image   8C5A393A 237E3C  14 2063804 Aug 23 1999 16:18:45 c6msfc-boot-mz
2  .. image   D86EE0AD 957CE8   9 7470636 Sep 20 1999 13:48:49 rp.halley
Router>
```

次に、すべてのブートフラッシュ情報を表示する例を示します。

```
Router> show bootflash: all
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
1  .. image   8C5A393A 237E3C  14 2063804 Aug 23 1999 16:18:45 c6msfc-boot-
mz
2  .. image   D86EE0AD 957CE8   9 7470636 Sep 20 1999 13:48:49 rp.halley

6456088 bytes available (9534696 bytes used)

----- F I L E   S Y S T E M   S T A T U S -----
Device Number = 0
DEVICE INFO BLOCK: bootflash
  Magic Number      = 6887635      File System Vers = 10000      (1.0)
  Length            = 1000000     Sector Size      = 40000
  Programming Algorithm = 39      Erased State     = FFFFFFFF
  File System Offset = 40000      Length = F40000
  MONLIB Offset     = 100        Length = C628
  Bad Sector Map Offset = 3FFF8    Length = 8
  Squeeze Log Offset = F80000    Length = 40000
  Squeeze Buffer Offset = FC0000    Length = 40000
  Num Spare Sectors = 0
  Spares:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  No Unrecovered Errors
  No Squeeze in progress
USAGE INFO:
  Bytes Used      = 917CE8      Bytes Available = 628318
  Bad Sectors    = 0          Spared Sectors = 0
  OK Files       = 2          Bytes = 917BE8
  Deleted Files  = 0          Bytes = 0
  Files w/Errors = 0          Bytes = 0
Router>
```

show bootvar

BOOT 環境変数に関する情報を表示するには、**show bootvar** コマンドを使用します。

show bootvar

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

show bootvar コマンドの出力は、ブート ステートメントの設定方法に応じて次のように変わります。

- ブート設定で **boot system flash bootflash:sup720_image** コマンドを入力した場合、**show bootvar** コマンドの出力では、ブートフラッシュの情報が表示されます。
- ブート設定で **boot system flash sup-bootflash:sup720_image** コマンドを入力した場合、**show bootvar** コマンドの出力では、サブブートフラッシュの情報が表示されます。この操作はブートステートメントを正しく設定する方法です。

show bootvar コマンドは、スイッチ プロセッサ CLI およびルート プロセッサ CLI から使用できます。スイッチ プロセッサ CLI の場合、表示は常に **bootflash** です。ブート ステートメントとして **bootflash** と **sup-bootflash** のいずれを使用しても、スイッチは正しく起動します。イメージがスイッチ プロセッサブートフラッシュに保存されるため、ブート設定ステートメントでは **sup-bootflash** を使用する必要があります。ルート プロセッサはそのイメージを **sup-bootflash** と見なします。

イメージ名の後ろに表示される数 (**c6sup12-js-mz.121-13.E,12** など) は、Catalyst 6500 シリーズ スイッチがファイルのリブートの試行を繰り返す回数を示しています。

次に、BOOT 環境変数に関する情報を表示する例を示します。

```
Router# show bootvar
BOOT variable = sup-bootflash:c6sup12-js-mz.121-13.E,12
CONFIG_FILE variable =
BOOTLDR variable = bootflash:c6msfc2-boot-mz.121-13.E.bin
Configuration register is 0x2102

Standby is up
Standby has 112640K/18432K bytes of memory.

Standby BOOT variable = bootflash:c6sup12-js-mz.121-13.E,12
Standby CONFIG_FILE variable =
Standby BOOTLDR variable = bootflash:c6msfc2-boot-mz.121-13.E.bin
Standby Configuration register is 0x2102
Router#
```

関連コマンド

コマンド	説明
<code>auto-sync</code>	NVRAM 内のコンフィギュレーション ファイルの自動同期化をイネーブルにします。

■ show bootvar

show cable-diagnostics tdr

TDR ケーブル診断のテスト結果を表示するには、**show cable-diagnostics tdr** コマンドを使用します。

show cable-diagnostics tdr {interface {interface interface-number}}

シンタックスの説明

interface interface インターフェイス タイプを指定します。有効値は **fastethernet** および **gigabitethernet** です。
interface-number モジュールおよびポート番号

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

show cable-diagnostics tdr コマンドは特定のモジュールでサポートされます。TDR をサポートするモジュールの一覧については、『*Release Notes for Cisco IOS Release 12.2 ZY Supervisor Engine 32 PISA*』を参照してください。

ケーブルがオープンまたは短絡されている場合、ケーブルがオープンまたは短絡されている長さの精度は、±2 m です。

ペアの長さは m、cm、または km 単位で表示できます。

TDR テストがポートで実行されていない場合、次のメッセージが表示されます。

```
TDR test was never run on Gi2/12
```

例

次に、TDR テストに関する情報を表示する例を示します。

```
Router> show cable-diagnostics tdr interface gigabitethernet8/1
TDR test last run on: February 25 11:18:31
Interface Speed Pair Cable length      Distance to fault  Channel Pair status
-----
Gi8/1      1000  1-2  1    +/- 6 m          N/A               Pair B  Terminated
           3-4  1    +/- 6 m          N/A               Pair A  Terminated
           5-6  1    +/- 6 m          N/A               Pair C  Terminated
           7-8  1    +/- 6 m          N/A               Pair D  Terminated
Router>
```

表 2-32 に、`show cable-diagnostics tdr` コマンド出力に含まれるフィールドの説明を示します。

表 2-32 show cable-diagnostics tdr コマンドの出力フィールド

フィールド	説明
Interface	テストするインターフェイス
Speed	現在の回線速度
Pair	ローカル ペアの名前
Cable Length	ケーブル長および精度。精度の単位は長さは m、cm、または km 単位です。
Channel	ペア指定
Pair status	表示されるペア ステータスは次のいずれかです。 <ul style="list-style-type: none"> Terminated : リンクはアップです。 Shorted : ケーブルで短絡が検出されています。 Open : ケーブルでオープニングが検出されています。 Not Completed : ポートでのテストが失敗しました。 Not Supported : ポートでのテストがサポートされていません。 Broken : ペアが不良。オープンまたは短絡されています。 ImpedanceMis : インピーダンスが不整合です。 InProgress : 診断テストが進行中です。

関連コマンド

コマンド	説明
<code>clear cable-diagnostics tdr</code>	TDR をサポートする特定のインターフェイスまたはすべてのインターフェイスをクリアします。
<code>test cable-diagnostics</code>	48 ポート 10/100/1000 BASE-T モジュール上の 10 ギガビットイーサネット リンクまたは銅ケーブルの状態をテストします。

show catalyst6000

Catalyst 6500 シリーズスイッチに関する情報を表示するには、**show catalyst6000** コマンドを使用します。

show catalyst6000 {all | chassis-mac-address | switching-clock | traffic-meter}

シンタックスの説明

all	MAC アドレス範囲、および現在とピーク時のトラフィック メータの値を表示します。
chassis-mac-address	MAC アドレス範囲を表示します。
switching-clock	スイッチングクロックの障害回復モードを表示します。
traffic-meter	バックプレーン（共有バス）の利用率（パーセント）を表示します。

コマンドのデフォルト

all

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

switching-clock キーワードを入力すると、アクティブクロックソースに障害が発生した場合に、Catalyst 6500 シリーズスイッチがバックプレーンでの冗長クロックソースのスイッチングが可能かどうかを表示します。

Catalyst 6500 シリーズスイッチには、ソフトウェア機能をサポートするために使用可能な MAC アドレスが 64 個または 1024 個あります。シャーシの MAC アドレス範囲を表示するには、**show catalyst6000 chassis-mac-address** コマンドを入力します。

例

次に、MAC アドレス範囲、および現在とピーク時のトラフィックメータの値を表示する例を示します。

```
Router> show catalyst6000 all
chassis MAC addresses: 64 addresses from 0001.6441.60c0 to 0001.6441.60ff
traffic meter = 0% Never cleared
peak = 0% reached at 08:14:38 UTC Wed Mar 19 2003
switching-clock: clock switchover and system reset is allowed
Router>
```

次に、MAC アドレス範囲を表示する例を示します。

```
Router# show catalyst6000 chassis-mac-address
chassis MAC addresses: 1024 addresses from 00d0.004c.1800 to 00d0.004c.1c00
Router#
```

次に、現在およびピーク時のメータの値を表示する例を示します。

```
Router> show catalyst6000 traffic-meter
```

■ show catalyst6000

```
traffic meter = 0% peak = 0% at 09:57:58 UTC Mon Nov 6 2000  
Router#
```

次に、スイッチング クロックの障害回復モードを表示する例を示します。

```
Router> show catalyst6000 switching-clock  
switching-clock: clock switchover and system reset is allowed  
Router>
```

show cdp neighbors

CDP により発見された近接装置の詳細情報を表示するには、**show cdp neighbors** コマンドを使用します。

show cdp neighbors [*type number*] [**detail**]

シンタックスの説明

<i>type</i>	(任意) 情報が必要なネイバに接続されたインターフェイス タイプ。有効値は、 ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 port-channel 、および vlan です。
<i>number</i>	(任意) 情報が必要なネイバに接続されたインターフェイス番号
detail	(任意) ネイバに関する詳細情報 (ネットワーク アドレス、イネーブルになっているプロトコル、ホールド時間、ソフトウェア バージョンなど) を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

port-channel の値は 0 ~ 282 です。257 ~ 282 の値は、CSM および FWSM だけでサポートされています。

例

次に、CDP ネイバに関する情報を表示する例を示します。

```
Router# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce   Holdtme    Capability  Platform  Port ID
lab-7206         Eth 0           157        R           7206VXR   Fas 0/0/0
lab-as5300-1     Eth 0           163        R           AS5300    Fas 0
lab-as5300-2     Eth 0           159        R           AS5300    Eth 0
lab-as5300-3     Eth 0           122        R           AS5300    Eth 0
lab-as5300-4     Eth 0           132        R           AS5300    Fas 0/0
lab-3621         Eth 0           140        R S         3631-telcoFas 0/0
008024 2758E0    Eth 0           132        T           CAT3000   1/2
```

表 2-33 に、この例で表示されるフィールドについて説明します。

表 2-33 show cdp neighbors のフィールドの説明

フィールド	定義
Device ID	設定された ID (名前)、MAC アドレス、または近接装置のシリアル番号
Local Intrfce	(ローカル インターフェイス) 接続メディアで使用するプロトコル
Holdtme	(ホールド時間) 現在の装置が、送信ルータからの CDP アドバタイズを廃棄せずに保持している残り時間 (秒単位)
Capability	装置上で発見される Capability コード。この装置タイプは、CDP ネイバテーブルに表示されます。表示される値は次のとおりです。 R : ルータ T : トランスペアレントブリッジ B : ソースルーティングブリッジ S : スイッチ H : ホスト I : IGMP 装置 r : リピータ P : 電話
Platform	装置の製品番号
Port ID	装置のプロトコルおよびポート番号

次に、CDP ネイバに関する詳細情報を表示する例を示します。

```
Router# show cdp neighbors detail
-----
Device ID: lab-7206
Entry address(es):
  IP address: 172.19.169.83
Platform: cisco 7206VXR, Capabilities: Router
Interface: Ethernet0, Port ID (outgoing port): FastEthernet0/0/0
Holdtime : 123 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 5800 Software (C5800-P4-M), Version 12.1(2)
Copyright (c) 1986-2002 by Cisco Systems, Inc.

advertisement version: 2
Duplex: half

-----
Device ID: lab-as5300-1
Entry address(es):
  IP address: 172.19.169.87
.
.
.
```

表 2-34 に、この例で表示されるフィールドについて説明します。

表 2-34 show cdp neighbors detail のフィールドの説明

フィールド	定義
Device ID	近接装置の名前、および MAC アドレスまたはシリアル番号
Entry address(es)	近接装置のネットワーク アドレスの一覧
[network protocol] address	近接装置のネットワーク アドレス。アドレスは、IP、IPX、AppleTalk、DECnet、または CLNS プロトコルの表記になります。
Platform	近接装置の製品名および製品番号
Capabilities	ネイバの装置タイプ。この装置には、ルータ、ブリッジ、トランスペアレントブリッジ、ソースルーティングブリッジ、スイッチ、ホスト、IGMP 装置、またはリピータがあります。
Interface	現在の装置でのポートのプロトコルおよびポート番号
Holdtime	現在の装置が、送信ルータからの CDP アドバタイズを廃棄せずに保持している残り時間 (秒単位)
Version:	近接装置で実行されているソフトウェアのバージョン
advertisement version:	CDP アドバタイズに使用されている CDP のバージョン
Duplex:	現在の装置と近接装置との間の接続のデュプレックス状態

関連コマンド

コマンド	説明
show cdp	グローバル CDP 情報を表示します。
show cdp entry	CDP により発見された特定の近接装置に関する情報を表示します。
show cdp interface	CDP をイネーブルにしたインターフェイスに関する情報を表示します。
show cdp traffic	CDP を使用して収集した装置間のトラフィックに関する情報を表示します。

show cef interface policy-statistics

インターフェイス単位のトラフィック統計情報を表示するには、**show cef interface policy-statistics** コマンドを使用します。

show cef interface policy-statistics

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドのデフォルト ユーザ EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、インターフェイス単位のトラフィック統計情報を表示する例を示します。

```
Router# show cef interface policy-statistics
POS7/0 is up (if_number 7)
Bucket PacketsBytes
1 0 0
2 0 0
3 0 0
4 0 0
5 100 10000
6 0 0
7 0 0
8 0 0
Router#
```

show class-map

クラス マップ情報を表示するには、**show class-map** コマンドを使用します。

show class-map [*class-name*]

シンタックスの説明

class-name (任意) クラス マップ名

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドのデフォルト

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、すべてのクラス マップに関するクラス マップ情報を表示する例を示します。

```
Router# show class-map
Class Map match-any class-default (id 0)
  Match any
Class Map match-any class-simple (id 2)
  Match any
Class Map match-all ipp5 (id 1)
  Match ip precedence 5

Class Map match-all agg-2 (id 3)
```

Router#

次に、特定のクラス マップに関するクラス マップ情報を表示する例を示します。

```
Router# show class-map ipp5
Class Map match-all ipp5 (id 1)
  Match ip precedence 5
```

Router#

関連コマンド

コマンド	説明
class-map	QoS クラス マップを設定するための QoS クラス マップ コンフィギュレーション モードにアクセスします。
show policy-map	ポリシー マップに関する情報を表示します。
show policy-map interface	インターフェイスに対応付けられた入力および出力ポリシーの統計情報およびコンフィギュレーションを表示します。

show counters interface

インターフェイス カウンタに関する情報を表示するには、**show counters interface** コマンドを使用します。

show counters interface {*type mod/port*} [**delta**]

シンタックスの説明

<i>type</i>	インターフェイス タイプ。有効値は ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 port-channel 、 pos 、 atm 、 null 、 tunnel 、および ge-wan です。
<i>mod/port</i>	モジュールおよびポート番号
delta	(任意) 前回の clear counters コマンド後のインターフェイス カウンタ値を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

show counters interface コマンドは SVI ではサポートされていません。

show counters interface delta コマンドは、最後に保存されたカウンタ値の詳細一覧を表示します。

例

次に、インターフェイス カウンタに関する情報を表示する例を示します。

```
Router# show counters interface fastethernet 5/2
64 bit counters:
0. rxHCTotalPkts = 1
1. txHCTotalPkts = 1
2. rxHCUnicastPkts = 0
3. txHCUnicastPkts = 0
4. rxHCMulticastPkts = 0
5. txHCMulticastPkts = 0
6. rxHCBroadcastPkts = 1
7. txHCBroadcastPkts = 1
8. rxHCOctets = 78
9. txHCOctets = 78
10. rxTxHCPkts64Octets = 0
11. rxTxHCPkts65to127Octets = 2
12. rxTxHCPkts128to255Octets = 0
13. rxTxHCPkts256to511Octets = 0
14. rxTxHCPkts512to1023Octets = 0
15. rxTxHCPkts1024to1518Octets = 0
16. txHCTrunkFrames = 0
17. rxHCTrunkFrames = 0
```

```
18. rxHCDropEvents = 0

32 bit counters:
0. rxCRCAlignErrors = 0
1. rxUndersizedPkts = 0
2. rxOversizedPkts = 0
3. rxFragmentPkts = 0
4. rxJabbers = 0
5. txCollisions = 0
6. ifInErrors = 0
7. ifOutErrors = 0
8. ifInDiscards = 0
9. ifInUnknownProtos = 0
10. ifOutDiscards = 0
11. txDelayExceededDiscards = 0
12. txCRC = 0
13. linkChange = 1
14. wrongEncapFrames = 0

All Port Counters
1. InPackets = 1
2. InOctets = 78
3. InUcastPkts = 0
4. InMcastPkts = 0
5. InBcastPkts = 1
6. OutPackets = 1
7. OutOctets = 78
8. OutUcastPkts = 0
9. OutMcastPkts = 0
10. OutBcastPkts = 1
11. AlignErr = 0
12. FCSErr = 0
13. XmitErr = 0
14. RcvErr = 0
15. UnderSize = 0
16. SingleCol = 0
17. MultiCol = 0
18. LateCol = 0
19. ExcessiveCol = 0
20. CarrierSense = 0
21. Runts = 0
22. Giants = 0
23. InDiscards = 0
24. OutDiscards = 0
25. InErrors = 0
26. OutErrors = 0
27. TrunkFramesTx = 0
28. TrunkFramesRx = 0
29. WrongEncap = 0
30. Broadcast_suppression_discards = 0
31. Multicast_suppression_discards = 0
32. Unicast_suppression_discards = 0
33. rxTxHCPkts64Octets = 0
34. rxTxHCPkts65to127Octets = 2
35. rxTxHCPkts128to255Octets = 0
36. rxTxHCPkts256to511Octets = 0
37. rxTxHCpkts512to1023Octets = 0
38. rxTxHCpkts1024to1518Octets = 0
39. DropEvents = 0
40. CRCAlignErrors = 0
41. UndersizedPkts = 0
42. OversizedPkts = 0
43. FragmentPkts = 0
44. Jabbers = 0
45. Collisions = 0
```

■ show counters interface

```

46.          DelayExceededDiscards = 0
47.          bpduOutlost = 0
48.          qos0Outlost = 0
49.          qos1Outlost = 0
50.          qos2Outlost = 0
51.          qos3Outlost = 0
52.          bpduCbicOutlost = 0
53.          qos0CbicOutlost = 0
54.          qos1CbicOutlost = 0
55.          qos2CbicOutlost = 0
56.          qos3CbicOutlost = 0
57.          bpduInlost = 0
58.          qos0Inlost = 0
59.          qos1Inlost = 0
60.          qos2Inlost = 0
61.          qos3Inlost = 0
62.          qos4Inlost = 0
63.          qos5Inlost = 0
64.          qos6Inlost = 0
65.          qos7Inlost = 0
66.          pqueInlost = 0
67.          Overruns = 0
68.          maxIndex = 0

```

Router#

次に、前回の **clear counters** コマンド後のインターフェイス カウンタ値を表示する例を示します。

```

Router# show counters interface gigabitethernet5/2 delta
Time since last clear
-----
1d08h
64 bit counters:
0. rxHCTotalPkts = 508473
1. txHCTotalPkts = 2366
2. rxHCUnicastPkts = 411611
3. txHCUnicastPkts = 193
4. rxHCMulticastPkts = 81868
5. txHCMulticastPkts = 2155
6. rxHCBroadcastPkts = 14994
7. txHCBroadcastPkts = 18
8. rxHCOctets = 36961992
.
.
.
Router#

```

関連コマンド

コマンド	説明
clear counters	インターフェイス カウンタをクリアします。

show diagnostic

オンライン診断のテスト結果を表示し、サポートされているテストスイートを一覧表示するには、**show diagnostic** コマンドを使用します。

- show diagnostic bootup level**
- show diagnostic content [module num]**
- show diagnostic events [module num] [event-type event-type]**
- show diagnostic {ondemand settings}**
- show diagnostic {result [module num] [detail]}**
- show diagnostic schedule [module num]**

シンタックスの説明	
bootup level	設定されたブートアップ診断のカバレッジレベルを表示します。
content	各テストおよびすべてのモジュールについて、テスト ID、テスト属性、およびサポートされているカバレッジテストレベルなどのテスト情報を表示します。
module num	(任意) モジュール番号を指定します。
events	診断イベントのイベントログを表示します。
event-type event-type	(任意) イベントタイプを指定します。有効値は、 error 、 info 、および warning です。
ondemand settings	オンデマンド診断の設定を表示します。
result	テスト結果を表示します。
detail	(任意) 各テストのテスト統計情報を表示します。
schedule	現在スケジューリング済みの診断タスクを表示します。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン `module num` を入力しないと、すべてのモジュールの情報が表示されます。コマンド出力では、テスト結果には次のものがあります。

- 合格 (.)
- 失敗 (F)
- 不明 (U)

例

次に、テストスイート、モニタリングインターバル、およびテスト属性を表示する例を示します。

```
Router# show diagnostic content module 1
Diagnostic Tests List for Module 1:
Module 1:

Diagnostics test suite attributes:
  M/C/* - Minimal level test / Complete level test / Not applicable
  B/* - Bypass bootup test / Not applicable
  P/* - Per port test / Not applicable
  D/N - Disruptive test / Non-disruptive test
  S/* - Only applicable to standby unit / Not applicable
  X/* - Not a health monitoring test / Not applicable
  F/* - Fixed monitoring interval test / Not applicable
  E/* - Always enabled monitoring test / Not applicable
  A/I - Monitoring is active / Monitoring is inactive

Testing Interval
ID  Test Name                               Attributes (day hh:mm:ss.ms)
=== =====
1)  TestDummy1 -----> M**D****A  000 00:01:00.000
2)  TestDummy2 -----> M**D**FEA  000 00:02:30.000
3)  TestGBICIntegrity -----> *BPD****I  not configured
4)  TestActiveToStandbyLoopback -----> M**PDS***I  not configured
5)  TestLoopback -----> M**PD****I  not configured
6)  TestNewLearn -----> M**N****I  not configured
7)  TestIndexLearn -----> M**N****I  not configured
8)  TestConditionalLearn -----> M**N****I  not configured
9)  TestBadBpdu -----> M**D****I  not configured
10) TestCapture -----> M**D****I  not configured
11) TestProtocolMatch -----> M**D****I  not configured
12) TestChannel -----> M**D****I  not configured
13) TestDontShortcut -----> M**Nrefer*I  not configured
14) TestL3Capture2 -----> M**N****I  not configured
15) TestL3VlanMet -----> M**N****I  not configured
16) TestIngressSpan -----> M**N****I  not configured
17) TestEgressSpan -----> M**N****I  not configured
18) TestAclPermit -----> M**N****I  not configured
19) TestAclDeny -----> M**D****I  not configured
20) TestNetflowInlineRewrite -----> C**PD****I  not configured

Router#
```

次に、設定されたブートアップ診断レベルを表示する例を示します。

```
Router# show diagnostic bootup level
Current Bootup Diagnostic Level = Complete
Router#
```

次に、診断のイベントログを表示する例を示します。

```
Router# show diagnostic events

Diagnostic events (storage for 500 events, 10 events recorded)
Event Type (ET):I - Info, W - Warning, E - Error

Time Stamp          ET [Card] Event Message
-----
08/26 15:51:04.335 I [1] TestIndexLearn Passed
08/26 15:51:04.335 I [1] Diagnostics Passed
08/26 15:51:15.511 I [8] TestLoopback Passed
08/26 15:51:15.511 I [8] Diagnostics Passed
08/26 16:15:02.247 I [1] TestDontLearn Passed
08/26 16:15:02.247 I [1] Diagnostics Passed
08/26 16:15:12.683 I [8] TestNetflowInlineRewrite Passed
08/26 16:15:12.683 I [8] Diagnostics Passed
```

```
08/26 16:15:42.207 I [2] TestActiveToStandbyLoopback Passed
08/26 16:15:42.207 I [2] Diagnostics Passed
Router#
```

次に、オンデマンド診断の設定を表示する例を示します。

```
Router# show diagnostic ondemand settings
Ondemand Run Iteration = 2
Ondemand Action-on-Error = CONTINUE
Router#
```

次に、指定されたスロットについて現在スケジューリング済みの診断タスクを表示する例を示します。

```
Router# show diagnostic schedule module 1
Current Time = 07:55:30 UTC Fri August 2 2002
```

Diagnostic for Module 1:

```
Schedule #1:
  To be run on January 3 2003 23:32
  Test ID(s) to be executed:1.
```

```
Schedule #2:
  To be run daily 14:45
  Test ID(s) to be executed:2.
```

```
Schedule #3:
  To be run weekly Monday 3:33
  Test ID(s) to be executed:all.
```

Router#

次に、指定されたスロットについてテスト結果を表示する例を示します。

```
Router# show diagnostic result module 3
```

Current bootup diagnostic level:complete

Module 3:

```
Overall Diagnostic Result for Module 8 :PASS
Diagnostic level at card bootup:complete
```

Test results:(. = Pass, F = Fail, U = Untested)

1) TestLoopback :

```
Port  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
-----
      .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
Port 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
-----
      .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
```

```
2) TestNewLearn -----> .
3) TestIndexLearn -----> .
4) TestDontLearn -----> .
5) TestConditionalLearn -----> .
6) TestDontLearn -----> .
7) TestConditionalLearn -----> .
8) TestBadBpdu -----> .
9) TestTrap -----> .
10) TestMatch -----> .
11) TestCapture -----> .
```

show diagnostic

```

12) TestProtocolMatch -----> .
13) TestChannel -----> .
14) TestIPFibShortcut -----> .
15) TestDontShortcut -----> .
16) TestL3Capture2 -----> .
17) TestL3VlanMet -----> .
18) TestIngressSpan -----> .
19) TestEgressSpan -----> .
20) TestAclPermit -----> .
21) TestAclDeny -----> .
22) TestNetflowInlineRewrite:

Port  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
-----
. . . . .
Port 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
-----
. . . . .

```

Router#

次に、指定されたスロットについて詳細なテスト結果を表示する例を示します。

Router# **show diagnostic result module 1 detail**

Current bootup diagnostic level:complete

Module 1:

Overall Diagnostic Result for Module 1 :PASS
Diagnostic level at card bootup:complete

Test results:(. = Pass, F = Fail, U = Untested)

```

1) TestDummy -----> .
   Error code -----> 0 (DIAG_SUCCESS)
   Total run count -----> 90
   Last test execution time ----> Dec 10 2002 12:34:30
   First test failure time ----> Dec 10 2002 11:57:39
   Last test failure time ----> Dec 10 2002 12:34:10
   Last test pass time -----> Dec 10 2002 11:34:30
   Total failure count -----> 65
   Consecutive failure count ---> 0

```

2) TestLoopback:

```

Port  1  2
-----
. .

Error code -----> 0 (DIAG_SUCCESS)
Total run count -----> 1
Last test execution time ----> Dec 10 2002 12:37:18
First test failure time ----> n/a
Last test failure time ----> n/a
Last test pass time -----> Dec 10 2002 12:37:18
Total failure count -----> 0
Consecutive failure count ---> 0

```

Router#

次に、診断のイベント ログを表示する例を示します。

```
Router# show diagnostic events
Diagnostic events (storage for 500 events, 10 events recorded)
EventType:I - Info, W - Warning, E - Error

TimeStamp          Type [Card] EventMessage
08/26 15:51:04.335 I    [1] TestIndexLearn Passed
08/26 15:51:04.335 I    [1] Diagnostics Passed
08/26 15:51:15.511 I    [8] TestLoopback Passed
08/26 15:51:15.511 I    [8] Diagnostics Passed
08/26 16:15:02.247 I    [1] TestDontLearn Passed
08/26 16:15:02.247 I    [1] Diagnostics Passed
08/26 16:15:12.683 I    [8] TestNetflowInlineRewrite Passed
08/26 16:15:12.683 I    [8] Diagnostics Passed
08/26 16:15:42.207 I    [2] TestActiveToStandbyLoopback Passed
08/26 16:15:42.207 I    [2] Diagnostics Passed
Router#
```

関連コマンド

コマンド	説明
diagnostic bootup level	ブートアップ診断レベルを設定します。
diagnostic cns	CNS 診断を設定します。
diagnostic event-log size	診断イベントログのサイズをダイナミックに変更します。
diagnostic monitor	ヘルス モニタリング診断テストを設定します。
diagnostic ondemand	オンデマンド診断を設定します。
diagnostic schedule test	特定モジュールに対するテストベースの診断テストのスケジュールを設定するか、スーパーバイザ エンジンのスイッチオーバーをスケジュールリングします。
diagnostic start	指定した診断テストを実行します。
diagnostic stop	テストを停止します。

show diagnostic cns

CNS サブジェクトに関する情報を表示するには、**show diagnostic cns** コマンドを使用します。

show diagnostic cns {publish | subscribe}

シンタックスの説明

publish	診断結果を発行するサブジェクトを表示します。
subscribe	加入したサブジェクトを表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドのデフォルト

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

CNS サブシステムは、CNS イベント エージェントを介してリモート ネットワーク アプリケーションと通信し、発行および加入モデルに従います。アプリケーションは、適切なイベント サブジェクト名に加入することにより、イベントの受信設定を行います。

例

次に、診断結果の発行先のサブジェクトを表示する例を示します。

```
Router# show diagnostic cns publish
Subject: cisco.cns.device.diag_results
Router#
```

次に、加入したサブジェクトを表示する例を示します。

```
Router# show diagnostic cns subscribe
Subject: cisco.cns.device.diag_get_results
Router#
```

関連コマンド

コマンド	説明
diagnostic cns	CNS 診断を設定します。

show diagnostic sanity

健全性チェックの結果を表示するには、**show diagnostic sanity** コマンドを使用します。

show diagnostic sanity

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドを引数なしで入力すると、Catalyst 6500 シリーズスイッチのすべてのギガビットイーサネット WAN インターフェイスに関する情報が表示されます。

コマンドモード 特権 EXEC (#)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン 健全性チェックでは、あらかじめ設定された一連のチェックが特定のシステム状態の可能な組み合わせでコンフィギュレーションに対して実行されて、警告状態のリストが作成されます。チェックは、不適當と思われるものを探すように設計されていて、システムの健全性の維持に役立つことを目的としています。

次に、実行されるチェックと状態が検出されたときに行われるアクションのリストを示します。

- デフォルト ゲートウェイに到達可能かどうかをチェックします。到達可能な場合、システムは ping を停止します。
- ポートが半二重に自動ネゴシエートする場合、システムはフラグを立てます。

トランキング チェック

- トランク ポートのモードがオンに設定されている場合、システムはフラグを立てます。
- ポートがトランキングしていて、モードが **auto** の場合、システムはフラグを立てます。
- トランク ポートがトランキングされていず、モードが **desirable** の場合、システムはフラグを立てます。
- トランク ポートが半二重に自動ネゴシエートする場合、システムはフラグを立てます。

チャンネル チェック

- ポートのチャンネル モードがオンに設定されている場合、システムはフラグを立てます。
- ポートがチャンネルングされていず、モードが **desirable** に設定されている場合、システムはフラグを立てます。
- VLAN に 32K のスパニングツリー ルートがある（ルートが設定されていない）場合、システムはフラグを立てます。

スパニングツリー VLAN チェック

- VLAN のスパニングツリー ルートの有効期限がデフォルトと違う場合、システムはフラグを立てます。

- VLAN のスパニングツリー ルートの転送遅延がデフォルトと違う場合、システムはフラグを立てます。
- VLAN のブリッジの転送遅延がデフォルトと違う場合、システムはフラグを立てます。
- VLAN のブリッジの転送遅延がデフォルトと違う場合、システムはフラグを立てます。
- VLAN のブリッジの hello タイムがデフォルトと違う場合、システムはフラグを立てます。

スパニングツリー ポート チェック

- ポートのポート コストがデフォルトと違う場合、システムはフラグを立てます。
- ポートのポート プライオリティがデフォルトと違う場合、システムはフラグを立てます。

UDLD チェック

- ポートの UDLD がディセーブルの場合、システムはフラグを立てます。
- ポートの UDLD がシャットダウンしている場合、システムはフラグを立てます。
- ポートの UDLD が未定の状態の場合、システムはフラグを立てます。

その他のポート チェック

- ポートの受信フロー制御がディセーブルの場合、システムはフラグを立てます。
- トランク ポートの PortFast がイネーブルの場合、システムはフラグを立てます。
- インライン電力ポートが次の状態の場合、システムはフラグを立てます。
 - 拒否
 - 障害
 - その他
 - オフ
- ポートのネイティブ VLAN が不一致の場合、システムはフラグを立てます。
- ポートのデュプレックスが不一致の場合、システムはフラグを立てます。

ブートストリングおよびコンフィギュレーション レジスタ チェック

- プライマリ スーパーバイザ エンジン (およびセカンダリ スーパーバイザ エンジン) のコンフィギュレーション レジスタは、0x2、0x102、または 0x2102 でなければなりません。
- システムはプライマリ スーパーバイザ エンジン (およびセカンダリ スーパーバイザ エンジン) のブートストリングを確認します。ブートストリングが空の場合、システムはメッセージを表示します。
- システムは、すべてのファイルがブートストリングで指定されていることを確認します。ファイルがない場合やチェックサムが正しくない場合、システムはメッセージを表示します。

device: だけがファイル名として指定されていた場合、システムは最初のファイルがそのデバイスにあるかどうかを確認します。

その他のチェック

- IGMP スヌーピングがディセーブルの場合、システムはメッセージを表示します。
- snmp コミュニティ アクセス ストリングの値 {RO,RW,RW-ALL} がデフォルトと同じ場合、システムはメッセージを表示します。
- モジュールのいずれかが Ok 以外の状態の場合、システムはメッセージを表示します。
- システムは、**show test all** コマンドで失敗したすべてのテスト ([F] と表示されます) を一覧表示するメッセージを表示します。
- スイッチのどの位置にも *fast が設定されていない場合、システムはメッセージを表示します。

- ブートフラッシュ上の **crashinfo** ファイルのための空き容量が不足している場合、システムはメッセージを表示します。
- マルチキャストルーティングがグローバルにイネーブルになっているのに、すべてのインターフェイスに適用されていない場合、システムはメッセージを表示します。
- IGMP スヌーピングがディセーブルであり、RGMP がイネーブルの場合、システムはメッセージを表示します。

例

次に、**show diagnostic sanity** コマンドで表示されるメッセージの例を示します。

```
Router# show diagnostic sanity
Pinging default gateway 10.6.141.1 ....
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.6.141.1, timeout is 2 seconds:
..!!!.
Success rate is 0 percent (0/5)

IGMP snooping disabled please enable it for optimum config.

IGMP snooping disabled but RGMP enabled on the following interfaces,
please enable IGMP for proper config :
Vlan1, Vlan2, GigabitEthernet1/1

Multicast routing is enabled globally but not enabled on the following
interfaces:
GigabitEthernet1/1, GigabitEthernet1/2

A programming algorithm mismatch was found on the device bootflash:
Formatting the device is recommended.

The bootflash: does not have enough free space to accomodate the crashinfo file.

Please check your confreg value : 0x0.

Please check your confreg value on standby: 0x0.

The boot string is empty. Please enter a valid boot string .
Could not verify boot image "disk0:" specified in the boot string on the
slave.

Invalid boot image "bootflash:asdasd" specified in the boot string on the
slave.

Please check your boot string on the slave.

UDLD has been disabled globally - port-level UDLD sanity checks are
being bypassed.
OR
[
The following ports have UDLD disabled. Please enable UDLD for optimum
config:
Fa9/45

The following ports have an unknown UDLD link state. Please enable UDLD
on both sides of the link:
Fa9/45
]

The following ports have portfast enabled:
Fa9/35, Fa9/45
```

■ show diagnostic sanity

The following ports have trunk mode set to on:
Fa4/1, Fa4/13

The following trunks have mode set to auto:
Fa4/2, Fa4/3

The following ports with mode set to desirable are not trunking:
Fa4/3, Fa4/4

The following trunk ports have negotiated to half-duplex:
Fa4/3, Fa4/4

The following ports are configured for channel mode on:
Fa4/1, Fa4/2, Fa4/3, Fa4/4

The following ports, not channeling are configured for channel mode
desirable:
Fa4/14

The following vlan(s) have a spanning tree root of 32768:
1

The following vlan(s) have max age on the spanning tree root different from
the default:
1-2

The following vlan(s) have forward delay on the spanning tree root different
from the default:
1-2

The following vlan(s) have hello time on the spanning tree root different
from the default:
1-2

The following vlan(s) have max age on the bridge different from the
default:
1-2

The following vlan(s) have fwd delay on the bridge different from the
default:
1-2

The following vlan(s) have hello time on the bridge different from the
default:
1-2

The following vlan(s) have a different port priority than the default
on the port FastEthernet4/1
1-2

The following ports have receive flow control disabled:
Fa9/35, Fa9/45

The following inline power ports have power-deny/faulty status:
Gi7/1, Gi7/2

The following ports have negotiated to half-duplex:
Fa9/45

The following vlans have a duplex mismatch:
Fas 9/45

The following interfaces have a native vlan mismatch:
interface (native vlan - neighbor vlan)

Fas 9/45 (1 - 64)

The value for Community-Access on read-only operations for SNMP is the same as default. Please verify that this is the best value from a security point of view.

The value for Community-Access on write-only operations for SNMP is the same as default. Please verify that this is the best value from a security point of view.

The value for Community-Access on read-write operations for SNMP is the same as default. Please verify that this is the best value from a security point of view.

Please check the status of the following modules:
8,9

Module 2 had a MINOR_ERROR.

The Module 2 failed the following tests:
TestIngressSpan

The following ports from Module2 failed test1:
1,2,4,48

show dot1q-tunnel

802.1Q トンネル対応ポートのリストを表示するには、**show dot1q-tunnel** コマンドを使用します。

```
show dot1q-tunnel [{interface interface interface-number}]
```

シンタックスの説明

interface interface	(任意) インターフェイス タイプを指定します。有効値は ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、および port-channel です。
interface-number	インターフェイス番号。有効値については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドのデフォルト

EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

キーワードを入力しないと、すべてのインターフェイスの 802.1Q トンネル ポートが表示されます。

interface-number 引数は、**ethernet**、**fastethernet**、**gigabitethernet**、および **tengigabitethernet** キーワードに対して、モジュールおよびポート番号を指定します。有効値は、使用するシャーシおよびモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合、スロット番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 です。

interface-number 引数は、**port-channel** キーワードに対してポート チャネル番号を指定します。有効値は 1 ~ 282 です。257 ~ 282 の値は、CSM および FWSM だけでサポートされています。

例

次の例は、ポートが起動していて、その上に 802.1Q トンネルが 1 つ設定されていることを示します。

```
Router# show dot1q-tunnel interface port-channel 10
Interface
-----
Po10
```

関連コマンド

コマンド	説明
switchport mode	インターフェイス タイプを設定します。
vlan dot1q tag native	トランク内のすべての VLAN の 802.1Q タギングをイネーブルにします。

show dot1x

802.1X 情報を表示するには、**show dot1x** コマンドを使用します。

```
show dot1x {interface interface interface-number}
```

```
show dot1x {all | brief | summary | {statistics {interface interface interface-number}}}
```

シンタックスの説明

interface interface	指定したインターフェイス タイプの 802.1X 情報を表示します。有効値は ethernet 、 fastethernet 、 gigabitethernet 、および tengigabitethernet です。
interface-number	インターフェイス番号。有効値については、「使用上のガイドライン」を参照してください。
all	すべてのインターフェイスの 802.1X 情報を表示します。
brief	すべてのインターフェイスの 802.1X ステータスに関する情報を表示します。
summary	システム全体の 802.1X サマリーに関する情報を表示します。
statistics	802.1X ポートに関する情報を表示します。詳細については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

show dot1x statistics コマンドを入力する場合は、コマンドを正しく実行するために、**interface interface interface-number** を入力する必要があります。

802.1X をグローバルにディセーブルにした場合、**show dot1x brief** コマンドの出力には何も表示されませんが、**show dot1x summary** コマンドの出力はすべてのフィールドに対して 0 を表示します。

interface-number 引数は、**ethernet**、**fastethernet**、**gigabitethernet**、および **tengigabitethernet** キーワードに対して、モジュールおよびポート番号を指定します。有効値は、使用するシャーシおよびモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合、スロット番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 です。

例

次に、特定のインターフェイスの 802.1X 情報を表示する例を示します。

```
Router# show dot1x interface fastethernet 5/1
Default Dot1x Configuration Exists for this interface FastEthernet5/1
AuthSM State      = FORCE AUTHORIZED
BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 2
```

show dot1x

```

MultiHosts          = Disabled
PortControl         = Force Authorized
QuietPeriod        = 60 Seconds
Re-authentication   = Disabled
ReAuthPeriod       = 3600 Seconds
ServerTimeout      = 30 Seconds
SuppTimeout        = 30 Seconds
TxPeriod           = 30 Seconds

```

```
Router#
```

次に、すべてのインターフェイスの 802.1X 情報を表示する例を示します。

```

Router# show dot1x all
Dot1x Info for interface FastEthernet3/2
-----
AuthSM State = FORCE UNAUTHORIZED
BendSM State = IDLE
PortStatus = UNAUTHORIZED
MaxReq = 2
MultiHosts = Disabled
Port Control = Force Unauthorized
QuietPeriod = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod = 3600 Seconds
ServerTimeout = 30 Seconds
SuppTimeout = 30 Seconds
TxPeriod = 30 Seconds
Dot1x Info for interface FastEthernet3/12
-----
AuthSM State = Unknown State
BendSM State = Unknown State
PortStatus = UNKNOWN
MaxReq = 2
MultiHosts = Disabled
Port Control = Auto
QuietPeriod = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod = 3600 Seconds
ServerTimeout = 30 Seconds
SuppTimeout = 30 Seconds
TxPeriod = 30 Seconds
Guest-Vlan = 91
Router#

```

次に、ポートの 802.1X 統計情報を表示する例を示します。

```

Router# show dot1x statistics interface fastethernet3/1
PortStatistics Parameters for Dot1x
-----
TxReqId = 0 TxReq = 0 TxTotal = 0
RxStart = 0 RxLogoff = 0 RxRespId = 0 RxResp = 0
RxInvalid = 0 RxLenErr = 0 RxTotal = 0
RxVersion = 0 LastRxSrcMac 0000.0000.0000
Router#

```

次に、システム全体の 802.1X 情報のサマリーを表示する例を示します。

```

Router# show dot1x summary

Total number of dot1x enabled ports:          336
Total number of FORCE_UNAUTHORIZED dot1x ports:  0
Total number of authorized dot1x enabled ports: 254
Total number of dot1x ports in single host mode: 336
Total number of dot1x ports in multi host mode:  0

```

```

Total number of dot1x authenticated supplicants:      254
Total number of supplicants in AUTH_DISCONNECTED state:  0
Total number of supplicants in AUTH_CONNECTING state:   0
Total number of supplicants in AUTH_AUTHENTICATING state: 0
Total number of supplicants in AUTH_HELD state:        0
Router#

```

次に、すべての 802.1X 対応ポートのステータスを表示する例を示します。

```

Router# show dot1x brief
RV - Radius returned VLAN

```

Port	Supplicant MAC	AuthSM State	BendSM State	Port Status	RV
Fa4/1	0000.0000.0000	N/A	N/A	N/A	-
Fa4/2	0000.0000.0000	N/A	N/A	N/A	-
Fa4/3	0000.0000.0000	N/A	N/A	N/A	-
Fa4/4	0000.0000.0000	N/A	N/A	N/A	-
Fa4/5	0000.0000.0000	N/A	N/A	N/A	-
Fa4/6	0000.0000.0000	N/A	N/A	N/A	-
Fa4/7	0000.0000.0000	N/A	N/A	N/A	-
.					
.					
. Output truncated					
Fa4/35	00fe.ed00.01ba	AUTHENTICATED	IDLE	AUTHORIZED	101
Fa4/36	00fe.ed00.01b8	AUTHENTICATED	IDLE	AUTHORIZED	101
Fa4/37	00fe.ed00.01e6	AUTHENTICATED	IDLE	AUTHORIZED	101
Fa4/38	00fe.ed00.01e4	AUTHENTICATED	IDLE	AUTHORIZED	101
Fa4/39	00fe.ed00.01e2	AUTHENTICATED	IDLE	AUTHORIZED	101
Fa4/40	00fe.ed00.01e0	AUTHENTICATED	IDLE	AUTHORIZED	101
Fa4/41	00fe.ed00.01de	AUTHENTICATED	IDLE	AUTHORIZED	101
Fa4/42	00fe.ed00.01dc	AUTHENTICATED	IDLE	AUTHORIZED	101

```

Router#

```

show dss log

NetFlow テーブルにおける DSS 範囲の無効化ルートを表示するには、**show dss log** コマンドを使用します。

```
show dss log {ip | ipv6}
```

シンタックスの説明

ip	DSS IP の範囲無効化プロファイルを表示します。
ipv6	DSS IPv6 の範囲無効化プロファイルを表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドのデフォルト

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

IPv6 エントリがルーティング テーブルから削除されるたびに、メッセージがスイッチ プロセッサに送信されてそのネットワークに関連付けられたエントリが削除されます。短時間に多数の無効化が発生した場合は、複数の IPv6 プレフィクスが、より大まかな 1 つのプレフィクスにまとめられます。

例

次に、DSS IP の範囲無効化プロファイルを表示する例を示します。

```
Router# show dss log ip
22:50:18.551 prefix 172.20.52.18 mask 172.20.52.18
22:50:20.059 prefix 127.0.0.0 mask 255.0.0.0
22:51:48.767 prefix 172.20.52.18 mask 172.20.52.18
22:51:52.651 prefix 0.0.0.0 mask 0.0.0.0
22:53:02.651 prefix 0.0.0.0 mask 0.0.0.0
22:53:19.651 prefix 0.0.0.0 mask 0.0.0.0
Router#
```

show environment alarm

環境アラームに関する情報を表示するには、**show environment alarm** コマンドを使用します。

show environment alarm [{*status* | *threshold*}] [*frutype*]

シンタックスの説明	
status	(任意) 動作上の FRU ステータスを表示します。
threshold	(任意) 事前にプログラミングされたアラームしきい値を表示します。
<i>frutype</i>	(任意) アラーム タイプ。有効値は all 、 backplane 、 clock number 、 earl slot 、 fan-tray 、 module slot 、 rp slot 、 power-supply number 、 supervisor slot 、および vtt number です。 <i>number</i> および <i>slot</i> の有効値のリストについては、「使用上のガイドライン」を参照してください。

コマンドのデフォルト *frutype* を入力しなかった場合、すべての環境アラーム ステータスに関する情報が表示されます。

コマンド モード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン *frutype* の有効値は次のとおりです。

- **clock number** : 1 および 2
- **earl slot** : 有効値については「使用上のガイドライン」を参照してください。
- **module slot** : 有効値については「使用上のガイドライン」を参照してください。
- **rp slot** : 有効値については「使用上のガイドライン」を参照してください。
- **power-supply number** : 1 および 2
- **supervisor slot** : 有効値については「使用上のガイドライン」を参照してください。
- **vtt number** : 1 ~ 3

slot 引数は、モジュールおよびポート番号を指定します。*slot* の有効値は、使用するシャーシおよびモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合、スロット番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 です。

例 次に、すべての環境アラームのステータスに関する情報を表示する例を示します。

```
Router> show environment alarm threshold
environmental alarm thresholds:

power-supply 1 fan-fail: OK
  threshold #1 for power-supply 1 fan-fail:
    (sensor value != 0) is system minor alarm
```

show environment alarm

```
power-supply 1 power-output-fail: OK
  threshold #1 for power-supply 1 power-output-fail:
    (sensor value != 0) is system minor alarm
fantray fan operation sensor: OK
  threshold #1 for fantray fan operation sensor:
    (sensor value != 0) is system minor alarm
operating clock count: 2
  threshold #1 for operating clock count:
    (sensor value < 2) is system minor alarm
  threshold #2 for operating clock count:
    (sensor value < 1) is system major alarm
operating VTT count: 3
  threshold #1 for operating VTT count:
    (sensor value < 3) is system minor alarm
  threshold #2 for operating VTT count:
    (sensor value < 2) is system major alarm
VTT 1 OK: OK
  threshold #1 for VTT 1 OK:
    (sensor value != 0) is system minor alarm
VTT 2 OK: OK
  threshold #1 for VTT 2 OK:
    (sensor value != 0) is system minor alarm
VTT 3 OK: OK
  threshold #1 for VTT 3 OK:
    (sensor value != 0) is system minor alarm
clock 1 OK: OK
  threshold #1 for clock 1 OK:
    (sensor value != 0) is system minor alarm
clock 2 OK: OK
  threshold #1 for clock 2 OK:
    (sensor value != 0) is system minor alarm
module 1 power-output-fail: OK
  threshold #1 for module 1 power-output-fail:
    (sensor value != 0) is system major alarm
module 1 outlet temperature: 21C
  threshold #1 for module 1 outlet temperature:
    (sensor value > 60) is system minor alarm
  threshold #2 for module 1 outlet temperature:
    (sensor value > 70) is system major alarm
module 1 inlet temperature: 25C
  threshold #1 for module 1 inlet temperature:
    (sensor value > 60) is system minor alarm
  threshold #2 for module 1 inlet temperature:
    (sensor value > 70) is system major alarm
module 1 device-1 temperature: 30C
  threshold #1 for module 1 device-1 temperature:
    (sensor value > 60) is system minor alarm
  threshold #2 for module 1 device-1 temperature:
    (sensor value > 70) is system major alarm
module 1 device-2 temperature: 29C
  threshold #1 for module 1 device-2 temperature:
    (sensor value > 60) is system minor alarm
  threshold #2 for module 1 device-2 temperature:
    (sensor value > 70) is system major alarm
module 5 power-output-fail: OK
  threshold #1 for module 5 power-output-fail:
    (sensor value != 0) is system major alarm
module 5 outlet temperature: 26C
  threshold #1 for module 5 outlet temperature:
    (sensor value > 60) is system minor alarm
  threshold #2 for module 5 outlet temperature:
    (sensor value > 75) is system major alarm
module 5 inlet temperature: 23C
  threshold #1 for module 5 inlet temperature:
```

```
(sensor value > 50) is system minor alarm
threshold #2 for module 5 inlet temperature:
(sensor value > 65) is system major alarm
EARL 1 outlet temperature: N/O
threshold #1 for EARL 1 outlet temperature:
(sensor value > 60) is system minor alarm
threshold #2 for EARL 1 outlet temperature:
(sensor value > 75) is system major alarm
EARL 1 inlet temperature: N/O
threshold #1 for EARL 1 inlet temperature:
(sensor value > 50) is system minor alarm
threshold #2 for EARL 1 inlet temperature:
(sensor value > 65) is system major alarm
Router>
```

関連コマンド

コマンド	説明
show environment status	動作上の FRU ステータスに関する情報を表示します。
show environment temperature	現在の温度値を表示します。

show environment cooling

冷却パラメータに関する情報を表示するには、**show environment cooling** コマンドを使用します。

show environment cooling

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、冷却パラメータに関する情報を表示する例を示します。

```
Router# show environment cooling
fan-tray 1:
  fan-tray 1 fan-fail: failed
fan-tray 2:
  fan 2 type: FAN-MOD-9
  fan-tray 2 fan-fail: OK
chassis cooling capacity: 690 cfm
ambient temperature: 55C
chassis per slot cooling capacity: 75 cfm

module 1 cooling requirement: 70 cfm
module 2 cooling requirement: 70 cfm
module 5 cooling requirement: 30 cfm
module 6 cooling requirement: 70 cfm
module 8 cooling requirement: 70 cfm
module 9 cooling requirement: 30 cfm
Router#
```

関連コマンド	コマンド	説明
	hw-module fan-tray version	ファンのバージョン (ハイまたはロー パワー) タイプを設定します。

show environment status

動作上の FRU ステータスに関する情報を表示するには、**show environment status** コマンドを使用します。

show environment status [*frutype*]

シンタックスの説明	<i>frutype</i> (任意) FRU タイプを指定します。有効値については、「使用上のガイドライン」を参照してください。
------------------	---

コマンドのデフォルト *frutype* を入力しなかった場合、すべての FRU ステータス情報が表示されます。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン *frutype* の有効値は次のとおりです。

- **all** : 引数なし
- **backplane** : 引数なし
- **clock number** : 1 および 2
- **earl slot** : 有効値については「使用上のガイドライン」を参照してください。
- **fan-tray** : 引数なし
- **module slot** : 有効値については「使用上のガイドライン」を参照してください。
- **power-supply number** : 1 および 2
- **rp slot** : 有効値については「使用上のガイドライン」を参照してください。
- **supervisor slot** : 有効値については「使用上のガイドライン」を参照してください。
- **vtt number** : 1 ~ 3

slot 引数は、モジュールおよびポート番号を指定します。*slot* の有効値は、使用するシャーシおよびモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合、スロット番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 です。

例 次に、環境ステータスに関する情報を表示する例を示します。

```
Router> show environment status
backplane:
  operating clock count: 2
  operating VTT count: 3
fan-tray:
```

show environment status

```

    fantray fan operation sensor: OK
VTT 1:
  VTT 1 OK: OK
VTT 2:
  VTT 2 OK: OK
VTT 3:
  VTT 3 OK: OK
clock 1:
  clock 1 OK: OK, clock 1 clock-inuse: not-in-use
clock 2:
  clock 2 OK: OK, clock 2 clock-inuse: in-use
power-supply 1:
  power-supply 1 fan-fail: OK
  power-supply 1 power-output-fail: OK
module 1:
  module 1 power-output-fail: OK
  module 1 outlet temperature: 21C
  module 1 inlet temperature: 25C
  module 1 device-1 temperature: 30C
  module 1 device-2 temperature: 29C
  EARL 1 outlet temperature: N/O
  EARL 1 inlet temperature: N/O
module 5:
  module 5 power-output-fail: OK
  module 5 outlet temperature: 26C
  module 5 inlet temperature: 23C
  module 5 device-1 temperature: 26C
  module 5 device-2 temperature: 27C
Router>

```

次に、大容量の電源装置に関する情報を表示する例を示します。

```

Router# show environment status power-supply 2
power-supply 2:
  power-supply 2 fan-fail: OK
  power-supply 2 power-input 1: none
  power-supply 2 power-input 2: AC low
  power-supply 2 power-input 3: AC high
  power-supply 2 power-output: low (mode 1)
  power-supply 2 power-output-fail: OK

```

表 2-35 に、この例で表示されるフィールドについて説明します。

表 2-35 show environment status コマンドの出カフィールド

フィールド	説明
operating clock count	物理的なクロック数
operating VTT count	物理的な VTT (電圧終端モジュール) 数
fan tray fan operation sensor	システム ファントレイの障害ステータス。システム ファントレイの障害は、マイナーアラームで示されます。
VTT 1、VTT2、および VTT3	シャーシ背面の背面カバーの下にあるシャーシバックプレーン電源モニタのステータス。システムが正常に機能するには、少なくとも 2 つの VTT が稼働している必要があります。マイナーシステムアラームは、3 つの VTT の 1 つが障害を起こすと信号が送られます。メジャーアラームは、複数の VTT が障害を起こし、スーパーバイザエンジンにコンソールポートからアクセスできる場合に信号が送られます。

表 2-35 show environment status コマンドの出力フィールド (続き)

フィールド	説明
clock # clock-inuse	クロック ステータス。いずれかのクロックに障害が発生した場合、障害はマイナー アラームとして処理されます。
power-supply # fan-fail	ファン障害。電源装置のいずれかまたは両方 (存在する場合) にファン障害が発生した場合、障害はマイナー アラームとして処理されます。
power-input-fail	電源入力障害ステータス (none、AC high、AC low)
power-output-fail	電源出力障害ステータス (high、low)
outlet temperature	排気温度値
inlet temperature	吸気温度値
device-1 および device-2 temperature	表示された各モジュールの内部温度を測定する 2 つの装置。表示された温度は、装置が記録している温度を示します。装置は吸気口または排気口に配置されていない、単なる参照ポイントです。

関連コマンド

コマンド	説明
show environment alarm	環境アラームに関する情報を表示します。
show environment temperature	現在の温度値を表示します。

show environment temperature

現在の温度値を表示するには、**show environment temperature** コマンドを使用します。

show environment temperature [*frutype*]

シンタックスの説明

frutype (任意) FRU タイプを指定します。有効値については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

frutype を入力しなかった場合、モジュールおよび EARL 温度値が表示されます。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

frutype の有効値は次のとおりです。

- **earl slot** : 有効値については「使用上のガイドライン」を参照してください。
- **module slot** : 有効値については「使用上のガイドライン」を参照してください。
- **rp slot** : 有効値については「使用上のガイドライン」を参照してください。
- **vtt number** : 1 ~ 3
- **clock number** : 1 および 2

slot 引数は、モジュールおよびポート番号を指定します。*slot* の有効値は、使用するシャーシおよびモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合、スロット番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 です。

show environment temperature module コマンドの出力には、SCP 応答受信後に更新された情報が含まれます。

出力の意味は、次のとおりです。

- N/O (動作不能) : センサが故障していて、使用不可能な値が返されています。
- N/A (利用不可) : センサの値は現在取得できません。あとで再試行してください。
- VTT 1、2、および 3 : シャーシ背面の背面カバーの下にある電源モニタを示します。

例 次に、特定のモジュールの温度情報を表示する例を示します。

```
Router> show environment temperature module 5
module 5 outlet temperature: 34C
module 5 inlet temperature: 27C
module 5 device-1 temperature: 42C
module 5 device-2 temperature: 41C
```

```

module 5 asic-1 (SSO-1) temp: 29C
module 5 asic-2 (SSO-2) temp: 29C
module 5 asic-3 (SSO-3) temp: 29C
module 5 asic-4 (SSO-4) temp: 28C
module 5 asic-5 (SSA-1) temp: 29C
module 5 asic-6 (HYPERION-1) temp: 29C
Router>

```

次に、すべてのモジュールの温度値を表示する例を示します。

```

Router> show environment temperature
VTT 1 outlet temperature: 25C
VTT 2 outlet temperature: 24C
VTT 3 outlet temperature: 28C
module 1 outlet temperature: 24C
module 1 device-2 temperature: 29C
RP 1 outlet temperature: 25C
RP 1 inlet temperature: 29C
EARL 1 outlet temperature: 25C
EARL 1 inlet temperature: 22C
module 5 outlet temperature: 27C
module 5 inlet temperature: 22C
Router#

```

表 2-36 に、この例で表示されるフィールドについて説明します。

表 2-36 show environment temperature コマンドの出カフィールド

フィールド	説明
outlet temperature	排気温度値
inlet temperature	吸気温度値
device-1 および device-2 temperature	表示されたモジュールの内部温度を測定する 2 つの装置。表示された温度は、装置が記録している温度を示します。装置は吸気口または排気口に配置されていない、単なる参照ポイントです。

関連コマンド

コマンド	説明
show environment alarm	環境アラームに関する情報を表示します。
show environment status	動作上の FRU ステータスに関する情報を表示します。

show eobc

EOBC インターフェイスに関する情報を表示するには、**show eobc** コマンドを使用します。

show eobc

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、EOBC インターフェイスに関する情報を表示する例を示します。

```
Router> show eobc
EOBC0/0 is up, line protocol is up
  Hardware is DEC21143, address is 0000.2100.0000 (bia 0000.2100.0000)
  MTU 0 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Unknown duplex, Unknown Speed, MII
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 25/2147483647, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    172196 packets input, 11912131 bytes
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast
    0 input packets with dribble condition detected
  172144 packets output, 11363476 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
Interface EOBC0/0
Hardware is DEC21143
dec21140_ds=0x618FB938, registers=0x3C018000, ib=0x38A9180
rx ring entries=128, tx ring entries=256, af setup failed=0
rxring=0x38A9280, rxr shadow=0x618FBB20, rx_head=28, rx_tail=0
txring=0x38A9AC0, txr shadow=0x618FBD4C, tx_head=72, tx_tail=72, tx_count=0
PHY link up
CSR0=0xF8024882, CSR1=0xFFFFFFFF, CSR2=0xFFFFFFFF, CSR3=0x38A9280
CSR4=0x38A9AC0, CSR5=0xF0660000, CSR6=0x320CA002, CSR7=0xF3FFA261
```

```

CSR8=0xE0000000, CSR9=0xFFFDC3FF, CSR10=0xFFFFFFFF, CSR11=0x0
CSR12=0xC6, CSR13=0xFFFF0000, CSR14=0xFFFFFFFF, CSR15=0x8FF80000
DEC21143 PCI registers:
  bus_no=0, device_no=6
  CFID=0x00191011, CFCS=0x02800006, CFRV=0x02000041, CFLT=0x0000FF00
  CBIO=0x20000801, CBMA=0x48018000, CFIT=0x28140120, CFDD=0x00000400
MII registers:
  Register 0x00:  FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
  Register 0x08:  FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
  Register 0x10:  FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
  Register 0x18:  FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
throttled=0, enabled=0, disabled=0
rx_fifo_overflow=0, rx_no_enp=0, rx_discard=0
tx_underrun_err=0, tx_jabber_timeout=0, tx_carrier_loss=0
tx_no_carrier=0, tx_late_collision=0, tx_excess_coll=0
tx_collision_cnt=0, tx_deferred=0, fatal_tx_err=0, tbl_overflow=0
HW addr filter: 0x38D2EE0, ISL Disabled
Entry= 0:  Addr=0000.0000.0000
Entry= 1:  Addr=0000.0000.0000
Entry= 2:  Addr=0000.0000.0000
Entry= 3:  Addr=0000.0000.0000
Entry= 4:  Addr=0000.0000.0000
Entry= 5:  Addr=0000.0000.0000
Entry= 6:  Addr=0000.0000.0000
Entry= 7:  Addr=0000.0000.0000
Entry= 8:  Addr=0000.0000.0000
Entry= 9:  Addr=0000.0000.0000
Entry=10:  Addr=0000.0000.0000
Entry=11:  Addr=0000.0000.0000
Entry=12:  Addr=0000.0000.0000
Entry=13:  Addr=0000.0000.0000
Entry=14:  Addr=0000.0000.0000
Entry=15:  Addr=0000.2100.0000
Router>

```

次に、ワード出力を含む行を除いて、EOBC インターフェイスに関する情報を表示する例を示します。

```

Router> show eobc | exclude output
EOBC0/0 is up, line protocol is up
  Hardware is DEC21143, address is 0000.2100.0000 (bia 0000.2100.0000)
  MTU 0 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Unknown duplex, Unknown Speed, MII
  ARP type: ARPA, ARP Timeout 04:00:00
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 25/2147483647, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
    175919 packets input, 12196443 bytes
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast
    0 input packets with dribble condition detected
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
Interface EOBC0/0
Hardware is DEC21143
dec21140_ds=0x618FB938, registers=0x3C018000, ib=0x38A9180
rx ring entries=128, tx ring entries=256, af setup failed=0
rxring=0x38A9280, rxr shadow=0x618FBB20, rx_head=7, rx_tail=0
txring=0x38A9AC0, txr shadow=0x618FBD4C, tx_head=209, tx_tail=209, tx_count=0
PHY link up

```

show eobc

```
CSR0=0xF8024882, CSR1=0xFFFFFFFF, CSR2=0xFFFFFFFF, CSR3=0x38A9280
CSR4=0x38A9AC0, CSR5=0xF0660000, CSR6=0x320CA002, CSR7=0xF3FFA261
CSR8=0xE0000000, CSR9=0xFFFDC3FF, CSR10=0xFFFFFFFF, CSR11=0x0
CSR12=0xC6, CSR13=0xFFFF0000, CSR14=0xFFFFFFFF, CSR15=0x8FF80000
DEC21143 PCI registers:
  bus_no=0, device_no=6
  CFID=0x00191011, CFCS=0x02800006, CFRV=0x02000041, CFLT=0x0000FF00
  CBIO=0x20000801, CBMA=0x48018000, CFIT=0x28140120, CFDD=0x00000400
MII registers:
  Register 0x00:  FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
  Register 0x08:  FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
  Register 0x10:  FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
  Register 0x18:  FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
throttled=0, enabled=0, disabled=0
rx_fifo_overflow=0, rx_no_enp=0, rx_discard=0
tx_underrun_err=0, tx_jabber_timeout=0, tx_carrier_loss=0
tx_no_carrier=0, tx_late_collision=0, tx_excess_coll=0
tx_collision_cnt=0, tx_deferred=0, fatal_tx_err=0, tbl_overflow=0
HW addr filter: 0x38D2EE0, ISL Disabled
Entry= 0:  Addr=0000.0000.0000
Entry= 1:  Addr=0000.0000.0000
Entry= 2:  Addr=0000.0000.0000
Entry= 3:  Addr=0000.0000.0000
Entry= 4:  Addr=0000.0000.0000
Entry= 5:  Addr=0000.0000.0000
Entry= 6:  Addr=0000.0000.0000
Entry= 7:  Addr=0000.0000.0000
Entry= 8:  Addr=0000.0000.0000
Entry= 9:  Addr=0000.0000.0000
Entry=10:  Addr=0000.0000.0000
Entry=11:  Addr=0000.0000.0000
Entry=12:  Addr=0000.0000.0000
Entry=13:  Addr=0000.0000.0000
Entry=14:  Addr=0000.0000.0000
Entry=15:  Addr=0000.2100.0000
Router>
```

show erm statistics

IPv4、IPv6、および MPLS プロトコルの FIB TCAM 例外ステータスを表示するには、**show erm statistics** コマンドを使用します。

show erm statistics

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン IPv4、IPv6、および MPLS 例外ステートでは、プロトコルが例外状態でない場合 FALSE を表示し、プロトコルが例外状態の場合に TRUE を表示します。

例 次に、IPv4、IPv6、および MPLS プロトコルの FIB TCAM 例外ステータスを表示する例を示します。

```
Router> show erm statistics
#IPv4 excep notified      = 0
#IPv6 excep notified      = 0
#MPLS excep notified      = 0
#IPv4 reloads done        = 0
#IPv6 reloads done        = 0
#MPLS reloads done        = 0
Current IPv4 excep state = FALSE
Current IPv6 excep state = FALSE
Current MPLS excep state = FALSE
#Timer expired            = 0
#of erm msgs               = 1
Router>
```

関連コマンド	コマンド	説明
	mls erm priority	例外ステータスから回復させるプロトコルの順番を定義するプライオリティを割り当てます。

show errdisable detect

errdisable 検出ステータスを表示するには、**show errdisable detect** コマンドを使用します。

show errdisable detect

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、errdisable 検出ステータスを表示する例を示します。

```
Router# show errdisable detect
ErrDisable Reason    Detection status
-----
udld                  Enabled
bpduguard             Enabled
rootguard             Enabled
packet-buffer-err    Enabled
pagp-flap             Enabled
dtp-flap              Enabled
link-flap             Enabled
Router#
```

関連コマンド	コマンド	説明
	errdisable detect cause	errdisable 検出をイネーブルにします。

show errdisable flap-value

errdisable 検出のフラップ値を表示するには、**show errdisable flap-value** コマンドを使用します。

show errdisable flap-value

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、errdisable 検出のフラップ値を表示する例を示します。

```
Router# show errdisable flap-value
ErrDisable Reason    Flaps    Time (sec)
-----
pagp-flap            3         30
dtp-flap              3         30
link-flap             5         10
Router#Router#
```

関連コマンド	コマンド	説明
	errdisable detect cause	errdisable 検出をイネーブルにします。

show errdisable recovery

errdisable 回復タイマーに関する情報を表示するには、**show errdisable recovery** コマンドを使用します。

show errdisable recovery

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、errdisable 回復タイマーに関する情報を表示する例を示します。

```
Router# show errdisable recovery
ErrDisable Reason    Timer Status
-----
udld                  Enabled
bpduguard            Enabled
rootguard            Enabled
pagp-flap            Enabled
dtp-flap             Enabled
link-flap            Enabled

Timer interval:300 seconds

Interfaces that will be enabled at the next timeout:

Interface    Errdisable reason    Time left(sec)
-----
Fa9/4        link-flap            279
```

関連コマンド

コマンド	説明
errdisable recovery	回復メカニズム変数を設定します。
show interfaces status	インターフェイス ステータスを表示したり、LAN ポートで errdisable ステートにあるインターフェイスだけのリストを表示したりします。

show etherchannel

チャンネルの EtherChannel 情報を表示するには、**show etherchannel** コマンドを使用します。

```
show etherchannel [channel-group] {port-channel | brief | detail | summary | port |
load-balance | protocol}
```

シンタックスの説明	
<i>channel-group</i>	(任意) チャンネル グループの番号。有効値は 1 ~ 282 の範囲の最大 64 個の値です。
port-channel	ポート チャンネル情報を表示します。
brief	EtherChannel 情報のサマリーを表示します。
detail	EtherChannel の詳細を表示します。
summary	各チャンネル グループのサマリーを 1 行で表示します。
port	EtherChannel ポート情報を表示します。
load-balance	ロードバランス情報を表示します。
protocol	イネーブル化されたプロトコルを表示します。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン *channel-group* を指定しない場合は、すべてのチャンネル グループが表示されます。257 ~ 282 の *channel-group* 値は、CSM および FWSM だけでサポートされています。

次の例の [Passive port] フィールドは、レイヤ 3 ポート チャンネルに対してだけ表示されます。このフィールドは、まだ起動していない物理インターフェイスが、チャンネル グループに含まれるように設定されている (かつ間接的にチャンネル グループ内の唯一のポート チャンネルである) ことを意味します。インターフェイスがモード ON のチャンネルの一部として設定されている場合、**show etherchannel protocol** の出力には、[Protocol: - (Mode ON)] が表示されます。

show etherchannel summary コマンドの出力には、次の注意事項が適用されます。

- チャンネル モードがオンの場合、チャンネルに使用されるプロトコルの表示カラムにはハイフン (-) が表示されます。
- LACP では、複数のアグリゲータがサポートされています。たとえば、2 つの異なるバンドルを作成した場合、Po1 はプライマリ アグリゲータを、Po1A と Po1B はセカンダリ アグリゲータを示します。

show etherchannel load-balance コマンドの出力には、次の注意事項が適用されます。

- IPv6 トラフィックの EtherChannel ロードバランシングでは、トラフィックが EtherChannel 上にブリッジされる場合（たとえば、レイヤ 2 チャンネルで同じ VLAN 内のトラフィックが全体にブリッジされる場合）、そのトラフィックは常に、設定に応じて IPv6 アドレス、src、dest、または src-dest によってロードバランシングされます。そのため、スイッチは IPv6 トラフィック ブリッジで MAC/IP/ports を無視します。src-dst-mac を設定する場合は、src-dst-ip(v6) アドレスが使用されます。src-mac を設定する場合は、src-ip(v6) アドレスが使用されます。
- レイヤ 2 またはレイヤ 3 チャンネルを通じてルーティングされる IPv6 トラフィックは、設定に応じて、MAC アドレスまたは IPv6 アドレスに基づいてロードバランシングされます。MAC/IP および src/dst/src-dest はサポートされますが、レイヤ 4 ポートに基づくロードバランシングはサポートされません。port キーワードを使用した場合、IPv6 アドレス、src、dst、または src-dest が使用されます。

例

次に、特定のグループのポート チャンネル情報を表示する例を示します。

```
Router# show etherchannel 12 port-channel
Group: 12
-----
                Port-channels in the group:
                -----
Port-channel: Po1
-----

Age of the Port-channel   = 143h:01m:12s
Logical slot/port        = 14/1           Number of ports = 2
GC                        = -             HotStandBy port = null
Port state                = Port-channel Ag-Inuse
Protocol                  = LACP

Ports in the Port-channel:

Index  Load  Port    EC state
-----+-----+-----+-----
    0    55    Fa4/1   active
    1    AA    Fa4/2   active

Time since last port bundled: 16h:28m:58s   Fa4/1
Time since last port Un-bundled: 16h:29m:00s   Fa4/4
Router#
```

次に、ロードバランス情報を表示する例を示します。

```
Router# show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
    dst-mac
    mpls label-ip
EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Destination MAC address
IPv4: Destination MAC address
IPv6: Destination MAC address (routed packets)
    Destination IP address (bridged packets)
MPLS: Label or IP
Router#
```

次に、特定のグループに関する情報のサマリーを表示する例を示します。

```
Router# show etherchannel 1 brief
Group: 1
-----
Group state = L2
Ports: 4   Maxports = 8
Port-channels: 1 Max Port-channels = 1
Protocol: LACP
Router#
```

次に、特定のグループに関する詳細情報を表示する例を示します。

```
Router# show etherchannel 12 detail
Group state = L2
Ports: 1   Maxports = 8
Port-channels: 1 Max Port-channels = 1
Protocol:   PAgP
          Ports in the group:
          -----
Port: Fa5/2
-----

Port state      = Down Not-in-Bndl
Channel group   = 12           Mode = Desirable-S1       Gcchange = 0
Port-channel    = null        GC   = 0x00000000       Pseudo port-channel = Po1
2
Port index      = 0           Load = 0x00           Protocol =   PAgP

Flags:  S - Device is sending Slow LACPDUs  F - Device is sending fast LACPDUs
        A - Device is in active mode         P - Device is in passive mode

Local information:

Port      Flags  State  LACP Port  Admin  Oper  Port  Port
Fa4/1    SA     bndl   Priority   Key    Key   Number State
          32768 100    100      0xc1  0x75

Partner's information:

Port      Partner          Partner          Partner
System ID System ID        Port Number     Age  Flags
Fa4/1    8000,00b0.c23e.d861  0x81           14s  SP

          LACP Partner  Partner  Partner
          Port Priority  Oper Key   Port State
          32768          128     0x81

Age of the port in the current state: 16h:27m:42s

          Port-channels in the group:
          -----
Port-channel: Po12
-----

Age of the Port-channel   = 04d:02h:52m:26s
Logical slot/port        = 14/1           Number of ports = 0
GC                        = 0x00000000       HotStandBy port = null
Port state                = Port-channel Ag-Not-Inuse
Protocol                  =   PAgP

Router#
```

show etherchannel

次に、各チャンネル グループのサマリーを 1 行で表示する例を示します。

```
Router# show etherchannel summary
Flags: D - down          P - in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator

Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
12    Po12 (SD)      PAgP       Fa5/2 (D)
24    Po24 (RD)      -          -
Router#
```

次に、特定のグループの EtherChannel ポートに関する情報を表示する例を示します。

```
Router# show etherchannel 1 port
Channel-group listing:
-----
Group: 1
-----
Ports in the group:
-----
Port: Fa5/4
-----
Port state = EC-Enbld Down Not-in-Bndl Usr-Config
Channel group = 1          Mode = Desirable      Gcchange = 0
Port-channel = null       GC = 0x00000000      Pseudo-agport = Pol
Port index = 0            Load = 0x00          Protocol = LACP

Flags: S - Device is sending Slow LACPDUs F - Device is sending fast LACPDUs
       A - Device is in active mode       P - Device is in passive mode

Local information:

Port      Flags  State      LACP Port  Admin  Oper  Port  Port
Fa5/4    SA    bndl      32768      100    100   0xc1  0x75

Partner's information:

Port      Partner
Fa5/4    System ID
          8000,00b0.c23e.d861
          Partner
          Port Number  Age  Flags
          0x81        14s SP

          LACP Partner  Partner  Partner
          Port Priority  Oper Key  Port State
          32768      128    0x81

Age of the port in the current state: 04d:02h:57m:38s
Router#
```

次に、イネーブル化されたプロトコルを表示する例を示します。

```
Router# show etherchannel protocol
Channel-group listing:
-----
Group: 12
-----
Protocol: PAgP

Group: 24
-----
```

```
Protocol: - (Mode ON)
Router#
```

関連コマンド

コマンド	説明
channel-group	EtherChannel インターフェイスの EtherChannel グループへの割り当ておよび設定を行います。
channel-protocol	チャンネルを管理するためにインターフェイスで使用するプロトコルを設定します。
interface port-channel	ポート チャンネル仮想インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。

show fm features

機能マネージャに関する情報を表示するには、**show fm features** コマンドを使用します。

show fm features

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、機能マネージャに関する情報を表示する例を示します。

```
Router> show fm features
Designated PISA:1 Non-designated PISA:1

Redundancy Status:designated
Interface:FastEthernet2/10 IP is enabled
  hw[EGRESS] = 1, hw[INGRESS] = 1
  hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 0
  mcast = 0
  priority = 2
  reflexive = 0
  inbound label:1
    protocol:ip
      feature #:1
      feature id:FM_IP_ACCESS
      ACL:106
  outbound label:2
    protocol:ip
      feature #:1
      feature id:FM_IP_ACCESS
      ACL:106
Interface:FastEthernet2/26 IP is enabled
  hw[EGRESS] = 1, hw[INGRESS] = 0
  hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 1
  mcast = 0
  priority = 2
  reflexive = 0
  inbound label:24
    protocol:ip
      feature #:1
      feature id:FM_IP_ACCESS
      ACL:113
  outbound label:3
    protocol:ip
      feature #:1
      feature
```

```

id:FM_IP_WCCP
    Service ID:0
    Service Type:0
Interface:Vlan55 IP is enabled
    hw[EGRESS] = 1, hw[INGRESS] = 1
    hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 0
    mcast = 0
    priority = 2
    reflexive = 0
    inbound label:4
        protocol:ip
        feature #:1
        feature id:FM_IP_ACCESS
        ACL:111
Interface:Vlan101 IP is enabled
    hw[EGRESS] = 1, hw[INGRESS] = 1
    hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 0
    mcast = 0
    priority = 2
    reflexive = 0
    inbound label:5
        protocol:ip
        feature #:1
        feature id:FM_IP_ACCESS
        ACL:101
    outbound label:6
        protocol:ip
        feature #:1
        feature id:FM_IP_ACCESS
        ACL:101
Router>

```

次に、先頭行が [Redundancy] で始まる機能マネージャ情報を表示する例を示します。

```

Router> show fm features | begin Redundancy
Redundancy Status: designated
Router>

```

show fm inband-counters

PISA から送信された SLB および WCCP の帯域内パケット数を表示するには、**show fm inband-counters** コマンドを使用します。

show fm inband-counters

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン **show fm inband-counters** コマンドの出力には、PISA により送信された SLB 帯域内パケット数、および PISA により送信された WCCP 帯域内パケット数が含まれます。

CBAC が設定されている場合、コマンドの出力は、PISA により CBAC に送信されたパケット数を表示します。

例 次に、PISA により送信された SLB および WCCP 帯域内パケット数を表示する例を示します。

```
Router# show fm inband-counters
      Inband Packets Sent
Slot  WCCP      SLB
  1    0         0
  2    0         0
  3    0         0
  4    0         0
  5    0         0
  6    0         0
  7    0         0
  8    0         0
  9    0         0
 10    0         0
 11    0         0
 12    0         0
 13    0         0
Router#
```

show fm insp

CBAC が設定された ACL およびポートのリストおよびステータスを表示するには、**show fm insp** コマンドを使用します。

show fm insp [detail]

シンタックスの説明	detail (任意) すべてのフロー情報を表示します。
-----------	-------------------------------------

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン CBAC を設定する前にポートに VAACL が設定されている場合は、ステータス INACTIVE が表示されます。それ以外の場合はステータス ACTIVE が表示されます。PFC リソースが枯渇している場合にこのコマンドを実行すると、BRIDGE が表示され、そのあとに、処理のために PISA に送信された、現在アクティブな失敗した NetFlow 要求の数が表示されます。

show fm insp コマンドの出力には、次の情報が含まれます。

- **interface:** - IP 検査機能がイネーブルであるインターフェイス
- **(direction)** - IP 検査機能がイネーブルである方向 (IN または OUT)
- **acl name:** - 検査中のパケットの識別に使用する名前
- **status:** - (ACTIVE または INACTIVE) このインターフェイスと方向の組み合わせがハードウェアでサポートされているかどうか (ハードウェアでサポートされている場合は ACTIVE、それ以外は INACTIVE)

オプションで **detail** キーワードを指定すると、指定されたインターフェイス方向の IP 検査に使用される ACL 内の ACE が表示されます。

例 次に、CBAC が設定された ACL およびポートのリストおよびステータスを表示する例を示します。

```
Router> show fm insp
interface:Vlan305(in) status :ACTIVE
acl name:deny
interfaces:
Vlan305(out):status ACTIVE
```

show fm interface

機能マネージャに関する詳細情報をインターフェイス単位で表示するには、**show fm interface** コマンドを使用します。

```
show fm interface {{interface interface-number} | {null interface-number} |
                  {port-channel number} | {vlan vlan-id}}
```

シンタックスの説明

<i>interface</i>	インターフェイス タイプ。有効値は ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、および ge-wan です。
<i>interface-number</i>	モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
null <i>interface-number</i>	ヌル インターフェイスを指定します。有効値は 0 です。
port-channel <i>number</i>	チャンネル インターフェイスを指定します。有効値は 1 ~ 282 の範囲の最大 64 個の値です。
vlan <i>vlan-id</i>	VLAN を指定します。有効値は 1 ~ 4094 です。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

interface-number 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

257 ~ 282 の **port-channel number** 値は、CSM および FWSM だけでサポートされています。

例

次に、指定されたインターフェイスの機能マネージャに関する詳細情報を表示する例を示します。

```
Router# show fm interface fastethernet 2/26
Interface:FastEthernet2/26 IP is enabled
  hw[EGRESS] = 1, hw[INGRESS] = 0
  hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 1
  mcast = 0
  priority = 2
  reflexive = 0
  inbound label:24
    protocol:ip
    feature #:1
```

```

feature id:FM_IP_ACCESS
ACL:113
  vmr IP value #1:0, 0, 0, 0, 0, 0, 0, 0, 6 - 1
  vmr IP mask #1:0, 0, FFFF, FFFF, 0, 0, 0, FF
  vmr IP value #2:642D4122, 0, 0, 0, 1, 0, 0, 6 - 1
  vmr IP mask #2:FFFFFFFF, 0, 0, 0, 1, 0, 0, FF
  vmr IP value #3:0, 64020302, 0, 0, 6, 0, 0, 6 - 1
  vmr IP mask #3:0, FFFFFFFF, 0, 0, 6, 0, 0, FF
  vmr IP value #4:0, 64020302, 0, 0, A, 0, 0, 6 - 1
  vmr IP mask #4:0, FFFFFFFF, 0, 0, A, 0, 0, FF
  vmr IP value #5:0, 64020302, 0, 0, 12, 0, 0, 6 - 1
  vmr IP mask #5:0, FFFFFFFF, 0, 0, 12, 0, 0, FF
  vmr IP value #6:0, 0, 0, 0, 0, 0, 0, 0 - 2
  vmr IP mask #6:0, 0, 0, 0, 0, 0, 0, 0
outbound label:3
  protocol:ip
  feature #:1
  feature id:FM_IP_WCCP
  Service ID:0
  Service Type:0
Router#

```

次に、特定の VLAN 上の機能マネージャに関する詳細情報を表示する例を示します。

```

Router# show fm interface vlan 21
Interface: Vlan21 IP is disabled
hw_state[INGRESS] = not reduced, hw_state[EGRESS] = not reduced
mcast = 0
priority = 0
flags = 0x0
inbound label: 8
Feature IP_VACL:
-----
FM_FEATURE_IP_VACL_INGRESS i/f: V121 map name: test
=====
IP Seq. No: 10 Seq. Result : VACL_ACTION_FORWARD_CAPTURE
-----
DPort - Destination Port SPort - Source Port Pro - Protocol
X - XTAG TOS - TOS Value Res - VMR Result
RFM - R-Recirc. Flag MRTNP - M-Multicast Flag R - Reflexive flag
- F-Fragment flag - T-Tcp Control N - Non-cachable
- M-More Fragments - P-Mask Priority(H-High, L-Low)
Adj. - Adj. Index T - M(Mask)/V(Value) FM - Flow Mask
NULL - Null FM SAO - Source Only FM DAO - Dest. Only FM
SADA - Sour.& Dest. Only VSADA - Vlan SADA Only FF - Full Flow
VFF - Vlan Full Flow F-VFF - Either FF or VFF A-VSD - Atleast VSADA
A-FF - Atleast FF A-VFF - Atleast VFF A-SON - Atleast SAO
A-DON - Atleast DAO A-SD - Atleast SADA SHORT - Shortest
A-SFF - Any short than FF A-EFF - Any except FF A-EVFF- Any except VFF
A-LVFF- Any less than VFF ERR - Flowmask Error
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|Indx|T| Dest Ip Addr | Source Ip Addr|DPort|SPort|Pro|RFM|X|ToS|MRTNP|Adj.| FM |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
1 V 22.2.2.2 21.1.1.1 0 0 0 --- 0 0 ----L ---- SHORT
M 255.255.255.255 255.255.255.255 0 0 0 000 0 0
TM_PERMIT_RESULT
2 V 32.2.2.2 31.1.1.1 0 0 0 --- 0 0 ----L ---- SHORT
M 255.255.255.255 255.255.255.255 0 0 0 000 0 0
TM_PERMIT_RESULT
3 V 0.0.0.0 0.0.0.0 0 0 0 --- 0 0 ----L ---- SHORT
M 0.0.0.0 0.0.0.0 0 0 0 000 0 0
TM_L3_DENY_RESULT

```

show fm interface

```

-----
IP Seq. No: 65536 Seq. Result : VACL_ACTION_DROP
-----
+---+-----+-----+-----+-----+-----+-----+-----+-----+
|Indx|T| Dest Ip Addr | Source Ip Addr|DPort|SPort|Pro|R|FM|X|ToS|MR|TNP|Adj.| FM |
+---+-----+-----+-----+-----+-----+-----+-----+-----+
1 V 0.0.0.0 0.0.0.0 0 0 0 --- 0 0 ----L ---- SHORT
M 0.0.0.0 0.0.0.0 0 0 0 000 0 0
TM_PERMIT_RESULT
Router#

```

show fm ipv6 traffic-filter

IPv6 情報を表示するには、**show fm ipv6 traffic-filter** コマンドを使用します。

show fm ipv6 traffic-filter {all | {interface interface interface-number}}

シンタックスの説明	パラメータ	説明
	all	IPv6 トラフィック フィルタ情報をすべてのインターフェイスについて表示します。
	interface interface	指定されたインターフェイスの IPv6 トラフィック フィルタ情報を表示します。有効値は ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 atm 、および ge-wan です。
	interface-number	モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン *interface-number* 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

例 次に、特定のインターフェイスの IPv6 情報を表示する例を示します。

```
Router# show fm ipv6 traffic-filter interface vlan 50
-----
FM_FEATURE_IPV6_ACG_INGRESS Name:testipv6 i/f: Vlan50
=====
DPort - Destination Port SPort - Source Port Pro - Protocol
X - XTAG TOS - TOS Value Res - VMR Result
RFM - R-Recirc. Flag MRTNP - M-Multicast Flag R - Reflexive flag
- F-Fragment flag - T-Tcp Control N - Non-cachable
- M-More Fragments - P-Mask Priority(H-High, L-Low)
Adj. - Adj. Index T - M(Mask)/V(Value) FM - Flow Mask
NULL - Null FM SAO - Source Only FM DAO - Dest. Only FM
SADA - Sour.& Dest. Only VSADA - Vlan SADA Only FF - Full Flow
VFF - Vlan Full Flow F-VFF - Either FF or VFF A-VSD - Atleast VSADA
A-FF - Atleast FF A-VFF - Atleast VFF A-SON - Atleast SAO
A-DON - Atleast DAO A-SD - Atleast SADA SHORT - Shortest
A-SFF - Any short than FF A-EFF - Any except FF A-EVFF- Any except VFF
A-LVFF- Any less than VFF ERR - Flowmask Error
```

show fm ipv6 traffic-filter

```

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|Indx|T| Dest IPv6 Addr | Source IPv6
Addr |Pro|RfM|X|MRTNP|Adj.| FM |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 V 0:200E::
200D::1 0 -F- - ----L ---- Shorte
M 0:FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 0 1
TM_SOFT_BRIDGE_RESULT
2 V 0:200E::
200D::1 17 --- - ----L ---- Shorte
M 0:FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 255 0
TM_PERMIT_RESULT
3 V 200E::
200D::1 0 -F- - ----L ---- Shorte
M FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 0 1
TM_SOFT_BRIDGE_RESULT
4 V 200E::
200D::1 17 --- - ----L ---- Shorte
M FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 255 0
TM_PERMIT_RESULT
5 V
:: : 0 -F- - ----L ---- Shorte
M
:: : 0 1
TM_SOFT_BRIDGE_RESULT
6 V
:: : 0 -F- - ----L ---- Shorte
M
:: : 0 1
TM_SOFT_BRIDGE_RESULT
7 V
:: : 58 --- - ----L ---- Shorte
M
:: : 255 0
TM_PERMIT_RESULT
8 V
:: : 58 --- - ----L ---- Shorte
M
:: : 255 0
TM_PERMIT_RESULT
9 V
:: : 58 --- - ----L ---- Shorte
M
:: : 255 0
TM_PERMIT_RESULT
10 V
:: : 58 --- - ----L ---- Shorte
M
:: : 255 0
TM_PERMIT_RESULT
11 V
:: : 58 --- - ----L ---- Shorte
M
:: : 255 0
TM_PERMIT_RESULT
12 V
:: : 58 --- - ----L ---- Shorte
M

```

```

:: :: 255 0
TM_PERMIT_RESULT
13 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
14 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
15 V
:: :: 0 --- - ----L ---- Shorte
M
:: :: 0 0
TM_L3_DENY_RESULT
Router#

```

次に、すべてのインターフェイスの IPv6 情報を表示する例を示します。

```
Router# show fm ipv6 traffic-filter all
```

```

-----
FM_FEATURE_IPV6_ACG_INGRESS Name:testipv6 i/f: Vlan50
=====
DPort - Destination Port SPort - Source Port Pro - Protocol
X - XTAG TOS - TOS Value Res - VMR Result
RFM - R-Recirc. Flag MRTNP - M-Multicast Flag R - Reflexive flag
- F-Fragment flag - T-Tcp Control N - Non-cachable
- M-More Fragments - P-Mask Priority(H-High, L-Low)
Adj. - Adj. Index T - M(Mask)/V(Value) FM - Flow Mask
NULL - Null FM SAO - Source Only FM DAO - Dest. Only FM
SADA - Sour.& Dest. Only VSADA - Vlan SADA Only FF - Full Flow
VFF - Vlan Full Flow F-VFF - Either FF or VFF A-VSD - Atleast VSADA
A-FF - Atleast FF A-VFF - Atleast VFF A-SON - Atleast SAO
A-DON - Atleast DAO A-SD - Atleast SADA SHORT - Shortest
A-SFF - Any short than FF A-EFF - Any except FF A-EVFF- Any except VFF
A-LVFF- Any less than VFF ERR - Flowmask Error
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
|Indx|T| Dest IPv6 Addr | Source IPv6
Addr |Pro|RFM|X|MRTNP|Adj.| FM |
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
1 V 0:200E::
200D::1 0 -F- - ----L ---- Shorte
M 0:FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 0 1
TM_SOFT_BRIDGE_RESULT
2 V 0:200E::
200D::1 17 --- - ----L ---- Shorte
M 0:FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 255 0
TM_PERMIT_RESULT
3 V 200E::
200D::1 0 -F- - ----L ---- Shorte
M FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 0 1
TM_SOFT_BRIDGE_RESULT
4 V 200E::
200D::1 17 --- - ----L ---- Shorte
M FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 255 0
TM_PERMIT_RESULT

```

■ show fm ipv6 traffic-filter

```
5 V
:: :: 0 -F- - ----L ---- Shorte
M
:: :: 0 1
TM_SOFT_BRIDGE_RESULT
6 V
:: :: 0 -F- - ----L ---- Shorte
M
:: :: 0 1
TM_SOFT_BRIDGE_RESULT
7 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
8 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
9 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
10 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
13 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
.
. Output is truncated
.
Interface(s) using this IPv6 Ingress Traffic Filter:
V150,
```

show fm nat netflow data

NAT に関する NetFlow データの情報を表示するには、**show fm nat netflow data** コマンドを使用します。

show fm nat netflow data

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、NAT 関連の NetFlow データに関する情報を表示する例を示します。

```
Router> show fm nat netflow data
FM Pattern with stat push disabled: 1
Default/TCP/UDP Timeouts:
Def s/w timeout: 86400 h/w timeout: 300 Pattern(ingress): 4
Pattern(egress): 4 Push interval: 1333
TCP s/w timeout: 86400 h/w timeout: 300 Pattern(ingress): 4
Pattern(egress): 4 Push interval: 1333
UDP s/w timeout: 300 h/w timeout: 300 Pattern(ingress): 3
Pattern(egress): 3 Push interval: 100
Port Timeouts:
Idle timeout :3600 secs
Fin/Rst timeout :10 secs
Fin/Rst Inband packets sent per timeout :10000
Netflow mode to Zero-out Layer4 information for fragment packet lookup :
Enabled
Router>
```

show fm reflexive

ダイナミック機能マネージャの再帰エントリに関する情報を表示するには、**show fm reflexive** コマンドを使用します。

show fm reflexive

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、ダイナミック機能マネージャの再帰エントリに関する情報を表示する例を示します。

```
Router# show fm reflexive
Reflexive hash table:
  Vlan613:refacl, OUT-REF, 64060E0A, 64060D0A, 0, 0, 7, 783, 6

Router#
```

show fm summary

機能マネージャ情報のサマリーを表示するには、**show fm summary** コマンドを使用します。

show fm summary

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、機能マネージャ情報のサマリーを表示する例を示します。

```
Router# show fm summary
Current global ACL merge algorithm:BDD
Interface:FastEthernet2/10
  ACL merge algorithm used:
    inbound direction: ODM
    outbound direction:BDD
  TCAM screening for features is ACTIVE outbound
  TCAM screening for features is ACTIVE inbound
Interface:FastEthernet2/26
  ACL merge algorithm used:
    inbound direction: ODM
    outbound direction:BDD
  TCAM screening for features is ACTIVE outbound
  TCAM screening for features is INACTIVE inbound
.
.
.
Router#
```

show fm vlan

VLAN 単位の機能マネージャに関する情報を表示するには、**show fm vlan** コマンドを使用します。

show fm vlan *vlan-id*

シンタックスの説明

vlan-id VLAN ID。有効値は 1 ~ 4094 です。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、VLAN 単位の機能マネージャに関する情報を表示する例を示します。

```
Router# show fm vlan 1
hw[EGRESS] = 1, hw[INGRESS] = 1
hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 0
mcast = 0
priority = 2
reflexive = 0
vacc_map : map1
inbound label: 5
merge_err: 0
protocol: ip
feature #: 1
feature id: FM_VACL
map_name: map1
seq #: 10
(only for IP_PROT) DestAddr SrcAddr Dpt Spt L4OP TOS Est prot Rslt
vmr IP value # 1: 0.0.0.0 0.0.0.0 0 0 0 0 0 6 permit
vmr IP mask # 1: 0.0.0.0 0.0.0.0 0 0 0 0 0 FF
vmr IP value # 2: 0.0.0.0 0.0.0.0 0 0 0 0 0 11 permit
vmr IP mask # 2: 0.0.0.0 0.0.0.0 0 0 0 0 0 FF
vmr IP value # 3: 0.0.0.0 0.0.0.0 0 0 0 0 0 0 deny
vmr IP mask # 3: 0.0.0.0 0.0.0.0 0 0 0 0 0 0
seq #: 65536
(only for IP_PROT) DestAddr SrcAddr Dpt Spt L4OP TOS Est prot Rslt
vmr IP value # 1: 0.0.0.0 0.0.0.0 0 0 0 0 0 0 permit
vmr IP mask # 1: 0.0.0.0 0.0.0.0 0 0 0 0 0 0
outbound label: 6
merge_err: 0
protocol: ip
feature #: 1
feature id: FM_VACL
map_name: map1
seq #: 10
(only for IP_PROT) DestAddr SrcAddr Dpt Spt L4OP TOS Est prot Rslt
vmr IP value # 1: 0.0.0.0 0.0.0.0 0 0 0 0 0 6 permit
```

```
vmr IP mask # 1: 0.0.0.0 0.0.0.0 0 0 0 0 0 FF
vmr IP value # 2: 0.0.0.0 0.0.0.0 0 0 0 0 0 11 permit
vmr IP mask # 2: 0.0.0.0 0.0.0.0 0 0 0 0 0 FF
vmr IP value # 3: 0.0.0.0 0.0.0.0 0 0 0 0 0 0 deny
vmr IP mask # 3: 0.0.0.0 0.0.0.0 0 0 0 0 0 0
seq #: 65536
(only for IP_PROT) DestAddr SrcAddr Dpt Spt L4OP TOS Est prot Rslt
vmr IP value # 1: 0.0.0.0 0.0.0.0 0 0 0 0 0 0 permit
vmr IP mask # 1: 0.0.0.0 0.0.0.0 0 0 0 0 0 0
```

show icc

ICC カウンタおよびステータスに関する情報を表示するには、**show icc** コマンドを使用します。

show icc {counters | status}

シンタックスの説明

counters	カウンタ情報を指定します。
status	ステータス情報を指定します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、ICC カウンタに関する情報を表示する例を示します。

```
Router# show icc counters
total tx RPC packets to slot 1 LCP = 0
  detail by request id: (<request-id>=<number-of-packets>)
    2 =0          7 =0          8 =0          10=0
    11=0         12=0         14=0         17=0
    18=0         19=0         20=0
total rx RPC packets from slot 1 LCP = 0
  detail by request id: (<request-id>=<number-of-packets>)
    2 =5          7 =7          8 =11         10=4
    11=1         12=2         14=1         17=67
    18=7         19=159       20=29
total tx MCAST-SP packets to slot 1 LCP = 0
  detail by request id: (<request-id>=<number-of-packets>)
    6 =0          7 =0          8 =0          9 =0
    12=0         14=0
total rx MCAST-SP packets from slot 1 LCP = 0
  detail by request id: (<request-id>=<number-of-packets>)
    6 =1          7 =1          8 =1          9 =1
    12=41        14=67
total tx L3-MGR packets to slot 1 LCP = 0
  detail by request id: (<request-id>=<number-of-packets>)
    1 =0          2 =0          3 =0
total rx L3-MGR packets from slot 1 LCP = 0
  detail by request id: (<request-id>=<number-of-packets>)
    1 =1          2 =2          3 =1
Router#
```

次に、ICC ステータスに関する情報を表示する例を示します。

```
Router# show icc status
Class Name           Msgs Pending   Max Pending   Total Sent
-----
  2 RPC                0              3             403
```

```
3 MSC 0 1 1
5 L3-MGR 0 4 4173
13 TCAM-API 0 10 26
Router#
```

show idprom

FRU の IDPROM を表示するには、**show idprom** コマンドを使用します。

show idprom {**all** | *frutype* | **interface** *interface slot*} [**detail**]

シンタックスの説明

all	すべての FRU タイプの情報を表示します。
<i>frutype</i>	情報を表示する FRU タイプを指定します。有効値については、「使用上のガイドライン」を参照してください。
interface <i>interface slot</i>	情報を表示するインターフェイスを指定します。有効値は次のとおりです。 <ul style="list-style-type: none"> <i>interface</i> : GigabitEthernet <i>slot</i> : 1 ~ 13 詳細については、「使用上のガイドライン」を参照してください。
detail	(任意) IDPROM データの詳細を表示します (詳細)。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

有効な *frutypes* は次のとおりです。

- **backplane** : 引数なし
- **clock number** : 1 および 2
- **earl slot** : 有効値については以下を参照してください。
- **module slot** : 有効値については以下を参照してください。
- **rp slot** : 有効値については以下を参照してください。
- **power-supply** : 1 および 2
- **supervisor slot** : 有効値については以下を参照してください。
- **vtt number** : 1 ~ 3

slot 引数は、モジュールおよびポート番号を指定します。*slot* の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロットシャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビットイーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

シャーシのシリアル番号を表示するには、**show idprom backplane** コマンドを使用します。

オプションの **interface interface slot** キーワードおよび引数は、GBIC セキュリティ対応インターフェイスだけでサポートされています。

例

次に、クロック 1 の IDPROM 情報を表示する例を示します。

```
Router> show idprom clock 1
IDPROM for clock #1
(FRU is 'Clock FRU')
OEM String = 'Cisco Systems'
Product Number = 'WS-C6000-CL'
Serial Number = 'SMT03073115'
Manufacturing Assembly Number = '73-3047-04'
Manufacturing Assembly Revision = 'A0'
Hardware Revision = 1.0
Current supplied (+) or consumed (-) = 0.000A
Router>
```

次に、電源装置 1 の IDPROM 情報を表示する例を示します。

```
Router> show idprom power-supply 1
IDPROM for power-supply #1
(FRU is '110/220v AC power supply, 1360 watt')
OEM String = 'Cisco Systems, Inc.'
Product Number = 'WS-CAC-1300W'
Serial Number = 'ACP03020001'
Manufacturing Assembly Number = '34-0918-01'
Manufacturing Assembly Revision = 'A0'
Hardware Revision = 1.0
Current supplied (+) or consumed (-) = 27.460A
Router>
```

次に、電源装置 1 の IDPROM 詳細情報を表示する例を示します。

```
Router# show idprom power-supply 1 detail
IDPROM for power-supply #1
IDPROM image:

(FRU is '110/220v AC power supply, 1360 watt')

IDPROM image block #0:
hexadecimal contents of block:
00: AB AB 01 90 11 BE 01 00 00 02 AB 01 00 01 43 69 .....Ci
10: 73 63 6F 20 53 79 73 74 65 6D 73 2C 20 49 6E 63 sCo Systems, Inc
20: 2E 00 57 53 2D 43 41 43 2D 31 33 30 30 57 00 00 ..WS-CAC-1300W..
30: 00 00 00 00 00 00 41 43 50 30 33 30 32 30 30 30 .....ACP0302000
40: 31 00 00 00 00 00 00 00 00 00 33 34 2D 30 39 31 1.....34-091
50: 38 2D 30 31 00 00 00 00 00 41 30 00 00 00 00 00 8-01.....A0....
60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
70: 00 00 00 01 00 00 00 00 00 00 00 09 00 0C 00 03 .....
80: 00 01 00 06 00 01 00 00 00 00 0A BA 00 00 00 00 .....

block-signature = 0xABAB, block-version = 1,
block-length = 144, block-checksum = 4542

*** common-block ***
IDPROM capacity (bytes) = 256 IDPROM block-count = 2
FRU type = (0xAB01,1)
OEM String = 'Cisco Systems, Inc.'
Product Number = 'WS-CAC-1300W'
Serial Number = 'ACP03020001'
```

show idprom

```

Manufacturing Assembly Number = '34-0918-01'
Manufacturing Assembly Revision = 'A0'
Hardware Revision = 1.0
Manufacturing bits = 0x0 Engineering bits = 0x0
SNMP OID = 9.12.3.1.6.1.0
Power Consumption = 2746 centiamperes RMA failure code = 0-0-0-0
*** end of common block ***

IDPROM image block #1:
hexadecimal contents of block:
00: AB 01 01 14 02 5F 00 00 00 00 00 00 00 0A BA .....
10: 0A BA 00 16 .....

block-signature = 0xAB01, block-version = 1,
block-length = 20, block-checksum = 607

*** power supply block ***
feature-bits: 00000000 00000000
rated current at 110v: 2746 rated current at 220v: 2746 (centiamperes)
CISCO-STACK-MIB SNMP OID = 22 *** end of power supply block ***

End of IDPROM image
Router#

```

次に、バックプレーンの IDPROM 情報を表示する例を示します。

```

Router# show idprom backplane
IDPROM for backplane #0
(FRU is 'Catalyst 6000 9-slot backplane')
OEM String = 'Cisco Systems'
Product Number = 'WS-C6009'
Serial Number = 'SCA030900JA'
Manufacturing Assembly Number = '73-3046-04'
Manufacturing Assembly Revision = 'A0'
Hardware Revision = 1.0
Current supplied (+) or consumed (-) = 0.000A
Router#

```

次に、GBIC セキュリティ対応インターフェイスから IDPROM 情報を表示する例を示します。

```

Router# show idprom interface g5/1
GBIC Serial EEPROM Contents:
Common block:
Identifier :
Connector :
Transceiver
Speed :
Media :
Technology :
Link Length :
GE Comp Codes :
SONET Comp Codes :
Encoding : 8B10B
BR, Nominal : 12x100 MHz
Length(9u) : GBIC does not support single mode fibre,
or the length information must be determined from
the transceiver technology.
Length(50u) : GBIC does not support 50 micron multi-mode fibre,
or the length information must be determined from
the transceiver technology.
Length(62.5u) : GBIC does not support 62.5 micron multi-mode fibre,
or the length information must be determined from
the transceiver technology.
Length(Copper) : GBIC does not support copper cables,

```

```
or the length information must be determined from
the transceiver technology.
Vendor Name : IBM
Vendor OUI : 0x8 0x0 0x5A
Vendor PN : IBM42P12SNY
Vendor rev : CS10
CC_BASE : 0xC6
Extended ID Fields
Options : Loss of Signal implemented TX_FAULT signal implemented
TX_D
ISABLE is implemented and disables the serial output
BR, max : 5%
BR, min : 5%
Vendor SN : 21P70420005D6
Date code : 02071001
CC_EXT : 0xCE
Vendor Specific ID Fields:
0x00: 00 00 00 70 2E DF C4 69 50 E6 54 F9 05 D4 83 A2
0x10: 4B 0E 8B 00 00 00 00 00 00 00 00 00 7D 3F D9 1E
Router#
```

show interfaces

特定のインターフェイスで認識されたトラフィックを表示するには、**show interfaces** コマンドを使用します。

show interfaces [*{interface interface-number}*] | *{null interface-number}* | *{vlan vlan-id}*]

シンタックスの説明

<i>interface</i>	(任意) インターフェイス タイプ。有効値は、 ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 port-channel 、 atm 、および ge-wan です。
<i>interface-number</i>	(任意) モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
null <i>interface-number</i>	(任意) ヌル インターフェイスを指定します。有効値は 0 です。
vlan <i>vlan-id</i>	(任意) VLAN ID を指定します。有効値は 1 ~ 4094 です。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

interface-number 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

ポート チャネルの有効な値は、1 ~ 308 です。257 ~ 282 のポート チャネル値は、内部的に割り当てられ、CSM および FWSM だけでサポートされます。

統計情報は、レイヤ 2 スイッチド パケットおよびレイヤ 3 スイッチド パケットについては、VLAN 単位で収集されます。統計情報はユニキャストとマルチキャストの両方のトラフィックで収集できます。レイヤ 3 スイッチド パケット数は、入力と出力の両方の方向で収集できます。各 VLAN の統計情報は、5 秒間隔で更新されます。

場合によっては、**show interfaces** コマンドと **show running-config** コマンドで表示されるデュプレックス モードが異なる場合があります。この場合は、**show interfaces** コマンドで表示されるデュプレックス モードが、インターフェイスが実際に実行しているデュプレックス モードです。**show interfaces** コマンドは、インターフェイスの動作モードを表示しますが、**show running-config** コマンドは、インターフェイスに設定されているモードを表示します。

キーワードを入力しなかった場合は、すべてのモジュールのすべてのカウンタが表示されます。

show interfaces GigabitEthernet コマンドの出力では、送受信された各パケットに対して 4 バイトを追加して表示します。これは、GE-WAN モジュールおよび他の Catalyst 6500 シリーズスイッチのギガビットイーサネット LAN モジュールの LAN ポートについて発生します。追加の 4 バイトはイーサネットフレーム CRC で、入力および出力バイトの統計情報に含まれます。

例

次に、特定のインターフェイスのトラフィックを表示する例を示します。

```
Router# show interfaces GigabitEthernet3/3
GigabitEthernet3/3 is up, line protocol is up (connected)
  Hardware is C6k 1000Mb 802.3, address is 000f.2305.49c0 (bia 000f.2305.49c0)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID 1., loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, media type is LH
  input flow-control is off, output flow-control is on
  Clock mode is auto
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:19, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  L2 Switched: ucast: 360 pkt, 23040 bytes - mcast: 0 pkt, 0 bytes
  L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast
  L3 out Switched: ucast: 0 pkt, 0 bytes mcast: 0 pkt, 0 bytes
    437 packets input, 48503 bytes, 0 no buffer
    Received 76 broadcasts (0 IP multicast)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    0 input packets with dribble condition detected
    86 packets output, 25910 bytes, 0 underruns <=====
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 PAUSE output
    0 output buffer failures, 0 output buffers swapped out
Router#
```

次に、FlexWAN モジュールのトラフィックを表示する例を示します。

```
Router# show interfaces pos 6/1/0.1
POS6/1/0.1 is up, line protocol is up
  Hardware is Packet over Sonet
  Internet address is 1.1.2.2/24
  MTU 4470 bytes, BW 155000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY <<<+++ no packets info after this line
Arches#sh mod 6
Mod Ports Card Type                               Model                               Serial No.
---
  6    0  2 port adapter FlexWAN                    WS-X6182-2PA                        SAD04340JY3

Mod MAC addresses                               Hw   Fw           Sw           Status
---
  6  0001.6412.a234 to 0001.6412.a273  1.3  12.2(2004022 12.2(2004022 Ok

Mod Online Diag Status
```

■ show interfaces

```
-----  
6 Pass  
Router#
```

show interfaces accounting

設定されたすべてのインターフェイスを経由して送信された各プロトコルタイプのパケット数を表示するには、**show interfaces accounting** コマンドを使用します。

show interfaces [*{interface interface-number}* | **null** *interface-number*] | **{vlan vlan-id}** **accounting**

シンタックスの説明

<i>interface</i>	(任意) インターフェイスタイプ。有効値は、 ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 port-channel 、 atm 、および ge-wan です。
<i>interface-number</i>	(任意) モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
null <i>interface-number</i>	(任意) マル インターフェイスを指定します。有効値は 0 です。
vlan <i>vlan-id</i>	(任意) VLAN ID を指定します。有効値は 1 ~ 4094 です。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



(注) Pkts Out および Chars Out フィールドでは、IPv6 パケット数だけを表示します。Pkts In および Chars In フィールドでは、トンネルインターフェイスの場合を除き、IPv4 と IPv6 の両方のパケット数を表示します。トンネルインターフェイスに関しては、IPv6 入力パケットは IPv6 パケットだけとしてカウントされます。

interface-number 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、指定されたインターフェイスタイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロットシャーシに 48 ポート 10/100BASE-T イーサネットモジュールが搭載されている場合に、ギガビットイーサネットインターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

ポートチャネル 257 ~ 282 は、内部的に割り当てられ、CSM および FWSM だけでサポートされます。キーワードを入力しなかった場合は、すべてのモジュールのすべてのカウンタが表示されます。

例

次に、設定されているすべてのインターフェイスを通じて送信された各プロトコルのパケット数を表示する例を示します。

show interfaces accounting

```

Router# show interfaces gigabitethernet5/2 accounting
GigabitEthernet5/2
Protocol Pkts In Chars In Pkts Out Chars Out
IP        50521  50521000 0      0
DEC MOP   0      0      1      129
CDP       0      0      1      592
IPv6     11      834    96     131658
Router#

```

表 2-37 に、この例で表示されるフィールドについて説明します。

表 2-37 show interfaces accounting コマンド出力フィールド

フィールド	説明
Protocol	インターフェイス上で動作するプロトコル
Pkts In	特定のプロトコルに対して受信された IPv4 パケット数
Chars In	特定のプロトコルに対して受信された IPv4 文字数
Pkts Out	特定のプロトコルに対して転送された、ハードウェア スイッチング済みの IPv6 パケット数
Chars Out	特定のプロトコルに対して転送された IPv6 文字数

show interfaces capabilities

特定のモジュール、特定のインターフェイス、またはすべてのインターフェイスのインターフェイス機能を表示するには、**show interfaces capabilities** コマンドを使用します。

show interfaces [*interface interface-number*] **capabilities** [{*module number*}]

シンタックスの説明	
<i>interface</i>	(任意) インターフェイス タイプ。有効値は、 ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 atm 、 port-channel 、および ge-wan です。
<i>interface-number</i>	モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
<i>module number</i>	(任意) モジュール番号を指定します。有効値については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン *interface-number* 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、使用するシャーシおよびモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合、スロット番号の有効値は 2 ~ 13、ポート番号の有効値は 1 ~ 48 です。

port-channel の値は 0 ~ 282 です。257 ~ 282 の値は、CSM および FWSM だけでサポートされています。

例 次に、特定のモジュールのインターフェイス機能を表示する例を示します。

```
Router# show interfaces capabilities module 6
FastEthernet6/1
Dot1x: yes
Model: WS-X6248-RJ-45
Type: 10/100BaseTX
Speed: 10,100,auto
Duplex: half,full
Trunk encap. type: 802.1Q,ISL
Trunk mode: on,off,desirable,nonegotiate
Channel: yes
Broadcast suppression: percentage(0-100)
Flowcontrol: rx-(off,on),tx-(none)
Membership: static
Fast Start: yes
```

■ show interfaces capabilities

```
QoS scheduling: rx-(1q4t), tx-(2q2t)
CoS rewrite: yes
ToS rewrite: yes
Inline power: no
SPAN: source/destination
UDLD yes
Link Debounce: yes
Link Debounce Time: no
Ports on ASIC: 1-12
Port-Security: yes
Router#
```

次に、特定のインターフェイスのインターフェイス機能を表示する例を示します。

```
Router# show interfaces fastethernet 4/1 capabilities
FastEthernet4/1
Model: WS-X6348-RJ-45
Type: 10/100BaseTX
Speed: 10,100,auto
Duplex: half,full
Trunk encap. type: 802.1Q,ISL
Trunk mode: on,off,desirable,nonegotiate
Channel: yes
Broadcast suppression: percentage(0-100)
Flowcontrol: rx-(off,on),tx-(none)
Fast Start: yes
QoS scheduling: rx-(1q4t), tx-(2q2t)
CoS rewrite: yes
ToS rewrite: yes
Inline power: no
SPAN: source/destination
```

次に、ポート チャネル インターフェイスの機能を表示する例を示します。

```
Router# show interfaces port-channel 12 capabilities
Port-channel12
Model: NO IDPROM
Type: unknown
Speed: 10,100,1000,auto
Duplex: half,full
Trunk encap. type: 802.1Q,ISL
Trunk mode: on,off,desirable,nonegotiate
Channel: yes
Broadcast suppression: percentage(0-100)
Flowcontrol: rx-(off,on),tx-(none)
Fast Start: yes
QoS scheduling: rx-(1q4t), tx-(1q4t)
CoS rewrite: yes
ToS rewrite: yes
Inline power: no
SPAN: source/destination
Router#
```

show interfaces counters

物理インターフェイスで認識されるトラフィックを表示するには、**show interfaces counters** コマンドを使用します。

show interfaces [*interface*] **counters** [**errors** | **etherchannel** | {*module number*} | {**protocol status**} | {**trunk** [*module number*]}]

シンタックスの説明

<i>interface</i>	(任意) インターフェイス タイプ。有効値のリストについては、「使用上のガイドライン」を参照してください。
errors	(任意) インターフェイスのエラー カウンタを表示します。
etherchannel	(任意) EtherChannel インターフェイスに関する情報を表示します。
<i>module number</i>	(任意) モジュール番号を表示します。有効値については、「使用上のガイドライン」を参照してください。
protocol status	(任意) イネーブルになっているプロトコルの現在のステータスを表示します。
trunk	(任意) インターフェイスのトランク カウンタを表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

show interfaces [*interface*] **counters** コマンドは、すべての着信パケット数を表示し、ストーム制御設定のためにインターフェイスによって廃棄された可能性のあるパケット数も表示します。廃棄された合計パケット数を表示するには、**show interfaces** [*interface*] **counters storm-control** コマンドを入力します。

キーワードを入力しなかった場合は、すべてのモジュールのすべてのカウンタが表示されます。

interface を入力する場合は、次のフォーマットを使用できます。

- *card-type* {*slot*}/*{first-port}* - *{last-port}*
- *card-type* {*slot*}/*{first-port}* - *{last-port}*

コマンド エントリごとにポート範囲を 1 つ定義できます。ポート範囲を指定する場合は、同じスロットおよびポート タイプで範囲を構成する必要があります。

範囲を定義する場合は、次のように、最初のポートとハイフン (-) の間にスペースを挿入する必要があります。

```
show interfaces gigabitethernet7/1 -7 counters
```

module number キーワードおよび引数はモジュール番号を指定し、表示対象をモジュール上のインターフェイスに限定します。有効値は、使用するシャーシによって異なります。たとえば、13 スロット シャーシを使用している場合、モジュール番号の有効値は 1 ~ 13 です。

card-type の有効値は次のとおりです。

- **ethernet**
- **fastethernet**
- **gigabitethernet**
- **tengigabitethernet**
- **port-channel interface-number**: 有効値は 1 ~ 282 です。257 ~ 282 の値は、CSM および FWSM だけでサポートされています。

show interfaces interface counters etherchannel コマンドを入力する場合は、次の注意事項に従ってください。

- *interface* が物理ポートを指定した場合は、[Etherchnl not enabled on this interface] というメッセージが表示されます。
- *interface* を省略した場合は、(システム内の) すべてのポート チャネルのカウンタ、および対応付けられた物理ポートのカウンタが表示されます。
- *interface* にポート チャネルを指定した場合、そのポート チャネルおよびそれに対応付けられたすべての物理ポートのカウンタが表示されます。さらに、複数のアグリゲータを持つ LACP ポート チャネルでプライマリ アグリゲータをコマンドにした場合、そのポート チャネルのすべてのアグリゲータ、およびそれらに対応付けられたポートの統計情報も表示されます。

例

次に、特定のモジュールのエラー カウンタを表示する例を示します。

```
Router# show interfaces counters errors module 1
Port          Align-Err    FCS-Err     Xmit-Err     Rcv-Err     UnderSize
Gi1/1         0            0           0            0           0
Gi1/2         0            0           0            0           0

Port          Single-Col  Multi-Col   Late-Col     Excess-Col  Carri-Sen   Runts       Giant
s
Gi1/1         0           0           0            0           0           0           0
Gi1/2         0           0           0            0           0           0           0
Router#
```

次に、特定のモジュールで認識されたトラフィックを表示する例を示します。

```
Router# show interfaces counters module 1

Port          InOctets    InUcastPkts  InMcastPkts  InBcastPkts
Gi1/1         0           0            0            0
Gi1/2         0           0            0            0

Port          OutOctets    OutUcastPkts  OutMcastPkts  OutBcastPkts
Gi1/1         0           0            0            0
Gi1/2         0           0            0            0
Router#
```

次に、特定のモジュールのトランク カウンタを表示する例を示します。

```
Router# show interfaces counters trunk module 1

Port          TrunkFramesTx  TrunkFramesRx  WrongEncap
Gi1/1         0              0              0
Gi1/2         0              0              0
Router#
```

次に、(システム内の) すべてのポート チャネル、および対応付けられた物理ポートのカウンタを表示する例を示します。

```
Router# show interfaces counters etherchannel
Port          InOctets    InUcastPkts  InMcastPkts  InBcastPkts
Po1           5518        1             29            1
Fa3/48        5518        1             29            1
Po2           11897       2             54            2
Fa3/45        5878        1             27            1
Fa3/46        6019        1             27            1
Po3           0           0             0             0
Po5           6073        1             27            1
Fa3/44        6073        1             27            1
Po5A          7811        1             53            1
Fa3/43        7811        1             53            1

Port          OutOctets    OutUcastPkts  OutMcastPkts  OutBcastPkts
Po1           4333        1             24            1
Fa3/48        4333        1             24            1
Po2           9532        2             46            2
Fa3/45        4766        1             23            1
Fa3/46        4766        1             23            1
Po3           0           0             0             0
Po5           17224       1             214           1
Fa3/44        17224       1             214           1
Po5A          174426     1             2669          1
Fa3/43        174426     1             2669          1
```

次に、特定のポート チャネルのカウンタ、および対応付けられた物理ポートのカウンタを表示する例を示します。

```
Router# show interfaces port-channel2 counters etherchannel

Port          InOctets    InUcastPkts  InMcastPkts  InBcastPkts
Po2           6007        1             31            1
Fa3/48        6007        1             31            1

Port          OutOctets    OutUcastPkts  OutMcastPkts  OutBcastPkts
Po2           4428        1             25            1
Fa3/48        4428        1             25            1
Router#
```

次に、各モードの廃棄数およびレベル設定を表示する例を示します。

```
Router# show interfaces counters storm-control

Port          UcastSupp %    McastSupp %    BcastSupp %    TotalSuppDiscards
Fa5/1         100.0          100.0          100.0          0
Fa5/2         100.0          100.0          100.0          0
Fa5/3         100.0          100.0          100.0          0
.
.
.
Router#
```

関連コマンド

コマンド	説明
clear counters	インターフェイス カウンタをクリアします。

show interfaces debounce

デバウンス タイマーのステータスおよび設定を表示するには、**show interfaces debounce** コマンドを使用します。

```
show interfaces [{interface interface-number} | {null interface-number} | {vlan vlan-id}]  

debounce [module num]
```

シンタックスの説明

<i>interface</i>	(任意) インターフェイス タイプ。有効値は、 ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 port-channel 、 pos 、 atm 、および ge-wan です。
<i>interface-number</i>	(任意) モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
null <i>interface-number</i>	(任意) ヌル インターフェイスを指定します。有効値は 0 です。
vlan <i>vlan-id</i>	(任意) VLAN を指定します。有効値は 1 ~ 4094 です。
module <i>num</i>	(任意) 表示対象を指定されたモジュールのインターフェイスに限定します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

デバウンス タイマーは 10 ギガビット イーサネット モジュール (WSX-6502-10GE) ではサポートされていません。

interface-number 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

port-channel の値は 0 ~ 282 です。257 ~ 282 の値は、CSM および FWSM だけでサポートされています。

例

次に、インターフェイスのデバウンス設定を表示する例を示します。

```
Router# show interfaces GigabitEthernet1/1 debounce  

Port    Debounce time    Value  

Gi1/1   enable           100  

Router#
```

関連コマンド

コマンド	説明
link debounce	インターフェイス上のデバウンス タイマーをイネーブルにします。

show interfaces description

インターフェイスの説明およびステータスを表示するには、**show interfaces description** コマンドを使用します。

show interfaces [*interface*] description

シンタックスの説明

interface (任意) インターフェイス タイプ。有効値のリストについては、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

interface 値を入力する場合は、次のフォーマットを使用できます。

- *card-type* {*slot*}/{*first-port*} - {*last-port*}
- *card-type* {*slot*}/{*first-port*} - {*last-port*}

コマンド エントリごとにポート範囲を 1 つ定義できます。ポート範囲を指定する場合は、同じスロットおよびポート タイプで範囲を構成する必要があります。範囲を定義する場合は、次のように、ハイフン (-) の前後にスペースを挿入する必要があります。

```
show interfaces gigabitethernet7/1 - 7 counters broadcast
```

card-type の有効値は、**ethernet**、**fastethernet**、**gigabitethernet**、**tengigabitethernet**、**port-channel**、**pos**、**atm**、および **ge-wan** です。

port-channel の値は 0 ~ 282 です。257 ~ 282 の値は、CSM および FWSM だけでサポートされています。

例

次に、すべてのインターフェイスの情報を表示する例を示します。

```
Router# show interfaces description
Interface Status      Protocol Description
PO0/0      admin down    down    First POS interface
PO0/1      admin down    down
Gi1/0      up            up      GigE to server farm
Router#
```

関連コマンド

コマンド	説明
description	DSP インターフェイスに関する特定の説明を含みます。

show interfaces flowcontrol

フロー制御情報を表示するには、**show interfaces flowcontrol** コマンドを使用します。

show interfaces [*interface* [*mod*]] **flowcontrol** [*module number*]

シンタックスの説明	
<i>interface</i>	(任意) インターフェイス タイプ。有効値は、 ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 port-channel 、 pos 、 atm 、および ge-wan です。
<i>mod</i>	(任意) モジュールおよびポート番号
<i>module number</i>	(任意) モジュール番号を指定します。有効値については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン *mod* 引数は、モジュールおよびポート番号を指定します。*mod* の有効値は、使用するシャーシおよびモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合、スロット番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 です。

module number キーワードおよび引数はモジュール番号を指定し、表示対象をモジュール上のインターフェイスに限定します。有効値は、使用するシャーシによって異なります。たとえば、13 スロット シャーシを使用している場合、モジュール番号の有効値は 1 ~ 13 です。

port-channel の値は 0 ~ 282 です。257 ~ 282 の値は、CSM および FWSM だけでサポートされています。

例 次に、すべてのインターフェイスのフロー制御情報を表示する例を示します。

Router# **show interfaces flowcontrol**

```

Port      Send      FlowControl  Receive FlowControl  RxPause TxPause
  admin    oper      admin      oper
-----
Gi1/1 desired  off        off         off         0         0
Gi1/2 desired  off        off         off         0         0
Gi3/1 on      on         on          on          0         0
.
.
.

```

show interfaces flowcontrol

```

Gi8/2 desired  off      off      off      0      0
Gi8/3 desired  off      off      off      0      0
Gi8/4 desired  off      off      off      0      0
Router#
    
```

次に、特定のインターフェイスのフロー制御情報を表示する例を示します。

```

Router# show interfaces gigabitethernet 8/2 flowcontrol
Port  Send      FlowControl  Receive  FlowControl  RxPause  TxPause
      admin    oper        admin    oper
-----
Gi8/2 desired  off      off      off      0      0
Router#
    
```

表 2-38 に、この例で表示されるフィールドについて説明します。

表 2-38 show interfaces flowcontrol コマンドの出カフィールド

フィールド	説明
Port	インターフェイス タイプ、およびモジュールとポート番号
Send admin	管理状態のフロー制御の動作。on は、ローカル ポートがリモート ポートにポーズ フレームを送信できることを示します。off は、ローカル ポートがリモート ポートにポーズ フレームを送信できないことを示します。desired は、リモート ポートが receive on 、 receive off 、または receive desired のいずれに設定されているかに関係なく、想定された結果を示します。
Send oper	現在のフロー制御の動作。on は、ローカル ポートがリモート ポートにポーズ フレームを送信できることを示します。off は、ローカル ポートがリモート ポートにポーズ フレームを送信できないことを示します。desired は、リモート ポートが receive on 、 receive off 、または receive desired のいずれに設定されているかに関係なく、想定された結果を示します。
Receive admin	管理状態のフロー制御の動作。on は、ローカル ポートがリモート ポートにポーズ フレームを送信できることを示します。off は、ローカル ポートがリモート ポートにポーズ フレームを送信できないことを示します。desired は、リモート ポートが send on 、 send off 、または send desired のいずれに設定されているかに関係なく、想定された結果を示します。
Receive oper	現在のフロー制御の動作。on は、ローカル ポートがリモート ポートにポーズ フレームを送信できることを示します。off は、ローカル ポートがリモート ポートにポーズ フレームを送信できないことを示します。desired は、リモート ポートが send on 、 send off 、または send desired のいずれに設定されているかに関係なく、想定された結果を示します。
RxPause	受信されたポーズ フレームの数
TxPause	送信されたポーズ フレームの数

関連コマンド

コマンド	説明
flowcontrol	ポートがポーズ フレームを送信または受信するよう設定します。

show interfaces private-vlan mapping

VLAN SVI の PVLAN マッピングに関する情報を表示するには、**show interfaces private-vlan mapping** コマンドを使用します。

show interfaces [*interface interface-number*] **private-vlan mapping** [**active**]

シンタックスの説明	
<i>interface</i>	(任意) インターフェイス タイプ。有効値は、 ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 atm 、および ge-wan です。
<i>interface-number</i>	モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
active	(任意) アクティブ インターフェイスだけを表示します。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドのデフォルト EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドは、SVI 情報だけを表示します。
interface-number 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、使用するシャーシおよびモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合、スロット番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 です。

例 次に、PVLAN マッピングに関する情報を表示する例を示します。

```
Router# show interfaces private-vlan mapping
Interface Secondary VLAN Type
-----
vlan2      301      community
vlan2      302      community
Router#
```

関連コマンド	コマンド	説明
	private-vlan	PVLAN、および PVLAN とセカンダリ VLAN とのアソシエーションを設定します。
	private-vlan mapping	プライマリ VLAN とセカンダリ VLAN のマッピングを作成して、両方の VLAN で同じプライマリ VLAN SVI を共有できるようにします。

show interfaces status

インターフェイス ステータスを表示したり、LAN ポートで errdisable ステートにあるインターフェイスだけのリストを表示したりするには、**show interfaces status** コマンドを使用します。

show interfaces [*interface interface-number*] **status** [**err-disabled** | **module number**]

シンタックスの説明

<i>interface</i>	(任意) インターフェイス タイプ。有効値は、 ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 atm 、および ge-wan です。
<i>interface-number</i>	モジュールおよびポート番号。有効値については、「 使用上のガイドライン 」を参照してください。
err-disabled	(任意) errdisable ステートにある LAN ポートを表示します。
module number	(任意) モジュール番号を指定します。有効値については、「 使用上のガイドライン 」を参照してください。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

interface-number 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、使用するシャーシおよびモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合、スロット番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 です。

このコマンドは、LAN ポートだけでサポートされます。

module number キーワードおよび引数はモジュール番号を指定し、表示対象をモジュール上のインターフェイスに限定します。有効値は、使用するシャーシによって異なります。たとえば、13 スロット シャーシを使用している場合、モジュール番号の有効値は 1 ~ 13 です。

インターフェイスが非アクティブかどうかを確認するには、**show interfaces status** コマンドを入力します。インターフェイスが非アクティブの場合、**Status** フィールドには [**inactive**] と表示されます。ポートが非アクティブでない場合、**Status** フィールドには [**none**] と表示されます。

パケット数とバイト数を調べるには、[show interfaces counters](#) コマンドまたは **show interfaces interface interface-number status** コマンドを入力します。推奨コマンドは、[show interfaces counters](#) コマンドです。場合によっては、**show interfaces interface interface-number status** コマンドのパケット数とバイト数は正しくないことがあります。

例

次に、すべての LAN ポートのステータスを表示する例を示します。

```
Router# show interfaces status

Port      Name              Status      Vlan      Duplex Speed Type
Gi1/1     Gi1/1             disabled    routed    full   1000 missing
Gi1/2     Gi1/2             notconnect  1         full   1000 unknown (4)
Fa5/1     Fa5/1             disabled    routed    auto   auto 10/100BaseTX
.
.
.
Port      Name              Status      Vlan      Duplex Speed Type
Fa5/18    Fa5/18            disabled    1         auto   auto 10/100BaseTX
Fa5/19    Fa5/19            disabled    1         auto   auto 10/100BaseTX
Gi7/1     Gi7/1             disabled    1         full   1000 WDM-RXONLY
Gi7/2     Gi7/2             disabled    1         full   1000 No Transceiver
Router#
```

次に、特定の LAN ポートのパケット数とバイト数を表示する例を示します。

```
Router# show interfaces fastethernet5/2 status
FastEthernet5/2
Switching path  Pkts In  Chars In  Pkts Out  Chars Out
Processor              17      1220      20        2020
Route cache            0         0         0         0
Distributed cache     17      1220    206712817 2411846570
Total                  34      2440    206712837 2411848590
Router#
```

次に、errdisable ステートにある LAN ポートのステータスを表示する例を示します。

```
Router# show interfaces status err-disabled

Port      Name              Status      Reason
Fa9/4     Fa9/4             notconnect  link-flap

informational error message when the timer expires on a cause
-----

5d04h:%PM-SP-4-ERR_RECOVER:Attempting to recover from link-flap err-disable state on Fa9/4
Router#
```

関連コマンド

コマンド	説明
errdisable detect cause	errdisable 検出をイネーブルにします。
show errdisable recovery	errdisable 回復タイマーに関する情報を表示します。

show interfaces summary

ネットワーク装置に設定されたすべてのインターフェイスについて統計情報のサマリーを表示するには、**show interfaces summary** コマンドを使用します。

show interfaces [*interface interface-number*] **summary** [*vlan*]

シンタックスの説明

<i>interface</i>	(任意) インターフェイス タイプ。有効値は、 ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 atm 、および ge-wan です。
<i>interface-number</i>	モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
vlan	(任意) VLAN インターフェイスの総数を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

サブインターフェイス用の個別カウンタは保持されておらず、**show interfaces summary** の出力には表示されません。

例

次に、ネットワーク装置に設定されたすべてのインターフェイスについて統計情報のサマリーを表示する例を示します。

```
Router# show interfaces summary
*: interface is up
IHQ: pkts in input hold queue IQD: pkts dropped from input queue
OHQ: pkts in output hold queue OQD: pkts dropped from output queue
RXBS: rx rate (bits/sec) RXPS: rx rate (pkts/sec)
TXBS: tx rate (bits/sec) TXPS: tx rate (pkts/sec)
TRTL: throttle count
Interface IHQ IQD OHQ OQD RXBS RXPS TXBS TXPS TRTL
-----
* FastEthernet0/0 0 0 0 0 0 0 0 0 0
Serial0/0 0 0 0 0 0 0 0 0 0
FastEthernet0/1 0 0 0 0 0 0 0 0 0
Serial0/1 0 0 0 0 0 0 0 0 0
Router#
```

次に、VLAN インターフェイスの総数を表示する例を示します。

```
Router# show interfaces summary vlan
Total number of Vlan interfaces: 7
Vlan interfaces configured:
1,5,20,2000,3000-3001,4000
Router#
```

show interfaces switchport

スイッチング（非ルーティング）ポートの管理ステータスおよび動作ステータスを表示するには、**show interfaces switchport** コマンドを使用します。

show interfaces [*interface interface-number*] **switchport** [**brief**] [*module number*]

シンタックスの説明	
<i>interface</i>	(任意) インターフェイス タイプ。有効値は、 ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 atm 、および ge-wan です。
<i>interface-number</i>	モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
brief	(任意) 簡単な要約情報を表示します。
<i>module number</i>	(任意) 指定されたモジュール上のインターフェイスだけを表示します。有効値については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン *interface-number* はモジュールおよびポート番号を指定します。有効値は、使用するシャーシおよびモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合、スロット番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 です。

例 次に、**include** 出力修飾子を使用してスイッチ ポート情報を表示する例を示します。

```
Router# show interfaces switchport | include VLAN
Name: Fa5/6
Access Mode VLAN: 200 (VLAN0200)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: ALL
.
.
.
```

Router#

次に、2 つの VLAN アクセス ポートの設定を表示する例を示します。

```
Router# show interfaces switchport
Name: Fa5/1
Switchport: Enabled
```

■ show interfaces switchport

```
Administrative Mode: access
Operational Mode: access
Dot1q Ethertype: 0x8200
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: off
Access Mode VLAN: 100
Voice VLAN: 102
Trunking Native Mode VLAN: 1 (default)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: 900 ((Inactive)) 901 ((Inactive))
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Name: Fa5/2
Switchport: Enabled
Administrative Mode: access
Operational Mode: down
Dot1q Ethertype: 0x8200
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 100
Voice VLAN: 103 ((inactive))
Trunking Native Mode VLAN: 1 (default)
.
.
.
```

次に、簡単な要約情報を表示する例を示します。

```
Router# show interfaces switchport brief module 3
Port Status Op.Mode Op.Encap Channel-id Vlan
Fa3/1 connected access native -- 1
Fa3/7 disabled -- dot1q Po26 1
Fa3/13 connected access native -- 666
Router#
```

show interfaces switchport backup

Flexlink ペアを表示するには、**show interfaces switchport backup** コマンドを使用します。

show interfaces [*interface interface-number*] **switchport backup**

シンタックスの説明

<i>interface</i>	(任意) インターフェイス タイプ。有効値は、 ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 atm 、および ge-wan です。
<i>interface-number</i>	モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

interface-number はモジュールおよびポート番号を指定します。有効値は、使用するシャーシおよびモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合、スロット番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 です。

例

次に、すべての Flexlink ペアを表示する例を示します。

```
Router# show interfaces switchport backup
Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
-----
FastEthernet3/1      FastEthernet4/1      Active Up/Backup Standby
FastEthernet5/1      FastEthernet5/2      Active Down/Backup Up
FastEthernet3/2      FastEthernet5/4      Active Standby/Backup Up
Po1                  Po2                  Active Down/Backup Down
Router#
```

■ show interfaces switchport backup

次に、特定の Flexlink ポートを表示する例を示します。

```
Router# show interfaces fastethernet 4/1 switchport backup
Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
-----
FastEthernet3/1      FastEthernet4/1      Active Up/Backup Standby
Router#
```

関連コマンド

コマンド	説明
switchport backup	Flexlink バックアップ インターフェイスとしてインターフェイスを設定します。

show interfaces transceiver

DOM がイネーブルになっているオプティカル トランシーバに関する情報を表示するには、**show interfaces transceiver** コマンドを使用します。

show interfaces [*interface interface-number*] **transceiver** [**threshold violations**] [**detail**] [**module number**]

シンタックスの説明	
<i>interface</i>	(任意) インターフェイス タイプ。有効値は、 gigabitethernet および tengigabitethernet です。
<i>interface-number</i>	モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
threshold violations	(任意) インターフェイス トランシーバしきい値違反に関する情報を表示します。
detail	(任意) インターフェイス トランシーバに関する詳細情報を表示します。
module number	(任意) モジュール番号を指定します。有効値については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード 特権 EXEC (#)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン トランシーバが挿入されたあと、ソフトウェアは約 10 秒間待ってから診断モニタリング情報を読み取ります。ソフトウェアが診断モニタリング情報を読み取る前に **show interfaces transceiver** コマンドを入力した場合、次のメッセージが表示されます。

```
Waiting for diagnostic monitoring information to settle down.
Please try again after a few seconds.
```

数秒待ってから、**show interfaces transceiver** コマンドを再入力してください。

interface interface-number 引数は、診断モニタリングがイネーブルになっていて、診断モニタリング情報の読み取りをサポートするモジュールにトランシーバがあるインターフェイスでサポートされます。

例 次に、トランシーバ情報を表示する例を示します。

```
Router# show interfaces transceiver
If device is externally calibrated, only calibrated values are printed.
++ : high alarm, + : high warning, - : low warning, -- : low alarm.
NA or N/A: not applicable, Tx: transmit, Rx: receive.
mA: milliamperes, dBm: decibels (milliwatts).
```

```
Optical Optical
```

show interfaces transceiver

Port	Temperature (Celsius)	Voltage (Volts)	Current (mA)	Tx Power (dBm)	Rx Power (dBm)
Gi1/1	40.6	5.09	0.4	-25.2	N/A
Gi2/1	35.5	5.05	0.1	-29.2	N/A
Gi2/2	49.5	3.30	0.0	7.1	-18.7

Router#

次に、詳細なトランシーバ情報を表示する例を示します。

Router# show interfaces transceiver detail

mA: milliamperes, dBm: decibels (milliwatts), NA or N/A: not applicable.
 ++ : high alarm, + : high warning, - : low warning, -- : low alarm.
 A2D readouts (if they differ), are reported in parentheses.
 The threshold values are calibrated.

Port	Temperature (Celsius)	High Alarm Threshold (Celsius)	High Warn Threshold (Celsius)	Low Warn Threshold (Celsius)	Low Alarm Threshold (Celsius)
Gi1/1	48.1	100.0	100.0	0.0	0.0
Gi1/2	34.9	100.0	100.0	0.0	0.0
Gi2/1	43.5	70.0	60.0	5.0	0.0
Gi2/2	39.1	70.0	60.0	5.0	0.0

Port	Voltage (Volts)	High Alarm Threshold (Volts)	High Warn Threshold (Volts)	Low Warn Threshold (Volts)	Low Alarm Threshold (Volts)
Gi1/1	3.30	6.50	6.50	N/A	N/A
Gi1/2	3.30	6.50	6.50	N/A	N/A
Gi2/1	5.03	5.50	5.25	4.75	4.50
Gi2/2	5.02	5.50	5.25	4.75	4.50

Port	Current (milliamperes)	High Alarm Threshold (mA)	High Warn Threshold (mA)	Low Warn Threshold (mA)	Low Alarm Threshold (mA)
Gi1/1	0.0	130.0	130.0	N/A	N/A
Gi1/2	1.7	130.0	130.0	N/A	N/A
Gi2/1	50.6 +	60.0	40.0	10.0	5.0
Gi2/2	25.8	60.0	40.0	10.0	5.0

Port	Optical Transmit Power (dBm)	High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi1/1	8.1 ++	8.1	8.1	N/A	N/A
Gi1/2	-9.8	8.1	8.1	N/A	N/A
Gi2/1	-16.7 --	3.4	3.2	-0.3	-0.5
Gi2/2	0.8	3.4	3.2	-0.3	-0.5

Port	Optical Receive Power (dBm)	High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi1/1	N/A	8.1	8.1	N/A	N/A
Gi1/2	-30.9	8.1	8.1	N/A	N/A
Gi2/1	N/A	5.9	-6.7	-28.5	-28.5
Gi2/2	N/A	5.9	-6.7	-28.5	-28.5

Router#

次に、Catalyst 6500 シリーズスイッチ上のすべてのトランシーバのしきい値違反を表示する例を示します。

```
Router# show interfaces transceiver threshold violations
Rx: Receive, Tx: Transmit.
DDDD: days, HH: hours, MM: minutes, SS: seconds

      Port      Time in slot      Time since Last Known
              (DDDD:HH:MM:SS)  Threshold Violation  Type(s) of Last Known
              -----  -----
Gi1/1      0000:00:03:41      Not applicable        Not applicable
Gi2/1      0000:00:03:40      0000:00:00:30        Tx bias high warning
                                           50.5 mA > 40.0 mA
                                           0000:00:00:30        Tx power low alarm
                                           -17.0 dBm < -0.5 dBm
Gi2/2      0000:00:03:40      Not applicable        Not applicable

Router#
```

次に、特定のモジュールのすべてのトランシーバのしきい値違反を表示する例を示します。

```
Router# show interfaces transceiver threshold violations module 2
lo: low, hi: high, warn: warning
DDDD: days, HH: hours, MM: minutes, SS: seconds

      Port      Time in slot      Time since Last Known
              (DDDD:HH:MM:SS)  Threshold Violation  Type(s) of Last Known
              -----  -----
Gi2/1      0000:00:03:40      0000:00:00:30        Tx bias high warning
                                           50.5 mA > 40.0 mA
                                           0000:00:00:30        Tx power low alarm
                                           -17.0 dBm < -0.5 dBm
Gi2/2      0000:00:03:40      Not applicable        Not applicable

Router#
```

次に、特定のインターフェイス上のトランシーバの違反を表示する例を示します。

```
Router# show interfaces Gi2/1 transceiver threshold violations
Rx: Receive, Tx: Transmit.
DDDD: days, HH: hours, MM: minutes, SS: seconds

      Port      Time in slot      Time since Last Known
              (DDDD:HH:MM:SS)  Threshold Violation  Type(s) of Last Known
              -----  -----
Gi2/1      0000:00:03:40      0000:00:00:30        Tx bias high warning
                                           50.5 mA > 40.0 mA
                                           0000:00:00:30        Tx power low alarm
                                           -17.0 dBm < -0.5 dBm

Router#
```

show interfaces trunk

インターフェイス トランク情報を表示するには、**show interfaces trunk** コマンドを使用します。

show interfaces [*interface interface-number*] **trunk** [*module number*]

シンタックスの説明

<i>interface</i>	(任意) インターフェイス タイプ。有効値は、 ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 atm 、および ge-wan です。
<i>interface-number</i>	(任意) モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
<i>module number</i>	(任意) モジュール番号を指定します。有効値については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

キーワードを指定しないと、トランキング ポートの情報だけが表示されます。

interface-number はモジュールおよびポート番号を指定します。有効値は、使用するシャーシおよびモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合、スロット番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 です。

module number キーワードおよび引数はモジュール番号を指定し、表示対象をモジュール上のインターフェイスに限定します。有効値は、使用するシャーシによって異なります。たとえば、13 スロット シャーシを使用している場合、モジュール番号の有効値は 1 ~ 13 です。

例

次に、モジュール 5 のインターフェイス トランク情報を表示する例を示します。

```
Router# show interfaces trunk module 5
```

Port	Mode	Encapsulation	Status	Native vlan
Fa5/1	routed	negotiate	routed	1
Fa5/2	routed	negotiate	routed	1
Fa5/3	routed	negotiate	routed	1
Fa5/4	routed	negotiate	routed	1
Fa5/5	routed	negotiate	routed	1
Fa5/6	off	negotiate	not-trunking	10
Fa5/7	off	negotiate	not-trunking	10
Fa5/8	off	negotiate	not-trunking	1
Fa5/9	desirable	n-isl	trunking	1
Fa5/10	desirable	negotiate	not-trunking	1
Fa5/11	routed	negotiate	routed	1

```

Fa5/12    routed      negotiate   routed      1
.
.
Fa5/48    routed      negotiate   routed      1

Port      Vlans allowed on trunk
Fa5/1     none
Fa5/2     none
Fa5/3     none
Fa5/4     none
Fa5/5     none
Fa5/6     none
Fa5/7     none
Fa5/8     200
Fa5/9     1-1005
Fa5/10    none
Fa5/11    none
Fa5/12    none

.
.
.
Fa5/48    none

Port      Vlans allowed and active in management domain
Fa5/1     none
Fa5/2     none
Fa5/3     none
Fa5/4     none
Fa5/5     none
Fa5/6     none
Fa5/7     none
Fa5/8     200
Fa5/9     1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005
Fa5/10    none
Fa5/11    none
Fa5/12    none

.
.
.
Fa5/48    none

Port      Vlans in spanning tree forwarding state and not pruned
Fa5/1     none
Fa5/2     none
Fa5/3     none
Fa5/4     none
Fa5/5     none
Fa5/6     none
Fa5/7     none
Fa5/8     200
Fa5/9     1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005
Fa5/10    none
Fa5/11    none

.
.

```

■ show interfaces trunk

```
.  
  
Fa5/48    none  
Router#
```

次に、アクティブなトランキング ポートのトランキング情報を表示する例を示します。

```
Router# show interfaces trunk
```

```
Port      Mode           Encapsulation  Status        Native vlan  
Fa5/9     desirable     n-isl          trunking     1  
  
Port      Vlans allowed on trunk  
Fa5/9     1-1005  
  
Port      Vlans allowed and active in management domain  
Fa5/9     1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-802,850,917,999,1002-1005  
  
Port      Vlans in spanning tree forwarding state and not pruned  
Fa5/9     1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-802,850,917,999,1002-1005  
Router#
```

show interfaces unidirectional

受信専用トランシーバがあるインターフェイスの動作状態を表示するには、**show interfaces unidirectional** コマンドを使用します。

show interfaces [*interface interface-number*] **unidirectional** [*module number*]

シンタックスの説明	
<i>interface</i>	(任意) インターフェイス タイプ。有効値は、 gigabitethernet および tengigabitethernet です。
<i>interface-number</i>	(任意) モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
<i>module number</i>	(任意) モジュール番号を指定します。有効値については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン キーワードを指定しないと、トランキング ポートの情報だけが表示されます。

interface-number はモジュールおよびポート番号を指定します。有効値は、使用するシャーシおよびモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合、スロット番号の有効値は 2 ~ 13、ポート番号の有効値は 1 ~ 48 です。

module number キーワードおよび引数はモジュール番号を指定し、表示対象をモジュール上のインターフェイスに限定します。有効値は、使用するシャーシによって異なります。たとえば、13 スロット シャーシを使用している場合、モジュール番号の有効値は 2 ~ 13 です。

例 次に、受信専用トランシーバがあるインターフェイスの動作状態を表示する例を示します。

```
Router# show interfaces gigabitethernet5/2 unidirectional
Unidirectional configuration mode: send only
Unidirectional operational mode: receive only
CDP neighbour unidirectional configuration mode: off
Router#
```

■ show interfaces unidirectional

関連コマンド

コマンド	説明
show interfaces status	インターフェイス ステータスを表示したり、LAN ポートで errdisable ステートにあるインターフェイスだけのリストを表示したりします。
unidirectional	ソフトウェアベースの UDE を設定します。

show interfaces vlan mapping

ポート上の VLAN マッピングのステータスを表示するには、**show interfaces vlan mapping** コマンドを使用します。

show interfaces [*interface interface-number*] **vlan mapping**

シンタックスの説明	
<i>interface</i>	(任意) インターフェイス タイプ。有効値は、 ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 vlan 、 pos 、 atm 、および ge-wan です。
<i>interface-number</i>	モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン *interface-number* はモジュールおよびポート番号または VLAN 番号を指定します。有効値は、使用するシャーシおよびモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合、スロット番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 です。

例 次に、特定のポートに設定されているすべての VLAN マッピングとそれらのマッピングのステータス (イネーブルまたはディセーブル) を表示する例を示します。

```
Router# show interfaces gigabitethernet5/2 vlan mapping
State: enabled
Original VLAN Translated VLAN
-----
    1649             755
Router#
```

関連コマンド	コマンド	説明
	show vlan mapping	802.1Q VLAN と ISL VLAN のマッピングを登録します。
	switchport vlan mapping enable	スイッチ ポート単位で VLAN マッピングをイネーブルにします。

show ip arp inspection

特定の範囲の VLAN について DAI のステータスを表示するには、**show ip arp inspection** コマンドを使用します。

```
show ip arp inspection [{interfaces [interface-name]} | {statistics [vlan vlan-range]}]
```

シンタックスの説明

interfaces <i>interface-name</i>	(任意) 指定したインターフェイスの ARP パケットの信頼状態およびレート制限を表示します。
statistics	(任意) この機能によって処理された次のタイプのパケットの統計を表示します。転送、廃棄、MAC 検証失敗、および IP 検証失敗。
vlan <i>vlan-range</i>	(任意) 選択した範囲の VLAN の統計を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

statistics キーワードを入力しなかった場合、選択した範囲の VLAN について DAI の設定および動作状態が表示されます。

インターフェイス名を指定しなかった場合は、システム内の該当するすべてのインターフェイスの信頼状態およびレート制限が表示されます。

例

次に、VLAN 3 の DAI によって処理されたパケットの統計を表示する例を示します。

```
Router# show ip arp inspection statistics vlan 3

Vlan      Forwarded      Dropped      DHCP Drops      ACL Drops
----      -
3         31753          102407       102407          0

Vlan      DHCP Permits   ACL Permits   Source MAC Failures
----      -
3         31753          0             0

Vlan      Dest MAC Failures  IP Validation Failures
----      -
3         0                 0

Router#
```

次に、すべてのアクティブな VLAN の DAI によって処理されたパケットの統計を表示する例を示します。

```
Router# show ip arp inspection statistics
```

Vlan	Forwarded	Dropped	DHCP Drops	ACL Drops
1	0	0	0	0
2	0	0	0	0
3	68322	220356	220356	0
4	0	0	0	0
100	0	0	0	0
101	0	0	0	0
1006	0	0	0	0
1007	0	0	0	0

Vlan	DHCP Permits	ACL Permits	Source MAC Failures
1	0	0	0
2	0	0	0
3	68322	0	0
4	0	0	0
100	0	0	0
101	0	0	0
1006	0	0	0
1007	0	0	0

Vlan	Dest MAC Failures	IP Validation Failures
1	0	0
2	0	0
3	0	0
4	0	0
100	0	0
101	0	0
1006	0	0
1007	0	0

Router#

次に、VLAN 1 の DAI の設定および動作状態を表示する例を示します。

```
Router# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
```

Vlan	Configuration	Operation	ACL Match	Static ACL
1	Enabled	Active		

Vlan	ACL Logging	DHCP Logging
1	Deny	Deny

Router#

次に、インターフェイス Fa6/3 の信頼状態を表示する例を示します。

```
Router# show ip arp inspection interfaces fastEthernet 6/3
Interface      Trust State      Rate (pps)      Burst Interval
-----
Fa6/1          Untrusted        20              5
Router#
```

次に、スイッチ上のインターフェイスの信頼状態を表示する例を示します。

```
Router# show ip arp inspection interfaces
Interface      Trust State      Rate (pps)
-----
Gi1/1          Untrusted        15
```

■ show ip arp inspection

```

Gi1/2          Untrusted          15
Gi3/1          Untrusted          15
Gi3/2          Untrusted          15
Fa3/3          Trusted             None
Fa3/4          Untrusted          15
Fa3/5          Untrusted          15
Fa3/6          Untrusted          15
Fa3/7          Untrusted          15
Router#

```

関連コマンド

コマンド	説明
arp access-list	ARP インспекションおよび QoS フィルタリング用の ARP ACL を設定し、ARP ACL コンフィギュレーション サブモードを開始します。
clear ip arp inspection log	ログ バッファのステータスをクリアします。
show ip arp inspection	特定の範囲の VLAN について Dynamic ARP Inspection (DAI; ダイナミック ARP インспекション) のステータスを表示します。

show ip arp inspection log

ログバッファのステータスを表示するには、**show ip arp inspection log** コマンドを使用します。

show ip arp inspection log

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード 特権 EXEC (#)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、バッファがクリアされる前後にログバッファの現在の内容を表示する例を示します。

```
Router# show ip arp inspection log
Total Log Buffer Size : 10
Syslog rate : 0 entries per 10 seconds.
```

Interface	Vlan	Sender MAC	Sender IP	Num of Pkts
Fa6/3	1	0002.0002.0002	1.1.1.2	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.3	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.4	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.5	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.6	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.7	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.8	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.9	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.10	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.11	1(12:02:52 UTC Fri Apr 25 2003)
--	--	--	--	5(12:02:52 UTC Fri Apr 25 2003)

```
Router#
```

次に、**clear ip arp inspection log** コマンドでバッファをクリアする例を示します。

```
Router# clear ip arp inspection log
Router# show ip arp inspection log
Total Log Buffer Size : 10
Syslog rate : 0 entries per 10 seconds.
No entries in log buffer.
Router#
```

■ show ip arp inspection log

関連コマンド

コマンド	説明
<code>clear ip arp inspection log</code>	ログ バッファのステータスをクリアします。
<code>show ip arp inspection log</code>	ログ バッファのステータスを表示します。

show ip auth-proxy watch-list

認証プロキシのウォッチ リストに関する情報を表示するには、**show ip auth-proxy watch-list** コマンドを使用します。

show ip auth-proxy watch-list

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、認証プロキシのウォッチ リストに関する情報を表示する例を示します。

```
Router# show ip auth-proxy watch-list
Authentication Proxy Watch-list is enabled
Watch-list expiry timeout is 2 minutes
Total number of watch-list entries: 3

Source IP      Type          Violation-count
12.0.0.2      MAX_RETRY    MAX_LIMIT
12.0.0.3      TCP_NO_DATA  MAX_LIMIT
1.2.3.4       CFGED        N/A

Total number of watch-listed users: 3
Router#
```

関連コマンド	コマンド	説明
	clear ip auth-proxy watch-list	1 つのウォッチ リスト エントリまたはすべてのウォッチ リスト エントリを削除します。
	ip auth-proxy max-login-attempts	ファイアウォール インターフェイスでログインの試行回数を制限します。
	ip auth-proxy watch-list	認証プロキシ ウォッチ リストをイネーブルにして設定します。

show ipc

IPC（プロセッサ間通信）情報を表示するには、**show ipc** コマンドを使用します。

show ipc {nodes | ports [open] | queue | status}

シンタックスの説明

nodes	参加ノードを表示します。
ports	ローカル IPC ポートを表示します。
open	(任意) オープン ポートだけを表示します。
queue	IPC 再送信キューの内容を表示します。
status	ローカル IPC サーバのステータスを表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、参加ノードを表示する例を示します。

```
Router# show ipc nodes
There are 66 nodes in this IPC realm.
  ID      Type      Name      Last Sent  Last Heard
  -----
  2210000 Local      Card33    0         0
  2000000 ICC         Card0     0         0
  2010000 ICC         Card1     0         0
  2020000 ICC         Card2     0         0
  2040000 ICC         Card4     0         0

<... output truncated ...>

  23E0000 ICC         Card62    0         0
  23F0000 ICC         Card63    0         0
  10000   ICC         IPC Master 270       17070
Router#
```

次に、ローカル IPC ポートを表示する例を示します。

```
Router# show ipc ports
There are 6 ports defined.

Port ID      Type      Name
-----
  2210000.1   unicast   Card33:Zone
  2210000.2   unicast   Card33:Echo
  2210000.3   unicast   Card33:Control
  2210000.4   unicast   Remote TTY Server Port
  10000.3     unicast   IPC Master:Control
  2210000.5   unknown   Card33:Request
```

```
port_index = 0 seat_id = 0x10000 last sent = 0 last heard = 1158
port_index = 1 seat_id = 0x10000 last sent = 0 last heard = 0
Router#
```

次に、オープン IPC ポートを表示する例を示します。

```
Router# show ipc ports open
There are 4 ports defined.

Port ID      Type      Name
10000.7     unicast  Unknown
port_index = 0 last sent = 2 last heard = 0

10000.8     unicast  Unknown
port_index = 0 last sent = 0 last heard = 0

10000.9     unicast  Unknown
port_index = 0 last sent = 17753 last heard = 0
port_index = 1 last sent = 0 last heard = 0
Router#
```

次に、IPC 再送信キューの内容を表示する例を示します。

```
Router# show ipc queue
There are 0 IPC messages waiting for acknowledgement in the transmit queue.
There are 0 IPC messages waiting for a response.
There are 0 IPC messages waiting for additional fragments.
There are 2 messages currently in use by the system.
Router#
```

次に、ローカル IPC サーバのステータスを表示する例を示します。

```
Router# show ipc status
IPC System Status:

This processor is a slave server.

1000 IPC message headers in cache
377053 messages in, 293133 out, 210699 delivered to local port,
83655 acknowledgements received, 83870 sent,
0 NACKS received, 0 sent,
0 messages dropped on input, 0 messages dropped on output
0 no local port, 0 destination unknown, 0 no transport
0 missing callback or queue, 0 duplicate ACKs, 0 retries,
0 message timeouts.
0 ipc_output failures, 0 mtu failures,
0 msg_alloc failed, 0 emer msg alloc failed, 0 no origs for RPC replies
0 pak_alloc failed, 0 memd_alloc failed
0 no hwq, 0 failed opens, 0 hardware errors
No regular dropping of IPC output packets for test purposes
Router#
```

show ip cache flow

NetFlow キャッシュ フロー エントリのサマリーを表示するには、**show ip cache flow** コマンドを使用します。

show ip cache flow [aggregation type [module num]]

シンタックスの説明

aggregation type	(任意) 特定の集約キャッシュの設定を表示します。有効値については、「使用上のガイドライン」を参照してください。
module num	(任意) 特定のモジュールに関する情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

aggregation type の有効値は次のとおりです。

- **as** : AS 集約キャッシュ
- **destination-prefix** : 宛先プレフィクス集約キャッシュ
- **prefix** : 送信元/宛先プレフィクス集約キャッシュ
- **protocol-port** : プロトコルおよびポート集約キャッシュ
- **source-prefix** : 送信元プレフィクス集約キャッシュ

module num を指定せずに **show ip cache flow aggregation** コマンドを入力した場合、ソフトウェアでスイッチングされる、ルートプロセッサ (RP) 上の集約キャッシュが表示されます。

例

次に、NetFlow キャッシュ フロー エントリのサマリーを表示する例を示します。

```
Router# show ip cache flow
IP packet size distribution (0 total packets):
 1-32 64 96 128 160 192 224 256 288 320 352 384 416
448
480
 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
 .000 .000

 512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 0 bytes
0 active, 0 inactive, 0 added
0 ager polls, 0 flow alloc failures
```

```

Active flows timeout in 30 minutes
Inactive flows timeout in 15 seconds
last clearing of statistics never
Protocol Total Flows Packets Bytes Packets Active(Sec)
Idle(Sec)
----- Flows /Sec /Flow /Pkt /Sec /Flow
/Flow

SrcIf SrcIPAddress DstIf DstIPAddress Pr SrcP
DstP
Pkts

Displaying Hardware entries in Module 7
SrcIf SrcIPAddress DstIPAddress Pr SrcP
DstP Pkts
Fa5/11 11.1.1.38 12.1.1.2 udp 63
63 986796
Fa5/11 11.1.1.39 12.1.1.2 udp 63
63 986796
Fa5/11 11.1.1.40 12.1.1.2 udp 63
63 986796
Fa5/11 11.1.1.41 12.1.1.2 udp 63
63 986796
Fa5/11 11.1.1.42 12.1.1.2 udp 63
63 986796
Fa5/11 11.1.1.43 12.1.1.2 udp 63
63 986796
Fa5/11 11.1.1.44 12.1.1.2 udp 63
63 986796
Fa5/11 11.1.1.45 12.1.1.2 udp 63
63 986796
Fa5/11 11.1.1.46 12.1.1.2 udp 63
63 986796
Fa5/11 11.1.1.47 12.1.1.2 udp 63
63 986796
Fa5/11 11.1.1.48 12.1.1.2 udp 63
63 986796
Router#

```

次に、特定のモジュールの宛先プレフィクス集約キャッシュに関する情報を表示する例を示します。

```

Router# show ip cache flow aggregation destination-prefix module 1
IPFLOW_DST_PREFIX_AGGREGATION records and statistics for module :1
IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 6 added
  236 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds

Dst If          Dst Prefix      Msk AS    Flows  Pkts B/Pk  Active
Gi7/9          9.1.0.0         /16 0       3003   12M   64   1699.8
Gi7/10        11.1.0.0        /16 0       3000   9873K  64   1699.8
Router#

```

表 2-39 に、show ip cache flow コマンド出力フィールドを示します。

表 2-39 show ip cache flow コマンドの出力フィールド：パケット サイズ分布

フィールド	説明
IP packet size distribution	この行の下の 2 行は、サイズ範囲ごとのパケット分布（パーセント）を示します。この出力例では、パケットの 55.4% が 33 ~ 64 バイトのサイズ範囲に分類されます。

表 2-40 に、フロー スイッチング キャッシュを示す出力行内のフィールドの説明を示します。

表 2-40 show ip cache flow コマンドの出力フィールド：フロー スイッチング キャッシュ

フィールド	説明
bytes	NetFlow キャッシュで使用されるメモリのバイト数
active	このコマンドを入力した時点における NetFlow キャッシュ内のアクティブフロー数
inactive	NetFlow キャッシュに割り当てられているが、このコマンドを入力した時点において特定のフローに割り当てられていないフロー バッファの数
added	サマリー期間の開始以降に作成されたフロー数
ager polls	エントリを期限切れにするために、NetFlow コードがキャッシュを参照した回数 (シスコが診断のためにだけ使用)
flow alloc failures	NetFlow コードがフローの割り当てを試行したにもかかわらず、割り当てることができなかった回数
Exporting flows to	フローのエクスポート先となるワークステーションの IP アドレスおよび UDP ポート番号
Exporting using source interface	送信元 IP アドレスとして使用されるインターフェイス タイプ
Version 5 flow records, peer-as	バージョン 5 フォーマットでエクスポートされたパケットおよび統計情報。エクスポート統計情報には、送信元および宛先のピア AS が含まれます。データグラムに格納されるレコード数は、バージョン 5 の場合、1 ~ 30 の範囲です。
Active flows timeout in	NetFlow キャッシュ内のアクティブ フローのタイムアウト期間
flows exported in udp datagrams	エクスポートされたフローの総数、およびフローをワークステーションにエクスポートするために使用された UDP データグラムの総数
failed	出力インターフェイスの制限のためにルータがエクスポートできなかったフロー数
last clearing of statistics	clear ip flow stats コマンドの実行からの経過標準時間出力 (hh:mm:ss)。24 時間が経過すると、この時間出力は日時に変わります。

表 2-41 に、出力のプロトコル行別の NetFlow アクティビティを示すフィールドの説明を示します。

表 2-41 show ip cache flow コマンドの出力フィールド：NetFlow プロトコル別アクティビティ

フィールド	説明
Protocol	RFC 1340 に記述されている IP プロトコルおよび well-known ポート番号
Total Flows	最後に統計情報がクリアされた以降のこのプロトコルのフロー総数
Flows/Sec	1 秒間に認識される、このプロトコルの平均フロー数。(総フロー数) / (このサマリー期間の秒数) に等しくなります。
Packets/Flow	このプロトコルで認識されるフローに対して観察された平均パケット数。(このプロトコルのパケット総数) / (このサマリー期間におけるこのプロトコルのフロー数) に等しくなります。
Bytes/Pkt	このプロトコルで認識されるパケットに対して観察された平均バイト数。(このプロトコルのバイト総数) / (このサマリー期間におけるこのプロトコルのパケット総数) に等しくなります。

表 2-41 show ip cache flow コマンドの出力フィールド : NetFlow プロトコル別アクティビティ (続)

フィールド	説明
Packets/Sec	1 秒間のこのプロトコルの平均パケット数。(このプロトコルのパケット総数) / (このサマリー期間の秒数) に等しくなります。
Active(Sec)/Flow	(期限切れフローの最初のパケットから最終パケット [TCP FIN、time-out など] までの全秒数の合計) / (このサマリー期間におけるこのプロトコルのフロー総数)
Idle(Sec)/Flow	(このプロトコルの各フロー (有効期限内) の最終パケットから、このコマンドの入力時点までの全秒数の合計) / (このサマリー期間におけるこのプロトコルのフロー総数)

表 2-42 に、現行フローを示す出力行内のフィールドの説明を示します。

表 2-42 show ip cache flow コマンドの出力フィールド : 現行フロー

フィールド	説明
SrcIf	送信元インターフェイスの内部ポート名
SrcIPAddress	このフローの送信元 IP アドレス
DstIf	宛先インターフェイスのルータの内部ポート名
DstIPAddress	このフローの宛先 IP アドレス
Pr	IP プロトコル (6=TCP、17=UDP など、RFC 1340 の定義に従います)
SrcP	送信元ポートアドレス、TCP/UDP の「well-known」のポート番号 (RFC 1340 の定義に従います)
DstP	宛先ポートアドレス、TCP/UDP の「well-known」のポート番号 (RFC 1340 の定義に従います)
Pkts	このフローに対して観察されたパケット数
B/Pkt	このフローに対してパケット単位で観察された平均バイト数
Active	フローの先頭パケットと最終パケット間の秒数

関連コマンド

コマンド	説明
ip flow-aggregation cache	フロー集約キャッシュを作成し、集約キャッシュ コンフィギュレーション モードを開始します。
ip flow-cache entries	NetFlow キャッシュに維持するエン트리数を変更します。
clear ip flow stats	NetFlow スイッチングの統計情報をクリアします。

show ip cache verbose flow

NetFlow 統計の詳細サマリーを表示するには、**show ip cache verbose flow** コマンドを使用します。

show ip cache verbose flow

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

show ip cache verbose flow コマンドを使用すると、**show ip cache flow** コマンドで表示されるフィールドに加えて、NetFlow キャッシュのフロー レコード フィールドを表示できます。表示される追加フィールドの値は、イネーブルになっている NetFlow 機能とフローで設定されているフラグによって異なります。



(注)

表示されるフラグとフィールドは、フローごとに異なります。

MPLS 対応 NetFlow 機能を設定すると、**show ip cache verbose flow** コマンドを使用してルータ モジュール上の NetFlow キャッシュの MPLS フローの IP 部分と MPLS 部分の両方を表示できます。MPLS アウェア NetFlow が設定されている場合に、NetFlow キャッシュのフロー レコードの IP 部分だけを表示するには、**show ip cache flow** コマンドを使用します。

例

次に、NetFlow 統計の詳細サマリーを表示する例を示します。

```
Router# show ip cache verbose flow
IP packet size distribution (1094508 total packets):
  1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 480
  .000 1.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

      512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
      .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  2 active, 65534 inactive, 2 added
  298 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 270600 bytes
  4 active, 16380 inactive, 4 added, 2 added to flow
  0 alloc failures, 0 force free
```

```

1 chunk, 1 chunk added
last clearing of statistics never
Protocol      Total    Flows   Packets Bytes   Packets Active(Sec) Idle(Sec)
-----      -
              Flows   /Sec    /Flow /Pkt    /Sec    /Flow    /Flow

SrcIf          SrcIPAddress   DstIf          DstIPAddress   Pr TOS Flgs Pkts
Port Msk AS    Port Msk AS    NextHop        B/Pk Active
IPM: OPkts    OBytes

SrcIf          SrcIPAddress   DstIf          DstIPAddress   Pr TOS Flgs Pkts
Port Msk AS    Port Msk AS    NextHop        B/Pk Active
IPM: OPkts    OBytes
Fa5/11         11.1.1.2       Fa5/12         12.1.1.2       06 5B 00   551K
0000 /16 0    0000 /16 0    12.1.1.2       46   149.7
FO: 1
Fa5/11         11.1.1.3       Fa5/12         12.1.1.2       06 5B 00   553K
0000 /16 0    0000 /16 0    12.1.1.2       46   150.4
FO: 1

Displaying Hardware entries in Module 7
SrcIf          SrcIPAddress   DstIPAddress   Pr      SrcP      DstP
Pkts
--             0.0.0.0       0.0.0.0       0       0         0         3

Router#

```

表 2-43 に、出力の NetFlow キャッシュ行に表示されるフィールドの説明を示します。

表 2-43 show ip cache verbose flow の NetFlow Cache 出力のフィールドの説明

フィールド	説明
bytes	NetFlow キャッシュで使用されるメモリのバイト数
active	このコマンドを入力した時点における NetFlow キャッシュ内のアクティブフロー数
inactive	NetFlow キャッシュに割り当てられているが、このコマンドを入力した時点において特定のフローに割り当てられていないフローバッファの数
added	サマリー期間の開始以降に作成されたフロー数
ager polls	NetFlow コードがエントリの期限切れを引き起こした回数 (シスコが診断のためにだけ使用)
flow alloc failures	NetFlow コードがフローの割り当てを試行したにもかかわらず、割り当てることができなかった回数
last clearing of statistics	clear ip flow stats 特権 EXEC コマンドが最後に実行されてからの経過標準時間出力 (hh:mm:ss)。24 時間が経過すると、この時間出力は日時に変わります。

show ip cache verbose flow

表 2-44 に、出力のプロトコル別アクティビティ行に表示されるフィールドの説明を示します。

表 2-44 show ip cache verbose flow のプロトコル別アクティビティ出力のフィールドの説明

フィールド	説明
Protocol	IP プロトコルとポート番号（最新の RFC 値については、 http://www.iana.org の『 <i>Protocol Assignment Number Services</i> 』を参照） (注) すべてのプロトコルの小さいサブセットだけが表示されます。
Total Flows	最後に統計情報がクリアされた以降のこのプロトコルのフロー総数
Flows/Sec	このプロトコルの 1 秒間の平均フロー数。(総フロー数) / (このサマリー期間の秒数) に等しくなります。
Packets/Flow	このプロトコルのフローの平均パケット数。(このプロトコルの合計パケット数) / (このサマリー期間のこのプロトコルのフロー数) に等しくなります。
Bytes/Pkt	このプロトコルのパケットの平均バイト数。(このプロトコルの合計バイト数) / (このサマリー期間のこのプロトコルの合計パケット数) に等しくなります。
Packets/Sec	このプロトコルの 1 秒間の平均パケット数。(このプロトコルの合計パケット数) / (このサマリー期間の秒数) に等しくなります。
Active(Sec)/Flow	(期限切れフローの最初のパケットから最終パケット (TCP FIN、time-out など) までの秒数) / (このサマリー期間におけるこのプロトコルのフロー総数)
Idle(Sec)/Flow	(このプロトコルの各フロー (有効期限内) の最終パケットから、このコマンドの入力時点までの秒数) / (このサマリー期間におけるこのプロトコルのフロー総数)

表 2-45 に、出力の NetFlow レコード行に表示されるフィールドの説明を示します。

表 2-45 show ip cache verbose flow の NetFlow レコード出力のフィールドの説明

フィールド	説明
SrcIf	パケットが受信されたインターフェイス
Port Msk AS	送信元ポート番号 (16 進形式で表示)、IP アドレス マスク、および自律システム番号。MPLS フローでは、このフィールドは常に 0 に設定されます。
SrcIPAddress	パケットを送信したデバイスの IP アドレス
DstIf	パケットが送信されたインターフェイス
Port Msk AS	宛先ポート番号 (16 進形式で表示)、IP アドレス マスク、および自律システム番号。MPLS フローでは、このフィールドは常に 0 に設定されます。
DstIPAddress	宛先デバイスの IP アドレス
NextHop	BGP ネクストホップアドレス。MPLS フローでは、このフィールドは常に 0 に設定されます。
Pr	IP プロトコルのポート番号。16 進形式で表示されます。 (最新の RFC 値については、 http://www.iana.org の『 <i>Protocol Assignment Number Services</i> 』を参照してください)

表 2-45 show ip cache verbose flow の NetFlow レコード出力のフィールドの説明 (続き)

フィールド	説明
TOS	サービスのタイプ (16 進形式で表示)
B/Pk	このプロトコルで認識されるパケットに対して観察された平均バイト数
Flgs	16 進形式で表示される TCP フラグ (フロー内のすべてのパケットの TCP フラグのビット単位 OR の結果)
Pkts	このフロー内のパケット数
Active	フローがアクティブだった時間
FO	フラグメント オフセット

関連コマンド

コマンド	説明
ip flow-cache mpls label positions	MPLS アウェア NetFlow をイネーブルにします。
ip route-cache flow	IP ルーティングの NetFlow スイッチングをイネーブルにします。
show ip cache flow	NetFlow キャッシュ フロー エントリのサマリーを表示します。

■ show ip cache verbose flow

show ip cef epoch

隣接テーブルおよびすべての FIB テーブルのエポック情報を表示するには、**show ip cef epoch** コマンドを使用します。

show ip cef epoch

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード 特権 EXEC (#)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン 次に示す **show** コマンドも、それぞれ次のエポック情報を表示します。

- **show ip cef summary** : 特定の FIB テーブルのテーブル エポックを表示します。
- **show ip cef detail** : 特定の FIB テーブルの各エントリのエポック値を表示します。
- **show adjacency summary** : 隣接テーブルのエポックを表示します。
- **show adjacency detail** : 隣接テーブルの各エントリのエポック値を表示します。

例 次に、エポック情報を表示する例を示します。

```
Router# show ip cef epoch
CEF epoch information:
```

```
Table:Default-table
  Table epoch:2 (164 entries at this epoch)
```

```
Adjacency table
  Table epoch:1 (33 entries at this epoch)
```

次に、エポック テーブルを削除し、エポック番号を増分したあとの出力例を示します。

```
Router# show ip cef epoch
CEF epoch information:
```

```
Table:Default-table
  Table epoch:2 (164 entries at this epoch)
```

```
Adjacency table
  Table epoch:1 (33 entries at this epoch)
```

■ show ip cef epoch

```

Router# clear ip cef epoch full
Router# show ip cef epoch
CEF epoch information:

Table:Default-table
  Table epoch:3 (164 entries at this epoch)

Adjacency table
  Table epoch:2 (33 entries at this epoch)
Router#

```

■ シンタックスの説明

コマンド	説明
clear ip cef epoch full	新しいエポックを開始し、すべてのテーブル（隣接テーブルを含む）のエポック番号を増分します。
show ip cef	FIB 内のエントリを表示するか、FIB のサマリーを表示します。

show ip cef inconsistency

IP CEF の不一致を表示するには、**show ip cef inconsistency** コマンドを使用します。

show ip cef [vrf vrf-name] inconsistency [records [detail]]

シンタックスの説明

vrf vrf-name	(任意) VRF インスタンスを指定します。
records	(任意) 記録されたすべての不一致を表示します。
detail	(任意) 各 CEF テーブル エントリの詳細情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、**lc-detect**、**scan-rp**、**scan-rib**、および **scan-lc** 検出メカニズムで検出された記録済み IP CEF 不一致レコードを表示します。

IP CEF プレフィックスの不一致検出メカニズムを設定するには、**ip cef table consistency-check** コマンドを使用します。

例

次に、記録された CEF 不一致レコードを表示する例を示します。

```
Router# show ip cef inconsistency
Table consistency checkers (settle time 65s)
lc-detect:running
  0/0/0 queries sent/ignored/received
scan-lc:running [100 prefixes checked every 60s]
  0/0/0 queries sent/ignored/received
scan-rp:running [100 prefixes checked every 60s]
  0/0/0 queries sent/ignored/received
scan-rib:running [1000 prefixes checked every 60s]
  0/0/0 queries sent/ignored/received
Inconsistencies:0 confirmed, 0/16 recorded
```

■ show ip cef inconsistency

表 2-46 に、この出力で表示されるフィールドについて説明します。

表 2-46 show ip cef inconsistency のフィールドの説明

フィールド	説明
settle time	記録された不一致を確認してからの時間
lc-detect running	一貫性チェッカー lc-detect が稼動中です。
0/0/0 queries	送信、無視、および受信されたクエリー数
Inconsistencies:	確認および記録された不一致数。記録される不一致レコードの最大数は 16 です。

■ 関連コマンド

コマンド	説明
clear ip cef inconsistency	CEF 一貫性チェッカーの統計情報および記録情報をクリアします。

show ip cef summary

IP CEF テーブルのサマリーを表示するには、**show ip cef summary** コマンドを使用します。

show ip cef summary

シンタックスの説明 このコマンドには、キーワードおよび引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、IP CEF テーブルのサマリーを表示する例を示します。

```
Router# show ip cef summary
IP Distributed CEF with switching (Table Version 25), flags=0x0
 21 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 1
 21 leaves, 16 nodes, 19496 bytes, 36 inserts, 15 invalidations
 0 load sharing elements, 0 bytes, 0 references
universal per-destination load sharing algorithm, id 5163EC15
3(0) CEF resets, 0 revisions of existing leaves
Resolution Timer: Exponential (currently 1s, peak 1s)
 0 in-place/0 aborted modifications
refcounts: 4377 leaf, 4352 node

Table epoch: 0 (21 entries at this epoch)

Adjacency Table has 9 adjacencies
Router#
```

show ip cef vlan

特定のインターフェイスの IP CEF VLAN インターフェイス ステータス、設定、およびプレフィクスに関する情報を表示するには、**show ip cef vlan** コマンドを使用します。

show ip cef vlan *vlan-id* [detail]

シンタックスの説明

<i>vlan-id</i>	VLAN 番号。有効値は 1 ~ 4094 です。
detail	(任意) IP CEF VLAN インターフェイスに関する詳細情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、特定の VLAN のプレフィクスを表示する例を示します。

```
Router> show ip cef vlan 1003
Prefix                Next Hop                Interface
0.0.0.0/0             172.20.52.1            FastEthernet3/3
0.0.0.0/32            receive
10.7.0.0/16           172.20.52.1            FastEthernet3/3
10.16.18.0/23         172.20.52.1            FastEthernet3/3
Router>
```

次に、特定の VLAN に関する詳細な IP CEF 情報を表示する例を示します。

```
Router> show ip cef vlan 1003 detail
IP Distributed CEF with switching (Table Version 2364), flags=0x0
 1383 routes, 0 reresolve, 0 unresolved (0 old, 0 new)
 1383 leaves, 201 nodes, 380532 bytes, 2372 inserts, 989 invalidations
 0 load sharing elements, 0 bytes, 0 references
 universal per-destination load sharing algorithm, id 9B6C9823
 3 CEF resets, 0 revisions of existing leaves
 refcounts: 54276 leaf, 51712 node
Adjacency Table has 5 adjacencies
Router>
```

show ip dhcp relay information trusted-sources

設定済みの信頼されたインターフェイスをすべて表示するには、**show ip dhcp relay information trusted-sources** コマンドを使用します。

show ip dhcp relay information trusted-sources

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、設定済みの信頼されたインターフェイスをすべて一覧表示する例を示します。

```
Router# show ip dhcp relay information trusted-sources
List of trusted sources of relay agent information option:
Vlan60          Vlan62
Router#
```

関連コマンド	コマンド	説明
	ip dhcp relay information option trust-all	DHCP のリレー エージェント情報オプションの信頼できる送信元としてすべてのインターフェイスをイネーブルにします。
	ip dhcp relay information trust	DHCP のリレー エージェント情報の信頼できる送信元としてインターフェイスをイネーブルにします。

show ip dhcp snooping

DHCP スヌーピングの設定を表示するには、**show ip dhcp snooping** コマンドを使用します。

show ip dhcp snooping [statistics [detail]]

シンタックスの説明

statistics	(任意) DHCP スヌーピングに関する統計情報を表示します。
detail	(任意) DHCP スヌーピングに関する詳細情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、DHCP スヌーピングの設定を表示する例を示します。

```
Router# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5 10
Insertion of option 82 is enabled
Interface          Trusted      Rate limit (pps)
-----
FastEthernet6/11   no          10
FastEthernet6/36   yes         50
Router#
```

次に、DHCP スヌーピングの統計情報を表示する例を示します。

```
Router# show ip dhcp snooping statistics
Packets Processed by DHCP Snooping          = 0
Packets Dropped Because
  IDB not known                             = 0
  Queue full                                = 0
  Interface is in errdisabled                = 0
  Rate limit exceeded                        = 0
  Received on untrusted ports                = 0
  Nonzero giaddr                             = 0
  Source mac not equal to chaddr             = 0
  No binding entry                           = 0
  Insertion of opt82 fail                    = 0
  Unknown packet                             = 0
  Interface Down                             = 0
  Unknown output interface                   = 0
Router#
```

次に、DHCP スヌーピングの詳細な統計情報を表示する例を示します。

```
Router# show ip dhcp snooping statistics detail
Packets Forwarded                            = 0
```

```
Packets Dropped = 0
Packets Dropped From untrusted ports = 0
Router#
```

関連コマンド

コマンド	説明
clear ip dhcp snooping	IP DHCP テーブル エントリをクリアします。
ip dhcp snooping	DHCP スヌーピングをグローバルにイネーブルにします。
ip dhcp snooping binding	DHCP バインディングの設定を確立および生成して、再起動後にバインディングを復元します。
ip dhcp snooping database	DHCP スヌーピングのデータベースを設定します。
ip dhcp snooping information option	DHCP option 82 データ挿入をイネーブルにします。
ip dhcp snooping limit rate	インターフェイスが秒単位で受信できる DHCP メッセージ数を設定します。
ip dhcp snooping packets	トンネル インターフェイス上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping verify mac-address	信頼できないポート上で DHCP パケットの送信元 MAC アドレスがクライアントのハードウェア アドレスに一致することを確認します。
ip dhcp snooping vlan	1 つの VLAN または VLAN のグループで DHCP スヌーピングをイネーブルにします。
show ip dhcp snooping binding	DHCP スヌーピングのバインディング エントリを表示します。
show ip dhcp snooping database	DHCP スヌーピング データベース エージェントのステータスを表示します。

show ip dhcp snooping binding

DHCP スヌーピングのバインディング エントリを表示するには、**show ip dhcp snooping binding** コマンドを使用します。

```
show ip dhcp snooping binding [ip-address] [mac-address] [vlan vlan]
[interface interface interface-num]
```

シンタックスの説明

<i>ip-address</i>	(任意) バインディング エントリの IP アドレス
<i>mac-address</i>	(任意) バインディング エントリの MAC アドレス
vlan <i>vlan</i>	(任意) 有効な VLAN 番号を指定します。有効値は 1 ~ 4094 です。
interface <i>interface</i>	(任意) インターフェイス タイプを指定します。有効値は ethernet 、 fastethernet 、 gigabithernet 、および tengigabithernet です。
<i>interface-num</i>	モジュールおよびポート番号

コマンドのデフォルト

引数を指定しなかった場合、スイッチは DHCP スヌーピング バインディング テーブル全体を表示します。

コマンド モード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

グローバル スヌーピングと VLAN スヌーピングの両方がイネーブルになっている場合だけ、DHCP スヌーピングが VLAN でイネーブルになります。

例

次に、スイッチの DHCP スヌーピング バインディング エントリを表示する例を示します。

```
Router# show ip dhcp snooping binding
```

```
MacAddress      IP Address      Lease (seconds)  Type              VLAN      Interface
-----
0000.0100.0201  10.0.0.1        1600              dhcp-snooping     100       FastEthernet3/1
Router#
```

次に、DHCP スヌーピング バインディング エントリの IP アドレスを表示する例を示します。

```
Router# show ip dhcp snooping binding 172.100.101.102
```

```
MacAddress      IP Address      Lease (seconds)  Type              VLAN      Interface
-----
0000.0100.0201  172.100.101.102  1600              dhcp-snooping     100       FastEthernet3/1
Router#
```

次に、DHCP スヌーピング バインディング エントリの MAC アドレスを表示する例を示します。

```
Router# show ip dhcp snooping binding 55.5.5.2 0002.b33f.3d5f
```

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:02:B3:3F:3D:5F	55.5.5.2	492	dhcp-snooping	99	FastEthernet6/36

次に、特定の VLAN の DHCP スヌーピング バインディング エントリの MAC アドレスを表示する例を示します。

```
Router# show ip dhcp snooping binding 55.5.5.2 0002.b33f.3d5f vlan 99
```

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:02:B3:3F:3D:5F	55.5.5.2	479	dhcp-snooping	99	FastEthernet6/36

次に、ダイナミック DHCP スヌーピング バインディング エントリを表示する例を示します。

```
Router# show ip dhcp snooping binding dynamic
```

MacAddress	IP Address	Lease (seconds)	Type	VLAN	Interface
0000.0100.0201	10.0.0.1	1600	dhcp-snooping	100	FastEthernet3/1

次に、VLAN 100 の DHCP スヌーピング バインディング エントリを表示する例を示します。

```
Router# show ip dhcp snooping binding vlan 100
```

MacAddress	IP Address	Lease (seconds)	Type	VLAN	Interface
0000.0100.0201	10.0.0.1	1600	dhcp-snooping	100	FastEthernet3/1

次に、イーサネット インターフェイス 0/1 の DHCP スヌーピング バインディング エントリを表示する例を示します。

```
Router# show ip dhcp snooping binding interface fastethernet3/1
```

MacAddress	IP Address	Lease (seconds)	Type	VLAN	Interface
0000.0100.0201	10.0.0.1	1600	dhcp-snooping	100	FastEthernet3/1

表 2-47 に、**show ip dhcp snooping** コマンド出力に含まれるフィールドの説明を示します。

表 2-47 show ip dhcp snooping コマンド出力

フィールド	説明
Mac Address	クライアント ハードウェア MAC アドレス
IP Address	DHCP サーバから割り当てられたクライアント IP アドレス
Lease (seconds)	IP アドレス リース時間
Type	バインディング タイプ。CLI からスタティックに設定されるか、ダイナミックに学習されます。
VLAN	クライアント インターフェイスの VLAN 番号
Interface	DHCP クライアント ホストに接続するインターフェイス

■ show ip dhcp snooping binding

関連コマンド

コマンド	説明
ip dhcp snooping	DHCP スヌーピングをグローバルにイネーブルにします。
ip dhcp snooping binding	DHCP バインディングの設定を確立および生成して、再起動後にバインディングを復元します。
ip dhcp snooping database	DHCP スヌーピングのデータベースを設定します。
ip dhcp snooping information option	DHCP option 82 データ挿入をイネーブルにします。
ip dhcp snooping limit rate	インターフェイスが秒単位で受信できる DHCP メッセージ数を設定します。
ip dhcp snooping packets	トンネル インターフェイス上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping verify mac-address	信頼できないポート上で DHCP パケットの送信元 MAC アドレスがクライアントのハードウェア アドレスに一致することを確認します。
ip dhcp snooping vlan	1 つの VLAN または VLAN のグループで DHCP スヌーピングをイネーブルにします。
show ip dhcp snooping	DHCP スヌーピングの設定を表示します。
show ip dhcp snooping database	DHCP スヌーピング データベース エージェントのステータスを表示します。

show ip dhcp snooping database

DHCP スヌーピング データベース エージェントのステータスを表示するには、**show ip dhcp snooping database** コマンドを使用します。

show ip dhcp snooping database [detail]

シンタックスの説明	detail (任意) 追加の動作状態と統計情報を表示します。
-----------	--

コマンドのデフォルト	このコマンドにはデフォルト設定がありません。
------------	------------------------

コマンドモード	特権 EXEC (#)
---------	-------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、DHCP スヌーピング データベースを表示する例を示します。

```
Router# show ip dhcp snooping database
Agent URL :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts      :          0   Startup Failures :          0
Successful Transfers :          0   Failed Transfers :          0
Successful Reads    :          0   Failed Reads     :          0
Successful Writes   :          0   Failed Writes    :          0
Media Failures      :          0
```

Router#

次に、追加の動作統計情報を表示する例を示します。

```
Router# show ip dhcp snooping database detail
Agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 7 (00:00:07)
Abort Timer Expiry : Not Running

Last Succeeded Time : None
```

show ip dhcp snooping database

```

Last Failed Time : 17:14:25 UTC Sat Jul 7 2001
Last Failed Reason : Unable to access URL.

Total Attempts      :      21   Startup Failures :      0
Successful Transfers :      0   Failed Transfers :     21
Successful Reads    :      0   Failed Reads    :      0
Successful Writes   :      0   Failed Writes   :     21
Media Failures     :      0

First successful access: Read

Last ignored bindings counters :
Binding Collisions   :      0   Expired leases   :      0
Invalid interfaces  :      0   Unsupported vlans :      0
Parse failures      :      0
Last Ignored Time   : None

Total ignored bindings counters:
Binding Collisions   :      0   Expired leases   :      0
Invalid interfaces  :      0   Unsupported vlans :      0
Parse failures      :      0

Router#
    
```

関連コマンド

コマンド	説明
ip dhcp snooping	DHCP スヌーピングをグローバルにイネーブルにします。
ip dhcp snooping binding	DHCP バインディングの設定を確立および生成して、再起動後にバインディングを復元します。
ip dhcp snooping database	DHCP スヌーピングのデータベースを設定します。
ip dhcp snooping information option	DHCP option 82 データ挿入をイネーブルにします。
ip dhcp snooping limit rate	インターフェイスが秒単位で受信できる DHCP メッセージ数を設定します。
ip dhcp snooping packets	トンネルインターフェイス上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping verify mac-address	信頼できないポート上で DHCP パケットの送信元 MAC アドレスがクライアントのハードウェアアドレスに一致することを確認します。
ip dhcp snooping vlan	1 つの VLAN または VLAN のグループで DHCP スヌーピングをイネーブルにします。
show ip dhcp snooping	DHCP スヌーピングの設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピングのバインディング エントリを表示します。

show ip flow-export

ソフトウェア スイッチングされるデータ エクスポートのフロー情報（メイン キャッシュや他のすべてのイネーブル化されたキャッシュなど）を表示するには、**show ip flow-export** コマンドを使用します。

show ip flow export [template | verbose]

シンタックスの説明	template	(任意) エクスポート テンプレート統計情報を表示します。
	verbose	(任意) 詳細なエクスポート統計情報を表示します。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、ソフトウェア スイッチングされる NDE のフロー情報を表示する例を示します。

```
Router# show ip flow export
Flow export v1 is disabled for main cache
Version 1 flow records
 0 flows exported in 0 udp datagrams
 0 flows failed due to lack of export packet
 0 export packets were sent up to process level
 0 export packets were dropped due to no fib
 0 export packets were dropped due to adjacency issues
 0 export packets were dropped due to fragmentation failures
 0 export packets were dropped due to encapsulation fixup failures
 0 export packets were dropped enqueueing for the RP
 0 export packets were dropped due to IPC rate limiting
Router#
```

次に、エクスポート テンプレート統計情報を表示する例を示します。

```
Router# show ip flow export template
No Template export information
No Option Templates exist
  Template Options Flag = 0
  Total number of Templates added = 0
  Total active Templates = 0
  Flow Templates active = 0
  Flow Templates added = 0
  Option Templates active = 0
  Option Templates added = 0
  Template ager polls = 0
  Option Template ager polls = 0
Main cache version 9 export is disabled
Router#
```

■ show ip flow-export

次に、詳細なエクスポート統計情報を表示する例を示します。

```
Router# show ip flow export verbose
Flow export v1 is disabled for main cache
  Version 1 flow records
    0 flows exported in 0 udp datagrams
    0 flows failed due to lack of export packet
    0 export packets were sent up to process level
    0 export packets were dropped due to no fib
    0 export packets were dropped due to adjacency issues
    0 export packets were dropped due to fragmentation failures
    0 export packets were dropped due to encapsulation fixup failures
    0 export packets were dropped enqueueing for the RP
    0 export packets were dropped due to IPC rate limiting
Router#
```

関連コマンド

コマンド	説明
clear adjacency	CEF 隣接テーブルをクリアします。
ip flow-aggregation cache	フロー集約キャッシュを作成し、集約キャッシュ コンフィギュレーションモードを開始します。

show ip igmp groups

ルータに直接接続し、IGMP によって学習されたレシーバーがあるマルチキャスト グループを表示するには、**show ip igmp groups** コマンドを使用します。

```
show ip igmp [vrf vrf-name] groups [group-name | group-address | interface-type
interface-number] [detail]
```

シンタックスの説明

<i>vrf vrf-name</i>	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
<i>group-name</i>	(任意) DNS ホスト テーブルで定義されているマルチキャスト グループの名前
<i>group-address</i>	(任意) 4 分割ドット 10 進表記によるマルチキャスト グループのアドレス
<i>interface-type</i>	(任意) インターフェイス タイプ
<i>interface-number</i>	(任意) インターフェイス番号
detail	(任意) IGMP Version 3 (IGMPv3)、IGMP v3lite、または URL Rendezvous Directory (URD) を通じて認識される送信元の詳細な説明を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

任意の引数とキーワードをすべて省略した場合、**show ip igmp groups** コマンドは、直接接続しているすべてのマルチキャスト グループをグループ アドレス、インターフェイス タイプ、およびインターフェイス番号別に表示します。

例

次に、**show ip igmp groups** コマンドの出力を表示する例を示します。

```
Router# show ip igmp groups

IGMP Connected Group Membership
Group Address      Interface      Uptime      Expires      Last Reporter
239.255.255.254    Ethernet3/1    1w0d        00:02:19    172.21.200.159
224.0.1.40         Ethernet3/1    1w0d        00:02:15    172.21.200.1
224.0.1.40         Ethernet3/3    1w0d        never        172.16.214.251
224.0.1.1          Ethernet3/1    1w0d        00:02:11    172.21.200.11
224.9.9.2          Ethernet3/1    1w0d        00:02:10    172.21.200.155
232.1.1.1          Ethernet3/1    5d21h       stopped     172.21.200.206
```

show ip igmp groups

次に、**show ip igmp groups** コマンドに *group-address* 引数と **detail** キーワードを指定した場合の出力を表示する例を示します。

```
Router# show ip igmp groups 232.1.1.1 detail

Interface:      Ethernet3/2
Group:          232.1.1.1
Uptime:         01:58:28
Group mode:     INCLUDE
Last reporter:  10.0.119.133
CSR Grp Exp:   00:02:38
Group source list: (C - Cisco Src Report, U - URD, R - Remote)
  Source Address  Uptime    v3 Exp   CSR Exp  Fwd  Flags
  172.16.214.1   01:58:28  stopped  00:02:31 Yes   C
```

表 2-48 に、この出力で表示されるフィールドについて説明します。

表 2-48 show ip igmp groups のフィールドの説明

フィールド	説明
Group Address	マルチキャストグループのアドレス
Interface	グループに到達可能なインターフェイス
Uptime	このマルチキャストグループが認識されていた時間（週、日、時間、分、および秒）
Expires	<p>エントリが期限切れになるまでの時間（週、日、時間、分、および秒）エントリが期限切れになる場合、エントリは削除される前に（短時間）[now] と表示されます。</p> <p>[never] は、このエントリのローカル レシーバーがこのルータ上にあるので、エントリがタイムアウトにならないことを示します。</p> <p>[stopped] は、このエントリのタイムアウトがこの有効期限タイマーでは判断できないことを示します。グループについてルータが INCLUDE モードの場合、最後の送信元エントリがタイムアウトになると、グループ エントリ全体がタイムアウトになります（タイムアウトになる前にモードが EXCLUDE モードに変更された場合を除きます）。</p>
Last Reporter	マルチキャストグループのメンバーであることを最後に報告したホスト。IGMP v3lite と URD のいずれも v2-report が必要です。
Group mode:	INCLUDE または EXCLUDE。グループ モードは、グループのインターフェイスで受信されるメンバーシップ レポートのタイプに基づきます。 show ip igmp groups detail コマンドの出力では、EXCLUDE モードの場合、グループ エントリ（出力には表示されない）の Expires: フィールドも表示されます。
CSR Grp Exp	SSM 範囲内のマルチキャストグループについて表示されます。最後の受信グループ メンバーシップ レポートが受信されてからの時間（時間、分、および秒）を示します。Cisco IOS ソフトウェアは、URD および IGMP v3lite の動作のためにこれらのレポートを使用する必要がありますが、レポートそのものによってグループ メンバーシップを示すわけではありません。
Group source list:	マルチキャストグループによって要求された送信元の詳細
Source Address	送信元の IP アドレス
Uptime	送信元状態が作成されてからの経過時間

表 2-48 show ip igmp groups のフィールドの説明 (続き)

フィールド	説明
v3 Exp	IGMP 動作に従って送信元のメンバーシップがタイムアウトになるまでの時間 (時間、分、および秒)。メンバーが IGMPv3 を使用していない場合 (IGMP v3lite または URD だけを使用している場合には、[stopped] と表示されます。
CSR Exp	IGMP v3lite または URD レポートに従って送信元のメンバーシップがタイムアウトになるまでの時間 (時間、分、および秒)。メンバーが IGMPv3 だけを使用している場合には、[stopped] と表示されます。
Fwd	このエントリにより、ルータがマルチキャスト トラフィックを転送しているかどうかのステータス
Flags	エントリに関する情報 Remote フラグは、IGMPv3 レポートがこの送信元によって受信されたことを示します。C フラグは、IGMP v3lite または URD レポートがこの送信元によって受信されたことを示します。U フラグは、URD レポートがこの送信元によって受信されたことを示します。

関連コマンド

コマンド	説明
ip igmp query-interval	CiscoIOS ソフトウェアが IGMP ホスト クエリー メッセージを送信する頻度を設定します。

show ip igmp interface

IGMP インターフェイスのステータスおよび設定に関する情報を表示するには、**show ip igmp interface** コマンドを使用します。

```
show ip igmp [vrf vrf-name] interface [{interface [interface-number]} | {null
interface-number} | {vlan vlan-id}]
```

シンタックスの説明

vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
<i>interface</i>	(任意) インターフェイスタイプ。有効値は、 ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 atm 、および ge-wan です。
<i>interface-number</i>	(任意) モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
null <i>interface-number</i>	ヌル インターフェイスを指定します。有効値は 0 です。
vlan vlan-id	VLAN を指定します。有効値は 1 ~ 4094 です。

コマンドのデフォルト

VLAN を指定しない場合は、VLAN 1 の情報が表示されます。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

interface-number 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、指定されたインターフェイスタイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロットシャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

オプションの引数を省略した場合、**show ip igmp interface** コマンドはすべてのインターフェイスの情報を表示します。

例

次に、VLAN 43 の IGMP 情報を表示する例を示します。

```
Router# show ip igmp interface vlan 43
Vlan43 is up, line protocol is up
Internet address is 43.0.0.1/24
IGMP is enabled on interface
Current IGMP host version is 2
Current IGMP router version is 2
IGMP query interval is 60 seconds
IGMP querier timeout is 120 seconds
IGMP max query response time is 10 seconds
```

```
Last member query count is 2
Last member query response interval is 1000 ms
Inbound IGMP access group is not set
IGMP activity: 1 joins, 0 leaves
Multicast routing is enabled on interface
Multicast TTL threshold is 0
Multicast designated router (DR) is 43.0.0.1 (this system)
IGMP querying router is 43.0.0.1 (this system)
Multicast groups joined by this system (number of users):
224.0.1.40(1)
IGMP snooping is globally enabled
IGMP snooping is enabled on this interface
IGMP snooping fast-leave is disabled and querier is disabled
IGMP snooping explicit-tracking is enabled on this interface
IGMP snooping last member query interval on this interface is 1000 ms
Router#
```

関連コマンド

コマンド	説明
clear ip igmp group	IGMP グループ キャッシュのエントリを削除します。
show ip igmp snooping mrouter	ダイナミックに学習された、および手動で設定されたマルチキャスト ルータ インターフェイスに関する情報を表示します。

show ip igmp snooping explicit-tracking

IGMPv3 ホストの明示的ホスト トラッキング ステータスに関する情報を表示するには、**show ip igmp snooping explicit-tracking** コマンドを使用します。

```
show ip igmp snooping explicit-tracking {vlan vlan-id}
```

シンタックスの説明	vlan <i>vlan-id</i>	VLAN を指定します。有効値については、「使用上のガイドライン」を参照してください。
-----------	----------------------------	---

コマンドのデフォルト VLAN を指定しない場合は、VLAN 1 の情報が表示されます。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン 明示的ホスト トラッキングは、IGMPv3 ホストだけでサポートされています。

例 次に、IGMPv3 ホストの明示的ホスト トラッキング ステータスに関する情報を表示する例を示します。

```
Router# show ip igmp snooping explicit-tracking vlan 25
```

```
Source/Group      Interface Reporter Filter_mode
-----
10.1.1.1/226.2.2.2 V125:1/2 16.27.2.3 INCLUDE
10.2.2.2/226.2.2.2 V125:1/2 16.27.2.3 INCLUDE
Router#
```

関連コマンド	コマンド	説明
	ip igmp snooping explicit-tracking	明示的なホスト トラッキングをイネーブルにします。

show ip igmp snooping mrouter

ダイナミックに学習されたマルチキャスト ルータ インターフェイス、および手動で設定されたマルチキャスト ルータ インターフェイスに関する情報を表示するには、**show ip igmp snooping mrouter** コマンドを使用します。

show ip igmp snooping mrouter [*{vlan vlan-id}*]

シンタックスの説明 *vlan vlan-id* (任意) VLAN を指定します。有効値は 1 ~ 4094 です。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン IGMP スヌーピングがイネーブルである VLAN の MAC アドレス テーブル内のエントリを表示する場合は、**show mac-address-table** コマンドも使用できます。

VLAN インターフェイスの IGMP スヌーピング情報を表示するには、**show ip igmp interface vlan *vlan-num*** コマンドを入力します。

例 次に、特定の VLAN の IGMP スヌーピングに関する情報を表示する例を示します。

```
Router# show ip igmp snooping mrouter interface 1
vlan          ports
-----+-----
1             Gi1/1,Gi2/1,Fa3/48,Router
Router#
```

関連コマンド	コマンド	説明
	ip igmp snooping mrouter	マルチキャスト ルータ ポートとしてレイヤ 2 ポートを設定します。

show ip igmp snooping rate-limit

IGMP スヌーピング レート制限に関する情報を表示するには、**show ip igmp snooping rate-limit** コマンドを使用します。

show ip igmp snooping rate-limit [statistics | vlan *vlan-id*]

シンタックスの説明

statistics (任意) IGMP スヌーピング統計情報を表示します。
vlan *vlan-id* (任意) VLAN を指定します。有効値は 1 ~ 4094 です。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、IGMP スヌーピング レート制限に関する統計情報を表示する例を示します。

```
Router# show ip igmp snooping rate-limit statistics

Max IGMP messages incoming rate : Not configured
Vlan   Incoming rate  Rate-limiting ON  Disable count  Time to Enable
-----+-----+-----+-----+-----+
222   1000           No                0
111   5999           Yes                3                185

Router#
```

次に、特定の VLAN の IGMP スヌーピング レート制限情報を表示する例を示します。

```
Router# show ip igmp snooping rate-limit vlan 19
Max IGMP messages incoming rate : 200 pps
Vlan   Incoming IGMP rate (in pps)
-----+-----
19     200

Router#
```

関連コマンド

コマンド	説明
ip igmp snooping rate	IGMP スヌーピング パケットのレート制限を設定します。

show ip igmp snooping statistics

IGMPv3 統計情報を表示するには、**show ip igmp snooping statistics** コマンドを使用します。

```
show ip igmp snooping statistics [{interface interface [interface-number]} |
    {port-channel number} | {vlan vlan-id}]
```

シンタックスの説明	interface interface	(任意) 指定されたインターフェイス タイプの IGMP 統計情報を表示します。指定できる有効値は ethernet 、 fastethernet および gigabitethernet です。
	interface-number	(任意) 指定されたモジュールおよびポートのマルチキャスト関連統計情報。有効値については、「使用上のガイドライン」を参照してください。
	port-channel number	(任意) 指定されたポート チャンネルのマルチキャスト関連統計情報を表示します。有効値は 1 ~ 282 です。
	vlan vlan-id	(任意) 指定された VLAN のマルチキャスト関連統計情報を表示します。vlan-id の有効値は 1 ~ 4094 です。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン **show ip igmp snooping statistics** コマンドは次の統計情報を表示します。

- グループのメンバー ポートのリスト
- フィルタ モード
- ポートのあとの Reporter アドレス
- その他の情報 (前回 **clear ip igmp snooping statistics** コマンドが明示的に発行されて以降に収集された Last-Join および Last-Leave など)

interface-number 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビットイーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

257 ~ 282 の **port-channel number** 値は、CSM および FWSM だけでサポートされています。

VLAN のあとに #hosts が表示されるのは、指定された VLAN で max-hosts ポリシーを定義し、log ポリシーをイネーブルにした場合だけです。

show ip igmp snooping statistics

例

次に、IGMPv3 統計情報を表示する例を示します。

```
Router# show ip igmp snooping statistics interface FastEthernet5/1

IGMP Snooping statistics
Service-policy: Policy1policy tied with this interface
#Channels: 3
#hosts : 3
Query Rx: 2901 GS Query Rx: 0 V3 Query Tot Rx: 0
Join Rx: 8686 Leave Rx: 0 V3 Report Rx: 2300
Join Rx from router ports: 8684 Leave Rx from router ports: 0
Total Rx: 11587
Channel/Group      Interface      Reporter      Uptime      Last-Join      Last-Leave
10.7.20.1,239.1.1.1 F5/1          10.5.20.1    00:12:00    1:10:00        -
10.7.30.1,239.1.1.1 F5/1          10.5.30.1    00:50:10    1:10:02        0:30:02
10.7.40.1,239.1.1.1 F5/1          10.5.40.1    00:10:10    1:10:03        -
Router#
```

表 2-49 に、この例で表示されるフィールドについて説明します。

表 2-49 show ip igmp snooping statistics のフィールドの説明

フィールド	説明
Service-policy: Policy1	このインターフェイスに関連付けられたポリシー
#Channels: 3	指定されたインターフェイスのあとのチャンネル数
#hosts	指定されたインターフェイスのあとのホスト数。このフィールドが表示されるのは、max-hosts ポリシーを使用する場合だけです。

関連コマンド

コマンド	説明
clear ip igmp snooping statistics	IGMP スヌーピングの統計情報をクリアします。

show ip igmp udlr

UniDirectional Link (UDL; 単一方向リンク) ヘルパー アドレスが設定されたインターフェイス上で、接続済みのマルチキャスト グループに関する UniDirectional Link Routing (UDLR; 単一方向リンクルーティング) 情報を表示するには、**show ip igmp udlr** コマンドを使用します。

show ip igmp udlr [*group-name* | *group-address* | *interface-type interface-number*]

シンタックスの説明

<i>group-name</i>	(任意) マルチキャスト グループ名
<i>group-address</i>	(任意) マルチキャスト グループのアドレス
<i>interface-type interface-number</i>	(任意) インターフェイス タイプおよびインターフェイス番号

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、どのグループが UDL で転送および受信されているかを表示します。

アップストリーム ルータでは、このコマンドはどのインターフェイスが UDL インターフェイスか、およびどの IP マルチキャスト グループがこのインターフェイスに転送されているかを示します。UDL Reporter は、受信ルータ上のダウンストリーム インターフェイスの IP アドレスです。複数のダウンストリーム ルータが存在している場合、このフィールドでは、どのダウンストリーム ルータが、アップストリーム ルータに地上ネットワークを介して IGMP ホスト レポートを転送したかを示します。このレポートは UDL を介して転送されるため、すべてのダウンストリーム ルータは、その他のダウンストリーム ルータがどのグループに要求したかを確認でき、それ以上の IGMP ホスト レポートは抑制されます。

ダウンストリーム ルータ上では、このコマンド (Interface フィールドで) は、どのローカル インターフェイスが IGMP ホスト レポート (特定のグループ用の接続済みホストからの) を受信したかを示します。UDL Reporter は、地上ネットワークを介して IGMP ホスト レポートをアップストリーム ルータに転送したルータの IP アドレスです。UDL Interfaces のカラムには、IP マルチキャスト パケットを受信するインターフェイスが表示されます。

例

次に、アップストリーム ルータ上の **show ip igmp udlr** コマンドの出力例を示します。

```
Router# show ip igmp udlr
```

```
IGMP UDLR Status, UDL Interfaces: Serial0
Group Address      Interface      UDL Reporter   Reporter Expires
224.2.127.254     Serial0       10.0.0.2       00:02:12
224.0.1.40        Serial0       10.0.0.2       00:02:11
225.7.7.7         Serial0       10.0.0.2       00:02:15
```

■ show ip igmp udlr

```
Router#
```

次に、ダウンストリーム ルータ上の **show ip igmp udlr** コマンドの出力例を示します。

```
Router# show ip igmp udlr
```

```
IGMP UDLR Status, UDL Interfaces: Serial0
Group Address      Interface          UDL Reporter      Reporter Expires
224.2.127.254     Serial0           10.0.0.2          00:02:49
224.0.1.40        Serial0           10.0.0.2          00:02:48
225.7.7.7         Serial0           10.0.0.2          00:02:52
Router#
```

表 2-50 に、**show ip igmp udlr** コマンドの出力で表示されるフィールドについて説明します。

表 2-50 show ip igmp udlr のフィールドの説明

フィールド	説明
Group Address	インターフェイス上のすべてのグループのヘルパー アドレス
Interface	グループの接続先のインターフェイスのタイプと番号
UDL Reporter	グループの IGMP ヘルパーである、UDL ネットワーク上のルータの IP アドレス
Reporter Expires	UDL Reporter が非アクティブになるまでの時間（時間、分、秒）。これは、次のような状況で発生します。 <ul style="list-style-type: none"> UDL Reporter が動作不能状態になった。 レポータへのリンクまたはネットワークが動作不能状態になった。 UDL Reporter に対応付けられたグループ メンバーがグループを脱退した。

show ip interface

IP 用に設定したインターフェイスのユーザビリティ ステータスを表示するには、**show ip interface** コマンドを使用します。

show ip interface [*type number*]

シンタクスの説明	<i>type</i>	(任意) インターフェイス タイプ
	<i>number</i>	(任意) インターフェイス番号

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン Cisco IOS ソフトウェアは、インターフェイスが使用可能な場合、直接接続ルートをルーティング テーブルに自動的に入力します。使用可能なインターフェイスとは、ソフトウェアがパケットを送受信できるインターフェイスです。インターフェイスを使用不能と判定した場合、ソフトウェアは直接接続ルーティング エントリをルーティング テーブルから削除します。エントリを削除すれば、ソフトウェアはダイナミック ルーティング プロトコルを使用して (存在する場合) ネットワークへのバックアップ ルートを決定できます。

インターフェイスが双方向通信を提供できる場合、回線プロトコルは **[up]** とマークされます。インターフェイス ハードウェアが使用可能な場合、そのインターフェイスは **[up]** とマークされます

オプションのインターフェイス タイプを指定すると、その特定のインターフェイスに関する情報だけが表示されます。

オプション引数を指定しなければ、すべてのインターフェイスに関する情報が表示されます。

非同期インターフェイスが Point-to-Point Protocol (PPP; ポイントツーポイント プロトコル) または Serial Line Internet Protocol (SLIP; シリアル ライン インターネット プロトコル) でカプセル化される場合、IP 高速スイッチングがイネーブルになります。 **show ip interface** コマンドを PPP または SLIP でカプセル化された非同期インターフェイスで実行すると、IP 高速スイッチングがイネーブルであることを示すメッセージが表示されます。

例 次に、特定の VLAN のユーザビリティ ステータスを表示する例を示します。

```
Router# show ip interface vlan 1
Vlan1 is up, line protocol is up
  Internet address is 10.6.58.4/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
```

show ip interface

```

Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is enabled
IP Fast switching turbo vector
IP Normal CEF switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled
Sampled Netflow is disabled
IP multicast multilayer switching is disabled
Netflow Data Export (hardware) is enabled
Router#

```

表 2-51 に、この例で表示されるフィールドについて説明します。

表 2-51 show ip interface のフィールドの説明

フィールド	説明
Ethernet0 is up	インターフェイス ハードウェアが使用可能な場合、そのインターフェイスは [up] とマークされます。インターフェイスが使用可能となるためには、インターフェイス ハードウェアおよび回線プロトコルの両方が up となる必要があります。
line protocol is up	インターフェイスが双方向通信を提供できる場合、回線プロトコルは [up] とマークされます。インターフェイスが使用可能となるためには、インターフェイス ハードウェアおよび回線プロトコルの両方が up となる必要があります。
Internet address and subnet mask	インターフェイスの IP アドレスとサブネット マスク
Broadcast address	ブロードキャスト アドレス
Address determined by...	インターフェイスの IP アドレスの決定方法を示すステータス
MTU	インターフェイスに設定されている MTU 値
Helper address	ヘルパー アドレス (設定されている場合)
Secondary address	セカンダリ アドレス (設定されている場合)
Directed broadcast forwarding	指定ブロードキャスト転送のステータス

表 2-51 show ip interface のフィールドの説明 (続き)

フィールド	説明
Multicast groups joined	このインターフェイスが属するマルチキャストグループ
Outgoing access list	インターフェイスが設定済みの発信アクセスリストを持つかどうかを示すステータス
Inbound access list	インターフェイスが設定済みの着信アクセスリストを持つかどうかを示すステータス
Proxy ARP	インターフェイスでプロキシアドレス解決プロトコル (ARP) がイネーブルかどうかを示すステータス
Security level	このインターフェイスに設定された IP Security Option (IPSO; IP セキュリティ オプション) のセキュリティレベル
Split horizon	スプリット ホライズンのステータス
ICMP redirects	このインターフェイス上のリダイレクトメッセージのステータス
ICMP unreachable	このインターフェイス上の到達不可能メッセージのステータス
ICMP mask replies	このインターフェイス上のマスク応答のステータス
IP fast switching	高速スイッチングがこのインターフェイスでイネーブルかどうかを示すステータス。高速スイッチングは通常、例のようなシリアルインターフェイスではイネーブルです。
IP SSE switching	IP Silicon Switching Engine (SSE; シリコンスイッチングエンジン) のステータス
Router Discovery	このインターフェイスの発見プロセスのステータス。これは通常、シリアルインターフェイスではディセーブルです。
IP output packet accounting	このインターフェイスの IP アカウンティングとしきい値 (エントリの最大数) のステータス
TCP/IP header compression	ヘッダー圧縮のステータス
Probe proxy name	HP プロブ プロキシ名応答が生成されるかどうかを示すステータス
WCCP Redirect outbound is enabled	インターフェイスで受信されたパケットがキャッシュエンジンにリダイレクトされるかどうかを示すステータス
WCCP Redirect exclude is disabled	インターフェイスに向けられたパケットが、キャッシュエンジンへのリダイレクトから除外されるかどうかを示すステータス
Netflow Data Export (hardware) is enabled	インターフェイス上の NDE ハードウェアフローステータス

show ip mcache

IP 高速スイッチング キャッシュの内容を表示するには、**show ip mcache** コマンドを使用します。

```
show ip mcache [vrf vrf-name] [group-address | group-name] [source-address |
source-name]
```

シンタックスの説明

vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
group-address group-name	(任意) 単一グループの高速スイッチング キャッシュ
source-address source-name	(任意) 送信元アドレスまたは名前も指定した場合は、単一のマルチキャスト キャッシュ エントリが表示されます。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

group-address | group-name には、クラス D IP アドレスまたは DNS 名を指定できます。

source-address | source-name には、ユニキャスト IP アドレスまたは DNS 名を指定できます。

例

次に、IP 高速スイッチング キャッシュの内容を表示する例を示します。このエントリには、World Radio Network グループ (224.2.143.24) に送信している特定の送信元 (wrn-source 226.62.246.73) が示されています。

```
Router> show ip mcache wrn wrn-source
```

```
IP Multicast Fast-Switching Cache
(226.62.246.73/32, 224.2.143.24), Fddi0, Last used: 00:00:00
 Ethernet0      MAC Header: 01005E028F1800000C1883D30800
 Ethernet1      MAC Header: 01005E028F1800000C1883D60800
 Ethernet2      MAC Header: 01005E028F1800000C1883D40800
 Ethernet3      MAC Header: 01005E028F1800000C1883D70800
```

表 2-52 に、この出力で表示されるフィールドについて説明します。

表 2-52 show ip mcache のフィールドの説明

フィールド	説明
226.62.246.73	送信元アドレス
224.2.143.24	宛先アドレス

表 2-52 show ip mcache のフィールドの説明 (続き)

フィールド	説明
Fddi0	パケットが受信される着信インターフェイスまたは予想されるインターフェイス
Last used:	正常に高速スイッチされたパケットについてエントリが最後にアクセスされた時間。[Semi-fast] は、発信インターフェイス リストの最初の部分が高速スイッチされ、リストの残りはプロセス レベルでスイッチされることを示します。
Ethernet0 MAC Header:	パケットを出力用書き換えするとき使用される発信インターフェイス リストと各 MAC ヘッダー。インターフェイスがトンネルの場合、MAC ヘッダーには実際のネクスト ホップ MAC ヘッダーとカッコ内に実際のインターフェイス名が表示されます。

show ip mds interface

モジュール上のすべてのインターフェイスの MDS 情報を表示するには、**show ip mds interface** コマンドを使用します。

show ip mds interface [vrf vrf-name]

シンタックスの説明

vrf vrf-name (任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、モジュール上のすべてのインターフェイスの MDS 情報を表示する例を示します。

```
Router# show ip mds interface
```

Interface	SW-Index	HW-Index	HW IDB	FS Vector	VRF
Ethernet1/0/0	2	1	0x60C2DB40	0x602FB7A4	default
Ethernet1/0/1	3	2	0x60C32280	0x603D52B8	default
Ethernet1/0/2	4	3	0x60C35E40	0x602FB7A4	default
Ethernet1/0/3	5	4	0x60C39E60	0x603D52B8	default
Ethernet1/0/4	6	5	0x60C3D780	0x602FB7A4	default
Ethernet1/0/5	7	6	0x60C41140	0x602FB7A4	default
Ethernet1/0/6	8	7	0x60C453A0	0x602FB7A4	default
Ethernet1/0/7	9	8	0x60C48DC0	0x602FB7A4	default
POS2/0/0	10	9	0x0		default
POS3/0/0	11	10	0x0		default
Virtual-Access1	13	11	0x0		default
Loopback0	14	12	0x0		default
Tunnel0	15	23	0x61C2E480	0x603D52B8	vrf1
Tunnel1	16	24	0x61C267E0	0x603D52B8	vrf2
Ethernet1/0/3.1	17	4	0x60C39E60	0x603D52B8	vrf1
Ethernet1/0/3.2	18	4	0x60C39E60	0x603D52B8	vrf2

表 2-53 に、この出力で表示されるフィールドについて説明します。

表 2-53 show ip mds interface のフィールドの説明

フィールド	説明
Interface	指定したインターフェイス
SW-Index	ソフトウェア インデックス
HW-Index	ハードウェア インデックス

表 2-53 show ip mds interface のフィールドの説明 (続き)

フィールド	説明
HW IDB	ハードウェア インターフェイス記述ブロック
VRF	VRF インスタンス

show ip mpacket

循環キャッシュ ヘッダー バッファの内容を表示するには、**show ip mpacket** コマンドを使用します。

```
show ip mpacket [vrf vrf-name] [group-address | group-name] [source-address |
source-name] [detail]
```

シンタックスの説明

vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
group-address group-name	(任意) 指定したグループ アドレスまたはグループ名に一致するキャッシュ ヘッダー
source-address source-name	(任意) 指定した送信元アドレスまたは送信元名に一致するキャッシュ ヘッダー
detail	(任意) サマリー情報に加えて、残りの IP ヘッダー フィールドを追加行に表示し、IP ヘッダーのあとの最初の 8 バイト (通常は UDP ポート番号) も表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、**ip multicast cache-headers** コマンドが有効なときだけに適用されます。

このコマンドを入力するたびに、新しいバッファが割り当てられます。サマリー表示 (**detail** キーワードを省略した場合) には、IP パケット識別子、存続可能時間 (TTL) 値、送信元および宛先 IP アドレス、およびパケット受信時のローカル タイム スタンプが表示されます。

2 つの引数と 1 つのキーワードを同じコマンドで自由に組み合わせて使用できます。

例

次に、循環キャッシュ ヘッダー バッファの内容を表示する例を示します。

```
Router # show ip mpacket smallgroup
```

```
IP Multicast Header Cache - entry count:6, next index: 7
```

```
Key: id/ttl timestamp (name) source group
```

```
D782/117 206416.908 (ABC-xy.company.com) 192.168.228.10 224.5.6.7
```

```
7302/113 206417.908 (school.edu) 147.12.2.17 224.5.6.7
```

```
6CB2/114 206417.412 (MSSRS.company.com) 154.2.19.40 224.5.6.7
```

```
D782/117 206417.868 (ABC-xy.company.com) 192.168.228.10 224.5.6.7
```

```
E2E9/123 206418.488 (Newman.com) 211.1.8.10 224.5.6.7
```

```
1CA7/127 206418.544 (teller.company.com) 192.168.6.10 224.5.6.7
```

表 2-54 に、この出力で表示されるフィールドについて説明します。

表 2-54 show ip mpacket のフィールドの説明

フィールド	説明
entry count	キャッシュされたパケット数（出力の 1 行で 1 パケット）。キャッシュの行には 0 ~ 1024 の番号が付けられます。
next index	キャッシュ内の次の要素のインデックス
id	IP パケットの識別番号
ttl	パケットの現在の TTL
timestamp	パケットのタイムスタンプ シーケンス番号
(name)	グループに送信している送信元の DNS 名。名前はカッコ内に表示されます。
source	グループに送信している送信元の IP アドレス
group	パケットが送信されるマルチキャスト グループ アドレス。この例では、グループ アドレスはグループ名 smallgroup です。

関連コマンド

コマンド	説明
ip multicast cache-headers	ルータが受信する IP マルチキャスト パケット ヘッダーを格納するために循環バッファを割り当てます。

show ip mroute

IP マルチキャスト ルーティング テーブルに関する情報を表示するには、**show ip mroute** コマンドを使用します。

```
show ip mroute [vrf vrf-name] [{interface interface-number} | {null interface-number} |
  {port-channel number} | {vlan vlan-id} | {{host-name | host-address} [source]} |
  {active [kbps | {interface-type num}]}] | {count | pruned | static | summary}]
```

シンタックスの説明

vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
interface	(任意) インターフェイス タイプ。有効値は、 ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 atm 、および ge-wan です。
interface-number	(任意) モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
null interface-number	(任意) ヌル インターフェイスを指定します。有効値は 0 です。
port-channel number	(任意) チャンネル インターフェイスを指定します。有効値は 1 ~ 282 の範囲の最大 64 個の値です。
vlan vlan-id	(任意) VLAN を指定します。有効値は 1 ~ 4094 です。
host-name host-address	(任意) DNS ホスト テーブルで定義されている名前または IP アドレスです。
source	(任意) マルチキャスト送信元の IP アドレスまたは名前
active	(任意) アクティブな送信元からマルチキャスト グループへの送信速度を表示します。
kbps	(任意) アクティブな送信元からマルチキャスト グループへの送信速度の最小値です。送信速度がこの速度以上であるアクティブな送信元が表示されます。有効値は、1 ~ 4,294,967,295 Kbps です。
count	(任意) ルートおよびパケット数に関する情報を表示します。
pruned	(任意) プルーニングされたルートを表示します。
static	(任意) スタティック マルチキャスト ルートを表示します。
summary	(任意) IP マルチキャスト ルーティング テーブル内の各エントリのサマリーを 1 行で表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

オプションの引数およびキーワードをすべて省略した場合、**show ip mroute** コマンドは IP マルチキャスト ルーティング テーブル内のすべてのエントリを表示します。

show ip mroute active kbps コマンドは、送信速度が *kbps* 以上であるすべての送信元を表示します。

interface-number 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

257 ~ 282 の **port-channel number** 値は、CSM および FWSM だけでサポートされています。

マルチキャスト ルーティング テーブルにデータを入力するには、スター グループ (*,G) エントリから送信元、グループ (S,G) エントリを作成します。スターはすべての送信元アドレス、[S] は単一の送信元アドレス、[G] は宛先マルチキャスト グループ アドレスを意味します。(S,G) エントリを作成する場合、ソフトウェアはユニキャスト ルーティング テーブル内で (RPF を経由して) 見つかった該当する宛先グループへの最適パスを使用します。

例

次に、IP マルチキャスト ルーティング テーブル内のすべてのエントリを表示する例を示します。

```
Router# show ip mroute 224.1.1.1
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel
       Y - Joined MDT-data group, y - Sending to MDT-data group, s - SSM
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 224.1.1.1), 00:00:07/00:02:59, RP 2.0.0.1, flags: BC
  Bidir-Upstream: Null, RPF nbr 0.0.0.0, RPF-MFD
  Outgoing interface list:
    Vlan202, Forward/Sparse-Dense, 00:00:07/00:02:59, H
Router#
```

次に、アクティブな送信元からマルチキャスト グループへの送信速度を表示し、送信速度がデフォルト以上であるアクティブな送信元だけを表示する例を示します。

```
Router# show ip mroute active

Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (sdr.cisco.com)
  Source: 146.137.28.69 (mbone.ipd.anl.gov)
  Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)

Group: 224.2.201.241, ACM 97
  Source: 130.129.52.160 (webcast3-el.acm97.interop.net)
  Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)

Group: 224.2.207.215, ACM 97
  Source: 130.129.52.160 (webcast3-el.acm97.interop.net)
  Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
Router#
```

show ip mroute

次に、ルートおよびパケット数に関する情報を表示する例を示します。

```
Router# show ip mroute count
IP Multicast Statistics
56 routes using 28552 bytes of memory
13 groups, 3.30 average sources per group
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Other counts:Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group:224.2.136.89, Source count:1, Group pkt count:29051
Source:132.206.72.28/32, Forwarding:29051/-278/1186/0, Other:85724/8/56665
Router#
```

次に、サマリー情報を表示する例を示します。

```
Router# show ip mroute summary
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, s - SSM Group, C - Connected, L - Local,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT, M - MSDP created entry, X - Proxy Join Timer Running
       A - Advertised via MSDP, U - URD, I - Received Source Specific Host
       Report
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

Router#
```

表 2-55 に、この例で表示されるフィールドについて説明します。

表 2-55 show ip mroute のフィールドの説明

フィールド	説明
Flags:	エントリーに関する情報
D - Dense	エントリーは dense (密) モードで動作しています。
S - Sparse	エントリーは sparse (疎) モードで動作しています。
s - SSM Group	エントリーは SSM グループのメンバーです。
C - Connected	マルチキャスト グループのメンバーは、直接接続されたインターフェイス上に存在します。
L - Local	ルータが、マルチキャスト グループのメンバーです。
P - Pruned	ルートがプルーンングされています。ダウンストリーム メンバーが送信元に参加する場合は、この情報が保持されます。
R - Rp-bit set	(S,G) エントリーがルート プロセッサ方向を指しているかどうかを示すステータス。このフィールドは、特定の送信元に関する共有 ツリーに沿ったプルーンング ステートを示します。
F - Register flag	ソフトウェアがマルチキャスト送信元に登録されているかどうかを示すステータス
T - SPT-bit set	パケットが最短パス ツリーで受信されているかどうかを示すステータス

表 2-55 show ip mroute のフィールドの説明 (続き)

フィールド	説明
J - Join SPT	<p>(* ,G) エントリの場合、共有ツリーの下方向に流れるトラフィックの速度が、グループの SPT しきい値の設定値を超えていることを示します (デフォルトの SPT しきい値の設定値は 0 Kbps です)。J - Join SPT フラグが設定されている場合に、共有ツリーの下流で次の (S,G) パケットが受信されると、送信元の方に (S,G) join メッセージがトリガーされます。これにより、ルータは送信元ツリーに加入します。</p> <p>(S,G) エントリの場合、グループの SPT しきい値を超過したためにエントリが作成されたことを示します。(S,G) エントリに J - Join SPT フラグが設定されている場合、ルータは送信元ツリー上のトラフィック速度をモニタします。送信元ツリーのトラフィック速度がグループの SPT しきい値を下回っている状況が 1 分以上継続した場合、ルータはこの送信元の共有ツリーに再び切り替えようとしています。</p> <p>ルータは共有ツリー上のトラフィック速度を測定し、この速度とグループの SPT しきい値を 1 秒ごとに比較します。トラフィック速度が SPT しきい値を超えた場合は、トラフィック速度の次の測定が行われるまで、(* ,G) エントリに J-Join SPT フラグが設定されます。共有ツリーに次のパケットが着信し、新しい測定インターバルが開始すると、フラグが解除されます。</p> <p>グループにデフォルトの SPT しきい値 (0 Kbps) が使用されている場合、(* ,G) エントリには常に J-Join SPT フラグが設定され、解除されません。デフォルトの SPT しきい値が使用されている場合に、新しい送信元からトラフィックを受信すると、ルータは最短パス ツリーにただちに切り替えます。</p>
Bidir-Upstream: Null, RPF nbr 0.0.0.0, RPF-MFD	PIM ルート プロセッサへの連絡に使用するインターフェイス。ルータが PIM ルート プロセッサか、または PIM ルート プロセッサへのルートが存在しない場合、ヌルを設定します。
Outgoing interface flags:	発信エントリに関する情報
H - Hardware switched	エントリはハードウェアによりスイッチングされます。
Timers:	Uptime/Expires
Interface state:	Interface、Next-Hop または VCD、State/Mode
(* , 224.0.255.1) (198.92.37.100/32, 224.0.255.1)	<p>IP マルチキャスト ルーティング テーブルのエントリです。エントリは、送信元ルータの IP アドレスと、それに続くマルチキャストグループの IP アドレスで構成されます。送信元ルータの位置に置かれたアスタリスク (*) は、すべての送信元を意味します。</p> <p>最初の形式のエントリは、(* ,G) (「スター カンマ G」と読む) エントリといます。2 番目の形式のエントリは、(S,G) (「S カンマ G」と読む) エントリといます。(* ,G) エントリは、(S,G) エントリを作成するために使用されます。</p>
uptime	IP マルチキャスト ルーティング テーブルにエントリが格納されていた期間 (時間、分、秒)
expires	発信インターフェイスの IP マルチキャスト ルーティング テーブルからエントリが削除されるまでの期間 (時間、分、秒)

表 2-55 show ip mroute のフィールドの説明 (続き)

フィールド	説明
RP	ルート プロセッサのアドレス。sparse (疎) モードで動作するルータおよびアクセス サーバの場合、このアドレスは常に 0.0.0.0 です。
flags:	エントリーに関する情報
Incoming interface:	送信元からのマルチキャスト パケットが着信する予定のインターフェイス。パケットがこのインターフェイスに着信しなかった場合、廃棄されます。
RPF neighbor	送信元に対するアップストリーム ルータの IP アドレス。Tunneling は、このルータがレジスタ パケットにカプセル化されたデータをルート プロセッサに送信していることを示します。カッコ内の 16 進数は、登録されているルート プロセッサを示します。1 つのグループに複数のルート プロセッサが使用されている場合、各ビットはそれぞれ異なるルート プロセッサを示します。
Dvmrp または Mroute	RPF 情報が DVMRP ルーティング テーブルから取得されたか、またはスタティック mroute コンフィギュレーションから取得されたかを示すステータス
Outgoing interface list:	パケットが転送される際に通過するインターフェイス。インターフェイス上で ip pim nbma-mode コマンドがイネーブルの場合、PIM ネイバの IP アドレスも表示されます。
Ethernet0	発信インターフェイス名および番号
Next hop or VCD	Next hop は、ダウンストリーム ネイバの IP アドレスを指定します。VCD は、仮想回線の記述子番号を指定します。VCD0 は、グループがスタティック マップ仮想回線を使用していることを示します。
Forward/Dense	アクセス リストまたは TTL しきい値による制限がない場合に、インターフェイス上でパケットが転送されるかどうかを示すステータス。スラッシュ (/) のあとに、インターフェイスの動作モード (密または疎) を示します。
Forward/Sparse	sparse (疎) モード インターフェイスが転送モードです。
time/time (uptime/expiration time)	エントリーが IP マルチキャスト ルーティング テーブルに格納されていた期間 (時間、分、秒) をインターフェイスごとに示します。スラッシュ (/) のあとに、エントリーが IP マルチキャスト ルーティング テーブルから削除されるまでの期間 (時間、分、秒) を指定します。

関連コマンド

コマンド	説明
IP multicast-routing	IP マルチキャスト ルーティングをイネーブルにします。
ip pim	インターフェイス上の PIM をイネーブルにします。

show ip mroute bidirectional

IP マルチキャストルーティングテーブルから Bidir 情報を表示するには、**show ip mroute bidirectional** コマンドを使用します。

```
show ip mroute bidirectional [ {interface interface-number} | {null interface-number} |
    {port-channel number} | {vlan vlan-id} | { {host-name | host-address} [source]} |
    {active [kbps | {interface-type num}]} | {count | pruned | static | summary} ]
```

シンタックスの説明

<i>interface</i>	(任意) インターフェイス タイプ。有効値は、 ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 atm 、および ge-wan です。
<i>interface-number</i>	モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
null <i>interface-number</i>	ヌル インターフェイスを指定します。有効値は 0 です。
port-channel <i>number</i>	チャンネル インターフェイスを指定します。有効値は 1 ~ 282 の範囲の最大 64 個の値です。
vlan <i>vlan-id</i>	VLAN を指定します。有効値は 1 ~ 4094 です。
<i>host-name</i> <i>host-address</i>	(任意) DNS ホスト テーブルで定義されている名前または IP アドレスです。
<i>source</i>	(任意) マルチキャスト送信元の IP アドレスまたは名前
active	(任意) アクティブな送信元からマルチキャスト グループへの送信速度を表示します。
<i>kbps</i>	(任意) アクティブな送信元からマルチキャスト グループへの送信速度の最小値です。送信速度がこの速度以上であるアクティブな送信元が表示されます。有効値は、1 ~ 4,294,967,295 Kbps です。
count	(任意) ルートおよびパケット数を表示します。
pruned	(任意) プルーニングされたルートを表示します。
static	(任意) スタティック マルチキャスト ルートを表示します。
summary	(任意) IP マルチキャスト ルーティング テーブル内の各エントリのサマリーを 1 行で表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

オプションの引数およびキーワードをすべて省略した場合、**mroute bidirectional** コマンドは IP マルチキャスト ルーティング テーブル内のエントリをすべて表示します。

例

次に、双方向 PIM に関する IP マルチキャスト ルーティング テーブル内の情報を表示する例を示します。

```
Router# show ip mroute bidirectional
(*, 225.1.3.0), 00:00:02/00:02:57, RP 3.3.3.3, flags:BC
Bidir-Upstream:GigabitEthernet2/1, RPF nbr 10.53.1.7, RPF-MFD
Outgoing interface list:
GigabitEthernet2/1, Bidir-Upstream/Sparse-Dense, 00:00:02/00:00:00,H
Vlan30, Forward/Sparse-Dense, 00:00:02/00:02:57, H
(*, 225.1.2.0), 00:00:04/00:02:55, RP 3.3.3.3, flags:BC
Bidir-Upstream:GigabitEthernet2/1, RPF nbr 10.53.1.7, RPF-MFD
Outgoing interface list:
GigabitEthernet2/1, Bidir-Upstream/Sparse-Dense, 00:00:04/00:00:00,H
Vlan30, Forward/Sparse-Dense, 00:00:04/00:02:55, H
(*, 225.1.4.1), 00:00:00/00:02:59, RP 3.3.3.3, flags:BC
Bidir-Upstream:GigabitEthernet2/1, RPF nbr 10.53.1.7, RPF-MFD
Outgoing interface list:
GigabitEthernet2/1, Bidir-Upstream/Sparse-Dense, 00:00:00/00:00:00,H
Vlan30, Forward/Sparse-Dense, 00:00:00/00:02:59, H
Router#
```

show ip msdp count

MSDP source-active メッセージを発信した送信元およびグループの数と、source-active キャッシュ内の MSDP ピアからの source-active メッセージ数を表示するには、**show ip msdp count** コマンドを使用します。

```
show ip msdp [vrf vrf-name] count [as-number]
```

シンタックスの説明

vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
as-number	(任意) 指定した自律システム番号からの source-active メッセージを発信した送信元とグループの数

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

show ip msdp コマンドの出力を取得するには、このコマンドの **ip msdp cache-sa-state** コマンドを入力する必要があります。

例

次に、MSDP source-active メッセージを発信した送信元およびグループの数と、source-active キャッシュ内の MSDP ピアからの source-active メッセージ数を表示する例を示します。

```
Router# show ip msdp count

SA State per Peer Counters, <Peer>: <# SA learned>
224.135.250.116: 24
172.16.240.253: 3964
172.16.253.19: 10
172.16.170.110: 11

SA State per ASN Counters, <asn>: <# sources>/<# groups>
Total entries: 4009
?: 192/98, 9: 1/1, 14: 107/57, 17: 7/5
18: 4/3, 25: 23/17, 26: 39/27, 27: 2/2
32: 19/7, 38: 2/1, 52: 4/4, 57: 1/1
68: 4/4, 73: 12/8, 81: 19/1, 87: 9/6
.
.
.
```

■ show ip msdp count

表 2-56 に、この出力で表示されるフィールドについて説明します。

表 2-56 show ip msdp count のフィールドの説明

フィールド	説明
224.135.250.116: 24	IP アドレス 224.135.250.116 の MSDP ピア。source-active キャッシュ内の MSDP ピアから 24 の source-active メッセージ。
Total entries	source-active キャッシュ内の source-active エントリの総数。
9: 1/1	自律システム 9。1 送信元 / 1 ポート。

関連コマンド

コマンド	説明
ip msdp cache-sa-state	ルータに source-active ステートを作成します。

show ip msdp peer

MSDP ピアに関する詳細情報を表示するには、**show ip msdp peer** コマンドを使用します。

show ip msdp [vrf vrf-name] peer [peer-address | peer-name]

シンタックスの説明	説明
vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
peer-address peer-name	(任意) 情報を表示する MSDP ピアの DNS 名または IP アドレス

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、MSDP ピアの詳細情報を表示する例を示します。

```
Router# show ip msdp peer 224.135.250.116

MSDP Peer 224.135.250.116 (rtp5-rp1.cisco.com), AS 109 (configured AS)
Description:
Connection status:
  State: Up, Resets: 9, Connection source: Loopback2 (228.69.199.17)
  Uptime(Downtime): 1d10h, Messages sent/received: 436765/429062
  Output messages discarded: 0
  Connection and counters cleared 1w2d ago
SA Filtering:
  Input (S,G) filter: none, route-map: none
  Input RP filter: none, route-map: none
  Output (S,G) filter: none, route-map: none
  Output RP filter: none, route-map: none
SA-Requests:
  Input filter: none
  Sending SA-Requests to peer: disabled
Peer ttl threshold: 0
SAs learned from this peer: 32, SAs limit: 500
Input queue size: 0, Output queue size: 0
```

表 2-57 に、この出力で表示されるフィールドについて説明します。

表 2-57 show ip msdp peer のフィールドの説明

フィールド	説明
MSDP Peer	MSDP ピアの IP アドレス
AS	MSDP ピアが属する自律システム

表 2-57 show ip msdp peer のフィールドの説明 (続き)

フィールド	説明
State:	MSDP ピアの状態
Connection source:	TCP ローカル接続アドレスの IP アドレスを取得するために使用されたインターフェイス
Uptime(Downtime):	MSDP ピアがアップまたはダウンしている日数と時間数。時間が 24 時間未満の場合は、時:分:秒で表示されます。
Messages sent/received:	MSDP ピアに送信された source-active メッセージの数/MSDP ピアから受信した source-active メッセージの数
SA Filtering:	source-active 入力および出力のアクセス リスト フィルタリングに関する情報
SA-Requests:	source-active 要求のアクセス リスト フィルタリングに関する情報 (存在する場合)
SAs learned from this peer:	source-active キャッシュ内の MSDP ピアからの source-active メッセージの数
SAs limit:	この MSDP ピアの source-active メッセージ制限

関連コマンド

コマンド	説明
ip msdp peer	MSDP ピアを設定します。

show ip msdp sa-cache

MSDP ピアから学習した (S,G) 状態を表示するには、**show ip msdp sa-cache** コマンドを使用します。

show ip msdp [vrf vrf-name] sa-cache [group-address | source-address | group-name | source-name] [group-address | source-address | group-name | source-name] [as-number]

シンタックスの説明	パラメータ	説明
vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。	
group-address source-address group-name source-name	(任意) (S,G) 情報を表示するグループまたは送信元のグループアドレス、送信元アドレス、グループ名、または送信元名	
as-number	(任意) 指定した自律システム番号によって発信された状態だけを表示します。	

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン **ip msdp cache-sa-state** コマンドを入力した場合だけ、状態がキャッシュされます。2つのアドレスまたは名前を指定した場合、それらのアドレスに該当する (S,G) エントリが表示されます。1つのグループアドレスだけを指定した場合は、そのグループのすべての送信元が表示されます。オプションを指定しなかった場合は、**source-active** キャッシュ全体が表示されます。

例 次に、MSDP ピアから学習した (S,G) 状態を表示する例を示します。

```
Router# show ip msdp sa-cache

MSDP Source-Active Cache - 2398 entries
(172.16.41.33, 238.105.148.0), RP 172.16.3.111, MBGP/AS 704, 2d10h/00:05:33
(172.16.112.8, 224.2.0.1), RP 192.168.200.65, MBGP/AS 10888, 00:03:21/00:02:38
(172.16.10.13, 227.37.32.1), RP 192.168.3.92, MBGP/AS 704, 05:22:20/00:03:32
(172.16.66.18, 233.0.0.1), RP 192.168.3.111, MBGP/AS 704, 2d10h/00:05:35
(172.16.66.148, 233.0.0.1), RP 192.168.3.111, MBGP/AS 704, 2d10h/00:05:35
(172.16.10.13, 227.37.32.2), RP 192.168.3.92, MBGP/AS 704, 00:44:30/00:01:31
(172.16.70.203, 224.2.236.2), RP 192.168.253.7, MBGP/AS 3582, 02:34:16/00:05:49
(172.18.42.104, 236.195.56.2), RP 192.168.3.92, MBGP/AS 704, 04:21:13/00:05:22
(172.16.10.13, 227.37.32.3), RP 192.168.3.92, MBGP/AS 704, 00:44:30/00:02:31
(172.18.15.43, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 6d09h/00:05:35
(172.18.15.111, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 16:18:08/00:05:35
(172.18.21.45, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 16:18:08/00:05:35
(172.18.15.75, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 08:40:52/00:05:35
```

■ show ip msdp sa-cache

```
(172.18.15.100, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 08:40:52/00:05:35
(172.16.10.13, 227.37.32.6), RP 192.168.3.92, MBGP/AS 704, 00:45:30/00:05:31
(172.18.41.33, 224.247.228.10), RP 192.168.3.111, MBGP/AS 704, 2d10h/00:05:35
(172.18.222.210, 224.2.224.13), RP 192.168.3.92, MBGP/AS 704, 01:51:53/00:05:22
(172.18.41.33, 229.231.124.13), RP 192.168.3.111, MBGP/AS 704, 2d10h/00:05:33
(172.18.32.138, 224.2.200.23), RP 192.168.253.7, MBGP/AS 3582, 21:33:40/00:05:49
(172.18.75.244, 224.2.200.23), RP 192.168.253.7, MBGP/AS 3582, 21:33:40/00:05:49
```

表 2-58 に、この出力で表示されるフィールドについて説明します。

表 2-58 show ip msdp sa-cache のフィールドの説明

フィールド	説明
(172.16.41.33, 238.105.148.0)	2 番目のアドレス (グループ) に送信している最初のアドレス (送信元)
RP 172.16.3.111	source-active メッセージが開始された発信元ドメインのランデブー ポイント アドレス
MBGP/AS 704	マルチプロトコル BGP に従った自律システム 704 内のランデブー ポイント
2d10h/00:05:33	2 日と 10 時間キャッシュされているルート。5 分 33 秒間、source-active メッセージを受信しなかった場合、ルートは source-active キャッシュから削除されます。

■ 関連コマンド

コマンド	説明
<code>clear ip msdp sa-cache</code>	MSDP 送信元のアクティブ キャッシュ エントリをクリアします。
<code>ip msdp cache-sa-state</code>	ルータに source-active ステータスを作成します。

show ip msdp summary

MSDP ピア ステータスを表示するには、**show ip msdp summary** コマンドを使用します。

show ip msdp [vrf vrf-name] summary

シンタックスの説明	vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
------------------	---------------------	--

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、MSDP ピア ステータスを表示する例を示します。

```
Router# show ip msdp summary

MSDP Peer Status Summary
Peer Address      AS      State   Uptime/  Reset SA   Peer Name
                  AS      State   Downtime Count Count
224.135.250.116  109    Up      1d10h    9      111    rtp5-rp1
*172.20.240.253  1239   Up      14:24:00 5      4010   sl-rp-stk
172.16.253.19    109    Up      12:36:17 5      10     shinjuku-rp1
172.16.170.110   109    Up      1d11h    9      12     ams-rp1
```

表 2-59 に、この出力で表示されるフィールドについて説明します。

表 2-59 show ip msdp summary のフィールドの説明

フィールド	説明
Peer Address	MSDP ピアの IP アドレス
AS	MSDP ピアが属する自律システム
State	MSDP ピアの状態
Uptime/Downtime	直前のカラムに表示されている State ごと MSDP ピアがアップまたはダウンしている日数と時間数。時間が 24 時間未満の場合は、時:分:秒で表示されます。
SA Count	source-active キャッシュ内のこの MSDP ピアからの source-active メッセージの数
Peer Name	MSDP ピアの名前

show ip nhrp

NHRP キャッシュに関する情報を表示するには、**show ip nhrp** コマンドを使用します。

```
show ip nhrp [summary | dynamic | static | incomplete] [{interface-type
interface-number} | ip-address] [detail | brief]
```

シンタックスの説明

summary	(任意) NHRP キャッシュ クリア情報のサマリーを表示します。
dynamic	(任意) ダイナミック (学習した) IP-to-NBMA キャッシュ エントリだけを表示します。
static	(任意) スタティック IP-to-NBMA アドレス キャッシュ エントリ (ip nhrp map コマンドを使用して設定) だけを表示します。
incomplete	(任意) 不完全なキャッシュに関する情報を表示します。
interface-type interface-number	(任意) 指定したインターフェイス タイプの NHRP キャッシュ情報だけを表示します。タイプ、番号の範囲、および説明については、表 2-60 を参照してください。
ip-address	(任意) 指定した IP アドレスの NHRP キャッシュ情報だけを表示します。
detail	(任意) NHRP キャッシュに関する詳細情報を表示します。
brief	(任意) NHRP キャッシュに関する基本情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

表 2-60 に、オプション引数の *type* および *number* について有効なタイプ、番号の範囲、および説明を示します。



(注)

有効なタイプは、プラットフォームとプラットフォーム上のインターフェイスによって異なります。

表 2-60 有効なタイプ、番号の範囲、およびインターフェイスの説明

有効なタイプ	番号の範囲	インターフェイスの説明
async	1	非同期
ctunnel	0 ~ 2,147,483,647	C トンネル
dialer	0 ~ 20049	ダイアラー
fastethernet	0 ~ 6	ファストイーサネット IEEE 802.3

表 2-60 有効なタイプ、番号の範囲、およびインターフェイスの説明 (続き)

有効なタイプ	番号の範囲	インターフェイスの説明
GigabitEthernet	0 ~ 6	ギガビット イーサネット IEEE 802.3
loopback	0 ~ 2,147,483,647	ループバック
mfr	0 ~ 2,147,483,647	マルチリンク フレーム リレー バンドル
multilink	0 ~ 2,147,483,647	マルチリンク グループ
null	0	ヌル
port-channel	1 ~ 282	インターフェイスの EtherChannel
pos-channel	1 ~ 4094	インターフェイスの PoS チャ ネル
tunnel	0 ~ 2,147,483,647	トンネル インターフェイス
vif	1	PGM マルチキャスト ホスト
tunnel	0 ~ 2,147,483,647	トンネル
virtual-template	1 ~ 1000	仮想テンプレート
virtual-tokenring	0 ~ 2,147,483,647	仮想トークンリング
xtagatm	0 ~ 2,147,483,647	拡張タグ ATM

例

次に、NHRP キャッシュに関する情報を表示する例を示します。

```
Router# show ip nhrp

10.0.0.2 255.255.255.255, ATM0/0 created 0:00:43 expire 1:59:16
  Type: dynamic Flags: authoritative
  NBMA address: 11.1111.1111.1111.1111.1111.1111.1111.1111.1111.11
10.0.0.1 255.255.255.255, Tunnel0 created 0:10:03 expire 1:49:56
  Type: static Flags: authoritative
  NBMA address: 11.1.1.2
```

表 2-61 に、この出力で表示されるフィールドについて説明します。

表 2-61 show ip nhrp のフィールドの説明

フィールド	説明
10.0.0.2 255.255.255.255	IP-to-NBMA アドレス キャッシュ内の IP アドレスとネット ワーク マスク。NHRP を通じた NBMA 情報の集約はサポート されていないので、マスクは現時点では常に 255.255.255.255 です。
ATM0/0 created 0:00:43	インターフェイスのタイプおよび番号 (この例では ATM ス ロット番号とポート番号) と作成時刻 (時:分:秒)
expire 1:59:16	正および負の正当な NBMA アドレスの期限が切れるまでの時 間 (時間:分:秒)。この値は、 ip nhrp holdtime コマンドに基 づきます。

表 2-61 show ip nhrp のフィールドの説明 (続き)

フィールド	説明
Type	<ul style="list-style-type: none"> dynamic : NBMA アドレスは NHRP 要求パケットから取得されました。 static : NBMA アドレスはスタティックに設定されました。
Flags	<ul style="list-style-type: none"> authoritative : 特定の宛先の NBMA-to-IP アドレス マッピングを維持しているネクスト ホップ サーバまたはルータから NHRP 情報が取得されたことを示します。 implicit : 情報はローカル ルータから生成された NHRP 要求から学習されたのではなく、ローカル ルータが転送している NHRP パケットまたはローカル ルータが受信している NHRP 要求から学習されたことを示します。 negative : ネガティブ キャッシングの場合。要求された NBMA マッピングを取得できなかったことを示します。
NBMA address	非ブロードキャスト マルチアクセス アドレス。アドレス形式は、使用されているネットワークのタイプ (ATM、イーサネット、SMDS、マルチポイント トンネルなど) に応じた形式です。

次に、特定の IP アドレスについてだけ、ダイナミック (学習された) IP-to-NBMA キャッシュ エントリに関する基本情報を表示する例を示します。

```
Router# show ip nhrp dynamic 255.255.255.255 brief
      Target      Via          NBMA          Mode      Intfc      Claimed
```

関連コマンド

コマンド	説明
ip nhrp holdtime	正当な NHRP 応答で有効な NHRP NBMA アドレスとしてアドバタイズされる秒数を変更します。
ip nhrp map	NBMA ネットワークに接続された IP 宛先の IP-to-NBMA アドレス マッピングをスタティックに設定します。

show ip pim bsr-router

BSR 情報を表示するには、**show ip pim bsr-router** コマンドを使用します。

show ip pim vrf vrf-name bsr-router

シンタックスの説明	vrf vrf-name	マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
------------------	---------------------	---

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン 出力には、選定された BSR 情報とローカルで設定された候補ランデブー ポイント アドバタイズに関する情報が含まれます。

例 次に、BSR 情報を表示する例を示します。

```
Router# show ip pim bsr-router

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.16.143.28
  Uptime: 04:37:59, BSR Priority: 4, Hash mask length: 30
  Next bootstrap message in 00:00:03 seconds

Next Cand_RP_advertisement in 00:00:03 seconds.
  RP: 172.16.143.28(Ethernet0), Group acl: 6
```

表 2-62 に、この出力で表示されるフィールドについて説明します。

表 2-62 show ip pim bsr のフィールドの説明

フィールド	説明
BSR address	ブートストラップ ルータの IP アドレス
Uptime	このルータがアップしている時間の長さ (時間、分、秒)
BSR Priority	ip pim bsr-candidate コマンドで設定されたプライオリティ
Hash mask length	ハッシュ関数が呼び出される前にグループアドレスと AND 演算されるマスクの長さ (最大 32 ビット)。この値は、 ip pim bsr-candidate コマンドで設定します。

表 2-62 show ip pim bsr のフィールドの説明 (続き)

フィールド	説明
Next bootstrap message in	この BSR からの次のブートストラップメッセージの予定時間 (時間、分、秒)
Next Cand_RP_advertisement in	次の候補ランデブー ポイント アドバタイズが送信される時間 (時間、分、秒)
RP	ランデブー ポイントの IP アドレスのリスト
Group acl	ランデブー ポイント アドレスと関連してアドバタイズされるグループ プレフィックスを定義する標準 IP アクセスリスト番号。この値は、 ip pim bsr-candidate コマンドで設定します。

関連コマンド

コマンド	説明
ip pim bsr-candidate	ルータが BSR として候補であることをアナウンスするよう設定します。
ip pim rp-candidate	ルータが自身を PIM バージョン 2 ランデブー ポイント候補として BSR にアドバタイズするよう設定します。
show ip pim rp-hash	指定したグループで選択されているランデブー ポイントを表示します。

show ip pim interface df

指定フォワーダ インターフェイスに関する情報を表示するには、**show ip pim interface df** コマンドを使用します。

```
show ip pim vrf vrf-name interface df [rp-addr]
```

シンタックスの説明

vrf <i>vrf-name</i>	マルチキャスト VRF インスタンスに割り当てられた名前を指定します。
<i>rp-addr</i>	(任意) 指定フォワーダのホスト名または IP アドレス

コマンドのデフォルト

rp-addr を指定しなければ、すべての指定フォワーダが表示されます。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、DF インターフェイスに関する情報を表示する例を示します。

```
Router# show ip pim interface df 10.18.1.31
Interface          RP           DF Winner      Metric    Uptime
Vlan70             10.18.1.31   10.70.1.55     0         14:16:24
FastEthernet5/5    10.18.1.31   10.16.1.30     0         14:16:24
FastEthernet5/6    10.18.1.31   10.18.1.31     0         14:16:24
Router#
```

show ip pim mdt bgp

MDT デフォルト グループのルート識別子の詳細な BGP アドバタイズを表示するには、**show ip pim mdt bgp** コマンドを使用します。

show ip pim vrf vrf-name mdt bgp

シンタックスの説明

vrf vrf-name マルチキャスト VRF インスタンスに割り当てられた名前を指定します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、MDT デフォルト グループのルート識別子の詳細な BGP アドバタイズを表示する例を示します。

```
Router# show ip pim mdt bgp

MDT-default group 232.2.1.4
  rid:1.1.1.1 next_hop:1.1.1.1
```

表 2-63 に、この出力で表示されるフィールドについて説明します。

表 2-63 show ip pim mdt bgp のフィールドの説明

フィールド	説明
MDT-default group	このルータにアドバタイズされた MDT デフォルト グループ
rid:10.1.1.1	アドバタイズしたルータの BGP ルータ ID
next_hop:10.1.1.1	アドバタイズに含まれていた BGP ネクスト ホップ アドレス

show ip pim mdt history

再利用されたデータ MDT に関する情報を表示するには、**show ip pim mdt history** コマンドを使用します。

show ip pim vrf *vrf-name* mdt history interval *minutes*

シンタックスの説明	パラメータ	説明
	vrf <i>vrf-name</i>	マルチキャスト VRF インスタンスに割り当てられた名前を指定します。
	interval <i>minutes</i>	インターバルを設定できる時間の長さ (分) を指定します。有効値は、1 ~ 71,582 分です (最大値は、71,582 分または 7 週間です)。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン **show ip pim mdt history** コマンドは、過去に設定されたインターバル中に再利用されたデータ MDT を表示します。

例 次に、再利用されたデータ MDT に関する情報を表示する例を示します。

```
Router# show ip pim vrf blue mdt history interval 20

MDT-data send history for VRF - blue for the past 20 minutes

MDT-data group          Number of reuse
-----
10.9.9.8                 3
10.9.9.9                 2
```

表 2-64 に、この出力で表示されるフィールドについて説明します。

表 2-64 show ip pim mdt history のフィールドの説明

フィールド	説明
MDT-data group	情報が表示されている MDT データ グループ
Number of reuse	このグループで再利用されたデータ MDT の数

show ip pim mdt receive

指定したルータが受信したデータ MDT アドバタイズを表示するには、**show ip pim mdt receive** コマンドを使用します。

show ip pim vrf vrf-name mdt receive [detail]

シンタックスの説明

vrf vrf-name	マルチキャスト VRF インスタンスに割り当てられた名前を指定します。
detail	(任意) 受信されたデータ MDT アドバタイズの詳細な説明を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ルータがデフォルトの MDT からデータ MDT に切り替えるときには、VRF 送信元、グループ ペア、およびトラフィックが送信されるグローバル マルチキャスト アドレスをアドバタイズします。リモートルータがこのデータを受信する場合は、このグローバル アドレス マルチキャスト グループに加入します。

例

次に、指定したルータが受信したデータ MDT アドバタイズを表示する例を示します。

```
Router# show ip pim vrf vpn8 mdt receive detail
```

```
Joined MDT-data groups for VRF:vpn8
group:232.2.8.0 source:10.0.0.100 ref_count:13
(10.101.8.10, 225.1.8.1), 1d13h/00:03:28/00:02:26, OIF count:1, flags:TY
(10.102.8.10, 225.1.8.1), 1d13h/00:03:28/00:02:27, OIF count:1, flags:TY
```

表 2-65 に、この出力で表示されるフィールドについて説明します。

表 2-65 show ip pim mdt receive のフィールドの説明

フィールド	説明
group:172.16.8.0	データ MDT を作成したグループ
source:10.0.0.100	データ MDT を作成した VRF 送信元
ref_count:13	このデータ MDT を再利用している送信元とグループのペアの数

表 2-65 show ip pim mdt receive のフィールドの説明 (続き)

フィールド	説明
OIF count:1	このマルチキャスト データを転送しているインターフェイスの数
flags:	<p>エントリに関する情報</p> <p>A - 候補 MSDP アドバタイズ</p> <p>B - Bidir グループ</p> <p>D - dense (密)</p> <p>C - 接続済み</p> <p>F - レジスタ フラグ</p> <p>I - 受信された送信元固有のホスト レポート</p> <p>J - 加入 SPT</p> <p>L - ローカル</p> <p>M - MSDP 作成エントリ</p> <p>P - プルーニング済み</p> <p>R - RP ビットセット</p> <p>S - sparse (疎)</p> <p>s - SSM グループ</p> <p>T - SPT ビットセット</p> <p>X - プロキシ加入タイマー実行中</p> <p>U - URD</p> <p>Y - 加入した MDT データ グループ</p> <p>y - MDT データ グループに送信中</p> <p>Z - マルチキャスト トンネル</p>

show ip pim mdt send

指定したルータが作成したデータ MDT アドバタイズを表示するには、**show ip pim mdt send** コマンドを使用します。

show ip pim vrf vrf-name mdt send

シンタックスの説明

vrf vrf-name マルチキャスト VRF インスタンスに割り当てられた名前を指定します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、指定したルータが作成したデータ MDT アドバタイズを表示するときに使用します。

例

次に、指定したルータが作成したデータ MDT アドバタイズを表示する例を示します。

```
Router# show ip pim mdt send
```

```
MDT-data send list for VRF:vpn8
(source, group)                MDT-data group    ref_count
(10.100.8.10, 225.1.8.1)      232.2.8.0         1
(10.100.8.10, 225.1.8.2)      232.2.8.1         1
(10.100.8.10, 225.1.8.3)      232.2.8.2         1
(10.100.8.10, 225.1.8.4)      232.2.8.3         1
(10.100.8.10, 225.1.8.5)      232.2.8.4         1
(10.100.8.10, 225.1.8.6)      232.2.8.5         1
(10.100.8.10, 225.1.8.7)      232.2.8.6         1
(10.100.8.10, 225.1.8.8)      232.2.8.7         1
(10.100.8.10, 225.1.8.9)      232.2.8.8         1
(10.100.8.10, 225.1.8.10)     232.2.8.9         1
```

表 2-66 に、この出力で表示されるフィールドについて説明します。

表 2-66 show ip pim mdt send のフィールドの説明

フィールド	説明
source, group	このルータがデータ MDT に切り替えた送信元とグループのアドレス
MDT-data group	これらのデータ MDT が送信されるマルチキャスト アドレス
ref_count	このデータ MDT を再利用している送信元とグループのペアの数

show ip pim neighbor

発見された PIM ネイバのリストを表示するには、**show ip pim neighbor** コマンドを使用します。

show ip pim vrf vrf-name neighbor [*interface-type interface-number*]

シンタックスの説明

vrf vrf-name	マルチキャスト VRF インスタンスに割り当てられた名前を指定します。
interface-type	(任意) インターフェイス タイプ
interface-number	インターフェイス番号

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、PIM 用に設定されている LAN 上のルータを調べるときに使用します。

例

次に、発見された PIM ネイバのリストを表示する例を示します。

```
Router# show ip pim neighbor
```

```
PIM Neighbor Table
Neighbor Address  Interface      Uptime      Expires     Mode
192.168.37.2      Ethernet0     17:38:16   0:01:25    Dense
192.168.37.33     Ethernet0     17:33:20   0:01:05    Dense (DR)
192.168.36.131    Ethernet1     17:33:20   0:01:08    Dense (DR)
192.168.36.130    Ethernet1     18:56:06   0:01:04    Dense
10.1.22.9         Tunnel0       19:14:59   0:01:09    Dense
```

表 2-67 に、この出力で表示されるフィールドについて説明します。

表 2-67 show ip pim neighbor のフィールドの説明

フィールド	説明
Neighbor Address	PIM ネイバの IP アドレス
Interface	ネイバに到達可能なインターフェイスのタイプと番号
Uptime	PIM ネイバ テーブルにエントリが格納されていた期間 (時間、分、秒)
Expires	IP マルチキャスト ルーティング テーブルからエントリが削除されるまでの期間 (時間、分、秒)
Mode	インターフェイスの動作モード
(DR)	このネイバが LAN 上の指定ルータであるかどうかを示すステータス

■ show ip pim neighbor

関連コマンド

コマンド	説明
ip pim state-refresh disable	PIM ルータ上で PIM dense (密) モード リフレッシュ制御メッセージの処理および転送をディセーブルにします。
ip pim state-refresh origination-interval	PIM ルータに PIM dense (密) モード リフレッシュ制御メッセージの送信元およびインターバルを設定します。
show ip pim interface df	指定フォワーダ インターフェイスに関する情報を表示します。

show ip pim rp-hash

指定したグループについて選択されているランデブーポイントを表示するには、**show ip pim rp-hash** コマンドを使用します。

```
show ip pim vrf vrf-name rp-hash {group-address | group-name}
```

シンタックスの説明	vrf vrf-name	マルチキャスト VRF インスタンスに割り当てられた名前を指定します。
	group-address group-name	DNS ホスト テーブルで定義された指定したグループ アドレスまたは名前のランデブーポイント情報

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドは、指定したグループについて選択されたランデブーポイントを表示します。また、このランデブーポイントが Auto-RP または PIM Version 2 ブートストラップメカニズムによって選択されたかどうかを示します。

例 次に、指定したグループについて選択されているランデブーポイントを表示する例を示します。

```
Router# show ip pim rp-hash 239.1.1.1

RP 172.16.24.12 (mt1-47a.cisco.com), v2
  Info source: 172.16.24.12 (mt1-47a.cisco.com), via bootstrap
  Uptime: 05:15:33, expires: 00:02:01
```

表 2-68 に、この出力で表示されるフィールドについて説明します。

表 2-68 show ip pim rp-hash のフィールドの説明

フィールド	説明
RP 172.16.24.12 (mt1-47a.cisco.com), v2	指定したグループのランデブー ポイントのアドレス (239.1.1.1)。カッコ内は、ランデブー ポイントの DNS 名です。ランデブー ポイントのアドレスが DNS に登録されていない場合は、疑問符 (?) が表示されます。PIM Version 2 が設定されています。
Info source: 172.16.24.12 (mt1-47a.cisco.com), via bootstrap	ルータがこのランデブー ポイント情報を学習したシステムと、送信元の DNS 名。ランデブー ポイントはブートストラップ メカニズムによって選択されました。この例では、BSR はランデブー ポイントでもあります。
Uptime	ルータがこのランデブー ポイントを認識していた時間の長さ (時、分、秒)
expires	このランデブー ポイントに関する情報が期限切れになるまでの時間の長さ (時、分、秒)。この時間内にルータがリフレッシュ メッセージを受信しなかった場合、ルータはこのランデブー ポイントに関する情報を廃棄します。

show ip pim rp mapping

アクティブなランデブーポイントへの PIM グループのマッピングを表示するには、**show ip pim rp mapping** コマンドを使用します。

show ip pim vrf vrf-name rp mapping [rp-address]

シンタックスの説明	パラメータ	説明
vrf vrf-name		マルチキャスト VRF インスタンスに割り当てられた名前を指定します。
rp-address		(任意) ランデブーポイントの IP アドレス

コマンドのデフォルト *rp-address* を指定しなければ、アクティブなランデブーポイントすべてのマッピングが表示されます。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、アクティブなランデブーポイントへの PIM グループのマッピングを表示する例を示します。

```
Router# show ip pim rp mapping
PIM Group-to-RP Mappings
This system is an RP-mapping agent
Group(s) 224.1.0.0/16
RP 6.6.6.6 (?), v2v1
Info source: 6.6.6.6 (?), elected via Auto-RP ---> learned via Auto-RP
and the elected RP.
Uptime: 22:36:49, expires: 00:02:04
Group(s) 225.2.2.0/24
RP 9.9.9.9 (?), v2v1, bidir
Info source: 9.9.9.9 (?), elected via Auto-RP
Uptime: 22:36:20, expires: 00:02:37
Group(s) 226.2.2.0/24
RP 2.2.2.2 (?), v2v1, bidir
Info source: 2.2.2.2 (?), elected via Auto-RP
Uptime: 22:36:24, expires: 00:02:29
Group(s) 227.2.2.0/24
RP 9.9.9.9 (?), v2v1, bidir
Info source: 9.9.9.9 (?), elected via Auto-RP
Uptime: 22:36:21, expires: 00:02:35
Router#
```

表 2-69 に、この例で表示されるフィールドについて説明します。

表 2-69 show ip pim rp mapping のフィールドの説明

フィールド	説明
Info source	ACL 番号
Static	スタティック ランデブー ポイント設定からのグループ/マッピング情報
Bidir Mode	ランデブー ポイントが双方向モードで動作しているかどうかを示すステータス
RP	当該グループのランデブー ポイントのアドレス
(?)	Domain Name System (DNS; ドメイン ネーム システム) が指定されていないことを示すステータス

show ip pim snooping

IP PIM スヌーピングに関する情報を表示するには、**show ip pim snooping** コマンドを使用します。

show ip pim snooping

```
show ip pim snooping vlan vlan-id [neighbor | mac-group | statistics | mroute [{src-ip | group-ip}]]
```

シンタックスの説明

vlan <i>vlan-id</i>	特定の VLAN の情報を表示します。有効値は 1 ~ 4094 です。
neighbor	(任意) 近接データベースに関する情報を表示します。
mac-group	(任意) レイヤ 2 の GDA データベースに関する情報を表示します。
statistics	(任意) VLAN 統計情報を表示します。
mroute	(任意) mroute データベースに関する情報を表示します。
<i>src-ip</i>	(任意) 送信元 IP アドレス
<i>group-ip</i>	(任意) グループ IP アドレス

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、グローバル ステータスに関する情報を表示する例を示します。

```
Router# show ip pim snooping
Global runtime mode: Enabled
Global admin mode   : Enabled
Number of user enabled VLANs: 1
User enabled VLANs: 10
Router#
```

次に、特定の VLAN に関する情報を表示する例を示します。

```
Router# show ip pim snooping vlan 10
3 neighbors (0 DR priority incapable, 0 Bi-dir incapable)
6 mroutes, 3 mac entries
DR is 10.10.10.4
RP DF Set
Router#
```

show ip pim snooping

次に、特定の VLAN の近接データベースに関する情報を表示する例を示します。

```
Router# show ip pim snooping vlan 10 neighbor
IP Address      Mac address     Port Uptime/Expires  Flags
10.10.10.2      000a.f330.344a 3/13 00:09:57/00:01:22
10.10.10.1      000a.f330.334a 3/12 00:09:44/00:01:21
10.10.10.4      000a.f330.3c00 15/01 00:09:57/00:01:22 DR
Number of Neighbors = 3
Router#
```

次に、レイヤ 2 内の特定の VLAN の GDA データベースに関する情報を表示する例を示します。

```
Router# show ip pim snooping vlan 10 mac-group
Mac address     Group address   Uptime/Expires  Outgoing Ports
0100.5e01.6465 224.1.100.101 00:20:26/00:02:43 3/12 3/13 15/1
0100.5e01.6464 224.1.100.100 00:20:28/00:02:41 3/12 3/13 15/1
0100.5e00.0128 224.0.1.1.40 00:20:27/00:02:47 3/12 3/13 15/1
Number of mac-groups = 3
Router#
```

次に、特定の VLAN の詳細統計情報を表示する例を示します。

```
Router# show ip pim snooping vlan 10 statistics
PIMv2 statistics for vlan 10:
Hello                               : 811
Join/Prunes                          : 1332
RP DF Election                       : 0
Asserts                              : 133
Other types                          : 0

Hello option holdtime [1]            : 811
Hello option Generation ID[20]       : 544
Hello option DR priority[19]         : 544
Hello option Bi-dir capable[22]     : 0
Hello option Fast Hold[65005]       : 0
Hello option Lan Prune Delay[2]     : 0
Hello option Tag switching [17]     : 0
Hello option PIM-DM State Refresh[21] : 544
Hello option Deprecated Cisco DR priority[18] : 0
Error - Hello length too short      : 0
Error - Hello hold option missing    : 0
Error - Hello option length         : 0
Error - Hello option unknown        : 0

Error - Join/Prune Address Family    : 0
Error - Join/Prune Parser malloc failure : 0
Error - Join/Prune Unknown up/down neighbor : 0
Error - Join/Prune Malformed packet discards : 0

Error - RPDF election Address Family : 0
Error - RPDF Unknown up/down neighbor : 0

Error - Generic packet input error   : 0
Router#
```

次に、特定の VLAN におけるすべてのマルチキャスト ルータの mroute データベースに関する情報を表示する例を示します。

```
Router# show ip pim snooping vlan 10 mroute
Number of Mroutes = 6
Flags: J/P - (*,G) Join/Prune, j/p - (S,G) Join/Prune
      SGR-P - (S,G,R) Prune

(*, 224.1.100.101), 00:16:14/00:02:58
10.10.10.1->10.10.10.2, 00:16:14/00:02:58, J
```

```

Downstream ports: 3/12
Upstream ports: 3/13
Outgoing ports: 3/12 3/13

(*, 224.1.100.100), 00:16:16/00:02:56
10.10.10.1->10.10.10.2, 00:16:16/00:02:56, J
Downstream ports: 3/12
Upstream ports: 3/13
Outgoing ports: 3/12 3/13

(10.10.10.2, 224.0.1.40), 00:16:10/00:03:03
10.10.10.1->10.10.10.2, 00:16:10/00:03:03, SGR-P
Downstream ports:
Upstream ports: 3/13
Outgoing ports: 3/13

(*, 224.0.1.40), 00:16:16/00:03:02
10.10.10.1->10.10.10.2, 00:16:16/00:03:02, J
Downstream ports: 3/12
Upstream ports: 3/13
Outgoing ports: 3/12 3/13

(*, 224.10.10.10), 00:02:23/00:01:06
Downstream ports:
Upstream ports:
Outgoing ports: 3/12 3/13

(123.123.123.123, 224.10.10.10), 00:02:23/00:01:06
10.10.10.1->10.10.10.2, 00:02:23/00:01:06, j
Downstream ports: 3/12
Upstream ports: 3/13
Outgoing ports: 3/12 3/13
Router#

```

次に、特定の送信元アドレスの PIM mroute に関する情報を表示する例を示します。

```

Router# show ip pim snooping vlan 10 mroute 224.1.100.100
(*, 224.1.100.100), 00:16:36/00:02:36
10.10.10.1->10.10.10.2, 00:16:36/00:02:36, J
Downstream ports: 3/12
Upstream ports: 3/13
Outgoing ports: 3/12 3/13
Router#

```

次に、特定の送信元アドレスおよびグループアドレスの PIM mroute に関する情報を表示する例を示します。

```

Router# show ip pim snooping vlan 10 mroute 123.123.123.123 224.10.10.10
(123.123.123.123, 224.10.10.10), 00:03:04/00:00:25
10.10.10.1->10.10.10.2, 00:03:04/00:00:25, j
Downstream ports: 3/12
Upstream ports: 3/13
Outgoing ports: 3/12 3/13
Router#

```

関連コマンド

コマンド	説明
ip pim snooping (global configuration mode)	PIM スヌーピングをグローバルにイネーブルにします。
ip pim snooping (interface configuration mode)	インターフェイス上の PIM スヌーピングをイネーブルにします。

show ip rpf events

トリガーされた RPF 統計情報を表示するには、**show ip rpf events** コマンドを使用します。

show ip rpf [vrf vrf-name] events

シンタックスの説明	vrf vrf-name	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
------------------	---------------------	--

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、トリガーされた RPF 統計情報を表示する例を示します。

```
Router# show ip rpf events
Last 15 triggered multicast RPF check events
RPF backoff delay: 500 msec
RPF maximum delay: 5 sec
DATE/TIME BACKOFF PROTOCOL EVENT RPF CHANGES
Jan 1 00:00:55.643 500 msec EIGRP Route UP 0
Jan 1 00:00:07.283 1000 sec Connected Route UP 0
Jan 1 00:00:06.283 500 msec Connected Route UP 0
Router#
```

関連コマンド	コマンド	説明
	ip multicast rpf backoff	PIM 待機インターバルを設定します。
	ip multicast rpf interval	RPF 一貫性チェック インターバルを設定します。

show ip wccp

WCCP 統計情報を表示するには、**show ip wccp** コマンドを使用します。

show ip wccp [*service-number* | *web-cache*] [**detail** | **view**]

シンタックスの説明	
<i>service-number</i>	(任意) ルータに制御されているキャッシュ エンジン サービス グループの識別番号を指定します。有効値は 0 ~ 99 です。
web-cache	(任意) Web キャッシュ サービスの統計情報を表示するようにルータに指示します。
detail	(任意) 現在設定されているクラスタのルータおよびすべてのキャッシュ エンジンに関する情報を表示します。
view	(任意) 特定のサービス グループの他のどのメンバーが検出されているかまたは検出されていないか表示します。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

[Total Packets Redirected] 数を提供するには、**show ip wccp service-number** コマンドを使用します。[Total Packets Redirected] 数とは、リダイレクトされるフローまたはセッションの数です。

[Packets Redirected] 数を提供するには、**show ip wccp service-number detail** コマンドを使用します。[Packets Redirected] 数とは、リダイレクトされるフローまたはセッションの数です。

レイヤ 2 リダイレクションを使用しているパケット数ではなくフロー数を示すには、**show ip wccp web-cache detail** コマンドを使用します。

シスコ製キャッシュ エンジンを使用するキャッシュ エンジン クラスタでは、リバース プロキシ *service-number* は、値 99 で指定されます。

[Packets Redirected] 情報のカウンタをリセットするには、**clear ip wccp** コマンドを使用します。

IP WCCP のコマンドの詳細については、『Cisco IOS Configuration Fundamentals Configuration Guide』の「Configuring Web Cache Services Using WCCP」を参照してください。

例 次に、レイヤ 2 リダイレクションを使用する接続済みキャッシュ エンジンを表示する例を示します。

```
Router# show ip wccp web-cache detail
WCCP Cache-Engine information:
  IP Address:          10.11.1.1
  Protocol Version:   2.0
  State:              Usable
  Redirection:        L2
```

show ip wccp

```

Initial Hash Info:      FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                        FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
Assigned Hash Info:    FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                        FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
Hash Allotment:        256 (100.00%)
Packets Redirected:    10273
Connect Time:          17:05:44
    
```

表 2-70 に、この例で表示されるフィールドについて説明します。

表 2-70 show ip wccp web-cache detail コマンドの出力フィールド

フィールド	説明
WCCP Cache-Engine information	サービス グループ内のキャッシュ エンジンに接続されているルータに対応付けられた WCCP の IP アドレスおよびバージョンに関するフィールドを含むエリアのヘッダー
IP Address	サービス グループ内のキャッシュ エンジンに接続されたルータの IP アドレス
Protocol Version	サービス グループ内のルータで使用されている WCCP のバージョン
WCCP Cache-Engine information	キャッシュ エンジン情報のフィールド
IP Address	サービス グループ内のキャッシュ エンジンの IP アドレス
Protocol Version	サービス グループ内のキャッシュ エンジンで使用されている WCCP のバージョン
State	キャッシュ エンジンが正常に稼働しているかどうか、およびサービス グループ内のルータおよび他のキャッシュ エンジンから通信できるかどうかを示すステータス
Initial Hash Info	ハッシュ バケット割り当ての初期状態
Assigned Hash Info	ハッシュ バケット割り当ての現在の状態
Hash Allotment	現在のキャッシュ エンジンに割り当てられたバケットのパーセント。値およびパーセントが両方とも表示されます。
Packets Redirected	キャッシュ エンジンにリダイレクトされたフローまたはセッションの数
Connect Time	キャッシュ エンジンがルータの接続に要する時間

関連コマンド

コマンド	説明
clear ip wccp	特定のサービスに対してルータで維持している WCCP 統計情報 (カウント) を削除します。
ip wccp	キャッシュ エンジン サービス グループに対するサポートをイネーブ爾またはディセーブルにするようにルータに指示します。
ip wccp redirect	WCCP を使用して発信または着信インターフェイス上でパケット リダイレクションをイネーブ爾にします。
ip wccp web-cache accelerated	WCCP バージョン 1 のハードウェア アクセラレーションをイネーブ爾にします。
show ip interface	IP 用に設定したインターフェイスのユーザビリティ ステータスを表示します。

show ipv6 mfib

IPv6 MFIB の転送エントリとインターフェイスを表示するには、**show ipv6 mfib** コマンドを使用します。

```
show ipv6 mfib [{group-ip-addr/prefix-length | group-name | group-address [source-name
| source-address]}] | {active kbps} | count | interface | status | summary | verbose]
```

```
show ipv6 mfib [link-local [active [kbps] | count | verbose]]
```

シンタックスの説明

<i>group-ip-addr/prefix-length</i>	(任意) インターフェイスに割り当てられた IPv6 ネットワークのグループ IPv6 アドレス/プレフィクス長
<i>group-name</i>	(任意) マルチキャスト グループ名
<i>group-address</i>	(任意) グループ IPv6 アドレス
<i>source-name</i>	(任意) 送信元名
<i>source-address</i>	(任意) 送信元 IP アドレス
active kbps	(任意) アクティブな送信元がマルチキャスト グループに送信する速度を表示します。有効値は 0 ~ 4,294,967,295 kbps (キロビット/秒) です。
count	(任意) ルートおよびパケット数に関する情報を表示します。
interface	(任意) インターフェイス設定およびステータスに関する情報を表示します。
status	(任意) 一般的な設定およびステータスに関する情報を表示します。
summary	(任意) サマリー統計に関する情報を表示します。
verbose	(任意) MAC カプセル化ヘッダーおよびプラットフォーム固有情報などの追加情報を表示します。
link-local	(任意) リンク ローカル グループを表示します。

コマンドのデフォルト

prefix-length は 128 です。

コマンドモード

ユーザ EXEC (>)
特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

MFIB エントリ、転送インターフェイス、およびこれらのトラフィック統計を表示するには、**show ipv6 mfib** コマンドを、使用します。ルータが分散モードで動作している場合、Virtual IP (VIP; 仮想 IP) 上でこのコマンドをイネーブルにできます。

パケットの転送に積極的に使用される MFIB エントリを表示するには、**show ipv6 mfib active** コマンドを使用します。多くの場合、オプションの *kbps* 引数を指定して、*kbps* 引数によって設定した量以上のトラフィック量を転送しているエントリのセットを表示すると便利です。

平均パケット サイズとデータ速度 (kbps) を表示するには、**show ipv6 mfib count** コマンドを使用します。

prefix-length は IPv6 プレフィックスの長さです。アドレスの上位連続ビットの数を示す 10 進値がプレフィックスになります (アドレスのネットワーク部分)。10 進値の前にスラッシュを付ける必要があります。

MFIB の転送エントリには、転送とシグナリングのデフォルト動作を決定するフラグがあり、エントリに一致するパケットで使用されます。エントリにはインターフェイス単位のフラグもあり、特定のインターフェイスで受信または転送されるパケットについての転送動作をさらに詳しく指定します。

表 2-71 に、MFIB 転送エントリとインターフェイス フラグを示します。

表 2-71 MFIB 転送エントリとインターフェイス フラグ

フラグ	説明
F	Forward : データは、このインターフェイスから転送されます。
A	Accept : このインターフェイス上で受信されたデータは、転送用として受け入れられます。
IC	Internal copy : このインターフェイスで受信または転送されたパケットのコピーをルータに送信します。
NS	Negate signal : このインターフェイスで受信されたパケットについては、デフォルトのエントリ シグナリング動作を逆にします。
DP	Do not preserve : このインターフェイスでのパケット受信を信号で通知するときに、コピーを保存しません (廃棄します)。
SP	Signal present : このインターフェイスでのパケットの受信が信号で通知されました。
S	Signal : デフォルトでは、このエントリに一致するパケットの受信を信号で通知します。
C	このエントリに一致するパケットについて、直接接続チェックを実行します。パケットが、直接接続されている送信元から発信されていた場合は、受信を信号で通知します。

例

次に、特定のグループ IPv6 アドレスの情報を表示する例を示します。

```
Router# show ipv6 mfib ff35::1:1
IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
                IC - Internal Copy, NP - Not platform switched
                SP - Signal Present
Interface Counts: Distributed FS Pkt Count/FS Pkt Count/PS Pkt Count
(1600::2,FF35::1:1) Flags:
  RP Forwarding: 7188/100/48/37, Other: 203619/203619/0
  LC Forwarding: 0/0/0/0, Other: 0/0/0
  Vlan25 Flags: A
  Vlan11 Flags: F NS
  Pkts: 0/7188/0
```

表 2-72 に、この出力で表示されるフィールドについて説明します。

表 2-72 show ipv6 mfib のフィールドの説明

フィールド	説明
Entry flags	エントリに関する情報
Forwarding Counts	受信されて、少なくとも 1 つのインターフェイスに転送されたパケットに関する統計
Pkt Count/	このカウンタが適用されるマルチキャスト転送状態の作成後に受信され転送されたパケットの総数
Pkts per second/	1 秒間に受信され転送されたパケット数
Avg Pkt Size/	このマルチキャスト転送状態についての合計バイト数/合計パケット数。合計バイト数は直接は表示されません。平均パケット サイズにパケット数を乗算すると、合計バイト数を計算できます。
Kbits per second	1 秒間のバイト数/1 秒間のパケット数/1000
Other counts:	受信パケットに関する統計。これらのカウンタには、受信され転送されたパケットと受信されても転送されなかったパケットに関する統計が含まれます。
Interface Flags:	インターフェイスに関する情報。インターフェイス フラグの詳細については、表 2-71 を参照してください。
Interface Counts:	インターフェイス統計情報

次に、グループアドレス FF03:1::1 と送信元アドレス 5002:1::2 が指定されている MFIB 内の転送エントリとインターフェイスを示します。

```
Router# show ipv6 mfib FF03:1::1 5002:1::2

IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A flag,
          AR - Activity Required, D - Drop
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:Total/RPF failed/Other drops
Interface Flags:A - Accept, F - Forward, NS - Negate Signalling
          IC - Internal Copy, NP - Not platform switched
          SP - Signal Present
Interface Counts:FS Pkt Count/PS Pkt Count
(5002:1::2,FF03:1::1) Flags:
  Forwarding:71505/0/50/0, Other:42/0/42
  GigabitEthernet5/0 Flags:A
  GigabitEthernet5/0.19 Flags:F NS
    Pkts:239/24
  GigabitEthernet5/0.20 Flags:F NS
    Pkts:239/24
  .
  .
  .
  GigabitEthernet5/0.16 Flags:F NS
    Pkts:71628/24
```

次に、グループアドレス FF03:1::1 とデフォルトプレフィクス 128 が指定されている MFIB 内の転送エントリとインターフェイスを示します。

```
Router# show ipv6 mfib FF03:1::1/128

IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A flag,
          AR - Activity Required, D - Drop
```

show ipv6 mfib

```
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:Total/RPF failed/Other drops
Interface Flags:A - Accept, F - Forward, NS - Negate Signalling
                IC - Internal Copy, NP - Not platform switched
                SP - Signal Present
Interface Counts:FS Pkt Count/PS Pkt Count
(*,FF03::1) Flags:C
  Forwarding:0/0/0/0, Other:0/0/0
  Tunnel1 Flags:A NS
  GigabitEthernet5/0.25 Flags:F NS
    Pkts:0/0
.
.
.
GigabitEthernet5/0.16 Flags:F NS
  Pkts:0/0
```

次に、アクティブな IP マルチキャスト送信元の情報送信速度に関する統計情報を示します。ルータはトラフィックを 2001::1:1:200 から FF05::1 に切り替えています。

```
Router# show ipv6 mfib active

Active IPv6 Multicast Sources - sending >= 4 kbps
Group: FF05::1
  Source: 2001::1:1:200
    Rate: 20 pps/16 kbps(1sec), 0 kbps(last 128 sec)
```

表 2-73 に、この出力で表示されるフィールドについて説明します。

表 2-73 show ipv6 mfib active のフィールドの説明

フィールド	説明
Group:	特定のグループ G について (*,G) のカウンタと (S,G) の範囲に関するサマリー情報。次の RP-tree: および Source: 出力フィールドには、このグループに属する個別の状態に関する情報が含まれています。 (注) PIM-SSM 範囲のグループの場合、Group: 出力フィールドは統計情報です。すべての SSM 範囲 (S,G) 状態は、無関係な個別の SSM チャンネルです。
Rate...kbps	1 秒間のバイト数/1 秒間のパケット数/1000。IP マルチキャスト高速スイッチングプラットフォームでは、1 秒間のパケット数は最後の 1 秒間のパケット数です。その他のプラットフォームでは、別の方法でこの数を計算することもあります。詳細については、『Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY』を参照してください。

次に、グループと送信元について MFIB からの統計情報を表示する例を示します。ルータはトラフィックを 2001::1:1:200 から FF05::1 に切り替えています。

```
Router# show ipv6 mfib count

IP Multicast Statistics
54 routes, 7 groups, 0.14 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Group: FF00::/8
  RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0
Group: FF00::/15
  RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0
Group: FF05::1
  RP-tree: Forwarding: 2/0/100/0, Other: 0/0/0
```

```

Source: 10::1:1:200, Forwarding: 367/10/100/7, Other: 0/0/0
Tot. shown: Source count: 1, pkt count: 369
Group: FF10::/15
  RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0
Group: FF20::/15
  RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0

```

表 2-74 に、この出力で表示されるフィールドについて説明します。

表 2-74 show ipv6 mfib count のフィールドの説明

フィールド	説明
Forwarding Counts	受信されて、少なくとも 1 つのインターフェイスに転送されたパケットに関する統計
Pkt Count/	このカウンタが適用されるマルチキャスト転送状態の作成後に受信され転送されたパケットの総数
Pkts per second/	1 秒間に受信され転送されたパケット数
Avg Pkt Size/	このマルチキャスト転送状態についての合計バイト数/合計パケット数。合計バイト数は直接は表示されません。平均パケット サイズにパケット数を乗算すると、合計バイト数を計算できます。
Kilobits per second	1 秒間のバイト数/1 秒間のパケット数/1000
Other counts:	受信パケットに関する統計。これらのカウンタには、受信され転送されたパケットと受信されても転送されなかったパケットに関する統計が含まれます。
Total/	受信パケット総数
RPF failed/	RPF またはアクセプタンス チェックの失敗のために転送されなかったパケット数 (双方向 PIM が設定されているとき)
Other drops (OIF-null, rate-limit etc)	RPF またはアクセプタンス チェック以外の理由で転送されなかったパケットの数 (発信インターフェイス (OIF) リストが空であったり、イネーブルになっている設定のためにパケットが廃棄されたなど)
Group:	特定のグループ G について (*,G) のカウンタと (S,G) の範囲に関するサマリー情報。次の RP-tree: および Source: 出力フィールドには、このグループに属する個別の状態に関する情報が含まれています。 (注) 送信元特定マルチキャスト (PIM-SSM) 範囲のグループの場合、Group: 出力フィールドは統計情報です。すべての SSM 範囲 (S,G) 状態は、無関係な個別の SSM チャンネルです。
RP-tree:	このグループ G の (*,G) 状態のカウンタ。これらのカウンタは、共有ツリー上のパケットを転送しない転送モードになっているグループについてだけ表示されます。これらの (*,G) グループは、双方向 PIM および PIM sparse (疎) モード (PIM-SM) のグループです。PIM SSM 範囲のグループについては、RP-tree は表示されません。

次に、MFIB の転送エントリおよびインターフェイスと、MAC カプセル化ヘッダーおよびプラットフォーム固有情報などの追加情報の例を示します。

```

Router# show ipv6 mfib ff33::1:1 verbose
IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, K - Keepalive
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Platform per slot HW-Forwarding Counts: Pkt Count/Byte Count
Platform flags: HF - Forwarding entry, HB - Bridge entry, HD - NonRPF Drop entry,

```

show ipv6 mfib

```

NP - Not platform switchable,RPL - RPF-ltl linkage,
MCG - Metset change,ERR - S/w Error Flag,RTY - In RetryQ,
LP - L3 pending,MP - Met pending,AP - ACL pending
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
                  IC - Internal Copy, NP - Not platform switched
                  SP - Signal Present
Interface Counts: Distributed FS Pkt Count/FS Pkt Count/PS Pkt Count
(10::2,FF33::1:1) Flags: K
  RP Forwarding: 0/0/0/0, Other: 0/0/0
  LC Forwarding: 0/0/0/0, Other: 0/0/0
  HW Forwd:    0/0/0/0, Other: NA/NA/NA
  Slot 6: HW Forwarding: 0/0, Platform Flags:  HF RPL
  Slot 1: HW Forwarding: 0/0, Platform Flags:  HF RPL
  Vlan10 Flags: A
  Vlan30 Flags: F NS
  Pkts: 0/0/0 MAC: 33330001000100D0FFFE180086DD
Router#
    
```

表 2-75 に、この出力で表示されるフィールドについて説明します。

表 2-75 show ipv6 mfib verbose のフィールドの説明

フィールド	説明
Platform flags	プラットフォームに関する情報
Platform per slot HW-Forwarding Counts	転送されたバイトあたりのパケット総数

表 2-76 に MFIB プラットフォーム フラグを示します。

表 2-76 MFIB プラットフォーム フラグ

フラグ	説明
H	エントリはハードウェアにインストールされています。
HF	転送エントリ
HB	ブリッジ エントリ
HD	NonRPF Drop エントリ
NP	ソフトウェア スイッチング
RPL	RPF-ltl リンケージ
MCG	Metset 変更
ERR	ソフトウェア エラー フラグ
RTY	再試行キュー内
LP	レイヤ 3 保留中
MP	Met 保留中
AP	ACL 保留中

show ipv6 mld snooping

MLDv2 スヌーピング情報を表示するには、**show ipv6 mld snooping** コマンドを使用します。

```
show ipv6 mld snooping {{explicit-tracking vlan} | {mrouter [vlan vlan]} |
                        {report-suppression vlan vlan} | {statistics vlan vlan}}
```

シンタックスの説明	パラメータ	説明
	explicit-tracking vlan vlan	明示的ホスト トラッキングのステータスを表示します。
	mrouter	オプションの VLAN 上のマルチキャスト ルータ インターフェイスを表示します。
	vlan vlan	(任意) マルチキャスト ルータ インターフェイス上の VLAN 番号を指定します。
	report-suppression vlan vlan	レポート抑制のステータスを表示します。
	statistics vlan vlan	VLAN 上の IGMP スヌーピング情報を表示します。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン **show ip igmp snooping** コマンドを使用して IGMP スヌーピングに関する情報を表示することもできます。

引数を指定せずに **show ipv6 mld snooping mrouter** コマンドを入力すると、すべてのマルチキャスト ルータ インターフェイスを表示することができます。

例 次に、VLAN 25 上の明示的トラッキング情報を表示する例を示します。

```
Router# show ipv6 mld snooping explicit-tracking vlan 25
Source/Group          Interface    Reporter    Filter_mode
-----
10.1.1.1/226.2.2.2    V125:1/2    16.27.2.3    INCLUDE
10.2.2.2/226.2.2.2    V125:1/2    16.27.2.3    INCLUDE
Router#
```

次に、VLAN 1 のマルチキャスト ルータ インターフェイスを表示する例を示します。

```
Router# show ipv6 mld snooping mrouter vlan 1
vlan          ports
-----+-----
1             Gi1/1,Gi2/1,Fa3/48,Router
Router#
```

■ show ipv6 mld snooping

次に、VLAN 25 の IGMP スヌーピング統計情報を表示する例を示します。

```
Router# show ipv6 mld snooping statistics interface vlan 25
```

```
Snooping statistics for Vlan25
```

```
#channels:2
```

```
#hosts :1
```

Source/Group	Interface	Reporter	Uptime	Last-Join	Last-Leave
10.1.1.1/226.2.2.2	Gi1/2:V125	16.27.2.3	00:01:47	00:00:50	-
10.2.2.2/226.2.2.2	Gi1/2:V125	16.27.2.3	00:01:47	00:00:50	-

```
Router#
```

関連コマンド

コマンド	説明
ipv6 mld snooping	MLDv2 スヌーピングをグローバルにイネーブルにします。
ipv6 mld snooping explicit-tracking	明示的なホスト トラッキングをイネーブルにします。
ipv6 mld snooping querier	MLDv2 スヌーピング クエリアをイネーブルにします。
ipv6 mld snooping report-suppression	VLAN 上でレポート抑制をイネーブルにします。

show l2protocol-tunnel

特定のインターフェイスまたはすべてのインターフェイス上のトンネリング プロトコルを表示するには、**show l2protocol-tunnel** コマンドを使用します。

show l2protocol-tunnel [**{interface interface modlport}**] | **{vlan vlan-id}** | **summary**]

シンタックスの説明

interface interface	(任意) インターフェイス タイプを指定します。有効値は ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 atm 、および ge-wan です。
modlport	モジュールおよびポート番号
vlan vlan-id	VLAN を指定します。有効値は 1 ~ 4094 です。
summary	(任意) トンネリング ポートのサマリーを表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

show l2protocol-tunnel コマンドは、プロトコル トンネリングがイネーブルであるポートだけを表示します。

show l2protocol-tunnel summary コマンドは、ポートがダウンしているかまたはトランクとして現在設定されているかに関係なく、プロトコル トンネリングがイネーブルであるポートを表示します。

例

次に、すべてのインターフェイスのトンネリング プロトコルを表示する例を示します。

```
Router# show l2protocol-tunnel
COS for Encapsulated Packets: 5
Drop Threshold for Encapsulated Packets: 3000
Port      Protocol Shutdown      Drop      Encapsulation Decapsulation      Drop
          Threshold Threshold      Counter      Counter      Counter
-----
Fa3/38   cdp      ----      3000      5           0           0
          stp      ----      3000      2653        0           0
          ----      ----      ----      ----      ----
```

Router#

次に、レイヤ 2 プロトコル トンネル ポートのサマリーを表示する例を示します。

```
Router# show l2protocol-tunnel summary
COS for Encapsulated Packets:5
Drop Threshold for Encapsulated Packets:0

Port      Protocol      Shutdown      Drop      Status
          Threshold      Threshold
```

show l2protocol-tunnel

```

-----
(cdp/stp/vtp)      (cdp/stp/vtp)
-----
Fa9/1  --- stp --- ----/----/----  ----/----/----  down
Fa9/9   cdp stp vtp ----/----/----  ----/----/----  up
Fa9/47  --- --- --- ----/----/----  1500/1500/1500  down (trunk)
Fa9/48  cdp stp vtp ----/----/----  ----/----/----  down (trunk)
Router>

```

関連コマンド

コマンド	説明
l2protocol-tunnel	インターフェイス上でプロトコル トンネリングをイネーブルにし、トンネリングするプロトコルのタイプを指定します。
l2protocol-tunnel drop-threshold	特定のインターフェイス上で、指定されたプロトコルに対し、廃棄される前に処理される最大のパケット数を指定します。
l2protocol-tunnel global drop-threshold	ソフトウェア レベルでのレート制限をイネーブルにします。
l2protocol-tunnel shutdown-threshold	特定のインターフェイス上で、指定されたプロトコルに対して、1 秒以内で処理可能な最大のパケット数を指定します。

show l3-mgr

レイヤ 3 マネージャに関する情報を表示するには、**show l3-mgr** コマンドを使用します。

show l3-mgr status

```
show l3-mgr {interface {{interface interface-number} | {null interface-number} |
              {port-channel number} | {vlan vlan-id} | status}}
```

シンタックスの説明

status	グローバル変数に関する情報を表示します。
interface	レイヤ 3 マネージャに関する情報を表示します。
<i>interface</i>	インターフェイス タイプ。有効値は ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 atm 、および ge-wan です。
<i>interface-number</i>	モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
null interface-number	ヌル インターフェイスを指定します。有効値は 0 です。
port-channel number	チャンネル インターフェイスを指定します。有効値は 1 ~ 282 の範囲の最大 64 個の値です。
vlan vlan-id	VLAN を指定します。有効値は 1 ~ 4094 です。
status	レイヤ 3 マネージャに関するステータス情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

interface-number 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

257 ~ 282 の **port-channel number** 値は、CSM および FWSM だけでサポートされています。

例

次に、レイヤ 3 マネージャのステータスを表示する例を示します。

```
Router# show l3-mgr status
l3_mgr_state:          2
l3_mgr_req_q.count:    0
l3_mgr_req_q.head:     0
l3_mgr_req_q.tail:     0
```

■ show l3-mgr

```
l3_mgr_max_queue_count: 1060
l3_mgr_shrunk_count: 0
l3_mgr_req_q.ip_inv_count: 303
l3_mgr_req_q.ipx_inv_count: 0
l3_mgr_outpak_count: 18871
l3_mgr_inpak_count: 18871

l3_mgr_max_pending_pak: 4
l3_mgr_pending_pak_count: 0

nde enable statue: 0
current nde addr: 0.0.0.0
```

Router#

次に、特定のインターフェイスのレイヤ 3 マネージャに関する情報を表示する例を示します。

```
Router# show l3-mgr interface fastethernet 5/40
vlan: 0
ip_enabled: 1
ipx_enabled: 1
bg_state: 0 0 0 0
hsrp_enabled: 0
hsrp_mac: 0000.0000.0000
state: 0
up: 0
Router#
```

show lacp

LACP 情報を表示するには、**show lacp** コマンドを使用します。

```
show lacp [channel-group] {counters | internal | neighbors | sys-id}
```

シンタックスの説明

<i>channel-group</i>	(任意) チャネル グループの番号。有効値は 1 ~ 282 です。
counters	LACP 統計に関する情報を表示します。
internal	LACP 内部情報を表示します。
neighbors	LACP ネイバに関する情報を表示します。
sys-id	LACP システム ID を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

channel-group を指定しない場合は、すべてのチャネル グループが表示されます。257 ~ 282 の *channel-group* 値は、CSM および FWSM だけでサポートされています。オプションの *channel-group* を入力すると、**sys-id** キーワードを除くすべてのキーワードにチャネルグループを指定できます。

例

次に、特定のチャネル グループの LACP 統計情報を表示する例を示します。

```
Router# show lacp 1 counters
          LACPDU          Marker          LACPDU
Port      Sent  Recv      Sent  Recv      Pkts  Err
-----
Channel group: 1
Fa4/1      8    15         0     0         3     0
Fa4/2     14   18         0     0         3     0
Fa4/3     14   18         0     0         0
Fa4/4     13   18         0     0         0
```

出力では次の情報が表示されます。

- [LACPDU Sent] および [Recv] カラムは、特定のインターフェイスで送受信された LACPDU 数を表示します。
- [LACPDU Pkts] および [Err] カラムは、マーカー プロトコル パケットを表示します。

次に、特定のチャネルに属するインターフェイスの内部情報を表示する例を示します。

```
Router# show lacp 1 internal
```

show lacp

Flags: S - Device sends PDUs at slow rate. F - Device sends PDUs at fast rate.
 A - Device is in Active mode. P - Device is in Passive mode.

Channel group 1

Port	Flags	State	LACPDUs Interval	LACP Port Priority	Admin Key	Oper Key	Port Number	Port State
Fa4/1	saC	bndl	30s	32768	100	100	0xc1	0x75
Fa4/2	saC	bndl	30s	32768	100	100	0xc2	0x75
Fa4/3	saC	bndl	30s	32768	100	100	0xc3	0x75
Fa4/4	saC	bndl	30s	32768	100	100	0xc4	0x75

Router#

表 2-77 に、この例で表示されるフィールドについて説明します。

表 2-77 show lacp internal コマンドの出力フィールド

フィールド	説明
State	現時点における特定のポートの状態が表示されます。有効な値は次のとおりです。 <ul style="list-style-type: none"> • <i>bndl</i> : ポートはアグリゲータに対応付けられ、他のポートにバンドルされています。 • <i>susp</i> : ポートは中断ステートです。アグリゲータに対応付けられていません。 • <i>indep</i> : ポートは独立ステートです (バンドルされていませんが、データトラフィックのスイッチングは可能です。この場合、LACP はパートナーポート上で稼動していません)。 • <i>hot-sby</i> : ポートはホットスタンバイステートです。 • <i>down</i> : ポートはダウンしています。
LACPDUs Interval	インターバル設定
LACP Port Priority	ポートプライオリティ設定
Admin Key	管理鍵
Oper Key	オペレータ鍵
Port Number	ポート番号
Port State	単一オクテット内の各ビットとして符号化されたポートのステート変数で、次の意味を持ちます [1]。 <ul style="list-style-type: none"> • bit0: <i>LACP_Activity</i> • bit1: <i>LACP_Timeout</i> • bit2: <i>Aggregation</i> • bit3: <i>Synchronization</i> • bit4: <i>Collecting</i> • bit5: <i>Distributing</i> • bit6: <i>Defaulted</i> • bit7: <i>Expired</i>

次に、特定のポート チャンネルの LACP ネイバに関する情報を表示する例を示します。

```
Router# show lacp 1 neighbors
Flags: S - Device sends PDUs at slow rate. F - Device sends PDUs at fast rate.
       A - Device is in Active mode.           P - Device is in Passive mode.

Channel group 1 neighbors
Port      Partner                               Partner      Age      Flags
Fa4/1     8000,00b0.c23e.d84e                   0x81         29s     P
Fa4/2     8000,00b0.c23e.d84e                   0x82         0s     P
Fa4/3     8000,00b0.c23e.d84e                   0x83         0s     P
Fa4/4     8000,00b0.c23e.d84e                   0x84         0s     P

          Port      Admin      Oper      Port
          Priority   Key        Key        State
Fa4/1     32768          200       200       0x81
Fa4/2     32768          200       200       0x81
Fa4/3     32768          200       200       0x81
Fa4/4     32768          200       200       0x81
Router#
```

PDU が受信されていない場合は、デフォルトの管理情報がカッコ内に表示されます。

次に、LACP のシステム ID を表示する例を示します。

```
Router> show lacp sys-id
8000,AC-12-34-56-78-90
```

システム ID は、システムのプライオリティおよび MAC アドレスで構成されます。先頭の 2 バイトはシステムのプライオリティです。最後の 6 バイトはシステムに対応付けられた、グローバルに管理された各 MAC アドレスです。

関連コマンド

コマンド	説明
clear lacp counters	特定のチャンネル グループに属するすべてのインターフェイスの統計情報をクリアします。
lacp port-priority	物理インターフェイスのプライオリティを設定します。
lacp system-priority	システムのプライオリティを設定します。

show logging ip access-list

ロギング IP アクセス リストに関する情報を表示するには、**show logging ip access-list** コマンドを使用します。

```
show logging ip access-list {cache | config}
```

シンタックスの説明

cache	OAL キャッシュ内のすべてのエントリに関する情報を表示します。
config	ロギング IP アクセス リスト設定に関する情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

OAL は、IPv4 ユニキャスト トラフィックだけでサポートされます。

例

次に、OAL キャッシュ内のすべてのエントリを表示する例を示します。

```
Router# show logging ip access-list cache
Matched flows:
id prot src_ip dst_ip sport dport status count
total lastlog
-----
1 17 20.2.1.82 21.2.12.2 111 63 Permit 0
3906 2d02h
2 17 20.2.1.82 21.2.12.2 1135 63 Permit 0
3906 2d02h
3 17 20.2.1.82 21.2.12.2 2159 63 Permit 0
3906 2d02h
4 17 20.2.1.82 21.2.12.2 3183 63 Permit 0
3906 2d02h
5 17 20.2.1.82 21.2.12.2 4207 63 Permit 0
3906 2d02h
6 17 20.2.1.82 21.2.12.2 5231 63 Deny 0
3906 2d02h
7 17 20.2.1.82 21.2.12.2 6255 63 Deny 0
3906 2d02h
8 17 20.2.1.82 21.2.12.2 7279 63 Permit 0
3906 2d02h
9 17 20.2.1.82 21.2.12.2 8303 63 Permit 0
3906 2d02h
10 17 20.2.1.82 21.2.12.2 9327 63 Permit 0
3905 2d02h
11 17 20.2.1.82 21.2.12.2 10351 63 Permit 0
3905 2d02h
```

```

12 17 20.2.1.82 21.2.12.2 11375 63 Permit 0
3905 2d02h
13 17 20.2.1.82 21.2.12.2 12399 63 Deny 0
3905 2d02h
14 17 20.2.1.82 21.2.12.2 13423 63 Permit 0
3905 2d02h
15 17 20.2.1.82 21.2.12.2 14447 63 Deny 0
3905 2d02h
16 17 20.2.1.82 21.2.12.2 15471 63 Permit 0
3905 2d02h
17 17 20.2.1.82 21.2.12.2 16495 63 Permit 0
3905 2d02h
18 17 20.2.1.82 21.2.12.2 17519 63 Permit 0
3905 2d02h
19 17 20.2.1.82 21.2.12.2 18543 63 Permit 0
3905 2d02h
20 17 20.2.1.82 21.2.12.2 19567 63 Permit 0
3905 2d02h

Number of entries: 20
Number of messages logged: 112
Number of packets logged: 11200
Number of packets received for logging: 11200
Router#

```

次に、ロギング IP アクセス リスト設定に関する情報を表示する例を示します。

```

Router# show logging ip access-list config
Logging ip access-list configuration
Maximum number of cached entries: 8192
Logging rate limiter: 0
Log-update interval: 300
Log-update threshold: 0
Configured on input direction:
    Vlan2
    Vlan1
Configured on output direction:
    Vlan2
Router#

```

関連コマンド

コマンド	説明
clear logging ip access-list cache	OAL キャッシュからすべてのエントリをクリアして、Syslog に送信します。
logging ip access-list cache (global configuration mode)	OAL パラメータを設定します。
logging ip access-list cache (interface configuration mode)	方向に基づいてインターフェイス上で OAL ロギング キャッシュをイネーブルにします。

show mac-address-table

MAC アドレス テーブルに関する情報を表示するには、**show mac-address-table** コマンドを使用します。

show mac-address-table

show mac-address-table {**address** *mac-addr*} [**all** | {**interface** *interface interface-number*} | {**vlan** *vlan-id*}]

show mac-address-table aging-time [**vlan** *vlan-id*]

show mac-address-table count [**vlan** *vlan-id*]

show mac-address-table dynamic [{**address** *mac-addr*} | {**interface** *interface interface-number*} | {**vlan** *vlan-id*}]

show mac-address-table {**interface** *interface interface-number*}

show mac-address-table limit [**vlan** *vlan-id* | {**interface** *interface*}]

show mac-address-table multicast [**count** | {{**igmp-snooping** | **mld-snooping**} [**count**]} | {**user** [**count**]} | {**vlan** *vlan-id*}]

show mac-address-table notification {**mac-move** | **threshold**}

show mac-address-table static [{**address** *mac-addr*} | **detail** | {**interface** *interface interface-number*} | {**vlan** *vlan-id*}]

show mac-address-table synchronize statistics

show mac-address-table unicast-flood

show mac-address-table vlan *vlan-id*

シンタックスの説明

address <i>mac-addr</i>	特定の MAC アドレスの MAC アドレス テーブルに関する情報を表示します。フォーマットの注意事項については「使用上のガイドライン」を参照してください。
all	(任意) 転送テーブル内にある、指定された MAC アドレスのすべてのインスタンスを表示します。
interface <i>interface</i>	(任意) 特定のインターフェイス タイプに関する情報を表示します。有効値は ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 atm 、および ge-wan です。
<i>interface-number</i>	モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
vlan <i>vlan-id</i>	(任意) 特定の VLAN に関する情報だけを表示します。有効な値は 1 ~ 4094 です。
aging-time	MAC アドレスのエージング タイムに関する情報を表示します。
count	MAC アドレス テーブル内の現在のエントリ数を表示します。
dynamic	ダイナミック MAC アドレス テーブル エントリに関する情報だけを表示します。

limit	MAC 使用情報を表示します。
multicast	マルチキャスト MAC アドレス テーブル エントリに関する情報だけを表示します。
igmp-snooping	IGMP スヌーピングによって学習されたアドレスを表示します。
mld-snooping	MLDv2 スヌーピングによって学習されたアドレスを表示します。
user	手動で入力された (スタティック) アドレスを表示します。
notification mac-move	MAC 移動通知ステータスを表示します。
notification threshold	CAM テーブル利用通知ステータスを表示します。
static	スタティック MAC アドレス テーブル エントリに関する情報だけを表示します。
synchronize statistics	スイッチ プロセッサで収集された統計に関する情報を表示します。
unicast-flood	ユニキャスト フラッディング情報を表示します。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード 特権 EXEC (#)

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン モジュール番号を指定しないと、**show mac-address-table** コマンドの出力にスーパーバイザ エンジンに関する情報が表示されます。スイッチ プロセッサの MAC アドレス テーブルに関する情報を表示するには、**all** キーワードを入力します。

mac-addr は 48 ビット MAC アドレスです。有効なフォーマットは H.H.H です。

interface-number 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

mac-group-address の有効値は 1 ~ 9 です。

オプションの **count** キーワードは、マルチキャスト エントリ数を表示します。

オプションの **multicast** キーワードは、VLAN 内のマルチキャスト MAC アドレス (グループ) を表示したり、スタティックに導入された、または IGMP スヌーピングによって学習されたレイヤ 2 テーブル内のすべてのエントリを表示したりします。

show mac-address-table unicast-flood コマンドの出力で表示される情報は次のとおりです。

- フィルタ モードの使用を設定されていないすべての VLAN で共有された、最大 50 のフラッディング エントリを記録できます。
- 出力フィールドの表示は、次のように定義されます。

show mac-address-table

- ALERT : 情報は約 3 秒ごとに更新されます。
- SHUTDOWN : 情報は約 3 秒ごとに更新されます。



(注) 宛先 MAC アドレスで表示される情報は、ポートがシャットダウンしてフラッディングが停止するとただちに削除されます。

- 情報はフィルタを導入するたびに更新されます。この情報はフィルタを削除するまで維持されます。

show mac-address-table protocol {assigned | ip | ipx | other} 構文は、Supervisor Engine 720 が搭載された Catalyst 6500 シリーズ スイッチではサポートされていません。

protocol 引数のキーワードの定義は、次のとおりです。

- **assigned** : 割り当てられたプロトコル エントリを指定します。
- **ip** : IP プロトコルを指定します。
- **ipx** : IPX プロトコルを指定します。
- **other** : その他のプロトコル エントリを指定します。

Learn フィールドに表示されるダイナミック エントリは、常に Yes に設定されます。

show mac-address-table limit コマンドの出力は、次の情報を表示します。

- MAC アドレスの現在の数
- 許可された MAC エントリの最大数
- 使用率 (%)

show mac-address-table synchronize statistics コマンドの出力は、次の情報を表示します。

- 各インターバルで処理されるメッセージ数
- 同期化用に送信されるアクティブ エントリの数
- 更新されたエントリ、作成されたエントリ、無視されたエントリ、または失敗したエントリの数

例



(注) 分散 EARL スイッチでは、アスタリスク (*) はこの EARL に対応付けられたポート上で学習された MAC アドレスを示します。

次に、特定の MAC アドレスの MAC アドレス テーブルに関する情報を表示する例を示します (Supervisor Engine 2 が搭載された Catalyst 6500 シリーズ スイッチ)。

```
Router# show mac-address-table address 001.6441.60ca
Codes: * - primary entry
```

```

vlan  mac address      type   learn qos      ports
-----+-----+-----+-----+-----+-----
Supervisor:
* --- 0001.6441.60ca   static No    -- Router
Router#
```

次に、特定の MAC アドレスの MAC アドレス テーブル情報を表示する例を示します (Supervisor Engine 720 が搭載された Catalyst 6500 シリーズ スイッチ)。

```
Router# show mac-address-table address 0100.5e00.0128
Legend: * - primary entry
        age - seconds since last seen
        n/a - not available

      vlan  mac address      type   learn   age           ports
-----+-----+-----+-----+-----+-----
Supervisor:
*   44  0100.5e00.0128    static Yes           -   Fa6/44,Router
*   1   0100.5e00.0128    static Yes           -   Router
Module 9:
*   44  0100.5e00.0128    static Yes           -   Fa6/44,Router
*   1   0100.5e00.0128    static Yes           -   Router
Router#
```

次に、すべての VLAN に現在設定されているエージング タイムを表示する例を示します。

```
Router# show mac-address-table aging-time
Vlan    Aging Time
----    -
*100    300
200     1000
Router#
```

次に、特定のスロットのエントリ数を表示する例を示します。

```
Router# show mac-address-table count slot 1
MAC Entries on slot 1 :
Dynamic Address Count:          4
Static Address (User-defined) Count: 25
Total MAC Addresses In Use:     29
Total MAC Addresses Available:  131072
Router#
```

次に、ダイナミック MAC アドレス エントリをすべて表示する例を示します。

```
Router# show mac-address-table dynamic
Legend: * - primary entry
        age - seconds since last seen
        n/a - not applicable

      vlan  mac address      type   learn   age           ports
-----+-----+-----+-----+-----+-----
*  10  0010.0000.0000    dynamic Yes    n/a          Gi4/1
*   3  0010.0000.0000    dynamic Yes     0           Gi4/2
*   1  0002.fcbc.ac64    dynamic Yes    265         Gi8/1
*   1  0009.12e9.adc0    static  No     -            Router
Router#
```

次に、特定のインターフェイスの MAC アドレス テーブルに関する情報を表示する例を示します (Supervisor Engine 720 が搭載された Catalyst 6500 シリーズ スイッチ)。

```
Router# show mac-address-table interface fastethernet 6/45
Legend: * - primary entry
        age - seconds since last seen
        n/a - not available

      vlan  mac address      type   learn   age           ports
-----+-----+-----+-----+-----+-----
*   45  00e0.f74c.842d    dynamic Yes           5   Fa6/45
Router#
```



(注) 先行アスタリスク (*) は、外部装置から特定のモジュールへの着信パケットに基づいて学習された MAC アドレスからのエントリを示します。

次に、MAC 移動通知ステータスを表示する例を示します。

```
Router# show mac-address-table notification mac-move
MAC Move Notification: Enabled
Router#
```

次に、CAM テーブル利用通知ステータスを表示する例を示します。

```
Router# show mac-address-table notification threshold
Status limit Interval
-----+-----+-----
enabled 1 120
Router#
```

次に、ユニキャスト フラディング情報を表示する例を示します。

```
Router# show mac-address-table unicast-flood
Unicast Flood Protection status: enabled
```

```
Configuration:
vlan Kfps action timeout
-----+-----+-----
2 2 alert none
```

```
Mac filters:
No. vlan souce mac addr. installed
on time left (mm:ss)
```

```
-----+-----+-----+-----+-----+-----
Flood details:
Vlan souce mac addr. destination mac addr.
```

```
-----+-----+-----+-----+-----+-----
2 0000.0000.cafe 0000.0000.bad0, 0000.0000.babe,
0000.0000.bac0
0000.0000.bac2, 0000.0000.bac4,
0000.0000.bac6
0000.0000.bac8
2 0000.0000.caff 0000.0000.bad1, 0000.0000.babf,
0000.0000.bac1
0000.0000.bac3, 0000.0000.bac5,
0000.0000.bac7
0000.0000.bac9
Router#
```

次に、スタティック MAC アドレス エントリをすべて表示する例を示します (Supervisor Engine 2 が搭載された Catalyst 6500 シリーズスイッチ)。

```
Router# show mac-address-table static
Codes: * - primary entry

  vlan  mac address      type   learn qos      ports
-----+-----+-----+-----+-----+-----
* ---  0001.6441.60ca      static No   -- Router

Router#
```

次に、特定の VLAN の MAC アドレス テーブルに関する情報を表示する例を示します。

```
Router# show mac-address-table vlan 100
vlan mac address      type      protocol  qos      ports
-----+-----+-----+-----+-----+-----
100  0050.3e8d.6400    static    assigned  --      Router
100  0050.7312.0cff     dynamic   ip        --      Fa5/9
100  0080.1c93.8040     dynamic   ip        --      Fa5/9
100  0050.3e8d.6400     static    ipx       --      Router
100  0050.3e8d.6400     static    other     --      Router
100  0100.0cdd.dddd     static    other     --      Fa5/9,Router,Switch
100  00d0.5870.a4ff     dynamic   ip        --      Fa5/9
100  00e0.4fac.b400     dynamic   ip        --      Fa5/9
100  0100.5e00.0001     static    ip        --      Fa5/9,Switch
100  0050.3e8d.6400     static    ip        --      Router
Router#
```

次に、MLDv2 スヌーピングの MAC アドレス テーブルに関する情報を表示する例を示します。

```
Router# show mac-address-table multicast mld-snooping
vlan mac address type learn qos ports
-----+-----+-----+-----+-----+-----
--- 3333.0000.0001 static Yes - Switch,Stby-Switch
--- 3333.0000.000d static Yes - Fa2/1,Fa4/1,Router,Switch
--- 3333.0000.0016 static Yes - Switch,Stby-Switch
Router#
```

関連コマンド

コマンド	説明
mac-address-table aging-time	レイヤ 2 テーブルでエントリのエージング タイムを設定します。
mac-address-table limit	MAC 制限をイネーブルにします。
mac-address-table notification mac-move	MAC 移動通知をイネーブルにします。
mac-address-table static	スタティック エントリを MAC アドレス テーブルに追加するか、IGMP スヌーピングをアドレスに対してディセーブルにしてスタティック MAC アドレスを設定します。
mac-address-table synchronize	レイヤ 2 MAC アドレス テーブルのエントリを PFC で同期化します。

show mac-address-table learning

MAC アドレス ラーニング ステートを表示するには、**show mac-address-table learning** コマンドを使用します。

```
show mac-address-table learning [{vlan vlan-id} | {interface interface slot/port}]
[module num]
```

シンタックスの説明

vlan <i>vlan-id</i>	(任意) 指定されたスイッチ ポート VLAN の MAC アドレス ラーニング ステートに関する情報を表示します。有効値は 1 ~ 4094 です。
interface <i>interface slot/port</i>	(任意) 指定されたルーテッド インターフェイス タイプ、スロット番号、およびポート番号の MAC アドレス ラーニング ステートに関する情報を表示します。
module <i>num</i>	(任意) 指定したモジュール番号の MAC アドレス ラーニング ステートに関する情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

スーパーバイザ エンジンだけを指定するには、**module num** キーワードおよび引数を使用します。

interface interface slot/port キーワードおよび引数は、ルーテッド インターフェイスだけで使用できません。**interface interface slot/port** キーワードおよび引数を使用してスイッチ ポート インターフェイスでの学習を設定できません。

vlan vlan-id を指定した場合、すべてのモジュール上の指定した VLAN の MAC アドレス ラーニング ステートがルータ インターフェイスも含めて表示されます。

vlan vlan-id および **module num** を指定した場合は、指定したモジュール上の指定した VLAN の MAC アドレス ラーニング ステートが表示されます。

interface interface slot/port キーワードおよび引数を指定した場合、すべてのモジュール上の指定したインターフェイスの MAC アドレス ラーニング ステートが表示されます。

interface interface slot/port キーワードおよび引数を指定した場合、指定したモジュール上の指定したインターフェイスの MAC アドレス ラーニング ステートが表示されます。

引数もキーワードも指定せずに **show mac-address-table learning** コマンドを入力した場合は、Catalyst 6500 シリーズ スイッチに設定されているすべてのスーパーバイザ エンジン上のすべての既存の VLAN の MAC ラーニング ステートが表示されます。

例 次に、すべてのスーパーバイザ エンジン上のすべての既存 VLAN の MAC アドレス ラーニング ステータスを表示する例を示します。

```
Router# show mac-address-table learning

VLAN/Interface          Mod1   Mod4   Mod7
-----
1                        yes    yes    yes
100                      yes    yes    yes
150                      yes    yes    yes
200                      yes    yes    yes
250                      yes    yes    yes
1006                    no     no     no
1007                    no     no     no
1008                    no     no     no
1009                    no     no     no
1010                    no     no     no
1011                    no     no     no
1012                    no     no     no
1013                    no     no     no
1014                    no     no     no
GigabitEthernet6/1     no     no     no
GigabitEthernet6/2     no     no     no
GigabitEthernet6/4     no     no     no
FastEthernet3/4        no     no     no
FastEthernet3/5        no     no     no
GigabitEthernet4/1     no     no     no
GigabitEthernet4/2     no     no     no
GigabitEthernet7/1     no     no     no
GigabitEthernet7/2     no     no     no
```

Router#

表 2-78 に、この例で表示されるフィールドについて説明します。

表 2-78 show mac-address-table learning のフィールドの説明

フィールド	説明
VLAN/Interface ¹	VLAN ID またはインターフェイス タイプ、モジュール、およびポート番号
Mod#	スーパーバイザ エンジンのモジュール番号
yes	MAC アドレス ラーニングはイネーブルです。
no	MAC アドレス ラーニングはディセーブルです。

1. 表示されるインターフェイスは、内部 VLAN が割り当てられているルーテッドインターフェイスです。

■ show mac-address-table learning

次に、1 台のスーパーバイザ エンジン上のすべての既存の VLAN の MAC アドレス ラーニング ステータスを表示する例を示します。

```
Router# show mac-address-table learning module 4
```

VLAN/Interface	Mod4
1	yes
100	yes
150	yes
200	yes
250	yes
1006	no
1007	no
1008	no
1009	no
1010	no
1011	no
1012	no
1013	no
1014	no
GigabitEthernet6/1	no
GigabitEthernet6/2	no
GigabitEthernet6/4	no
FastEthernet3/4	no
FastEthernet3/5	no
GigabitEthernet4/1	no
GigabitEthernet4/2	no
GigabitEthernet7/1	no
GigabitEthernet7/2	no

```
Router#
```

次に、すべてのスーパーバイザ エンジン上の特定の VLAN の MAC アドレス ラーニング ステータスを表示する例を示します。

```
Router# show mac-address-table learning vlan 100
```

VLAN	Mod1	Mod4	Mod7
100	no	no	yes

```
Router
```

次に、特定のスーパーバイザ エンジン上の特定の VLAN の MAC アドレス ラーニング ステータスを表示する例を示します。

```
Router# show mac-address-table learning vlan 100 module 7
```

VLAN	Mod7
100	yes

```
Router
```

次に、特定のスーパーバイザ エンジンの MAC アドレス ラーニング ステータスを表示する例を示します。

```
Router# show mac-address-table learning interface FastEthernet 3/4
```

Interface	Mod1	Mod4	Mod7
Fa3/4	no	yes	no

```
Router
```

次に、特定のスーパーバイザ エンジン上の特定のインターフェイスの MAC アドレス ラーニング ステータスを表示する例を示します。

```
Router# show mac-address-table learning interface FastEthernet 3/4 module 1
```

```
Interface      Mod1
-----
Fa3/4         no
Router
```

関連コマンド

コマンド	説明
mac-address-table learning	MAC アドレス ラーニングをイネーブルにします。

show memory dead

すでに終了しているプロセスによって割り当てられたメモリの統計情報を表示するには、**show memory dead** コマンドを使用します。

show memory dead [totals]

シンタックスの説明

totals (任意) 終了したプロセスのメモリの合計を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

ユーザ EXEC (>)
特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

show memory dead コマンドは、すでに終了しているプロセスに関する情報を表示します。終了したプロセスは、別のプロセスで割り当てられたメモリとして示されます。

例

次に、**show memory dead** コマンドの出力例を示します。

```
Router# show memory dead

          Head   Total (b)   Used (b)   Free (b)   Lowest (b)   Largest (b)
I/O      600000    2097152    461024    1636128    1635224      1635960

Processor memory

Address  Bytes Prev.   Next   Ref  PrevF  NextF  Alloc PC  What
1D8310   60 1D82C8 1D8378  1                3281FFE  Router Init
2CA964   36 2CA914 2CA9B4  1                3281FFE  Router Init
2CAA04  112 2CA9B4 2CAAA0  1                3A42144  OSPF Stub LSA RBTree
2CAAA0   68 2CAA04 2CAB10  1                3A420D4  Router Init
2ED714   52 2ED668 2ED774  1                3381C84  Router Init
2F12AC   44 2F124C 2F1304  1                3A50234  Router Init
2F1304   24 2F12AC 2F1348  1                3A420D4  Router Init
2F1348   68 2F1304 2F13B8  1                3381C84  Router Init
300C28   340 300A14 300DA8  1                3381B42  Router Init
```

表 2-79 に、この出力で表示される重要なフィールドについて説明します。

表 2-79 show memory dead のフィールドの説明

フィールド	説明
Head	メモリ割り当てチェーンのヘッドの 16 進数表記によるアドレス
Total(b)	使用バイトとフリー バイトの合計
Used(b)	使用中のメモリ容量
Free(b)	未使用のメモリ容量 (バイト単位)
Lowest(b)	起動後のフリー メモリの最小容量 (バイト単位)
Largest(b)	利用可能な最大のフリー ブロックのサイズ (バイト単位)
Address	ブロックの 16 進数表記によるアドレス (バイト単位)
Bytes	ブロックのサイズ (バイト単位)
Prev.	前のブロックのアドレス
Next	次のブロックのアドレス
Ref	そのメモリ ブロックの参照カウント (そのメモリ ブロックを使用しているプロセスの数を示す)
PrevF	前のフリー ブロックのアドレス (フリーの場合)
NextF	次のフリー ブロックのアドレス (フリーの場合)
Alloc PC	ブロックを割り当てたシステム コールのアドレス
What	ブロックを所有しているプロセスの名前。または、ブロックがフラグメント化している場合は「fragment」、ブロックが隣接するフリー ブロックと合体している場合は「coalesced」

show mls asic

ASIC バージョンを表示するには、**show mls asic** コマンドを使用します。

show mls asic

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、ASIC バージョンを表示する例を示します。

```
Router# show mls asic
Earl in Module 2
  Tycho - ver:1 Cisco-id:1C8 Vendor-id:49
Router#
```

show mls cef

MLS ハードウェア レイヤ 3 スイッチング テーブル エントリを表示するには、**show mls cef** コマンドを使用します。

```
show mls cef [ip] [prefix [mask-length | load-info]] [detail] [module number]
```

```
show mls cef [ip] [{lookup ...} | {multicast ...} | {rpf ...} | {vpn ...} | {vrf ...}]
```

```
show mls cef [{adjacency ...} | {block block-number [entries]} | {config-register
reg-address} | {diags [detail]} | {entry index [detail]} | {exact-route ...} | {hardware
[module number]} | {inconsistency ...} | {lookup ...} | {masks [type] [module
number]} | {rpf ...} | {statistics ...} | {summary [module number]} | {tunnel
fragment} | {used-blocks [type] [module number]} | {vpn ...} | {vrf ...}]
```

```
show mls cef [{eom ...} | {ip ...} | {ipv6 ...} | {mpls ...}]
```

シンタックスの説明

ip	(任意) MLS ハードウェア レイヤ 3 スイッチング テーブル内の IPv6 ユニキャスト エントリを表示します。詳細については、「使用上のガイドライン」を参照してください。
prefix	(任意) A.B.C.D のフォーマットによるエントリのプレフィクス
mask-length	(任意) マスクの長さ。有効値は 0 ~ 32 です。
load-info	(任意) 出力の各隣接値の横にハッシュ値を表示します。
detail	(任意) ハードウェアの詳細情報を表示します。詳細については、「使用上のガイドライン」を参照してください。
module number	(任意) 特定のモジュールのエントリに関する情報を表示します。
lookup ...	(任意) MLS ハードウェア レイヤ 3 スイッチング テーブル内の IP エントリを、指定された宛先 IP アドレスについて表示します。 show mls cef lookup コマンドを参照してください。
multicast ...	(任意) MLS ハードウェア レイヤ 3 スイッチング テーブル内の IP エントリを、コンパクト CEF テーブル表示フォーマットで表示します。 show mls cef ip multicast コマンドを参照してください。
rpf ...	(任意) MLS ハードウェア レイヤ 3 スイッチング テーブル内の RPF ハードウェアに関する情報を表示します。 show mls cef rpf コマンドを参照してください。
vpn ...	(任意) VPN ID CEF テーブル情報を表示します。詳細については、「使用上のガイドライン」を参照してください。
vrf ...	(任意) CEF テーブルに関する情報を、指定された VRF 名について表示します。
adjacency ...	(任意) MLS ハードウェア レイヤ 3 スイッチング隣接ノードに関する情報を表示します。 show mls cef adjacency コマンドを参照してください。
blockblock-number	(任意) マスク ブロック利用に関する情報を特定のブロックについて表示します。有効値は 0 ~ 4,294,967,295 です。詳細については、「使用上のガイドライン」を参照してください。
entries	(任意) マスク ブロック利用エントリを表示します。詳細については、「使用上のガイドライン」を参照してください。
config-register reg-address	(任意) ハードウェア コンフィギュレーション レジスタに関する情報を特定のレジスタについて表示します。詳細については、「使用上のガイドライン」を参照してください。

diags	(任意) 診断エントリに関する情報を表示します。詳細については、「使用上のガイドライン」を参照してください。
entry index	(任意) 表示するプレフィクス エントリ インデックスを指定します。有効値は 0 ~ 4,294,967,295 です。詳細については、「使用上のガイドライン」を参照してください。
exact-route ...	(任意) ハードウェア ロード シェアリングに関する情報を表示します。 show mls cef exact-route コマンドを参照してください。
hardware	(任意) ハードウェア情報のサマリーを表示します。詳細については、「使用上のガイドライン」を参照してください。
inconsistency ...	(任意) 一貫性チェッカーに関する情報を表示します。 show mls cef inconsistency コマンドを参照してください。
masks ...	(任意) マスクに関する情報を表示します。詳細については、「使用上のガイドライン」を参照してください。
statistics ...	(任意) スイッチングされたパケット数とバイト数を表示します。 show mls cef statistics コマンドを参照してください。
tunnel fragment	(任意) トンネル フラグメンテーションの動作ステータスを表示します。
summary ...	(任意) ハードウェアのレートのサマリーを各プロトコルについて表示します。 show mls cef summary コマンドを参照してください。
used-blocks	(任意) 使用されているブロックのリストを表示します。詳細については、「使用上のガイドライン」を参照してください。
eom ...	EoM プロトコルに関する情報を表示します。このキーワードはサポートされていません。
ip ...	IP プロトコルに関する情報を表示します。詳細については、「使用上のガイドライン」を参照してください。
ipv6 ...	IPv6 プロトコルに関する情報を表示します。
mpls ...	MPLS に関する情報を表示します。 show mls cef mpls コマンドを参照してください。

コマンドのデフォルト プロトコルを指定しない場合、デフォルト表示は IP およびグローバル CEF テーブルとなります。

コマンド モード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン ... は、追加情報があることを示します。

次のオプションはエキスパート ユーザ向けであり、マニュアルに記載されていません。

- **load-info**
- **detail**
- **block block-number [entries]**
- **config-register reg-address}**

- **diags** [**detail**]
- **entry** *index* [**detail**]
- **hardware** [**module number**]
- **masks** [*type*]
- **used-blocks** [*type*]
- **vpn**

MLS ハードウェア レイヤ 3 スイッチングは IP トラフィックだけに適用されます。

VRF CEF テーブル エントリを表示するには、**show mls cef [ip] vrf** コマンドを使用します。

このコマンドは、スーパーバイザ エンジンまたはスイッチのコンソール上で入力できます。このコマンドを入力するには、**remote login** コマンドを入力して、スーパーバイザ エンジンへのセッションを開始します。

show mls cef コマンドは、次のような 3 つのレベルのオプションを提供します。

- プロトコルに依存しないオプション：次のキーワードはプロトコル固有ではありません。
 - **adjacency**
 - **exact-route**
 - **inconsistency**
 - **module**
 - **rpf**
 - **statistics**
 - **summary**
 - **used-blocks**
 - **vpn**
 - **vrf**
- プロトコルに依存するキーワード：次のキーワードはプロトコルを指定します。
 - **eom**
 - **ip**
 - **ipv6**
 - **mpls**
- デフォルト キーワード：次のキーワードは、**show mls cef** コマンドと **show mls cef ip** コマンドの両方について、同じ出力を表示します。
 - *prefix*
 - **lookup**
 - **multicast**：このキーワードは、Supervisor Engine 720 が搭載されたシステムではサポートされていません。
 - **module**
 - **rpf**
 - **vpn**
 - **vrf**

show mls cef

例

次に、**show mls cef** コマンドと **show mls cef ip** コマンドが同一となる例を示します。

```
Router# show mls cef

Codes: decap - Decapsulation, + - Push Label
Index Prefix Adjacency
64 127.0.0.51/32 punt
65 127.0.0.0/32 punt
66 127.255.255.255/32 punt
67 1.1.1.100/32 punt
68 1.1.1.0/32 punt
69 1.1.1.255/32 punt
70 2.2.2.100/32 punt
71 2.2.2.0/32 punt
72 2.2.2.255/32 punt
73 2.2.2.5/32 Gi5/2, 0000.c005.0205
74 0.0.0.0/32 punt
75 255.255.255.255/32 punt
76 200.1.22.22/32 punt
77 200.0.0.0/32 punt
78 200.255.255.255/32 punt
79 200.1.1.153/32 V130, 0050.808b.8200
81 200.1.1.91/32 V130, 0004.4eef.8800
82 200.1.1.100/32 V130, 00d0.bb02.0400
83 200.12.223.3/32 V130, 00d0.061b.7000
84 200.2.5.3/32 V130, 00d0.061d.200a
85 200.1.1.101/32 V130, 0007.ecfc.e40a
86 200.0.100.1/32 V130, 0050.2a8d.700a
87 200.1.1.104/32 V130, 0050.0f2d.ac00
88 223.255.254.226/32 V130, 0050.2a8d.700a
89 2.2.2.7/32 Gi5/2, 0000.c005.0207
90 1.1.1.5/32 Gi5/1, 0000.0101.0105
3200 224.0.0.0/24 punt
3201 1.1.1.0/24 punt
3202 2.2.2.0/24 punt
134400 200.0.0.0/8 punt
134432 0.0.0.0/0 drop
524256 0.0.0.0/0 drop
Router#
```

次に、MLS ハードウェア レイヤ 3 スイッチング テーブルの IP エントリをすべて表示する例を示します。

```
Router# show mls cef ip

Codes: decap - Decapsulation, + - Push Label
Index Prefix Adjacency
64 127.0.0.51/32 punt
65 127.0.0.0/32 punt
66 127.255.255.255/32 punt
67 1.1.1.100/32 punt
68 1.1.1.0/32 punt
69 1.1.1.255/32 punt
70 2.2.2.100/32 punt
71 2.2.2.0/32 punt
72 2.2.2.255/32 punt
73 2.2.2.5/32 Gi5/2, 0000.c005.0205
74 0.0.0.0/32 punt
75 255.255.255.255/32 punt
76 200.1.22.22/32 punt
77 200.0.0.0/32 punt
78 200.255.255.255/32 punt
79 200.1.1.153/32 V130, 0050.808b.8200
81 200.1.1.91/32 V130, 0004.4eef.8800
```

```

82      200.1.1.100/32      V130,          00d0.bb02.0400
83      200.12.223.3/32     V130,          00d0.061b.7000
84      200.2.5.3/32        V130,          00d0.061d.200a
85      200.1.1.101/32      V130,          0007.ecfc.e40a
86      200.0.100.1/32     V130,          0050.2a8d.700a
87      200.1.1.104/32     V130,          0050.0f2d.ac00
88      223.255.254.226/32 V130,          0050.2a8d.700a
89      2.2.2.7/32          Gi5/2,         0000.c005.0207
90      1.1.1.5/32           Gi5/1,         0000.0101.0105
3200   224.0.0.0/24          punt
3201   1.1.1.0/24           punt
3202   2.2.2.0/24           punt
134400 200.0.0.0/8             punt
134432 0.0.0.0/0             drop
524256 0.0.0.0/0             drop
Router#

```

表 2-80 に、この出力で表示されるフィールドについて説明します。

表 2-80 show mls cef コマンドの出力フィールド

フィールド	説明
Index	MLS ハードウェア レイヤ 3 スイッチング テーブル エントリのインデックスです。最大エントリ数は 256,000 です。
Prefix	エントリのプレフィクス アドレス/マスク
Adjacency	隣接タイプは、次のとおりです。 <ul style="list-style-type: none"> • drop : プレフィクス エントリに一致するパケットが廃棄されます。 • punt : 詳細処理のために PISA にパケットがリダイレクトされます。 • mac-address : プレフィクスに一致するパケットは、特定のネクスト ホップ、または直接添付されている場合は、最終的な宛先ホストに転送されます。

次に、トンネル フラグメンテーションの動作ステータスを表示する例を示します。

```

Router# show mls cef tunnel fragment
Tunnel Fragmentation:      Enabled
Router#

```

関連コマンド

コマンド	説明
show mls cef summary	MLS ハードウェア レイヤ 3 スイッチング テーブル内のルート数を、すべてのプロトコルについて表示します。

show mls cef adjacency

MLS ハードウェア レイヤ 3 スイッチング隣接ノードに関する情報を表示するには、**show mls cef adjacency** コマンドを使用します。

```
show mls cef adjacency [all | decap-tunnel | {encap-tunnel ip-src-addr} | {entry index [to
end-range]} | {flags lower-flag upper-flag} | mac-address number | mac-rewrite |
macv4 | {mpls [label]} | multicast | nat | recirculation | special | tcp | usage] [detail]
[module number]
```

シンタックスの説明

all	(任意) アプリケーションが割り当てられたエントリをすべて表示します。
decap-tunnel	(任意) カプセル化解除されたトンネリング パケット情報を表示します。
encap-tunnel ip-src-addr	(任意) 指定されたアドレスに一致する、カプセル化されたトンネル隣接エントリを表示します。
entry index	(任意) 指定されたインデックスの隣接エントリ情報を表示します。有効値は 0 ~ 1,048,575 です。
to end-range	(任意) 隣接エントリ情報を表示するインデックス範囲を指定します。有効値は 0 ~ 1,048,575 です。
flags	(任意) 指定されたビット フラグに関する情報を表示します。詳細については、「使用上のガイドライン」を参照してください。
lower-flag	表示する下位 32 ビットのフラグ値。有効値は 0 ~ FFFFFFFF です。
upper-flag	表示する上位 32 ビットのフラグ値。有効値は 0 ~ FFFFFFFF です。
mac-address number	(任意) 指定された 48 ビット ハードウェア アドレスについて、対応する隣接 MAC アドレスに関する情報を H.H.H フォーマットで表示します。
mac-rewrite	(任意) MAC 書き換え隣接情報を表示します。
macv4	(任意) MACv4 隣接情報を表示します。
mpls	(任意) MPLS 隣接情報を表示します。
label	(任意) 隣接エントリ情報を表示する MPLS ラベル。有効値は 0 ~ 1048575 です。
multicast	(任意) マルチキャスト隣接情報を表示します。
nat	(任意) NAT 隣接情報を表示します。
recirculation	(任意) 再循環隣接エントリ情報を表示します。
special	(任意) 特別隣接情報を表示します。
tcp	(任意) TCP アプリケーション隣接情報を表示します。
usage	(任意) 隣接使用情報を表示します。
detail	(任意) ハードウェア エントリの詳細を表示します。
module number	(任意) 特定のモジュールの隣接ノードに関する情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

decap-tunnel および **and endcap-tunnel** キーワードは、トンネルノードの表示に使用します。カプセル化ノードはトンネル入口ポイントと見なされ、カプセル化解除ノードはトンネル出口ポイントと見なされます。複数の送信元/宛先ペアが、カプセル化ノードおよびカプセル化解除ノード間の同じトンネルを使用できます。

decap-tunnel および **endcap-tunnel** キーワードは、Supervisor Engine 720 が搭載された Catalyst 6500 シリーズスイッチではサポートされていません。

flags キーワードは、すべての隣接フォーマット (**mac-rewrite**、**mpls**、**multicast** など) に適用され、特定の隣接について隣接設定されたビットを示します。

module number キーワードおよび引数は、モジュールおよびポート番号を指定します。有効値は、使用するシャーシおよびモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 です。

MLS ハードウェア レイヤ 3 スイッチングは IP トラフィックだけに適用されます。

MLS ハードウェア レイヤ 3 スイッチング隣接統計情報は、60 秒間隔で更新されます。

ハードウェアによりスイッチングされる IP 転送ブロードキャスト情報を表示するには、**show mls cef adjacency mac-address number detail** コマンドを入力します。

MLS ハードウェア レイヤ 3 スイッチング FIB エントリごとに、MLS ハードウェアレイヤ 3 スイッチングは隣接ノードの PISA から MLS ハードウェア レイヤ 3 スイッチング隣接テーブルにレイヤ 2 情報を格納します。隣接ノードはレイヤ 2 で直接接続されています。トラフィックを転送するために、MLS ハードウェア レイヤ 3 スイッチングは MLS ハードウェア レイヤ 3 スイッチング FIB エントリから MLS ハードウェア レイヤ 3 スイッチング隣接エントリを示すルートを選択し、この隣接テーブルエントリ内の隣接ノードのレイヤ 2 ヘッダーを使用して、レイヤ 3 スイッチング中にパケットを書き換えます。MLS ハードウェア レイヤ 3 スイッチングは、100 万個の隣接テーブル エントリをサポートします。

例

次に、すべての隣接ノードの情報を表示する例を示します。

```
Router# show mls cef adjacency all

Index: 5      smac: 0000.0000.0000, dmac: 0000.0000.0000
             mtu: 0, vlan: 0, dindex: 0x0, l3rw_vld: 0
             packets: 0, bytes: 0

Index: 32773  smac: 0000.0000.0000, dmac: 0000.0000.0000
             mtu: 0, vlan: 0, dindex: 0x0, l3rw_vld: 0
             packets: 0, bytes: 0
<Output is truncated>
```

次に、特定のインデックスの隣接エントリ情報を表示する例を示します。

```
Router# show mls cef adjacency entry 132

Index: 132    smac: 0000.0000.0000, dmac: 0000.0000.0000
             mtu: 0, vlan: 0, dindex: 0x0, l3rw_vld: 0
             packets: 0, bytes: 0
```

次に、一連のインデックスの隣接エントリ情報を表示する例を示します。

■ show mls cef adjacency

```
Router# show mls cef adjacency entry 132 to 134

Index: 132      smac: 0000.0000.0000, dmac: 0000.0000.0000
                mtu: 0, vlan: 0, dindex: 0x0, l3rw_vld: 0
                packets: 0, bytes: 0

Index: 133      smac: 0000.0000.0000, dmac: 0000.0000.0000
                mtu: 0, vlan: 0, dindex: 0x0, l3rw_vld: 0
                packets: 0, bytes: 0

Index: 134      smac: 0000.0000.0000, dmac: 0000.0000.0000
                mtu: 0, vlan: 0, dindex: 0x0, l3rw_vld: 0
                packets: 0, bytes: 0

Router#
```

次に、再循環隣接情報を表示する例を示します。

```
Router# show mls cef adjacency recirculation detail
Index: 6        smac: 0000.0000.0000, dmac: 0000.0000.0000
                mtu: 65535, vlan: 0, dindex: 0x0, ccc = 110,
                format: RECIR, l3rw_vld: 1

Router#
```

次に、特定のビット フラグを表示する例を示します。

```
Router# show mls cef adjacency flags 8408 0

STAT_REQUIRED NO_STAT CAP1 IQO UTTL UTOS

Router#
```

次に、特定の MAC アドレスの隣接ノード情報を表示する例を示します。

```
Router# show mls cef adjacency mac-address 00e0.f74c.842d

Index: 133138  smac: 00d0.061d.200a, dmac: 00e0.f74c.842d
                mtu: 1518, vlan: 45, dindex: 0x0, l3rw_vld: 1
                packets: 0, bytes: 0

Index: 133144  smac: 00d0.061d.200a, dmac: 00e0.f74c.842d
                mtu: 1518, vlan: 45, dindex: 0x0, l3rw_vld: 1
                packets: 0, bytes: 0

Router#
```

次に、MAC 書き換え隣接情報を表示する例を示します。

```
Router# show mls cef adjacency mac-rewrite

Index: 133132  smac: 0000.0000.0000, dmac: 0000.0000.0000
                mtu: 0, vlan: 0, dindex: 0x0, l3rw_vld: 0
                packets: 0, bytes: 0

Index: 133133  smac: 000a.421f.3000, dmac: 0050.2a8d.700a
                mtu: 1518, vlan: 1, dindex: 0x0, l3rw_vld: 1
                packets: 0, bytes: 0

Index: 133134  smac: 000a.421f.3000, dmac: 0000.7201.0001
                mtu: 1518, vlan: 72, dindex: 0x0, l3rw_vld: 1
                packets: 0, bytes: 0

Index: 133135  smac: 000a.421f.3000, dmac: 0000.7301.0001
                mtu: 1518, vlan: 73, dindex: 0x0, l3rw_vld: 1
                packets: 0, bytes: 0

<Output is truncated>
```

次に、MPLS 隣接情報を表示する例を示します。

```
Router# show mls cef adjacency mpls detail
Index: 32768 smac: 0000.0000.0000, dmac: 0000.0000.0000
mtu: 1514, vlan: 0, dindex: 0x7FFA, l3rw_vld: 1
format: MPLS, flags: 0x1000408600
label0: 0, exp: 0, ovr: 0
label1: 0, exp: 0, ovr: 0
label2: 0, exp: 0, ovr: 0
op: POP
packets: 0, bytes: 0
Router#
```

次に、マルチキャスト隣接情報を表示する例を示します。

```
Router# show mls cef adjacency multicast detail
Index: 22 smac: 0000.0000.0000, dmac: 0000.0000.0000
mtu: 0, vlan: 0, dindex: 0x0, l3rw_vld: 0
format: MULTICAST, flags: 0x800
met2: 0, met3: 0
packets: 2232, bytes: 180684
Router#
```

次に、NAT 隣接情報を表示する例を示します。

```
Router# show mls cef adjacency nat detail
Index: 200 mtu: 1522, vlan: 1063, dindex: 0x7FFA, l3rw_vld: 1
format: NAT, flags: 0x8600
ip_sa: 2.2.2.2, src_port: 100
ip_da: 3.3.3.3, dst_port: 300
delta_seq: 0, delta_ack: 0
packets: 0, bytes: 0
Router#
```

次に、特別隣接情報を表示する例を示します。

```
Router# show mls cef adjacency special

Index: 0          smac: 0000.0000.0000, dmac: 0000.0000.0000
                  mtu: 9234, vlan: 0, dindex: 0x0, l3rw_vld: 0
                  format: MULTICAST, flags: 0x800 (mcast_fib_fail)
                  met2: 0, met3: 0
                  packets: 0, bytes: 0

Index: 1          smac: 0000.0000.0000, dmac: 0000.0000.0000
                  mtu: 9234, vlan: 0, dindex: 0x0, l3rw_vld: 0
                  format: MULTICAST, flags: 0x800 (mcast_fib_rf_cr)
                  met2: 0, met3: 0
                  packets: 0, bytes: 0
```

<Output is truncated>

次に、TCP 隣接情報を表示する例を示します。

```
Router# show mls cef adjacency tcp detail
Index: 200 smac: abcd.abcd.abcd, dmac: 0000.1000.2000
mtu: 1518, vlan: 1063, dindex: 0x0, l3rw_vld: 1
format: MAC_TCP, flags: 0x8408
delta_seq: 10, delta_ack: 0
packets: 0, bytes: 0
Router#
```

次に、隣接使用情報を表示する例を示します。

```
Router# show mls cef adjacency usage

Adjacency Table Size: 1048576
```

■ show mls cef adjacency

```
ACL region usage: 2
Non-stats region usage: 128
Stats region usage: 31
Total adjacency usage: 161
Router#
```

show mls cef exact-route

ハードウェアのロードシェアリングに関する情報を表示するには、**show mls cef exact-route** コマンドを使用します。

```
show mls cef exact-route src-ip {dest-ip | src-l4port} [dest-l4port | {module num}]
```

```
show mls cef exact-route {vrf instance-name} src-ip {dest-ip | src-l4port} [dest-l4port | {module num}]
```

シンタックスの説明

<i>src-ip</i>	送信元 IP アドレス。
<i>dest-ip</i>	宛先 IP アドレス。
<i>src-l4port</i>	レイヤ 4 送信元ポート番号。有効値は 0 ~ 65,535 です。
<i>dest-l4port</i>	(任意) レイヤ 4 宛先ポート番号。有効値は 0 ~ 65,535 です。
module num	(任意) モジュール番号。
vrf instance-name	指定された VRF インスタンス名について VRF の数値 ID を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

vrf instance-name キーワードおよび引数は、Supervisor Engine 2 が搭載された Catalyst 6500 シリーズスイッチではサポートされません。

例

次に、ハードウェアのロードシェアリング情報を表示する例を示します。

```
Router# show mls cef exact-route 172.20.52.16 172.20.52.31
```

```
Interface: Gi2/1, Next Hop: 255.255.255.255, Vlan: 4073, Destination Mac: 00d0.061d.200a
```

```
Router#
```

関連コマンド

コマンド	説明
show ip cef exact-route	送信元/宛先 IP アドレス ペアの厳密なルートを表示します。

show mls cef exception

CEF 例外に関する情報を表示するには、**show mls cef exception** コマンドを表示します。

show mls cef exception {status [detail] | priorities}

シンタックスの説明

status	CEF 例外ステータスに関する情報を表示します。
detail	(任意) ハードウェアの詳細情報を表示します。詳細については、「使用上のガイドライン」を参照してください。
priorities	CEF 例外プライオリティに関する情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

detail キーワードはエキスパート ユーザ向けであり、マニュアルに記載されていません。

show mls cef exception status コマンドの出力には、次の定義が適用されます。

- FALSE : プロトコルが例外の状態でないことを示します。
- TRUE : プロトコルが例外の状態であることを示します。

例

次に、CEF 例外ステータスの詳細情報を表示する例を示します。

```
Router# show mls cef exception status
Current IPv4 FIB exception state = FALSE
Current IPv6 FIB exception state = FALSE
Current MPLS FIB exception state = FALSE
Router#
```

次に、FIB ERM 例外プライオリティを表示する例を示します。

```
Router# show mls cef exception priorities
Priority Protocol
=====
1 IPv4
2 IPv6
3 MPLS
Router#
```

関連コマンド

コマンド	説明
mls erm priority	例外ステータスから回復させるプロトコルの順番を定義するプライオリティを割り当てます。

show mls cef hardware

MLS ハードウェア レイヤ 3 スイッチング テーブル エントリを表示するには、**show mls cef hardware** コマンドを使用します。

show mls cef hardware [*module number*]

シンタックスの説明

module number (任意) 特定のモジュールの隣接ノード情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

MLS ハードウェア レイヤ 3 スイッチングは IP トラフィックだけに適用されます。

例

次に、MLS ハードウェア レイヤ 3 スイッチング テーブルのエントリをすべて表示する例を示します。

```
Router# show mls cef hardware

CEF TCAM v2:
Size:
  65536 rows/device, 4 device(s), 262144 total rows
  32 entries/mask-block
  8192 total blocks (32b wide)
  1212416 s/w table memory
Options:
  sanity check: on
  sanity interval: 301 seconds
  consistency check: on
  consistency interval: 61 seconds
  redistribution: off
    redistribution interval: 120 seconds
    redistribution threshold: 10
  compression: on
    compression interval: 31 seconds
  tcam/ssram shadowing: on
Operation Statistics:
  Entries inserted:          0000000000000024
  Entries deleted:          0000000000000005
  Entries compressed:       0000000000000000
  Blocks inserted:          0000000000000018
  Blocks deleted:           0000000000000004
  Blocks compressed:        0000000000000000
  Blocks shuffled:          0000000000000002
  Blocks deleted for exception: 0000000000000000
```

```
Direct h/w modifications:          0000000000000000

Background Task Statistics:
Consistency Check count:          0000000000014066
Consistency Errors:               0000000000000000
SSRAM Consistency Errors:         0000000000000000
Sanity Check count:               0000000000002855
Sanity Check Errors:              0000000000000000
Compression count:                0000000000004621

Exception Handling status   : on
L3 Hardware switching status : on
Fatal Error Handling Status : Reset
Fatal Errors:               0000000000000000
Fatal Error Recovery Count: 0000000000000000

SSRAM ECC error summary:
Uncorrectable ecc entries   : 0
Correctable ecc entries    : 0
Packets dropped             : 0
Packets software switched  : 0

FIB SSRAM Entry status
-----
Key: UC - Uncorrectable error, C - Correctable error
      SSRAM banks : Bank0   Bank1
No ECC errors reported in FIB SSRAM.
```

show mls cef inconsistency

一貫性チェッカー情報を表示するには、**show mls cef inconsistency** コマンドを使用します。

show mls cef inconsistency [module num | now | records] [detail] [module num]

シンタックスの説明

module num	(任意) 指定されたモジュールの不一致情報を表示します。
now	(任意) 一貫性チェックを実行し、問題があれば表示します。
records	(任意) 不一致の記録を表示します。
detail	(任意) ハードウェア エントリの詳細を表示します。
module num	(任意) 特定のモジュールの隣接ノード情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

show mls cef inconsistency コマンドを引数なしで入力すると、次の情報が表示されます。

- 一貫性チェック カウント
- TCAM 一貫性チェック エラー
- SSRAM 一貫性チェック エラー

例

次に、一貫性チェッカーに関する情報を表示する例を示します。

```
Router# show mls cef inconsistency
Consistency Check Count      : 81
TCAM Consistency Check Errors : 0
SSRAM Consistency Check Errors : 0
Router#
```

次に、特定のモジュールの一貫性チェッカー情報を表示する例を示します。

```
Router# show mls cef inconsistency module 7
Consistency Check Count      : 11033
TCAM Consistency Check Errors : 0
SSRAM Consistency Check Errors : 0
Router#
```

次に、一貫性チェックを実行し、問題があれば表示する例を示します。

```
Router# show mls cef inconsistency now
Performing TCAM check now ...done
No. of FIB TCAM Consistency Check Errors : 0
Performing SSRAM check now ...done
No. of FIB SSRAM Consistency Check Errors : 0
```

Router#

次に、一貫性の記録を表示する例を示します。

```
Router# show mls cef inconsistency records
Consistency Check Count      : 11044
TCAM Consistency Check Errors : 0
SSRAM Consistency Check Errors : 0
```

Router#

show mls cef ip

MLS ハードウェア レイヤ 3 スイッチング テーブル内の IP エントリを表示するには、**show mls cef ip** コマンドを使用します。

show mls cef ip [*prefix* [*mask-length*]] [**detail**] [*module number*]

show mls cef ip accounting per-prefix

show mls cef ip {*lookup ...*} | {**multicast team** ...} | {**rpf** ...} | {**vpn** ...} | {**vrf** ...}

シンタックスの説明

<i>prefix</i>	(任意) A.B.C.D のフォーマットによるエントリのプレフィクス
<i>mask-length</i>	(任意) マスクの長さ。有効値は 0 ~ 32 です。
detail	(任意) ハードウェア エントリの詳細を表示します。
<i>module number</i>	(任意) 特定のモジュールのエントリを表示します。
accounting per-prefix	統計情報の収集のために設定されたプレフィクスをすべて表示します。
lookup ...	指定された宛先 IP ユニキャストアドレスの TCAM エントリ インデックスを表示します。 show mls cef lookup コマンドを参照してください。
multicast team ...	MLS ハードウェア レイヤ 3 スイッチング テーブル内の IP エントリを、コンパクト CEF テーブル表示フォーマットで表示します。詳細については、「使用上のガイドライン」を参照してください。
rpf ...	MLS ハードウェア レイヤ 3 スイッチング テーブル内の RPF ハードウェア情報を表示します。 show mls cef rpf コマンドを参照してください。
vpn ...	(任意) VPN ID CEF テーブルの情報を表示します。詳細については、「使用上のガイドライン」を参照してください。
vrf ...	VPN インスタンス CEF テーブルに関する情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドの詳細については、**show mls cef ip multicast team** コマンドの項を参照してください。

... は、追加情報があることを示します。

vpn キーワードはエキスパート ユーザ向けであり、マニュアルに記載されていません。

show mls cef ip コマンド出力の情報は、**show mls cef** コマンドの出力にも表示されます。

検索は「最長プレフィクス一致」として実行され、指定された宛先 IP アドレスに適用される TCAM エントリ インデックスが表示されます。

情報は、インデックス、プレフィクス、マスク、隣接のフォーマットで出力されます。

例

次に、**show mls cef** コマンドと **show mls cef ip** コマンドが同一となる例を示します。

```
Router# show mls cef

Codes: decap - Decapsulation, + - Push Label
Index  Prefix                Adjacency
64     127.0.0.51/32         punt
65     127.0.0.0/32          punt
66     127.255.255.255/32   punt
67     1.1.1.100/32         punt
68     1.1.1.0/32           punt
69     1.1.1.255/32         punt
70     2.2.2.100/32         punt
71     2.2.2.0/32           punt
72     2.2.2.255/32         punt
73     2.2.2.5/32           Gi5/2,          0000.c005.0205
74     0.0.0.0/32           punt
75     255.255.255.255/32   punt
76     200.1.22.22/32       punt
77     200.0.0.0/32         punt
78     200.255.255.255/32   punt
79     200.1.1.153/32       V130,          0050.808b.8200
81     200.1.1.91/32        V130,          0004.4eef.8800
82     200.1.1.100/32       V130,          00d0.bb02.0400
83     200.12.223.3/32      V130,          00d0.061b.7000
84     200.2.5.3/32         V130,          00d0.061d.200a
85     200.1.1.101/32       V130,          0007.ecfc.e40a
86     200.0.100.1/32       V130,          0050.2a8d.700a
87     200.1.1.104/32       V130,          0050.0f2d.ac00
88     223.255.254.226/32   V130,          0050.2a8d.700a
89     2.2.2.7/32           Gi5/2,          0000.c005.0207
90     1.1.1.5/32           Gi5/1,          0000.0101.0105
3200   224.0.0.0/24         punt
3201   1.1.1.0/24           punt
3202   2.2.2.0/24           punt
134400 200.0.0.0/8          punt
134432 0.0.0.0/0            drop
524256 0.0.0.0/0            drop
Router#
```

次に、MLS ハードウェア レイヤ 3 スイッチング テーブルの IP エントリをすべて表示する例を示します。

```
Router# show mls cef ip

Codes: decap - Decapsulation, + - Push Label
Index  Prefix                Adjacency
64     127.0.0.51/32         punt
65     127.0.0.0/32          punt
66     127.255.255.255/32   punt
67     1.1.1.100/32         punt
68     1.1.1.0/32           punt
69     1.1.1.255/32         punt
70     2.2.2.100/32         punt
71     2.2.2.0/32           punt
72     2.2.2.255/32         punt
73     2.2.2.5/32           Gi5/2,          0000.c005.0205
74     0.0.0.0/32           punt
```

show mls cef ip

```

75    255.255.255.255/32  punt
76    200.1.22.22/32     punt
77    200.0.0.0/32      punt
78    200.255.255.255/32 punt
79    200.1.1.153/32    V130,          0050.808b.8200
81    200.1.1.91/32     V130           0004.4eef.8800
82    200.1.1.100/32    V130           00d0.bb02.0400
83    200.12.223.3/32   V130           00d0.061b.7000
84    200.2.5.3/32      V130           00d0.061d.200a
85    200.1.1.101/32    V130           0007.ecfc.e40a
86    200.0.100.1/32    V130           0050.2a8d.700a
87    200.1.1.104/32    V130           0050.0f2d.ac00
88    223.255.254.226/32 V130           0050.2a8d.700a
89    2.2.2.7/32        Gi5/2          0000.c005.0207
90    1.1.1.5/32         Gi5/1          0000.0101.0105
3200  224.0.0.0/24        punt
3201  1.1.1.0/24         punt
3202  2.2.2.0/24         punt
134400 200.0.0.0/8         punt
134432 0.0.0.0/0         drop
524256 0.0.0.0/0         drop
Router#

```

表 2-81 に、この出力で表示されるフィールドについて説明します。

表 2-81 show mls cef ip コマンドの出力フィールド

フィールド	説明
Index	MLS ハードウェア レイヤ 3 スイッチング テーブル エントリのインデックスです。最大エントリ数は 256,000 です。
Prefix	エントリのプレフィクス アドレス/マスク
Adjacency	隣接情報

次に、詳細な MLS ハードウェア レイヤ 3 スイッチング テーブルのエントリを表示する例を示します。

```
Router# show mls cef ip 127.0.0.52 detail
```

```

Codes: M - mask entry, V - value entry, A - adjacency index, P - priority bit
       D - full don't switch, m - load balancing modnumber, B - BGP Bucket sel
       V0 - Vlan 0,C0 - don't comp bit 0,V1 - Vlan 1,C1 - don't comp bit 1
       RVTEN - RPF Vlan table enable, RVTSEL - RPF Vlan table select
Format: IPV4_DA - (8 | xtag vpn pi cr recirc tos prefix)
Format: IPV4_SA - (9 | xtag vpn pi cr recirc prefix)
M(194   ): E | 1 FFF  0 0 0 0   255.255.255.255
V(194   ): 8 | 1 0   0 0 0 0   127.0.0.52           (A:133120 ,P:1,D:0,m:0 ,B:0)
Router#

```

次に、統計情報の収集のために設定されたプレフィクスをすべて表示する例を示します。

```

Router# show mls cef ip accounting per-prefix
      VRF                Prefix/Mask                Packets                Bytes

A - Active, I - Inactive
Router#

```

関連コマンド

コマンド	説明
show mls cef	MLS ハードウェア レイヤ 3 スイッチング テーブル エントリを表示します。

show mls cef ip multicast

スイッチ プロセッサ上のマルチレイヤ スイッチング (MLS) ハードウェア レイヤ 3 スイッチング テーブル内の IP エントリを表示するには、**show mls cef ip multicast** コマンドを使用します。

```
show mls cef ip multicast {bidir | grp-only | source source-ip} [detail | group group-id |
vlan rpf-vlanid]
```

```
show mls cef ip multicast control [detail | prefix prefix | vlan rpf-vlanid]
```

```
show mls cef ip multicast group group-id [detail | vlan rpf-vlanid]
```

```
show mls cef ip multicast src-grp [detail | group group-ip | source | vlan rpf-vlanid]
```

```
show mls cef ip multicast subnet [detail | prefix prefix | vlan rpf-vlanid]
```

```
show mls cef ip multicast summary [vpn-num]
```

```
show mls cef ip multicast tcam [prefix [mask]] [detail] [module num] [vrf src-ip {src-port
| dst-ip} [dst-port | module num]]
```

```
show mls cef ip multicast {grp-mask | vlan rpf-vlanid | vpn vpn-id} [detail]
```

シンタックスの説明

bidir	Bidir 情報を表示します。
grp-only	(*G) ショートカットに基づくハードウェア エントリ情報を表示します。詳細については、「使用上のガイドライン」を参照してください。
source source-ip	指定された送信元 IP アドレスに基づくハードウェア エントリ情報を表示します。
detail	(任意) ハードウェア エントリの詳細を表示します。
group group-id	(任意) 指定されたグループ IP アドレスに基づくハードウェア エントリ情報を表示します。
vlan rpf-vlanid	(任意) 特定の RPF VLAN ID の情報を表示します。有効値は 0 ~ 4095 です。
control	(任意) (*G/m) エントリに基づくハードウェア エントリ情報を表示します。詳細については、「使用上のガイドライン」を参照してください。
prefix prefix	(任意) IP サブネット プレフィクスに基づくハードウェア エントリ情報を表示します。
src-grp	(S,G) ショートカットに基づくハードウェア エントリ情報を表示します。詳細については、「使用上のガイドライン」を参照してください。
subnet	(S/m,*) ショートカットに基づくハードウェア エントリ情報を表示します。詳細については、「使用上のガイドライン」を参照してください。
summary	導入済みのハードウェア ショートカットのサマリーを表示します。
tcam	CEF テーブル情報をコンパクト フォーマットで表示します。詳細については、「使用上のガイドライン」を参照してください。
mask	(任意) 指定されたサブネット マスクに基づくハードウェア エントリ情報を表示します。
vrf src-ip	(任意) 指定された送信元 IP アドレスの数値 VRF ID を表示します。
src-port	(任意) レイヤ 4 送信元ポート。有効値は 0 ~ 65,535 です。
dst-ip	(任意) 宛先 IP アドレス。
dst-port	(任意) レイヤ 4 宛先ポート。有効値は 0 ~ 65,535 です。

grp-mask	Bidir (*,G/m) ショートカットに基づくハードウェア エントリ情報を表示します。
vpn vpn-id	指定された VPN ID に基づくハードウェア エントリ情報を表示します。有効値は 0 ~ 4095 です。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン MMLS モードには入力と出力の 2 つがあります。表示される出力はモードごとに異なります。

ハードウェア エントリのタイプは次のとおりです。

- {S/m,*} : 直接接続された送信元のキャッチに使用するインターフェイス/マスク (またはサブネット) エントリ
- {*,G/m} : ルート プロセッサによってグループ/マスクとして提供されるグループ
- {G,C} : G は IP マルチキャスト アドレスに基づく宛先 MAC アドレスを示し、C は入力 VLAN を示します。
- {S,G,C} : S は送信元 IP アドレスを示し、G はマルチキャスト アドレスである宛先 IP アドレスを示し、C は通常、フローの RPF VLAN である入力 VLAN を示します。
- {S,G} : ソフトウェアにより保持されるマルチキャスト ルーティング テーブル エントリ、または FIB テーブル内で作成されるマルチキャスト転送テーブル エントリです。
- {*,G} : 送信元アドレスがワイルドカードであることを除き、{S,G} と同じです。

DF インデックス フィールドは 1 ~ 4 の範囲で、アクセプタンス (PIM ルート プロセッサ × DF) テーブルへのインデックスです。アクセプタンス テーブルは DF 転送で使用され、一連の DF インターフェイスを VPN 内の各 4 つの RP について特定するために使用されます。

例 次に、Bidir (*,G/m) ショートカットに基づく入力ハードウェア エントリの情報を表示する例を示します。

```
Router# show mls cef ip multicast grp-mask
```

```
Multicast CEF Entries for VPN#0
Flags: R - Control, S - Subnet, B - Bidir, C - Complete, P - Partial,
       c - Central Rewrite, p - Primary Input, r - Recirculation
Source/mask      Destination/mask  RPF/DF  Flags #packets      #bytes
rwinde  Output Vlan/Info
-----+-----+-----+-----+-----+-----+-----+
-----+-----+-----+-----+-----+-----+-----+
*                226.2.2.0/24      Df0    BCp    0          0          -
Vl150 [1 oifs]
*                225.2.2.0/24      Df1    BCp    0          0          -
Vl151 [1 oifs]
```

```
*
          227.2.2.0/24          Df1    BCp    0          0          -
Vl51 [1 oifs]
Found 3 entries. 3 are mfd entries
Router#
```

次に、Bidir (*,G/m) ショートカットに基づく入力ハードウェア エントリの詳細情報を表示する例を示します。

```
Router# show mls cef ip multicast grp-mask detail
(*, 226.2.2.0/24)
  PI:1 (1) CR:0 (0) Recirc:0 (1)
  DFidx:0 AdjPtr:7,32775,65543,98311 FibRpfNf:0 FibRpfDf:0 FibAddr:0x100
  rwlans:0 rwindex:0x0 adjmac:0006.d606.e240 rdt:0 E:0 CAP1:0
  fmt:mcast l3rwvld:1 DM:0 mtu:1518 rwtype:L3 met2:0x0 met3:0x5
  packets:000000000000 bytes:000000000000000000
  Starting Offset: 0x0005
  V E C: 50 I:0x00449

(*, 225.2.2.0/24)
  PI:1 (1) CR:0 (0) Recirc:0 (1)
  DFidx:1 AdjPtr:8,32776,65544,98312 FibRpfNf:0 FibRpfDf:0 FibAddr:0x102
  rwlans:0 rwindex:0x0 adjmac:0006.d606.e240 rdt:0 E:0 CAP1:0
  fmt:mcast l3rwvld:1 DM:0 mtu:1518 rwtype:L3 met2:0x0 met3:0x6
  packets:000000000000 bytes:000000000000000000
  Starting Offset: 0x0006
  V E C: 51 I:0x0044B

(*, 227.2.2.0/24)
  PI:1 (1) CR:0 (0) Recirc:0 (1)
  DFidx:1 AdjPtr:19,32787,65555,98323 FibRpfNf:0 FibRpfDf:0 FibAddr:0x104
  rwlans:0 rwindex:0x0 adjmac:0006.d606.e240 rdt:0 E:0 CAP1:0
  fmt:mcast l3rwvld:1 DM:0 mtu:1518 rwtype:L3 met2:0x0 met3:0x7
  packets:000000000000 bytes:000000000000000000
  Starting Offset: 0x0007
  V E C: 51 I:0x0044B
```

```
Found 3 entries. 3 are mfd entries
Router#
```

次に、入力 Bidir 情報を表示する例を示します。

```
Router# show mls cef ip multicast bidir

Multicast CEF Entries for VPN#0
Flags: R - Control, S - Subnet, B - Bidir, C - Complete, P - Partial,
       c - Central Rewrite, p - Primary Input, r - Recirculation
Source/mask      Destination/mask    RPF/DF  Flags #packets      #bytes
rwindex  Output Vlans/Info
+-----+-----+-----+-----+-----+-----+-----+
-----+-----+-----+-----+-----+-----+-----+
*          225.2.2.2/32          Df1    BCp    0          0          -
Vl51,Vl30 [2 oifs]
*          225.2.2.1/32          Df1    BCp    0          0          -
Vl51,Vl30 [2 oifs]
Found 2 entries. 2 are mfd entries
Router#
```

次に、入力 Bidir の詳細情報を表示する例を示します。

```
Router# show mls cef ip multicast bidir detail

(*, 225.2.2.2)
  PI:1 (1) CR:0 (0) Recirc:0 (1)
  DFidx:1 AdjPtr:10,32778,65546,98314 FibRpfNf:0 FibRpfDf:0 FibAddr:0x0E2
```

show mls cef ip multicast

```

rwlans:0 rwindex:0x0 adjmac:0006.d606.e240 rdt:0 E:0 CAP1:0
fmt:mcast l3rwlvd:1 DM:0 mtu:1518 rwtype:L3 met2:0x0 met3:0xA
packets:000000000000 bytes:000000000000000000
Starting Offset: 0x000A
  V C:  51 I:0x004B5 P->19A0
- V
  V E C: 30 I:0x0049B
    
```

```

(*, 225.2.2.1)
PI:1 (1) CR:0 (0) Recirc:0 (1)
DFidx:1 AdjPtr:9,32777,65545,98313 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE0
rwlans:0 rwindex:0x0 adjmac:0006.d606.e240 rdt:0 E:0 CAP1:0
fmt:mcast l3rwlvd:1 DM:0 mtu:1518 rwtype:L3 met2:0x0 met3:0x8
packets:000000000000 bytes:000000000000000000
Starting Offset: 0x0008
  V C:  51 I:0x004B1 P->199C
- V
  V E C: 30 I:0x00499
    
```

Found 2 entries. 2 are mfd entries
Router#

次に、Bidir (*,G/m) ショートカットに基づく出力ハードウェア エントリの情報を表示する例を示します。

Router# **show mls cef ip multicast grp-mask**

```

Multicast CEF Entries for VPN#0
Flags: R - Control, S - Subnet, B - Bidir, C - Complete, P - Partial,
       c - Central Rewrite, p - Primary Input, r - Recirculation
Source/mask      Destination/mask  RPF/DF  Flags #packets  #bytes
rwindex  Output Vlans/Info
+-----+-----+-----+-----+-----+-----+-----+
-----+-----+-----+-----+-----+-----+-----+
*           225.2.2.0/24      Df0    BCp  0          0          -
*           225.2.2.0/24      -      Bpr  0          0
0x4AE  V151 [1 oifs]
*           225.2.2.0/24      -      Br   0          0
0x40E  V151 [1 oifs]
*           226.2.2.0/24      Df1    BCp  0          0          -
*           226.2.2.0/24      -      Bpr  0          0
0x4AE  V150 [1 oifs]
*           226.2.2.0/24      -      Br   0          0
0x40E  V150 [1 oifs]
*           227.2.2.0/24      Df0    BCp  0          0          -
*           227.2.2.0/24      -      Bpr  0          0
0x4AE  V151 [1 oifs]
*           227.2.2.0/24      -      Br   0          0
0x40E  V151 [1 oifs]
    
```

Found 3 entries. 3 are mfd entries
Router#

次に、Bidir (*,G/m) ショートカットに基づく出力ハードウェア エントリの詳細情報を表示する例を示します。

Router# **show mls cef ip multicast grp-mask detail**

```

(*, 225.2.2.0/24)
PI:1 (1) CR:0 (0) Recirc:0 (1)
DFidx:0 AdjPtr:7,32775,65543,98311 FibRpfNf:0 FibRpfDf:0 FibAddr:0x120
rwlans:0 rwindex:0x0 rdt:0 E:0 CAP1:0
fmt:recir l3rwlvd:1 DM:0 mtu:1522 rwtype:RECIR
packets:000000000000 bytes:000000000000000000

PI:1 (1) CR:0 (0) Recirc:1 (1)
    
```

```
AdjPtr:8,32776,65544,98312 FibRpfNf:0 FibRpfDf:0 FibAddr:0x122
rwlans:0 rwindeX:0x4AE adjmac:0006.d606.e240 rdt:1 E:1 CAP1:0
fmt:mcast l3rwlD:1 DM:0 mtu:1522 rWtype:L3 met2:0x0 met3:0x5
packets:000000000000 bytes:000000000000000000
Starting Offset: 0x0005
V E C: 51 I:0x0044C

PI:0 (1) CR:0 (0) Recirc:1 (1)
AdjPtr:9,32777,65545,98313 FibRpfNf:0 FibRpfDf:0 FibAddr:0x124
rwlans:0 rwindeX:0x40E adjmac:0006.d606.e240 rdt:1 E:0 CAP1:0
fmt:mcast l3rwlD:1 DM:0 mtu:1522 rWtype:L3 met2:0x0 met3:0x5
packets:000000000000 bytes:000000000000000000
Starting Offset: 0x0005
V E C: 51 I:0x0044C

(*, 226.2.2.0/24)
PI:1 (1) CR:0 (0) Recirc:0 (1)
DFidx:1 AdjPtr:10,32778,65546,98314 FibRpfNf:0 FibRpfDf:0 FibAddr:0x126
rwlans:0 rwindeX:0x0 rdt:0 E:0 CAP1:0
fmt:recir l3rwlD:1 DM:0 mtu:1522 rWtype:RECIR
packets:000000000000 bytes:000000000000000000

PI:1 (1) CR:0 (0) Recirc:1 (1)
AdjPtr:11,32779,65547,98315 FibRpfNf:0 FibRpfDf:0 FibAddr:0x128
rwlans:0 rwindeX:0x4AE adjmac:0006.d606.e240 rdt:1 E:1 CAP1:0
fmt:mcast l3rwlD:1 DM:0 mtu:1522 rWtype:L3 met2:0x0 met3:0x1C
packets:000000000000 bytes:000000000000000000
Starting Offset: 0x001C
V E C: 50 I:0x00447

PI:0 (1) CR:0 (0) Recirc:1 (1)
AdjPtr:12,32780,65548,98316 FibRpfNf:0 FibRpfDf:0 FibAddr:0x12A
rwlans:0 rwindeX:0x40E adjmac:0006.d606.e240 rdt:1 E:0 CAP1:0
fmt:mcast l3rwlD:1 DM:0 mtu:1522 rWtype:L3 met2:0x0 met3:0x1C
packets:000000000000 bytes:000000000000000000
Starting Offset: 0x001C
V E C: 50 I:0x00447

(*, 227.2.2.0/24)
PI:1 (1) CR:0 (0) Recirc:0 (1)
DFidx:0 AdjPtr:13,32781,65549,98317 FibRpfNf:0 FibRpfDf:0 FibAddr:0x12C
rwlans:0 rwindeX:0x0 rdt:0 E:0 CAP1:0
fmt:recir l3rwlD:1 DM:0 mtu:1522 rWtype:RECIR
packets:000000000000 bytes:000000000000000000

PI:1 (1) CR:0 (0) Recirc:1 (1)
AdjPtr:14,32782,65550,98318 FibRpfNf:0 FibRpfDf:0 FibAddr:0x12E
rwlans:0 rwindeX:0x4AE adjmac:0006.d606.e240 rdt:1 E:1 CAP1:0
fmt:mcast l3rwlD:1 DM:0 mtu:1522 rWtype:L3 met2:0x0 met3:0x1D
packets:000000000000 bytes:000000000000000000
Starting Offset: 0x001D
V E C: 51 I:0x0044C

PI:0 (1) CR:0 (0) Recirc:1 (1)
AdjPtr:15,32783,65551,98319 FibRpfNf:0 FibRpfDf:0 FibAddr:0x130
rwlans:0 rwindeX:0x40E adjmac:0006.d606.e240 rdt:1 E:0 CAP1:0
fmt:mcast l3rwlD:1 DM:0 mtu:1522 rWtype:L3 met2:0x0 met3:0x1D
packets:000000000000 bytes:000000000000000000
Starting Offset: 0x001D
V E C: 51 I:0x0044C

Found 3 entries. 3 are mfd entries
Router#
```

show mls cef ip multicast

次に、出力 Bidir 情報を表示する例を示します。

```
Router# show mls cef ip multicast bidir

Multicast CEF Entries for VPN#0
Flags: R - Control, S - Subnet, B - Bidir, C - Complete, P - Partial,
       c - Central Rewrite, p - Primary Input, r - Recirculation
Source/mask      Destination/mask   RPF/DF  Flags #packets      #bytes
rwinde   Output Vlan/Info
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
*           225.2.2.2/32      Df0    BCp  0           0           -
*           225.2.2.2/32      -      Bpr  0           0
0x4AE   V151,V130 [2 oifs]
*           225.2.2.2/32      -      Br   0           0
0x40E   V151,V130 [2 oifs]
*           225.2.2.1/32      Df0    BCp  0           0           -
*           225.2.2.1/32      -      Bpr  0           0
0x4AE   V151,V130 [2 oifs]
*           225.2.2.1/32      -      Br   0           0
0x40E   V151,V130 [2 oifs]

Found 2 entries. 2 are mfd entries
Router#
```

次に、出力 Bidir の詳細情報を表示する例を示します。

```
Router# show mls cef ip multicast bidir detail

(*, 225.2.2.2)
  PI:1 (1) CR:0 (0) Recirc:0 (1)
  DFidx:0 AdjPtr:19,32787,65555,98323 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE6
  rwlans:0 rwinde:0x0 rdt:0 E:0 CAP1:0
  fmt:recir l3rwlvd:1 DM:0 mtu:1522 rwtype:RECIR
  packets:0000000000000 bytes:00000000000000000

  PI:1 (1) CR:0 (0) Recirc:1 (1)
  AdjPtr:20,32788,65556,98324 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE8
  rwlans:0 rwinde:0x4AE adjmac:0006.d606.e240 rdt:1 E:1 CAP1:0
  fmt:mcast l3rwlvd:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x22
  packets:0000000000000 bytes:00000000000000000
  Starting Offset: 0x0022
  V C: 51 I:0x004B3 P->24
  V E C: 30 I:0x004B6

  PI:0 (1) CR:0 (0) Recirc:1 (1)
  AdjPtr:21,32789,65557,98325 FibRpfNf:0 FibRpfDf:0 FibAddr:0xEA
  rwlans:0 rwinde:0x40E adjmac:0006.d606.e240 rdt:1 E:0 CAP1:0
  fmt:mcast l3rwlvd:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x22
  packets:0000000000000 bytes:00000000000000000
  Starting Offset: 0x0022
  V C: 51 I:0x004B3 P->24
  V E C: 30 I:0x004B6

(*, 225.2.2.1)
  PI:1 (1) CR:0 (0) Recirc:0 (1)
  DFidx:0 AdjPtr:16,32784,65552,98320 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE0
  rwlans:0 rwinde:0x0 rdt:0 E:0 CAP1:0
  fmt:recir l3rwlvd:1 DM:0 mtu:1522 rwtype:RECIR
  packets:0000000000000 bytes:00000000000000000

  PI:1 (1) CR:0 (0) Recirc:1 (1)
  AdjPtr:17,32785,65553,98321 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE2
  rwlans:0 rwinde:0x4AE adjmac:0006.d606.e240 rdt:1 E:1 CAP1:0
```

```
fmt:mcast l3rwvld:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x1E
packets:00000000000000 bytes:000000000000000000
Starting Offset: 0x001E
  V C:  51 I:0x004AF P->20
  V E C: 30 I:0x004B2
```

```
PI:0 (1) CR:0 (0) Recirc:1 (1)
AdjPtr:18,32786,65554,98322 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE4
rwvlans:0 rwindex:0x40E adjmac:0006.d606.e240 rdt:1 E:0 CAP1:0
fmt:mcast l3rwvld:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x1E
packets:00000000000000 bytes:000000000000000000
Starting Offset: 0x001E
  V C:  51 I:0x004AF P->20
  V E C: 30 I:0x004B2
```

```
Found 2 entries. 2 are mfd entries
Router#
```

次に、TCAM 情報を表示する例を示します。

```
Router# show mls cef ip multicast tcam
```

Index	Group	Source	RPF/DF	Interface
64	224.0.1.39	0.0.0.0		NULL
66	224.0.1.40	0.0.0.0		NULL
96	224.0.0.0	0.0.0.0		NULL

```
Router#
```

show mls cef ipv6

ハードウェア IPv6 スイッチング テーブル エントリを表示するには、**show mls cef ipv6** コマンドを使用します。

```
show mls cef ipv6 [vrf-number] [ip-address/mask] [accounting per-prefix] [module number]
```

```
show mls cef ipv6 exact-route src-addr [L4-src-port] dst-addr [L4-dst-port]
```

```
show mls cef ipv6 multicast tcam [v6mcast-address] [detail] [internal]
```

シンタックスの説明

<i>vrf-number</i>	(任意) VRF 番号。有効値は 0 ~ 4095 です。
<i>ip-address/mask</i>	(任意) エントリの IPv6 アドレスおよびプレフィクス マスクを指定します。フォーマットの詳細については、「使用上のガイドライン」を参照してください。
accounting per-prefix	(任意) プレフィクス単位のアカウントリング統計情報を表示します。
module number	(任意) 特定のモジュールのエントリを表示します。
exact-route <i>src-addr</i>	ハードウェアのロードシェアリング結果を表示するには、送信元 IP アドレスを指定します。
<i>L4-src-port</i>	(任意) レイヤ 4 送信元ポート番号。有効値は 0 ~ 65,535 です。
<i>dst-addr</i>	宛先 IP アドレス。
<i>L4-dst-port</i>	(任意) レイヤ 4 宛先ポート番号。有効値は 0 ~ 65,535 です。
multicast tcam	IPv6 マルチキャスト エントリを表示します。
<i>v6mcast-address</i>	(任意) IPv6 マルチキャスト アドレス。
detail	(任意) ハードウェアの詳細情報を表示します。
internal	(任意) 内部ハードウェア情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドを入力できるのは、スーパーバイザ エンジンおよび MLS ハードウェア レイヤ 3 スイッチング モジュール コンソール上だけです。このコマンドを入力するには、**remote login** コマンドを入力して、スーパーバイザ エンジンへのセッションを開始します。

ip-address/mask 引数を入力する場合は、*X:X:X:X::X/mask* のフォーマットを使用します。ここでは、*mask* の有効値は 0 ~ 128 です。

最大 64 の IPv6 プレフィクスがサポートされています。

ロードシェアリング モードがフルに設定されている場合、たとえば、レイヤ 4 ポートがロードシェアリング ハッシュ アルゴリズムに含まれる場合などは、*L4-src-port* および *L4-dst-port* 引数を入力する必要があります。

例

次に、ハードウェア IPv6 スイッチング テーブル エントリを表示する例を示します。

```
Router# show mls cef ipv6
Codes:M-MPLS encap, + - Push label
Index Prefix Adjacency
524384 BEEF:6::6/128 punt
524386 5200::6/128 punt
524388 2929::6/128 punt
524390 6363::30/128 Fa1/48 , 0000.0001.0002
524392 3FFE:1B00:1:1:0:5EFE:1B00:1/128 punt
524394 2002:2929:6:2::6/128 punt
524396 2002:2929:6:1::6/128 punt
524398 6363::6/128 punt
524416 BEEF:6::/64 drop
524418 5200::/64 punt
524420 2929::/64 punt
524422 2002:2929:6:2::/64 punt
524424 2002:2929:6:1::/64 punt
524426 6363::/64 punt
524428 3FFE:1B00:1:1::/64 Tu4 , V6 auto-tunnel
524448 FEE0::/11 punt
524480 FE80::/10 punt
524512 FF00::/8 punt
524544 ::/0 drop
Router#
```

次に、IPv6 エントリを特定の IPv6 アドレスおよびマスクについて表示する例を示します。

```
Router# show mls cef ipv6 2001:4747::/64

Codes:R - Recirculation, I-IP encap
M-MPLS encap, + - Push label
Index Prefix Out i/f Out Label
160 2001:4747::/64 punt
Router#
```

次に、プレフィクス単位の統計情報を利用できる IPv6 FIB エントリをすべて表示する例を示します。

```
Router# show mls cef ipv6 accounting per-prefix
(I) BEEF:2::/64: 0 packets, 0 bytes

A - Active, I - Inactive
Router#
```

次に、ハードウェアの詳細情報を表示する例を示します。

```
Router# show mls cef ipv6 detail

Codes: M - mask entry, V - value entry, A - adjacency index, P - FIB Priority
D - FIB Don't short-cut, m - mod-num
Format: IPv6_DA - (C | xtag vpn uvo prefix)
M(128 ): F | 1 FF 1 FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
V(128 ): C | 1 0 1 2001:4747::1253 (A:12 ,P:1,D:0,m:0 )
M(160 ): F | 1 FF 1 FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
```

■ show mls cef ipv6

```

V(160 ): C | 1 0 1 2001:4747:: (A:11 ,P:1,D:0,m:0 )
M(224 ): F | 1 FF 1 FFE0::
V(224 ): C | 1 0 1 FEE0:: (A:11 ,P:1,D:0,m:0 )
M(256 ): F | 1 FF 1 FFC0::
V(256 ): C | 1 0 1 FE80:: (A:12 ,P:1,D:0,m:0 )
M(352 ): F | 1 FF 1 FF00::
V(352 ): C | 1 0 1 FF00:: (A:12 ,P:1,D:0,m:0 )
M(480 ): F | 1 FF 1 ::
V(480 ): C | 1 0 1 :: (A:14 ,P:1,D:0,m:0
Router#

```

関連コマンド

コマンド	説明
mls ipv6 acl compress address unicast	IPv6 のアドレスの圧縮をオンにします。

show mls cef logging

TCAM 不一致バッファの内容を表示するには、**show mls cef logging** コマンドを表示します。

```
show mls cef logging [module num]
```

シンタックスの説明

module num	(任意) 特定のモジュールのエントリを表示します。
-------------------	---------------------------

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

TCAM 不一致バッファは、TCAM で見つかった不一致をすべて記録します。
MLS ハードウェア レイヤ 3 スイッチングは IP トラフィックだけに適用されます。

例

次に、TCAM 不一致バッファの内容を表示する例を示します。

```
Router# show mls cef logging
PFIB_ERR:TCAM_SHADOW_CONSISTENCY_ERR:value : Index: 100
Expected: 0 -0 -0
Hardware: 5 -1020304 -0
PFIB_ERR:TCAM_SHADOW_CONSISTENCY_ERR:Mask : Index: 3
Expected: 4 -0 -0
Hardware: 6 -FFF00000-0
Router#
```

show mls cef lookup

MLS ハードウェア レイヤ 3 スイッチング テーブル内の IP エントリを、指定された宛先 IP アドレスについて表示するには、**show mls cef lookup** コマンドを使用します。

show mls cef [ip] lookup address [detail] [module number]

シンタックスの説明

ip	(任意) MLS ハードウェア レイヤ 3 スイッチング テーブル内の IP エントリを表示します。詳細については、「使用上のガイドライン」を参照してください。
address	A.B.C.D フォーマットの IP アドレス
detail	(任意) ハードウェア エントリの詳細を表示します。
module number	(任意) 特定のモジュールのエントリを表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

検索は「最長プレフィクス一致」として実行され、指定された宛先 IP アドレスに適用される TCAM エントリ インデックスが表示されます。

情報は、インデックス、プレフィクス、マスク、隣接のフォーマットで出力されます。

show mls cef lookup ip コマンドと **show mls cef lookup** コマンドの出力は同じです。

例

次に、特定の IPv4 ユニキャスト アドレスに適用される最長プレフィクス一致を表示する例を示します。

```
Router# show mls cef lookup 224.0.0.0

Codes: decap - Decapsulation, + - Push Label
Index  Prefix                               Adjacency
3200   224.0.0.0/24                          punt
Router#
```

show mls cef maximum-routes

現在の最大ルート システム コンフィギュレーションを表示するには、**show mls cef maximum-routes** コマンドを使用します。

show mls cef maximum-routes

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン ユーザが **mls cef maximum-routes** コマンドを入力してコンフィギュレーションを変更する場合、**show mls cef maximum-routes** コマンドの出力に次の追加フィールドが表示されます。

- User configured : 実行したコンフィギュレーションの変更が表示されます。
- Upon reboot : システム リブート後のコンフィギュレーションを表示します。

これらのフィールドは、**mls cef maximum-routes** コマンドを入力した後、(**copy system:running-config nvram: startup-config** コマンドを使用して) 変更を保存しなかった場合に表
示されます。詳細については、「例」を参照してください。

例 次に、**mls cef maximum-routes** コマンドを入力したあと、(**copy system:running-config nvram: startup-config** コマンドで) 変更を保存し、システムを再起動する例を示します。

```
Router# show mls cef maximum-routes
FIB TCAM maximum routes :
=====
Current :-
-----
IPv4 - 1k (default)
MPLS - 239k
IPv6 + IP Multicast - 8k (default)
Router#
```

次に、**mls cef maximum-routes** コマンドの入力後に、変更を保存しなかった場合の出力例を示しま
す。

```
Router# show mls cef maximum-routes
FIB TCAM maximum routes :
=====
Current :-
-----
IPv4 - 1k (default)
```

show mls cef maximum-routes

```
MPLS - 239k
IPv6 + IP Multicast - 8k (default)
User configured :-
-----
IPv4 + MPLS - 192k (default)
IPv6 + IP multicast - 32k (default)
Upon reboot :-
-----
IPv4 - 1k (default)
MPLS - 239k
IPv6 + IP multicast - 8k (default)
Router#
```

次に、コンフィギュレーションの変更を行って (`copy system:running-config nvram: startup-config` コマンドで) 変更を保存した場合の出力例を示します。

```
Router# show mls cef maximum-routes
FIB TCAM maximum routes :
=====
Current :-
-----
IPv4 - 1k (default)
MPLS - 239k
IPv6 + IP Multicast - 8k (default)
User configured :-
-----
IPv4 + MPLS - 192k (default)
IPv6 + IP multicast - 32k (default)
Router#
```

関連コマンド

コマンド	説明
<code>copy system:running-config nvram:startup-config</code>	設定を NVRAM に保存します。
<code>mls cef maximum-routes</code>	プロトコル単位でハードウェアにプログラミング可能な最大ルート数を制限します。

show mls cef mpls

MLS ハードウェア レイヤ 3 スイッチング テーブル内の MPLS エントリを表示するには、**show mls cef mpls** コマンドを使用します。

```
show mls cef mpls [detail] [internal] [labels value] [module number] [vpn instance]
                  [vrf instance]
```

シンタックスの説明

detail	(任意) ハードウェア エントリの詳細を表示します。
internal	(任意) 内部 CEF エントリを表示します。
labels value	(任意) 特定のラベルのエントリを表示します。有効値は 0 ~ 1,048,575 です。
module number	(任意) 特定のモジュールのエントリを表示します。
vpn instance	(任意) 特定の VPN インスタンスの VPN MPLS テーブル エントリを表示します。有効値は 0 ~ 4095 です。
vrf instance-name	(任意) 特定の VRF の MPLS CEF テーブル エントリを表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、MPLS エントリを表示する例を示します。

```
Router# show mls cef mpls

Codes: + - Push label, - - Pop Label          * - Swap Label
Index  Local   Label          Out i/f
      Label   Op
Router#
```

show mls cef rpf

MLS ハードウェア レイヤ 3 スイッチング テーブル内の RPF ハードウェアに関する情報を表示するには、**show mls cef rpf** コマンドを使用します。

show mls cef [ip] rpf [ip-address] [module num]

シンタックスの説明

ip	(任意) MLS ハードウェア レイヤ 3 スイッチング テーブル内の IP エントリを表示します。詳細については、「使用上のガイドライン」を参照してください。
ip-address	(任意) IP アドレス
module num	(任意) 特定のモジュールのエントリを表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

show mls cef ip rpf コマンドを引数なしで入力すると、RPF グローバル モード ステータスが表示されます。

show mls cef ip rpf コマンドと **show mls cef rpf** コマンドの出力は同じです。

例

次に、RPF グローバル モードのステータスを表示する例を示します。

```
Router# show mls cef rpf

RPF global mode:          not enabled
Router#
```

次に、特定の IP アドレスの RPF 情報を表示する例を示します。

```
Router# show mls cef rpf 10.100.0.0
RPF information for prefix 10.100.0.0/24
uRPF check performed in the hardware for interfaces :
GigabitEthernet1/1
Router#
```

関連コマンド

コマンド	説明
mls ip cef rpf multipath	RPF モードを設定します。

show mls cef statistics

スイッチングされたパケット数およびバイト数を表示するには、**show mls cef statistics** コマンドを使用します。

```
show mls cef statistics [module number]
```

シンタックスの説明

module number (任意) 特定のモジュールの情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、MLS ハードウェア レイヤ 3 スwitching の統計情報を表示する例を示します。

```
Router# show mls cef statistics

Total CEF switched packets: 0000000000000000
Total CEF switched bytes:   0000000000000000
Router#
```

show mls cef summary

MLS ハードウェア レイヤ 3 スイッチング テーブル内のルート数を、すべてのプロトコルについて表示するには、**show mls cef summary** コマンドを使用します。

show mls cef summary [module number]

シンタックスの説明

module number (任意) 特定のモジュールの情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

MLS ハードウェア レイヤ 3 スイッチング テーブル内のプレフィクス数は、IPv4 と IPv6 ユニキャスト、IPv4 マルチキャスト、MPLS、および EoM ルートのそれぞれの数を示します。

例

次に、MLS ハードウェア レイヤ 3 スイッチング情報のサマリーを表示する例を示します。

```
Router# show mls cef summary
Total routes:                80385
  IPv4 unicast routes:       42
  IPv4 Multicast routes:     5
  MPLS routes:               0
  IPv6 unicast routes:       2
  EoM routes:                0
Router#
```

表 2-82 に、**show mls cef summary** コマンド出力に含まれるフィールドの説明を示します。

表 2-82 show mls cef summary コマンドの出力フィールド

フィールド	説明
Total MLS-hardware Layer 3-switching switched packets	MLS ハードウェア レイヤ 3 スイッチング エンジンにより転送された MLS ハードウェア レイヤ 3 スイッチングの packets 数
Total MLS-hardware Layer 3-switching switched bytes	MLS ハードウェア レイヤ 3 スイッチング エンジンにより転送されたバイト数
Total routes	ルート エントリ数
IP unicast routes	IP ユニキャスト ルート エントリ数

表 2-82 `show mls cef summary` コマンドの出力フィールド (続き)

フィールド	説明
IPX routes	IPX ルート エントリ数
IP multicast routes	IP マルチキャスト ルート エントリ数

関連コマンド

コマンド	説明
<code>show mls cef</code>	MLS ハードウェア レイヤ 3 スイッチング テーブル エントリを表示します。

show mls cef vrf

特定の VRF 名に対する VRF インスタンス CEF テーブルに関する情報を表示するには、**show mls cef vrf** コマンドを使用します。

```
show mls cef vrf instance-name [prefix] [detail] [lookup ip-address] [module num]
[rpf ip-address]]
```

シンタックスの説明

<i>instance-name</i>	VRF 名。有効値は 0 ~ 4095 です。
<i>prefix</i>	(任意) 表示するエントリのプレフィクス
detail	(任意) ハードウェア エントリの詳細を表示します。
lookup ip-address	(任意) 指定されたアドレスの最長プレフィクス一致ルックアップ エントリを表示します。
<i>module num</i>	(任意) 特定のモジュールのエントリを表示します。
rpf ip-address	(任意) 指定した IP アドレスの情報に対する uRPF チェック情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

show mls cef ip コマンドは、デフォルト VRF の CEF エントリを表示します。特定の (デフォルトではない) VRF エントリを表示するには、**show mls cef [ip] vrf vrf-name** コマンドを使用します。

例

次に、特定の VRF 名に対する VRF の CEF テーブルに関する情報を表示する例を示します。

```
Router# show mls cef vrf vpn-1

Codes: decap - Decapsulation, + - Push Label
Index Prefix Adjacency
64 0.0.0.0/32 receive
65 255.255.255.255/32 receive
280 7.50.27.1/32 receive
281 7.50.27.0/32 receive
282 7.50.27.255/32 receive
298 2.1.1.1/32 receive
```

```
299 2.1.1.0/32 receive
300 2.1.1.255/32 receive
656 2.1.99.1/32 receive
Router#
```

関連コマンド

コマンド	説明
show mls cef ip	MLS ハードウェア レイヤ 3 スイッチング テーブルの IP エントリを表示します。

show mls df-table

DF テーブルに関する情報を表示するには、**show mls df-table** コマンドを使用します。

show mls df-table start-vlan end-vlan

シンタックスの説明

<i>start-vlan</i>	VLAN ID 範囲の開始 ID。有効値は 1 ~ 4094 です。
<i>end-vlan</i>	VLAN ID 範囲の終了 ID。有効値は 1 ~ 4094 です。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

スイッチ プロセッサ—EXEC (Switch-sp#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

出力の意味は、次のとおりです。

- 1 は DF がイネーブルであることを示します。
- 0 は DF がディセーブルであることを示します。

例

次に、DF テーブルの内容を一連の VLAN について表示する例を示します。

```
Switch-sp# show mls df-table 201 212
TYCHO FIB DF Table

vlan    df_index
      3 2 1 0
-----+-----
201    1 1 1 1
202    1 1 1 1
203    1 1 1 1
204    1 1 1 1
205    1 1 1 1
206    1 1 1 1
207    1 1 1 1
208    1 1 1 1
209    1 1 1 1
210    1 1 1 1
211    1 1 1 1
212    1 1 1 1
Switch-sp#
```

show mls ip

MLS IP 情報を表示するには、**show mls ip** コマンドを使用します。

```
show mls ip [any | destination {hostname | ip-address} | detail | flow {tcp | udp} | {vlan
vlan-id} | {macd destination-mac-address} | {macs source-mac-address} | {module
number} | source {hostname | ip-address} | count | static]
```

```
show mls {ipv6 | mpls}
```

シンタックスの説明

any	(任意) すべての MLS IP 情報を表示します。
destination <i>hostname</i>	(任意) 特定の宛先ホスト名のエントリを表示します。
destination <i>ip-address</i>	(任意) 特定の宛先 IP アドレスのエントリを表示します。
detail	(任意) 詳細出力を指定します。
flow	(任意) フロータイプを指定します。
tcp udp	フロータイプを選択します。
vlan <i>vlan-id</i>	(任意) VLAN ID を指定します。有効値は 1 ~ 4094 です。
macd <i>destination-mac-address</i>	(任意) 宛先 MAC アドレスを指定します。
macs <i>source-mac-address</i>	(任意) 送信元 MAC アドレスを指定します。
module <i>number</i>	(任意) 指定されたモジュールにダウンロードされたエントリを表示します。有効値については、「使用上のガイドライン」を参照してください。
source <i>hostname</i>	(任意) 特定の送信元アドレスのエントリを表示します。
source <i>ip-address</i>	(任意) 特定の送信元 IP アドレスのエントリを表示します。
count	(任意) MLS エントリの総数を表示します。
static	(任意) スタティック エントリの総数を表示します。
ipv6	IPv6 エントリの総数を表示します。
mpls	MPLS エントリの総数を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

interface-number 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、指定されたインターフェイスタイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロットシャーシに 48 ポート 10/100BASE-T イーサネットモジュールが搭載されている場合に、ギガビットイーサネットインターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。この定義は、**module number** キーワードおよび引数にも適用されます。

出力を参照するときは、フィールド区切りにコロン (:) が使用されていることに注意してください。

例

次に、MLS IP 情報をすべて表示する例を示します。

```
Router# show mls ip any
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts          Bytes          Age   LastSeen  Attributes
-----
0.0.0.0       0.0.0.0        0    :0        :0        0    : 0x0
82            3772           1329 20:46:03  L3 - Dynamic
Router#
```

次に、特定の IP アドレスの MLS 情報を表示する例を示します。

```
Router# show mls ip destination 172.20.52.122
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Dst i/f:DstMAC        Pkts          Bytes
-----
SrcDstPorts    SrcDstEncap   Age   LastSeen
-----
172.20.52.122  0.0.0.0        5    : 00e0.4fac.b3ff 684          103469
Fa5/9,Fa5/9 ARPA,ARPA 281 07:17:02

Number of Entries Found = 1
Router#
```

次に、特定のフロータイプの MLS 情報を表示する例を示します。

```
Router# show mls ip flow udp
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts          Bytes          Age   LastSeen  Attributes
-----
0.0.0.0       0.0.0.0        0    :0        :0        0    : 0x0
78            3588           1259 20:44:53  L3 - Dynamic
Router#
```

次に、MLS の詳細情報を表示する例を示します。

```
Router# show mls ip detail
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts          Bytes          Age   LastSeen  Attributes
-----

Mask Pi R CR Xt Prio Dsc IP_EN OP_EN Pattern Rpf FIN_RDT FIN/RST
---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
Ig/acli Ig/aclo Ig/qosi Ig/qoso Fpkt Gemini MC-hit Dirty Diags
---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

QoS      Police Count Threshold   Leak      Drop Bucket  Use-Tbl Use-Enable
```

```

-----+-----+-----+-----+-----+-----+-----+-----+-----+
127.0.0.19      127.0.0.16      udp :68      :67      1009: 0x0
72              3312            1170 20:43:24    L3 - Dynamic
0   1   0   0   1   0   0   1   1   0   0   0   0
0              0              0      0      0      0      0      0      0
      0x0          0              0      0      NO   64      NO      NO
Router#
    
```

関連コマンド

コマンド	説明
mls ip	インターフェイス上で内部ルータの MLS IP をイネーブルにします。
show mls netflow ip	ハードウェア NetFlow IP に関する情報を表示します。

show mls ip cef rpf-table

RPF CEF テーブルの設定を表示するには、**show mls ip cef rpf-table** コマンドを使用します。

show mls ip cef rpf-table

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、RPF CEF テーブル エントリを表示する例を示します。

```
Router# show mls ip cef rpf-table
-----
172.10.10.0/24      [0] Fa2/1, Fa2/2, Fa2/3, Fa2/4
172.10.20.0/24
172.10.30.0/24
10.10.0.0/16      [1] Gi1/1, Gi1/2
10.20.0.0/16
Router#
```

関連コマンド	コマンド	説明
	mls ip cef rpf interface-group	RPF-VLAN テーブルでインターフェイス グループを定義します。

show mls ip multicast

MLS IP 情報を表示するには、**show mls ip multicast** コマンドを使用します。

```
show mls ip multicast [ {capability [module num]} | connected | group } {hostname |
ip-address} [ip-mask]} | {interface {interface interface-number}} | {module number} |
mdt | {source {hostname | ip-address}} | statistics | summary]
```

```
show mls ip multicast consistency-check [mroute-mlsm | {rp-sp [log [clear] | statistics]]]
```

シンタックスの説明

capability	マルチキャスト レプリケーション機能に関する情報を表示します。
module num	(任意) モジュール番号を指定します。
connected	(任意) 搭載されているインターフェイス エントリまたはマスク エントリを表示します。
group	(任意) 特定のマルチキャスト グループアドレスのエントリを表示します。
hostname	グループ IP ホスト名
ip-address	グループ IP アドレス
ip-mask	(任意) グループ IP アドレスの IP マスク
interface	(任意) インターフェイスを指定します。
interface	インターフェイス タイプ。有効値は ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 atm 、および ge-wan です。
interface-number	モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
module number	(任意) 指定されたモジュールにダウンロードされたエントリを表示します。有効値については、「使用上のガイドライン」を参照してください。
mdt	(任意) ハードウェア アクセラレーション MDT 情報を表示します。
source hostname	(任意) 特定の送信元アドレスのエントリを表示します。
source ip-address	(任意) 特定の送信元 IP アドレスのエントリを表示します。
statistics	(任意) マルチキャスト エントリからの統計情報を表示します。
summary	(任意) マルチキャスト エントリからの統計情報のサマリーを表示します。
consistency-check	一貫性チェッカー情報を表示します。
mroute-mlsm	(任意) mroute/MLSM 一貫性チェッカー情報を表示します。
rp-sp	(任意) ルート プロセッサ/スイッチ プロセッサ一貫性チェッカー情報を表示します。
log	(任意) 検出され修正された不整合のログを表示します。
clear	(任意) 不整合ログをクリアします。
statistics	(任意) チェックされたプレフィックスの統計を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

interface-number 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、指定されたインターフェイスタイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロットシャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。これらの有効値は、**module number** キーワードおよび引数を入力するときにも適用されます。

出力を参照するときは、フィールド区切りにコロン (:) が使用されていることに注意してください。

例

次に、一般的な MLS IP マルチキャスト情報を表示する例を示します。

```
Router# show mls ip multicast
Multicast hardware switched flows:
(*, 224.1.1.1) Incoming interface: Vlan0, Packets switched: 0
Hardware switched outgoing interfaces: Vlan202
RPF-MFD installed
Total hardware switched flows : 1
Router#
```

次に、MLS 情報のサマリーを表示する例を示します。

```
Router# show mls ip multicast summary
1 MMLS entries using 168 bytes of memory
Number of partial hardware-switched flows: 0
Number of complete hardware-switched flows: 1
Directly connected subnet entry install is enabled
Aggregation of routed oif is enabled
Hardware shortcuts for mvpn mroutes supported
Egress Mode of replication is enabled
Maximum route support is enabled
Router#
```

次に、特定のインターフェイスの MLS 情報を表示する例を示します。

```
Router# show mls ip multicast interface fastethernet 5/9
DstIP          SrcIP          Dst i/f:DstMAC  Pkts          Bytes
-----
SrcDstPorts    SrcDstEncap   Age             LastSeen
-----
172.20.52.37   0.0.0.0       100: 00d0.5870.a4ff 1              129
Fa5/9,----- ARPA,ARPA    107            06:10:02
172.20.52.36   0.0.0.0       100 : 0050.7312.0cff 50             6403
Fa5/9,----- ARPA,ARPA    107            06:10:04
Number of Entries Found = 2
Router#
```

次に、マルチキャスト レプリケーション機能に関する情報を表示する例を示します。

```
Router# show mls ip multicast capability
Current mode of replication is Ingress
auto replication mode detection is ON

Slot          Multicast replication capability
  2              Egress
  5              Egress
  6              Egress
```

```

      8                               Ingress
      9                               Ingress
Router#

```

次に、mroute 一貫性チェッカー ログに関する情報を表示する例を示します。

```

Router# show mls ip multicast consistency-check mroute-mlsm
MMLS Consistency checker of mroute-scan type is enabled
Inter scan period = 2 sec
Number of entry scanned = 20
Settle time = 60 sec
Storage for 1000 events (40000 bytes)
Mroute entry missed for a Shortcut : 0
Mroute entry was uneligible for a Shortcut : 0
Mroute entry rpf i/f mismatched with Shortcut : 0
Mroute oif in hw and Shortcut oif in sw : 0
Mroute oif in sw and Shortcut oif in sw : 0
Mroute oif in sw and Shortcut oif in hw : 0
Mroute #oif mismatched with Shortcut #oif : 0
.
.
.
<Output is truncated>

```

次に、検出され修正された不整合のログを表示する例を示します。

```

Router# show mls ip multicast consistency-check rp-sp log
MLSM RP<->SP Consistency Checker Mismatch log for Table 0:
size 512 current-index 0

0 total used entries in log
Router#

```

関連コマンド

コマンド	説明
mls ip multicast (interface configuration mode)	インターフェイス上で MLS IP ショートカットをイネーブルにします。

show mls ip multicast bidir

ハードウェアでスイッチングされる Bidir エントリを表示するには、**show mls ip multicast bidir** コマンドを使用します。

```
show mls ip multicast bidir [{group} {{hostname | ip-address} [ip-mask]}] | {interface}
{interface interface-number}} | {source} {hostname | ip-address}}]
```

シンタックスの説明

group	(任意) 特定のマルチキャスト グループ アドレスのエントリを表示します。
<i>hostname</i>	グループ IP ホスト名
<i>ip-address</i>	グループ IP アドレス
<i>ip-mask</i>	(任意) グループ IP アドレスの IP マスク
interface	(任意) インターフェイスを指定します。
<i>interface</i>	インターフェイス タイプ。有効値は ethernet 、 fastethernet 、 gigabitethernet 、および tengigabitethernet です。
<i>interface-number</i>	モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
source hostname	(任意) 特定の送信元アドレスのエントリを表示します。
source ip-address	(任意) 特定の送信元 IP アドレスのエントリを表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、ハードウェアでスイッチングされる Bidir エントリを表示する例を示します。

```
Router# show mls ip multicast bidir
Multicast hardware switched flows:
(*, 226.1.4.0) Incoming interface: Vlan51, Packets switched: 0
Hardware switched outgoing interfaces: Vlan51 Vlan30
RPF-MFD installed
(*, 227.1.4.0) Incoming interface: Gi2/1, Packets switched: 0
Hardware switched outgoing interfaces: Gi2/1 Vlan30
RPF-MFD installed
Router#
```

関連コマンド

コマンド	説明
mls ip multicast bidir gm-scan-interval	Bidir ランデブー ポイントの RPF スキャン インターバルを設定します。

show mls ip multicast rp-mapping

アクティブな Rendezvous Point (RP; ランデブー ポイント) への PIM-Bidir グループのマッピングを表示するには、**show mls ip multicast rp-mapping** コマンドを使用します。

show mls ip multicast rp-mapping [*rp-address*] [**df-cache** | **gm-cache**]

シンタックスの説明	
<i>rp-address</i>	(任意) RP のアドレス
df-cache	(任意) ハードウェアの RP マッピング キャッシュ内の DF リストに基づく情報を表示します。
gm-cache	(任意) ハードウェアの RP マッピング キャッシュ内のグループ/マスク範囲に基づく情報を表示します。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、アクティブな RP への PIM グループのマッピングを表示する例を示します。

```
Router# show mls ip multicast rp-mapping
RP Address State DF-count GM-count
2.2.2.2 H 1 1
9.9.9.9 H 1 2
Router#
```

次に、ルートプロセッサのマッピング キャッシュ内の DF リストに基づく情報を表示する例を示します。

```
Router# show mls ip multicast rp-mapping df-cache
RP Address State DF State
9.9.9.9 H V130 H
Router#
```

次に、ルートプロセッサのマッピング キャッシュに基づく情報を表示する例を示します。

```
Router# show mls ip multicast rp-mapping gm-cache
State: H - Hardware Switched, I - Install Pending, D - Delete Pending,
Z - Zombie
RP Address State Group Mask State Packet/Byte-count
60.0.0.60 H 230.31.0.0 255.255.0.0 H 100/6400
Router#
```

show mls ip multicast sso

マルチキャスト ハイ アベイラビリティ SSO に関する情報を表示するには、**show mls ip multicast sso** コマンドを使用します。

show mls ip multicast sso [statistics]

シンタックスの説明

statistics (任意) マルチキャスト ハイ アベイラビリティ SSO の統計情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、マルチキャスト ハイ アベイラビリティ SSO の情報を表示する例を示します。

```
Router> show mls ip multicast sso
Multicast SSO is enabled
Multicast HA Parameters
-----+-----+
protocol convergence timeout          120 secs
flow leak percent                     10
flow leak interval                    20 secs
heartquake#
```

次に、マルチキャスト ハイ アベイラビリティ SSO の統計情報を表示する例を示します。

```
Router# show mls ip multicast sso statistics

Multicast HA Statistics: ACTIVE
-----+-----+
CHKPT msgs sent                       5
CHKPT msgs send failed                 0
CHKPT msgs send aborted                0
CHKPT met add msg sent                 5
CHKPT met del msg sent                 1
CHKPT icroif msg sent                  1
MET HA met add enqueued                 5
MET HA met del enqueued                 1
ICROIF HA add enqueued                  1
ICROIF HA del enqueued                  0
CHKPT buffer failure                   0

MET HA Reconstruction Statistics
-----+-----+
Number of met blks reconstructed       0
Number of normal sets reconstructed    0
Number of fixed sets reconstructed     0
Number of sets deleted                  0
```

```
Number of blks not found          0
normal sets reconstruction failed  0
fixed set reconstruction failed    0

Multicast HA Statistics: STANDBY
-----+-----+
CHKPT msgs rcvd                   5
CHKPT met add msg rcvd             5
CHKPT met del msg rcvd             1
CHKPT icroif msg rcvd              1
CHKPT msg unknown                  0
CHKPT buffer failure               0
Router#
```

関連コマンド

コマンド	説明
mls ip multicast sso	SSO パラメータを設定します。

show mls ip non-static

ソフトウェアにより導入された非スタティックエントリの情報を表示するには、**show mls ip non-static** コマンドを使用します。

show mls ip non-static [**count** [**module number**] | **detail** [**module number**] | **module number**]

シンタックスの説明

count	(任意) 非スタティック エントリの総数を表示します。
module number	(任意) モジュール番号を指定します。
detail	(任意) フロー単位で詳細出力を指定します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、ソフトウェアにより導入された非スタティック エントリを表示する例を示します。

```
Router> show mls ip non-static
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts           Bytes          Age   LastSeen  Attributes
-----
Router>
```

次に、ソフトウェアにより導入された非スタティック エントリの詳細情報を表示する例を示します。

```
Router> show mls ip non-static detail
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts           Bytes          Age   LastSeen  Attributes
-----
QoS    Police Count Threshold   Leak   Drop Bucket  Use-Tbl Use-Enable
-----+-----+-----+-----+-----+-----+-----+
Router>
```

次に、ソフトウェアにより導入された非スタティック エントリの総数を表示する例を示します。

```
Router> show mls ip non-static count
Displaying Netflow entries in Supervisor Earl

Number of shortcuts = 0
Router>
```

show mls ip routes

NetFlow ルーティング エントリを表示するには、**show mls ip routes** コマンドを使用します。

```
show mls ip routes [non-static | static] [count [module number] | detail [module number]
| module number]
```

シンタックスの説明	non-static
	(任意) ソフトウェアにより導入された非スタティック エントリを表示します。
	static (任意) ソフトウェアにより導入されたスタティック エントリを表示します。
	count (任意) NetFlow ルーティング エントリの総数を表示します。
	module number (任意) 指定されたモジュールにダウンロードされたエントリを表示します。有効値については、「使用上のガイドライン」を参照してください。
	detail (任意) フロー単位で詳細出力を指定します。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、ソフトウェアにより導入された非スタティック ルーティング エントリを表示する例を示します。

```
Router> show mls ip routes non-static
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts           Bytes          Age   LastSeen  Attributes
-----
Router>
```

次に、ソフトウェアにより導入された非スタティック ルーティング エントリの詳細情報を表示する例を示します。

```
Router> show mls ip routes non-static detail
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts           Bytes          Age   LastSeen  Attributes
-----
QoS           Police Count Threshold  Leak   Drop Bucket  Use-Tbl Use-Enable
-----+-----+-----+-----+-----+-----+-----+
Router>
```

■ show mls ip routes

次に、ソフトウェアにより導入されたルーティング エントリの総数を表示する例を示します。

```
Router> show mls ip routes count
Displaying Netflow entries in Supervisor Earl

Number of shortcuts = 0
Router>
```

関連コマンド

コマンド	説明
show mls netflow ip sw-installed	ソフトウェアにより導入された IP エントリの情報を表示します。

show mls ip static

ソフトウェアにより導入されたスタティック IP エントリの情報を表示するには、**show mls ip static** コマンドを使用します。

show mls ip static [**count** [**module number**] | **detail** [**module number**] | **module number**]

シンタックスの説明

count	(任意) スタティック エントリの総数を表示します。
module number	(任意) モジュール番号を指定します。
detail	(任意) フロー単位で詳細出力を指定します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドのデフォルト

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、ソフトウェアにより導入されたスタティック エントリを表示する例を示します。

```
Router> show mls ip static
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts           Bytes          Age   LastSeen  Attributes
-----
Router>
```

次に、ソフトウェアにより導入されたスタティック エントリの詳細情報を表示する例を示します。

```
Router> show mls ip static detail
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts           Bytes          Age   LastSeen  Attributes
-----
QoS           Police Count Threshold  Leak   Drop Bucket  Use-Tbl Use-Enable
-----+-----+-----+-----+-----+-----+-----+
Router>
```

次に、ソフトウェアにより導入されたスタティック エントリの総数を表示する例を示します。

```
Router> show mls ip static count
Displaying Netflow entries in Supervisor Earl

Number of shortcuts = 0
Router>
```

show mls ip statistics

NetFlow IP エントリの統計情報を表示するには、**show mls ip statistics** コマンドを使用します。

show mls ip statistics [count [module number] | detail [module number] | module number]

シンタックスの説明

count	(任意) NetFlow エントリの総数を表示します。
module number	(任意) 指定されたモジュールにダウンロードされたエントリを表示します。
detail	(任意) フロー単位で詳細出力を指定します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、NetFlow IP エントリの統計情報を表示する例を示します。

```
Router> show mls ip statistics
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts           Bytes         Age  LastSeen  Attributes
-----
Router>
```

次に、NetFlow IP エントリの統計の詳細情報を表示する例を示します。

```
Router> show mls ip statistics detail
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts           Bytes         Age  LastSeen  Attributes

      QoS      Police Count Threshold      Leak      Drop Bucket  Use-Tbl Use-Enable
-----+-----+-----+-----+-----+-----+-----+
Router>
```

show mls nde

ハードウェアでスイッチングされる NDE フローに関する情報を表示するには、**show mls nde** コマンドを使用します。

show mls nde

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン Catalyst 6500 シリーズ スイッチの出力には、現在の NDE モードが含まれます。

例 次に、Catalyst 6500 シリーズ スイッチ上のハードウェアでスイッチングされる NDE フローに関する情報を表示する例を示します。

```
Router# show mls nde
Netflow Data Export enabled (Interface Mode)
Exporting flows to 172.20.55.71 (9991)
Exporting flows from 10.6.60.120 (59020)
Version: 7
Include Filter not configured
Exclude Filter not configured
Total Netflow Data Export Packets are:
    0 packets, 0 no packets, 0 records
Router#
```

関連コマンド	コマンド	説明
	mls nde sender	MLS NDE エクスポートをイネーブルにします。
	show ip flow-export	ハードウェア スイッチングおよびソフトウェア スイッチングされるデータ エクスポートのフローに関する情報（メイン キャッシュや他のすべてのイネーブル化されたキャッシュなど）を表示します。
	show mls netflow	NetFlow ハードウェアに関する設定情報を表示します。

show mls netflow

NetFlow ハードウェアに関する設定情報を表示するには、**show mls netflow** コマンドを使用します。

```
show mls netflow {aging | aggregation flowmask | creation | flowmask |
                 {table-contention {detailed | summary}} | usage}
```

```
show mls netflow [ip | ipv6 | mpls] [any | count | destination {hostname | ip-address} |
detail | dynamic | flow {tcp | udp} | module number | nowrap | source {hostname |
ip-address} | sw-installed [non-static | static]]
```

シンタックスの説明

aging	NetFlow エージング情報を表示します。
aggregation flowmask	現在の NetFlow アグリゲーション用に設定されたフロー マスクを表示します。
creation	設定されたプロトコル作成フィルタを表示します。
flowmask	現在の NetFlow IP および IPX フロー マスクを表示します。
table-contention	NetFlow テーブル コンテンション レベル情報を表示します。
detailed	NetFlow テーブル コンテンション レベルの詳細情報を表示します。
summary	NetFlow テーブル コンテンション レベルのサマリーを表示します。
usage	NetFlow テーブル使用の通知ステータスを表示します。
ip	(任意) NetFlow IP テーブルに関する情報を表示します。 show mls netflow ip コマンドを参照してください。
ipv6	(任意) NetFlow IPv6 テーブルに関する情報を表示します。 show mls netflow ipv6 コマンドを参照してください。
mpls	(任意) NetFlow MPLS テーブルに関する情報を表示します。
any	(任意) NetFlow テーブル エントリの詳細情報をテスト ラップなしで表示します。
count	(任意) MLS NetFlow IP エントリの総数を表示します。
destination hostname	(任意) 特定の宛先ホスト名のエントリを表示します。
destination ip-address	(任意) 特定の宛先 IP アドレスのエントリを表示します。
detail	(任意) 詳細出力を指定します。
dynamic	(任意) ハードウェアによって作成されたダイナミック エントリを表示します。
flow tcp	(任意) TCP フローに関する情報を表示します。
flow udp	(任意) UDP フローに関する情報を表示します。
module number	(任意) 指定されたモジュールにダウンロードされたエントリを表示します。有効値については、「 使用上のガイドライン 」を参照してください。
nowrap	(任意) 情報をテキスト ラップなしで表示します。
source hostname	(任意) 特定の送信元アドレスのエントリを表示します。
source ip-address	(任意) 特定の送信元 IP アドレスのエントリを表示します。
sw-installed	(任意) ルーティング NetFlow エントリ を表示します。 show mls netflow ip sw-installed コマンドを参照してください。

non-static	(任意) ソフトウェアによって組み込まれたスタティック IP エントリの情報を表示します。 show mls netflow ip sw-installed コマンドを参照してください。
static	(任意) ソフトウェアによって組み込まれた非スタティック IP エントリの情報を表示します。 show mls netflow ip sw-installed コマンドを参照してください。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン **interface**、**macd**、および **macs** キーワードはサポートされていません。
 引数なしで **show mls netflow ip** コマンドを入力すると、**show mls netflow ip routes** および **show mls netflow ip dynamic** コマンドの出力が表示されます。

出力を参照するときは、フィールド区切りにコロン (:) が使用されていることに注意してください。

NetFlow テーブル使用の通知をイネーブルにし、NetFlow テーブル使用が事前に設定されたしきい値パーセンテージを超えると、警告メッセージが表示されます。 **mls netflow usage notify** コマンドを使用して、しきい値パーセンテージおよび間隔を設定して、NetFlow テーブル使用をチェックできます。

interface-number 引数はモジュールおよびポート番号を指定します。 **interface-number** の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。これらの有効値は、**module number** キーワードおよび引数を入力するときにも適用されます。

例 次に、NetFlow エージング設定を表示する例を示します。

```
Router# show mls netflow aging
          enable timeout  packet threshold
          -----
normal aging true        300          N/A
fast aging  true         32           100
long aging  true         900          N/A
Router#
```

次に、設定されたプロトコル作成フィルタを表示する例を示します。

```
Router# show mls netflow creation
Excluded protocols:
port protocol
-----+-----
10      tcp
8       udp/tcp
Router#
```

show mls netflow

次に、現在の NetFlow アグリゲーション用に設定されたフロー マスクを表示する例を示します。

```
Router# show mls netflow aggregation flowmask
Current flowmask set for netflow aggregation : Dest only
Minimum flowmask required for netflow aggregation schemes
-----+-----
Aggregation Scheme Min. Flowmask Status
-----+-----
as Intf Src Dest disabled
protocol-port Full Flow disabled
source-prefix Intf Src Dest disabled
destination-prefix Dest only enabled
prefix Intf Src Dest disabled
Router#
```

次に、NetFlow テーブル コンテンション レベルに関する詳細情報を表示する例を示します。

```
Router# show mls netflow table-contention detailed
Earl in Module 2
Detailed Netflow CAM (TCAM and ICAM) Utilization
=====
TCAM Utilization   :    0%
ICAM Utilization   :    0%
Netflow TCAM count :    0
Netflow ICAM count :    0
Router#
```

次に、NetFlow テーブル コンテンション レベルのサマリーを表示する例を示します。

```
Router# show mls netflow table summary
Earl in Module 2
Summary of Netflow CAM Utilization (as a percentage)
=====
TCAM Utilization   :    0%
ICAM Utilization   :    0%
Router#
```

次に、NetFlow テーブル使用の通知ステータスを表示する例を示します。

```
Router# show mls netflow usage
Netflow table usage notification enabled at 80% every 300 seconds
Netflow table utilization of module 7 is 99%
Netflow table utilization of module 10 is 24%
Router#
```

関連コマンド

コマンド	説明
ip flow-aggregation cache	フロー集約キャッシュを作成し、集約キャッシュ コンフィギュレーション モードを開始します。
mls netflow usage notify	スイッチ プロセッサ上での NetFlow テーブル使用率をモニタします。
show ip cache flow	NetFlow キャッシュ フロー エントリのサマリーを表示します。

show mls netflow ip

ハードウェア NetFlow IP に関する情報を表示するには、**show mls netflow ip** コマンドを使用します。

show mls netflow ip any

show mls netflow ip count [*module number*]

show mls netflow ip destination {*hostname* | *ip-address*} [*/ip-mask*] [**count** [*module number*]] | **detail** | **dynamic** | **flow** {**icmp** | **tcp** | **udp**} | **module number** | **nowrap** | **qos** | **source** {*hostname* | *ip-address*} [*/ip-mask*] | **sw-installed** [**non-static** | **static**]

show mls netflow ip detail [*module number* | **nowrap** [*module number*]]

show mls netflow ip dynamic [**count** [*module number*]] [**detail**] [*module number*] [**nowrap** [*module number*]] [{**qos** [*module number*] [**nowrap** [*module number*]]}]

show mls netflow ip {**flow** {**icmp** | **tcp** | **udp**}} [**count** [*module number*]] | {**destination** {*hostname* | *ip-address*} [*/ip-mask*]} | **detail** | **dynamic** | **flow** {**icmp** | **tcp** | **udp**} | **module number** | **nowrap** | **qos** | **source** {*hostname* | *ip-address*} | **sw-installed** [**non-static** | **static**]

show mls netflow ip {*module number*}

show mls netflow ip qos [*module number* | **nowrap** [*module number*]]

show mls netflow ip source {*hostname* | *ip-address*} [*/ip-mask*] [**count** [*module number*]] | **detail** | **dynamic** | **flow** {**icmp** | **tcp** | **udp**} | **module number** | **nowrap** | **qos** | **sw-installed** [**non-static** | **static**]

シンタックスの説明

any	NetFlow テーブル エントリの詳細情報をテスト ラップなしで表示します。
count	MLS NetFlow IP エントリの総数を表示します。
module number	(任意) 指定されたモジュールにダウンロードされたエントリを表示します。有効値については、「使用上のガイドライン」を参照してください。
destination <i>hostname</i>	特定の宛先ホスト名のエントリを表示します。
destination <i>ip-address</i>	特定の宛先 IP アドレスのエントリを表示します。
<i>ip-mask</i>	(任意) 宛先 IP アドレスの IP マスク
detail	(任意) 詳細出力を指定します。
dynamic	ハードウェアによって作成されたダイナミック エントリを表示します。 show mls nde コマンドを参照してください。
flow icmp	ICMP フローに関する情報を表示します。
flow tcp	TCP フローに関する情報を表示します。
flow udp	UDP フローに関する情報を表示します。
nowrap	情報をテキスト ラップなしで表示します。
qos	QoS マイクロフロー ポリシング情報を表示します。
source <i>hostname</i>	特定の送信元アドレスのエントリを表示します。


```

QoS Police Count Threshold Leak Drop Bucket Use-Tbl Use-Enable
-----+-----+-----+-----+-----+-----+-----+-----+-----+
172.30.46.2 172.30.45.2 4 :0 :0 Gi7/1: 0x0
140063 6442898 15 01:42:52 L3 - Dynamic
1 1 0 0 1 0 0 1 1 0 0 0 0
0 0 0 0 0 0 0 0 0 0
0x0 672645504 0 0 NO 31784 NO NO
Router#

```

次に、NetFlow テーブル エントリ情報をテスト ラップなしで表示する例を示します。

```

Router# show mls netflow ip nowrap
Displaying Netflow entries in Supervisor Earl
DstIP SrcIP Prot:SrcPort:DstPort Src i/f
:AdjPtr Pkts Bytes Age LastSeen Attributes
-----
-
-----
12.1.1.2 11.1.1.92 udp :63 :63 Fa5/11
:0x0 176339 8111594 912 22:31:15 L3 - Dynamic
12.1.1.2 11.1.1.93 udp :63 :63 Fa5/11
:0x0 176338 8111548 912 22:31:15 L3 - Dynamic
12.1.1.2 11.1.1.94 udp :63 :63 Fa5/11
:0x0 176338 8111548 912 22:31:15 L3 - Dynamic
12.1.1.2 11.1.1.95 udp :63 :63 Fa5/11
:0x0 176338 8111548 912 22:31:15 L3 - Dynamic
12.1.1.2 11.1.1.96 udp :63 :63 Fa5/11
:0x0 176338 8111548 912 22:31:15 L3 - Dynamic
12.1.1.2 11.1.1.97 udp :63 :63 Fa5/11
:0x0 176337 8111502 912 22:31:15 L3 - Dynamic
12.1.1.2 11.1.1.98 udp :63 :63 Fa5/11
:0x0 176337 8111502 912 22:31:15 L3 - Dynamic
12.1.1.2 11.1.1.99 udp :63 :63 Fa5/11
:0x0 176337 8111502 912 22:31:15 L3 - Dynamic
12.1.1.2 11.1.1.100 udp :63 :63 Fa5/11
:0x0 176337 8111502 912 22:31:15 L3 - Dynamic
Router#

```

次に、特定の IP アドレスの MLS NetFlow に関する情報を表示する例を示します。

```

Router# show mls netflow ip destination 172.20.52.122
Displaying Netflow entries in Supervisor Earl
DstIP SrcIP Prot:SrcPort:DstPort Src i/f:AdjPtr
-----
Pkts Bytes Age LastSeen Attributes
-----
Router#

```

次に、特定のフローの MLS NetFlow に関する情報を表示する例を示します。

```

Router# show mls netflow ip flow udp
Displaying Netflow entries in Supervisor Earl
DstIP SrcIP Prot:SrcPort:DstPort Src i/f:AdjPtr
-----
Pkts Bytes Age LastSeen Attributes
-----
172.20.52.19 0.0.0.0 :0 :0 :0 :0
0 0 1407 11:01:32 L3 - Dynamic
Router#

```

■ show mls netflow ip

次に、フルフロー マスクの MLS NetFlow に関する詳細情報を表示する例を示します。

```
Router# show mls netflow ip detail
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts           Bytes         Age  LastSeen  Attributes
-----
      QoS      Police Count Threshold      Leak      Drop Bucket  Use-Tbl Use-Enable
-----+-----+-----+-----+-----+-----+-----+
172.20.52.19   0.0.0.0        0    :0        :0        0      : 0
0              0              1464  11:02:31  L3 - Dynamic
0x0           0              0      0        NO      64      NO      NO
Router#
```

次に、特定のフロー タイプの詳細情報を表示する例を示します。

```
Router# show mls netflow ip flow icmp
Displaying Netflow entries in Supervisor Earl
DstIP SrcIP Prot:SrcPort:DstPort Src i/f
:AdjPtr
>
>-----
-
-
Pkts Bytes Age LastSeen Attributes
-----
12.1.1.2 11.1.10.151 icmp:0 :0 Fa5/11
:0x0
1945 89470 1062 08:45:15 L3 - Dynamic
12.1.1.2 11.1.10.153 icmp:0 :0 Fa5/11
:0x0
1945 89470 1062 08:45:15 L3 - Dynamic
12.1.1.2 11.1.10.155 icmp:0 :0 Fa5/11
:0x0
1945 89470 1062 08:45:15 L3 - Dynamic
12.1.1.2 11.1.10.157 icmp:0 :0 Fa5/11
:0x0
1945 89470 1062 08:45:15 L3 - Dynamic
12.1.1.2 11.1.10.159 icmp:0 :0 Fa5/11
:0x0
1945 89470 1062 08:45:15 L3 - Dynamic
12.1.1.2 11.1.10.161 icmp:0 :0 Fa5/11
:0x0
1945 89470 1062 08:45:15 L3 - Dynamic
12.1.1.2 11.1.10.163 icmp:0 :0 Fa5/11
:0x0
Router#
```

次に、QoS 情報を表示する例を示します。

```
Router# show mls netflow ip qos
Displaying netflow qos information in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts           Bytes         LastSeen  QoS  PoliceCount Threshold Leak
-----
Drop  Bucket
-----
xxx.xxxx.xxx.xxx xxx.xxx.xxx.xxx xxxx:63      :63      Fa5/11 :0x0
772357      35528422      17:59:01  xxx  xxx      xxx      xxx
xxx  xxx
Router#
```

関連コマンド

コマンド	説明
clear mls netflow	MLS NetFlow のショートカット エントリをクリアします。
ip flow-aggregation cache	フロー集約キャッシュを作成し、集約キャッシュ コンフィギュレーション モードを開始します。
show ip cache flow	NetFlow キャッシュ フロー エントリのサマリーを表示します。

show mls netflow ip sw-installed

ソフトウェアにより導入された IP エントリの情報を表示するには、**show mls netflow ip sw-installed** コマンドを使用します。

show mls netflow ip sw-installed {non-static | static} [count [module number] | detail [module number] | module number]

シンタックスの説明

non-static	ソフトウェアにより導入されたルーティング エントリを表示します。
static	ソフトウェアにより導入されたスタティック ルーティング エントリを表示します。
count	(任意) 非スタティック エントリの総数を表示します。
module number	(任意) 指定されたモジュールにダウンロードされたエントリを表示します。有効値については、「使用上のガイドライン」を参照してください。
detail	(任意) フロー単位で詳細出力を指定します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、ソフトウェアにより導入された非スタティック エントリを表示する例を示します。

```
Router> show mls netflow ip sw-installed non-static
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts           Bytes          Age   LastSeen  Attributes
-----
Router>
```

次に、ソフトウェアにより導入された非スタティック エントリの詳細情報を表示する例を示します。

```
Router> show mls netflow ip sw-installed non-static detail
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts           Bytes          Age   LastSeen  Attributes

      QoS      Police Count Threshold   Leak   Drop Bucket  Use-Tbl Use-Enable
-----+-----+-----+-----+-----+-----+-----+
Router>
```

次に、ソフトウェアにより導入された非スタティック エントリの総数を表示する例を示します。

```
Router> show mls netflow ip sw-installed non-static count
Displaying Netflow entries in Supervisor Earl

Number of shortcuts = 0
Router>
```

show mls netflow ipv6

ハードウェア NetFlow IPv6 設定に関する情報を表示するには、**show mls netflow ipv6** コマンドを使用します。

show mls netflow ipv6 any

show mls netflow ipv6 count [*module number*]

show mls netflow ipv6 destination *ipv6-address*[*/ipv6-prefix*] [**count** [*module number*]] | **detail** | **dynamic** | **flow** {**icmp** | **tcp** | **udp**} | **module number** | **nowrap** | **qos** | **source** *ipv6-address*[*/ipv6-prefix*] | **sw-installed** [**non-static** | **static**]

show mls netflow ipv6 detail [*module number* | **nowrap** [*module number*]]

show mls netflow ipv6 dynamic [**count** [*module number*]] [**detail**] [*module number*] [**nowrap** [*module number*]] [{**qos** [*module number*]}] [**nowrap** [*module number*]]}]

show mls netflow ipv6 {**flow** {**icmp** | **tcp** | **udp**}} [**count** [*module number*]] | {**destination** *ipv6-address*[*/ipv6-prefix*]} | **detail** | **dynamic** | **flow** {**icmp** | **tcp** | **udp**} | **module number** | **nowrap** | **qos** | {**source** *ipv6-address*[*/ipv6-prefix*]} | **sw-installed** [**non-static** | **static**]]

show mls netflow ipv6 {*module number*}

show mls netflow ipv6 qos [*module number* | **nowrap** [*module number*]]

show mls netflow ipv6 source *ipv6-address*[*/ipv6-prefix*] [**count** [*module number*]] | **detail** | **dynamic** | **flow** {**icmp** | **tcp** | **udp**} | **module number** | **nowrap** | **qos** | **sw-installed** [**non-static** | **static**]

シンタックスの説明

any	NetFlow エージング情報を表示します。
count	MLS NetFlow IPv6 エントリの総数を表示します。
module number	(任意) 指定されたモジュールにダウンロードされたエントリを表示します。有効値については、「使用上のガイドライン」を参照してください。
destination <i>ipv6-address</i> <i>/ipv6-prefix</i>	特定の宛先 IPv6 アドレスのエントリを表示します。 IPv6 プレフィクス。有効値は、0 ~ 128 です。
detail	詳細出力を指定します。
dynamic	ハードウェアにより作成されたダイナミック エントリを表示します。
flow icmp tcp udp	フロー タイプを指定します。
nowrap	(任意) テキスト ラッピングをオフにします。
qos	QoS 統計に関する情報を表示します。
source <i>ipv6-address</i>	特定の送信元 IPv6 アドレスのエントリを表示します。
sw-installed	(任意) ルーティング NetFlow エントリを表示します。
non-static	(任意) ソフトウェアにより導入されたスタティック IPv6 エントリに関する情報を表示します。
static	(任意) ソフトウェアにより導入された非スタティック IPv6 エントリに関する情報を表示します。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドのデフォルト EXEC (>)

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、ハードウェア NetFlow 設定に関する情報を表示する例を示します。

```
Router# show mls netflow ipv6
Displaying Netflow entries in Supervisor Earl
DstIP                               SrcIP
-----
Prot:SrcPort:DstPort  Src i/f      :AdjPtr
Pkts      Bytes      Age  LastSeen  Attributes
-----
50::2
tcp :16      :32      V147      :0x0
23758      1425480   4    23:48:36  L3 (IPv6) - Dynamic
50::2
tcp :16      :32      V147      :0x0
23758      1425480   4    23:48:36  L3 (IPv6) - Dynamic
50::2
tcp :16      :32      V147      :0x0
23758      1425480   4    23:48:36  L3 (IPv6) - Dynamic
50::2
tcp :16      :32      V147      :0x0
23758      1425480   4    23:48:36  L3 (IPv6) - Dynamic
50::2
tcp :16      :32      V147      :0x0
23758      1425480   4    23:48:36  L3 (IPv6) - Dynamic
50::2
tcp :16      :32      V147      :0x0
23758      1425480   4    23:48:36  L3 (IPv6) - Dynamic
Router#
```

次に、IPv6 マイクロフロー ポリシング情報を表示する例を示します。

```
Router# show mls netflow ipv6 qos
Displaying Netflow entries in Supervisor Earl
DstIP                               SrcIP
-----
Prot:SrcPort:DstPort  Src i/f      :AdjPtr  Pkts      Bytes
-----
LastSeen  QoS    PoliceCount  Threshold  Leak      Drop  Bucket
-----
101::3
icmp:0    :0     --           0x0        0         0     0
22:22:09  0x0    0           0          0         NO    0
101::2
icmp:0    :0     --           0x0        0         0     0
22:22:09  0x0    0           0          0         NO    0
Router#
```

■ show mls netflow ipv6

次に、特定のモジュールの IPv6 マイクロフロー ポリシング情報を表示する例を示します。

```
Router# show mls netflow ipv6 qos module 7
Displaying Netflow entries in module 7
DstIP                               SrcIP
-----
Prot:SrcPort:DstPort  Src i/f          :AdjPtr  Pkts      Bytes
-----
LastSeen  QoS    PoliceCount  Threshold  Leak      Drop  Bucket
-----
101::2
icmp:0    :0      --          0x0        0         0      0
22:22:56  0x0    0           0          0         NO    0
101::3
icmp:0    :0      --          0x0        0         0      0
22:22:56  0x0    0           0          0         NO    0
Router#
```

次に、テキスト ラッピングをオフにしたときの出力例を示します。

```
Router# show mls netflow ipv6 qos nowrap
Displaying Netflow entries in Supervisor Earl
DstIP                               SrcIP
Prot:SrcPort:DstPort  Src i/f          :AdjPtr  Pkts      Bytes      LastSeen
QoS    PoliceCount  Threshold  Leak      Drop  Bucket
-----
-----
101::3
:0      --          0x0        0         0         22:22:19  0x0    0      icmp:0
0       0          NO    0
101::2
:0      --          0x0        0         0         22:22:19  0x0    0      icmp:0
0       0          NO    0
Router#
```

次に、特定のモジュールについてテキスト ラッピングをオフにしたときの出力例を示します。

```
Router# show mls netflow ipv6 qos nowrap module 7
Displaying Netflow entries in module 7
DstIP                               SrcIP
Prot:SrcPort:DstPort  Src i/f          :AdjPtr  Pkts      Bytes      LastSeen
QoS    PoliceCount  Threshold  Leak      Drop  Bucket
-----
-----
101::3
:0      --          0x0        0         0         22:22:38  0x0    0      icmp:0
0       0          NO    0
101::2
:0      --          0x0        0         0         22:22:38  0x0    0      icmp:0
0       0          NO    0
Router#
```

関連コマンド

コマンド	説明
clear mls netflow	MLS NetFlow のショートカット エントリをクリアします。

show mls qos

MLS QoS 情報を表示するには、**show mls qos** コマンドを使用します。

```
show mls qos [{arp | ipv6 | ip | ipx | last | mac | maps [map-type]}] [{interface
interface-number} | {slot slot} | {null interface-number} | {port-channel number} |
{vlan vlan-id}]]
```

シンタックスの説明

arp	(任意) ARP 情報を表示します。
ipv6	(任意) IPv6 情報を表示します。
ip ipx	(任意) MLS IP または IPX ステータスに関する情報を表示します。
last	(任意) 最終パケットのポリシングに関する情報を表示します。
mac	(任意) MAC アドレスベースの QoS ステータスに関する情報を表示します。
maps	(任意) QoS マッピングに関する情報を表示します。
<i>map-type</i>	(任意) マップタイプ。有効値については、「使用上のガイドライン」を参照してください。
<i>interface</i>	(任意) インターフェイスタイプ。有効値は ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 ge-wan 、 pos 、および atm です。
<i>interface-number</i>	(任意) モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
slot slot	(任意) スロット番号を指定します。グローバルおよびインターフェイス単位の QoS イネーブルおよびディセーブル設定、およびグローバル QoS カウンタを表示します。
null interface-number	(任意) ヌルインターフェイスを指定します。有効値は 0 です。
port-channel number	(任意) チャネルインターフェイスを指定します。有効値は 1 ~ 282 の範囲の最大 64 個の値です。
vlan vlan-id	(任意) VLAN ID を指定します。有効値は 1 ~ 4094 です。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

interface-number 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、指定されたインターフェイスタイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

257 ~ 282 の **port-channel number** 値は、CSM および FWSM だけでサポートされています。

map-types の有効値は次のように定義されます。

- **cos-dscp** : 表示する入力 CoS/DSCP マッピングを指定します。有効値は 0 ~ 7 です。
- **dscp-cos** : 出力 DSCP/CoS マッピングを表示します。
- **dscp-exp** : MPLS ドメイン入力および出力における DSCP/EXP マッピングを表示します。このキーワードはサポートされていません。
- **exp-dscp** : MPLS ドメイン入力および出力における EXP/DSCP マッピングを表示します。このキーワードはサポートされていません。
- **ip-prec-dscp value** : 表示する入力 IP precedence/DSCP マッピングを指定します。有効値は 0 ~ 7 です。
- **policed-dscp** : ポリシング済み DSCP 値とマーキング済み DSCP 値のマッピングを表示します。

dscp-exp および **exp-dscp** オプションは、Supervisor Engine 720 が搭載された Catalyst 6500 シリーズスイッチだけでサポートされます。

例

次に、最後に記録されたパケットに関する情報を表示する例を示します。

```
Router# show mls qos last
QoS engine last packet information:
  Packet was transmitted
  Output TOS/DSCP: 0xC0/48[unchanged]   Output COS: 0[unchanged]
  Aggregate policer index: 0(none)
  Microflow policer index: 0(none)
Router#
```

次に、QoS マップの設定を表示する例を示します。

```
Router# show mls qos maps
Policed-dscp map:
-----
00: 00 01 02 03 04 05 06 07 08 09
10: 10 11 12 13 14 15 16 17 18 19
20: 20 21 22 23 24 25 26 27 28 29
30: 30 31 32 33 34 35 36 37 38 39
40: 40 41 42 43 44 45 46 47 48 49
50: 50 51 52 53 54 55 56 57 58 59
60: 60 61 62 63

Dscp-cos map:
-----
00: 00 00 00 00 00 00 00 00 01 01
10: 01 01 01 01 01 01 02 02 02 02
20: 02 02 02 02 03 03 03 03 03 03
30: 03 03 04 04 04 04 04 04 04 04
40: 05 05 05 05 05 05 05 05 06 06
50: 06 06 06 06 06 06 07 07 07 07
60: 07 07 07 07

Cos-dscp map:
-----
cos: 0 1 2 3 4 5 6 7
-----
dscp: 0 8 16 24 32 40 48 56

IpPrecedence-dscp map:
-----
ipprec: 0 1 2 3 4 5 6 7
-----
```

```
dscp: 0 8 16 24 32 40 48 56
```

```
Router#
```

次に、DSCP 変換マッピング設定を確認する例を示します。

```
Router# show mls qos maps | begin DSCP mutation
DSCP mutation map mutmap1: (dscp= d1d2)
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 00 01 02 03 04 05 06 07 08 09
1 : 10 11 12 13 14 15 16 17 18 19
2 : 20 21 22 23 24 25 26 27 28 29
3 : 08 31 32 33 34 35 36 37 38 39
4 : 40 41 42 43 44 45 46 47 48 49
5 : 50 51 52 53 54 55 56 57 58 59
6 : 60 61 62 63
<...Output Truncated...>
Router#
```



(注)

DSCP 変換マップの表示では、マーキング済み DSCP 値がマトリックスの本体部分に表示されます。元の DSCP 値の 1 桁めは d1 のラベルがついたカラムに表示され、2 桁めは 1 番上の行に表示されます。たとえば、DSCP 30 は DSCP 08 にマッピングされます。

次に、IPv6 情報を表示する例を示します。

```
Router# show mls qos ipv6
QoS Summary [IPv6]: (* - shared aggregates, Mod - switch module)

Int Mod Dir Class-map DSCP Agg Trust Fl AgForward-By AgPoliced-By
      Id      Id
-----
All 7 - Default 0 0* No 0 189115356 0
Router#
```

次に、QoS 情報を表示する例を示します。

```
Router# show mls qos
QoS is enabled globally
Microflow policing is enabled globally
QoS ip packet dscp rewrite enabled globally

QoS is disabled on the following interfaces:
Fa6/3 Fa6/4

QoS DSCP-mutation map is enabled on the following interfaces:
Fa6/5
Vlan or Portchannel(Multi-Earl) policies supported: Yes
Egress policies supported: Yes

----- Module [5] -----
QoS global counters:
Total packets: 164
IP shortcut packets: 0
Packets dropped by policing: 0
IP packets with TOS changed by policing: 0
IP packets with COS changed by policing: 0
Non-IP packets with COS changed by policing: 0
MPLS packets with EXP changed by policing: 0
Router#
```

■ show mls qos

関連コマンド

コマンド	説明
mls qos (global configuration mode)	QoS 機能をグローバルにイネーブルにします。
mls qos (interface configuration mode)	インターフェイス上の QoS 機能をイネーブルにします。

show mls qos free-agram

スイッチ プロセッサ上の空の集約 RAM インデックス数を表示するには、**show mls qos free-agram** コマンドを使用します。

show mls qos free-agram

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドのデフォルト EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、スイッチ プロセッサ上の空の集約 RAM インデックス数を表示する例を示します。

```
Router# show mls qos free-agram
Total Number of Avalable AG RAM indices : 1023

Module [1]
Free AGIDs : 1023

Module [6]
Free AGIDs : 1023

Router#
```

show mls qos maps

QoS マップ設定および実行バージョンに関する情報を表示するには、**show mls qos maps** コマンドを使用します。

show mls qos maps [cos-dscp | cos-mutation | dscp-cos | dscp-exp | dscp-mutation | exp-dscp | exp-mutation | ip-prec-dscp | policed-dscp]

シンタックスの説明

cos-dscp	(任意) CoS/DSCP マップに関する情報を表示します。
cos-mutation	(任意) CoS 変換マップに関する情報を表示します。
dscp-cos	(任意) DSCP/CoS マップに関する情報を表示します。
dscp-exp	(任意) DSCP/exp マップに関する情報を表示します。
dscp-mutation	(任意) DSCP 変換マップに関する情報を表示します。
exp-dscp	(任意) exp/DSCP マップに関する情報を表示します。
exp-mutation	(任意) exp 変換マップに関する情報を表示します。
ip-prec-dscp	(任意) IP precedence/DSCP マップに関する情報を表示します。
policed-dscp	(任意) ポリシング設定 DSCP マップに関する情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、QoS マップ設定および実行バージョンに関する情報を表示する例を示します。

```
Router# show mls qos maps
Normal Burst Policed-dscp map: (dscp= d1d2)
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 00 01 02 03 04 05 06 07 08 09
1 : 10 11 12 13 14 15 16 17 18 19
2 : 20 21 22 23 24 25 26 27 28 29
3 : 30 31 32 33 34 35 36 37 38 39
4 : 40 41 42 43 44 45 46 47 48 49
5 : 50 51 52 53 54 55 56 57 58 59
6 : 60 61 62 63

Maximum Burst Policed-dscp map: (dscp= d1d2)
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 00 01 02 03 04 05 06 07 08 09
1 : 10 11 12 13 14 15 16 17 18 19
2 : 20 21 22 23 24 25 26 27 28 29
3 : 30 31 32 33 34 35 36 37 38 39
4 : 40 41 42 43 44 45 46 47 48 49
```

```

5 :    50 51 52 53 54 55 56 57 58 59
6 :    60 61 62 63

Dscp-cos map:                                (dscp= d1d2)
d1 :  d2 0  1  2  3  4  5  6  7  8  9
-----
0 :    00 00 00 00 00 00 00 00 00 01 01
1 :    01 01 01 01 01 01 01 02 02 02 02
2 :    02 02 02 02 03 03 03 03 03 03 03
3 :    03 03 04 04 04 04 04 04 04 04 04
4 :    05 05 05 05 05 05 05 05 05 06 06
5 :    06 06 06 06 06 06 07 07 07 07 07
6 :    07 07 07 07

Cos-dscp map:
cos:   0  1  2  3  4  5  6  7
-----
dscp:  0  8 16 24 32 40 48 56

IpPrecedence-dscp map:
ipprec: 0  1  2  3  4  5  6  7
-----
dscp:   0  8 16 24 32 40 48 56

```

Router#

次に、CoS/CoS マップの設定および実行バージョンを表示する例を示します。

Router# **show mls qos maps cos-mutation**

CoS mutation map test-map:

In-CoS : Out-CoS

```

-----
0 :      0
1 :      1
2 :      2
3 :      1
4 :      1
5 :      1
6 :      6
7 :      7

```

Router#

関連コマンド

コマンド	説明
mls qos map cos-dscp	信頼されたインターフェイスに入力 CoS/DSCP マップを定義します。
mls qos map cos-mutation	パケットの CoS を新しい CoS 値にマッピングします。
mls qos map dscp-cos	出力 DSCP/CoS マップを定義します。
mls qos map dscp-mutation	指定した DSCP 変換マップを定義します。
mls qos map ip-prec-dscp	信頼されたインターフェイスに入力 IP precedence/DSCP マップを定義します。
mls qos map policed-dscp	ポリシング済み DSCP 値とマーキング済み DSCP 値のマップを設定します。

show mls qos mpls

ポリシー マップの MPLS QoS クラスのインターフェイス サマリーを表示するには、**show mls qos mpls** コマンドを使用します。

```
show mls qos mpls [{interface interface-number} | {module slot}]
```

シンタックスの説明

<i>interface</i>	(任意) インターフェイス タイプ。有効値は fastethernet 、 gigabitethernet 、および tengigabitethernet です。
<i>interface-number</i>	モジュールおよびポート番号。有効値については、「 使用上のガイドライン 」を参照してください。
<i>module slot</i>	(任意) モジュールのスロット番号を指定します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、PFC3BXL または PFC3B モードだけでサポートされます。

interface-number 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

例

次に、ポリシー マップの MPLS QoS クラスのインターフェイス サマリーを表示する例を示します。

```
Router# show mls qos mpls
QoS Summary [MPLS]: (* - shared aggregates, Mod - switch module)
Int Mod Dir Class-map DSCP Agg Trust Fl AgForward-By AgPoliced-By
Id Id
-----
-----
Fa3/38 5 In exp2 0 1 dscp 0 378900 0
Fa3/41 5 In exp4 0 3 dscp 0 0 0
All 5 - Default 0 0* No 0 1191011240 0
Router#
```

関連コマンド

コマンド	説明
mls qos exp-mutation	出力 EXP 変換マップをインターフェイスに付加します。
mls qos map exp-dscp	内部 DSCP マップに入力 EXP 値を定義します。
mls qos map exp-mutation	パケットの EXP を新しい EXP 値にマッピングします。

show mls qos protocol

プロトコル パススルー情報を表示するには、**show mls qos protocol** コマンドを使用します。

show mls qos protocol [module num]

シンタックスの説明

module num	(任意) モジュール番号を指定します。
-------------------	---------------------

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドのデフォルト

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、プロトコル パススルー情報を表示する例を示します。

```
Router# show mls qos protocol
RIP : Passthru mode
OSPF : Passthru mode
ND : Policing mode Cir = 32000 Burst = 1000
----- Module [5] -----
Routing protocol RIP is using AgId 0*
Routing protocol OSPF is using AgId 0*
Routing protocol ND is using AgId 1
----- Module [6] -----
Routing protocol RIP is using AgId 0*
Routing protocol OSPF is using AgId 0*
Router#
```

関連コマンド

コマンド	説明
mls qos protocol	ルーティング プロトコル パケット ポリシングを定義します。

show mls qos statistics-export info

MLS 統計データ エクスポートのステータスおよび設定に関する情報を表示するには、**show mls qos statistics-export info** コマンドを使用します。

show mls qos statistics-export info

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、MLS 統計データ エクスポートのステータスおよび設定に関する情報を表示する例を示します。

```
Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
-----
Export Status : enabled
Export Interval : 250 seconds
Export Delimiter : @
Export Destination : 172.20.52.3, UDP port 514 Facility local6, Severity debug

QoS Statistics Data Export is enabled on following ports:
-----
FastEthernet5/24

QoS Statistics Data export is enabled on following shared aggregate policers:
-----
aggr1M

QoS Statistics Data Export is enabled on following class-maps:
-----
class3
Router#
```

関連コマンド

コマンド	説明
mls qos statistics-export (global configuration mode)	QoS 統計データのエクスポートをグローバルにイネーブルにします。
mls qos statistics-export (interface configuration mode)	ポート単位の QoS 統計データのエクスポートをイネーブルにします。
mls qos statistics-export aggregate-policer	名前付き集約ポリサー上で QoS 統計データのエクスポートをイネーブルにします。
mls qos statistics-export class-map	クラス マップの QoS 統計データのエクスポートをイネーブルにします。
mls qos statistics-export delimiter	QoS 統計データのエクスポート フィールドのデリミタを設定します。
mls qos statistics-export destination	QoS 統計データのエクスポートの宛先ホストおよび UDP ポート番号を設定します。
mls qos statistics-export interval	ポートまたは集約ポリサー QoS 統計データの読み込み頻度およびエクスポート頻度を指定します。

show mls rate-limit

MLS レート リミッタに関する情報を表示するには、**show mls rate-limit** コマンドを使用します。

show mls rate-limit [usage]

シンタックスの説明

usage (任意) レート リミッタ レジスタで使用される機能を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドの出力では、レート制限ステータスは次のいずれかとなります。

- **On** は、特定のケースが設定されているレートを示します。
- **Off** は、レート リミッタ タイプが設定されておらず、そのケースのパケットがレート制限を受けないことを示します。
- **On/Sharing** は、(手動設定ではない) 特定のケースが、同じ共有グループに属する別のレート リミッタの設定により影響を受けることを示します。
- ハイフンは、マルチキャスト パーシャル SC レート リミッタがディセーブルにされていることを示します。

コマンド出力では、レート制限の共有が次の情報を示しています。

- 共有がスタティックかダイナミック
- グループ ダイナミック共有コード

show mls rate-limit usage コマンドは、レート リミッタ タイプにより使用されるハードウェア レジスタを表示します。レジスタがどのレート リミッタ タイプによっても使用されない場合、出力には **Free** と表示されます。レジスタがあるレート リミッタ タイプにより使用される場合、**Used** およびそのレート リミッタ タイプが表示されます。

例

次に、レート制限ステータスに関する情報を表示する例を示します。

```
Router# show mls rate-limit
Sharing Codes: S - static, D - dynamic
Codes dynamic sharing: H - owner (head) of the group, g - guest of the group
```

Rate Limiter Type	Status	Packets/s	Burst	Sharing
MCAST NON RPF	Off	-	-	-
MCAST DFLT ADJ	On	100000	100	Not sharing
MCAST DIRECT CON	Off	-	-	-

show mls rate-limit

```

ACL BRIDGED IN      Off          -          -          -
ACL BRIDGED OUT    Off          -          -          -
IP FEATURES         Off          -          -          -
ACL VACL LOG       On           2000       1          Not sharing
CEF RECEIVE        Off          -          -          -
CEF GLEAN          Off          -          -          -
MCAST PARTIAL SC   On           100000     100       Not sharing
IP RPF FAILURE     On           100        10        Group:0 S
TTL FAILURE        On           1000       100       Not sharing
ICMP UNREAC. NO-ROUTE On          100        10        Group:0 S
ICMP UNREAC. ACL-DROP On          100        10        Group:0 S
ICMP REDIRECT      Off          -          -          -
MTU FAILURE        On           1000       100       Not sharing
MCAST IP OPTION    Off          -          -          -
UCAST IP OPTION    Off          -          -          -
LAYER_2 PDU        Off          -          -          -
LAYER_2 PT         Off          -          -          -
LAYER_2 PORTSEC    On           10000     1          Not sharing
IP ERRORS          On           100        10        Group:0 S
CAPTURE PKT       Off          -          -          -
MCAST IGMP         Off          -          -          -
MCAST IPv6 DIRECT CON Off         -          -          -
MCAST IPv6 ROUTE CNTL Off         -          -          -
MCAST IPv6 *G M BRIDG Off         -          -          -
MCAST IPv6 SG BRIDGE Off         -          -          -
MCAST IPv6 DFLT DROP Off         -          -          -
MCAST IPv6 SECOND. DR Off         -          -          -
MCAST IPv6 *G BRIDGE Off         -          -          -
MCAST IPv6 MLD     Off         -          -          -
IP ADMIS. ON L2 PORT Off         -          -          -
Router#

```

次に、レート制限の使用に関する情報を表示する例を示します。

```

Router# show mls rate-limit usage
Rate Limiter Type          Packets/s  Burst
-----
Layer3 Rate Limiters:
RL# 0: Free                -          -
RL# 1: Free                -          -
RL# 2: Free                -          -
RL# 3: Used                MCAST DFLT ADJ  100000     100
RL# 4: Used                MTU FAILURE     1000       100
RL# 5: Used                TTL FAILURE     1000       100
RL# 6: Used                IP RPF FAILURE  100        10
                        ICMP UNREAC. NO-ROUTE  100        10
                        ICMP UNREAC. ACL-DROP  100        10
                        IP ERRORS  100        10
RL# 7: Used                ACL VACL LOG    2000       1
RL# 8: Rsvd for capture    -          -
Layer2 Rate Limiters:
RL# 9: Reserved
RL#10: Reserved
RL#11: Free                -          -
RL#12: Used                LAYER_2 PORTSEC  10000     1
Router #

```

関連コマンド

コマンド	説明
mls rate-limit layer2	レイヤ 2 制御パケットに対するレート リミッタのイネーブル化および設定を行います。
mls rate-limit multicast ipv4	IPv4 マルチキャスト パケットに対するレート リミッタのイネーブル化および設定を行います。
mls rate-limit multicast ipv6	IPv6 マルチキャスト レート リミッタを設定します。
mls rate-limit unicast acl	ACL ブリッジド レート リミッタのイネーブル化および設定を行います。

show mls sampling

サンプリング済み NDE ステータスに関する情報を表示するには、**show mls sampling** コマンドを使用します。

show mls sampling

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

サンプリング済み NetFlow は、レイヤ 3 インターフェイスだけでサポートされています。

例

次に、サンプリング済み NDE ステータスに関する情報を表示する例を示します。

```
Router# show mls sampling
time-based sampling is enabled
1 out of every 1024 packets is being sampled.
Sampling Interval and Period is 4 millisec per 4096 millisec
Router#
```

関連コマンド

コマンド	説明
mls netflow sampling	インターフェイス上でサンプリング済み NetFlow をイネーブルにします。
mls sampling	サンプリング済み NetFlow のイネーブル化およびサンプリング方式の指定を行います。

show mls statistics

IP、マルチキャスト、レイヤ 2 プロトコル、QoS の MLS 統計情報を表示するには、**show mls statistics** コマンドを使用します。

show mls statistics [module num | protocol type]

シンタックスの説明	パラメータ	説明
	module num	(任意) 特定のモジュールの MLS 統計情報を表示します。
	protocol type	(任意) 1 つのプロトコル (Telnet、FTP、WWW など) に基づいて MLS 統計情報を表示します。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン スイッチングされた総パケットの表示されるパフォーマンスは、最後の 30 秒間の平均レートとして計算されたレートです。

入力 ACL 拒否パケット数は、Total packets L3 Switched フィールドと Total packets dropped by ACL フィールドに表示されます。

RPF 障害パケット数は、Total packets L3 Switched フィールドに表示されます。

IP マルチキャスト送信元が mroute テーブルに (*,G) エントリがないマルチキャスト グループにトラフィックを送信した場合、**show mls statistics** コマンドは、これらのパケットを Total Mcast Packets Switched/Routed フィールドに増分として表示します。これらのパケットは、該当グループにはレシーバーがなく、mroute テーブルにエントリがないので、ハードウェアで廃棄されます。

例 次に、すべてのモジュールの MLS 統計情報を表示する例を示します。

```
Router# show mls statistics

Statistics for Earl in Module 2

L2 Forwarding Engine
  Total packets Switched          : 20273@ 22552 pps

L3 Forwarding Engine
  Total Packets Bridged           : 20273
  Total Packets FIB Switched     : 7864
  Total Packets ACL Routed       : 0
  Total Packets Netflow Switched : 0
  Total Mcast Packets Switched/Routed : 220598
  Total ip packets with TOS changed : 0
  Total ip packets with COS changed : 0
```

■ show mls statistics

```
Total non ip packets COS changed      : 0
Total packets dropped by ACL           : 0
Total packets dropped by Policing      : 705757744
```

Statistics for Earl in Module 9

```
L2 Forwarding Engine
  Total packets Switched                : 16683@ 1 pps
```

```
L3 Forwarding Engine
  Total Packets Bridged                  : 0
  Total Packets FIB Switched            : 0
  Total Packets ACL Routed              : 0
  Total Packets Netflow Switched        : 0
  Total Mcast Packets Switched/Routed   : 0
  Total ip packets with TOS changed     : 0
  Total ip packets with COS changed     : 0
  Total non ip packets COS changed     : 0
  Total packets dropped by ACL          : 0
  Total packets dropped by Policing     : 277949053
```

Router#

次に、特定のモジュールの MLS 統計情報を表示する例を示します。

```
Router# show mls statistics module 1
```

Statistics for Earl in Module 1

```
L2 Forwarding Engine
  Total packets Switched                : 2748166@ 22332 pps
```

>>

```
L3 Forwarding Engine
  Total Packets Bridged                  : 92750@ 34 pps
  Total Packets FIB Switched            : 7
  Total Packets ACL Routed              : 0
  Total Packets Netflow Switched        : 0
  Total Mcast Packets Switched/Routed   : 3079200
  Total ip packets with TOS changed     : 0
  Total ip packets with COS changed     : 0
  Total non ip packets COS changed     : 0
  Total packets dropped by ACL          : 0
  Total packets dropped by Policing     : 0
  Total Unicast RPF failed packets     : 0
```

Errors

```
MAC/IP length inconsistencies         : 0
Short IP packets received              : 0
IP header checksum errors              : 0
MAC/IPX length inconsistencies        : 0
Short IPX packets received             : 0
```

Router#

show mls table-contention

TCL 情報を表示するには、**show mls table-contention** コマンドを使用します。

show mls table-contention {detailed | summary | aggregate}

シンタックスの説明	オプション	説明
	detailed	TCL の詳細情報を表示します。
	summary	TCL レベルを表示します。
	aggregate	Supervisor Engine 720 内のすべてのミス フローの集約カウントおよび Supervisor Engine 2 内のページ ヒットおよびページ ミスを表示します。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン **aggregate** キーワードを入力すれば、Supervisor Engine 720 における NetFlow 作成障害や NetFlow ハッシュ エイリアスの統計情報を表示できます。

aggregate キーワードを入力すれば、Supervisor Engine 2 内のページ ヒットおよびページ ミスを表示できます。

Supervisor Engine 720 の場合、**summary** および **detailed** キーワードでは、対応するレジスタの最新の値が表示されます。

例 次に、TCL 情報の詳細リストを表示する例を示します。

```
Router# show mls table-contention detailed
Detailed Table Contention Level Information
=====
Layer 3
-----
L3 Contention Level:      0
Page Hits Requiring 1 Lookup   =      31
Page Hits Requiring 2 Lookups  =       0
Page Hits Requiring 3 Lookups  =       0
Page Hits Requiring 4 Lookups  =       0
Page Hits Requiring 5 Lookups  =       0
Page Hits Requiring 6 Lookups  =       0
Page Hits Requiring 7 Lookups  =       0
Page Hits Requiring 8 Lookups  =       0
Page Misses                   =       0
Router#
```

次に、TCL 情報のサマリーを表示する例を示します。

■ show mls table-contention

```
Router# show mls table-contention summary
Summary of Table Contention Levels (on a scale of 0 (lowest) to 3 (highest))
=====
L3 Contention Level: 0
```

次に、Supervisor Engine 720 内のすべてのミス フローの集約カウントおよび Supervisor Engine 2 内のページ ヒットおよびページ ミスを表示する例を示します。

```
Router# show mls table-contention aggregate
Earl in Module 1
Detailed Table Contention Level Information
=====
Layer 3
-----
L3 Contention Level:      0
Page Hits Requiring 1 Lookup   =      24000
Page Hits Requiring 2 Lookups  =       480
Page Hits Requiring 3 Lookups  =        0
Page Hits Requiring 4 Lookups  =        0
Page Hits Requiring 5 Lookups  =        0
Page Hits Requiring 6 Lookups  =        0
Page Hits Requiring 7 Lookups  =        0
Page Hits Requiring 8 Lookups  =        0
Page Misses                   =        0
```

show mmls igmp explicit-tracking

ホスト トラッキング データベースに関する情報を表示するには、**show mmls igmp explicit-tracking** コマンドを使用します。

show mmls igmp explicit-tracking [*vlan-id*]

シンタックスの説明 *vlan-id* (任意) VLAN ID を指定します。有効値は 1 ~ 4094 です。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード スイッチ プロセッサ — 特権 EXEC (Switch-sp#)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、特定の VLAN のホスト トラッキング データベースに関する情報を表示する例を示します。

Switch-sp# **show mmls igmp explicit-tracking 27**

Source/Group	Interface	Reporter	Filter_mode
10.1.1.1/224.1.1.1	V127:3/25	16.27.2.3	INCLUDE
10.2.2.2/224.1.1.1	V127:3/25	16.27.2.3	INCLUDE

Router#

show mmls msc

MMLS に関する情報を表示するには、**show mmls msc** コマンドを使用します。

show mmls msc [cache | entry | icroif-cache | rpdf-cache | statistics | vpn]

シンタックスの説明

cache	(任意) プロセス キャッシュのマルチキャスト ショートカットに関する情報を表示します。
entry	(任意) レイヤ 3 内のダンプ ハードウェア エントリに関する情報を表示します。
icroif-cache	(任意) ダンプ ICROIF キャッシュに関する情報を表示します。
rpdf-cache	(任意) ダンプ Bidir RPDF キャッシュに関する情報を表示します。
statistics	(任意) マルチキャスト ショートカット プロセスに関する統計情報を表示します。
vpn	(任意) VPN に関する情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

スイッチ プロセッサ — 特権 EXEC (Switch-sp#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、MMLS に関する情報を表示する例を示します。

```
Switch-sp# show mmls msc

General Info
-----+-----+
Number shortcuts in software database      1890
Number of MFD in software database         1890
Router MAC                                  0001.64f8.1b00
Internal Vlan                               4093
Aggregation Vlan                           0
Aggregation Indexes                        0
Current Size of inputQ                      0
Maximum Size of inputQ                      2
flow statistics timeout [sec]              25
non-rpf MFDs purge timeout [sec]           20
non-rpf MFDs aging timeout [sec]           2.0
Switch-sp#
```

次に、MMLS ショートカット プロセス キャッシュに関する情報を表示する例を示します。

```
Switch-sp# show mmls msc cache

-----macg cache buckets for vpn 0-----
Bucket 90 #g: 1
Group mac address: 0100.5e01.0105
```

```

$$$ (S,G,C): (100.0.0.4, 224.1.1.5, 100)      mfd_flag: 1 type: Sparse
$$$ (S,G,C): (0.0.0.0, 224.1.1.5, 1)        mfd_flag: 1 type: Sparse
### vlan: 100  sc_count: 0 rpf_count: 1
### vlan: 1    sc_count: 0 rpf_count: 1
Bucket 91 #g: 1
Group mac address: 0100.5e01.0104
$$$ (S,G,C): (100.0.0.4, 224.1.1.4, 100)      mfd_flag: 1 type: Sparse
$$$ (S,G,C): (0.0.0.0, 224.1.1.4, 1)        mfd_flag: 1 type: Sparse
### vlan: 100  sc_count: 0 rpf_count: 1
### vlan: 1    sc_count: 0 rpf_count: 1
Bucket 92 #g: 1
Group mac address: 0100.5e01.0103
$$$ (S,G,C): (100.0.0.4, 224.1.1.3, 100)      mfd_flag: 1 type: Sparse
$$$ (S,G,C): (0.0.0.0, 224.1.1.3, 1)        mfd_flag: 1 type: Sparse
### vlan: 100  sc_count: 0 rpf_count: 1
### vlan: 1    sc_count: 0 rpf_count: 1
Bucket 93 #g: 1
Group mac address: 0100.5e01.0102
$$$ (S,G,C): (100.0.0.4, 224.1.1.2, 100)      mfd_flag: 1 type: Sparse
$$$ (S,G,C): (0.0.0.0, 224.1.1.2, 1)        mfd_flag: 1 type: Sparse
### vlan: 100  sc_count: 0 rpf_count: 1
### vlan: 1    sc_count: 0 rpf_count: 1
Bucket 94 #g: 1
Group mac address: 0100.5e01.0101
$$$ (S,G,C): (100.0.0.4, 224.1.1.1, 100)      mfd_flag: 1 type: Sparse
$$$ (S,G,C): (0.0.0.0, 224.1.1.1, 1)        mfd_flag: 1 type: Sparse
### vlan: 100  sc_count: 0 rpf_count: 1
### vlan: 1    sc_count: 0 rpf_count: 1
Switch-sp#

```

次に、ダンプ ICROIF キャッシュ情報を表示する例を示します。

```

Switch-sp# show mmls msc icroif-cache

msc_local_icroif_index: 0x493
msc_global_icroif_index: 0x494

ICROIF CACHE:
-----
Module mask: 0x8      Icroif_index: 0x495
Switch-sp#

```

次に、PIM-RP の DF インターフェイスのダンプ リストを表示する例を示します。

```

Switch-sp# show mmls msc rpdf-cache

----- RP-CACHE [VPN-0] -----

Bucket# :0

RP-addr: 1.0.0.1, Rpf: 0 Vpn: 0
DF-index: 0
DF-list: 201 202 203 204 205 206 207 208 209 210
         211 212
Group-list:
          (224.1.0.0/24, H)
G/m-count: 1, G/32-count: 1

Bucket# :2

RP-addr: 3.0.0.1, Rpf: 0 Vpn: 0
DF-index: 2
DF-list: 201 202 203 204 205 206 207 208 209 210
         211 212

```

show mmls msc

```

Group-list:
    (224.1.2.0/24, H)
G/m-count: 1, G/32-count: 0

Bucket# :3

RP-addr: 2.0.0.1, Rpf: 0 Vpn: 0
DF-index: 1
DF-list: 201 202 203 204 205 206 207 208 209 210
         211 212
Group-list:
    (224.1.1.0/24, H)
G/m-count: 1, G/32-count: 1

Bucket# :5

RP-addr: 4.0.0.1, Rpf: 0 Vpn: 0
DF-index: 3
DF-list: 201 202 203 204 205 206 207 208 209 210
         211 212
Group-list:
    (224.1.3.0/24, H)
G/m-count: 1, G/32-count: 0

Switch-sp#
    
```

次に、マルチキャスト ショートカット プロセスの統計情報を表示する例を示します。

Switch-sp# **show mmls msc statistics**

```

Communication Statistics
-----+-----+
Number MSM PDU Received          1
Number MSM PDU Sent              1
Unsolicited Feature Notification Sent 1
Feature Notification Received    2
Feature Notification Sent        2
Stop retry Sent                  0
Stop download Sent               0

Error Statistics
-----+-----+
L2 entry not found               0
LTL full error                   0
MET full error                   0

Debug Statistics
-----+-----+
HW Met failure                   0
HW Dist failure                  0
HW L3 Install failure            0
HW L3 Update failure             0

TLV Statistics
-----+-----+
INSTALL TLV Received             0
SELECTIVE DELETE TLV Received   0
GROUP DELETE TLV Received       0
UPDATE TLV Received              0
INPUT VLAN DELETE TLV Received  0
OUTPUT VLAN DELETE TLV Received 0
GLOBAL DELETE TLV Received      0
MFD INSTALL TLV Received        0
MFD DELETE TLV Received         0
MFD GLOBAL DELETE Received      0
    
```

```

NRPF MFD INSTALL TLV Received          0
NRPF MFD DELETE TLV Received           0
SUBNET INSTALL TLV Received            15
SUBNET DELETE TLV Received             0
MVPN INSTALL TLV Received              0
MVPN SELECTIVE DELETE TLV Received     0
MVPN UPDATE TLV Received               0
MVPN GROUP DELETE TLV Received         0
MVPN MFD INSTALL TLV Received          0
MVPN MFD DELETE TLV Received           0
MVPN BIDIR RPDF UPDATE TLV Received    0
MVPN BIDIR RP UPDATE TLV Received      0
MVPN BIDIR CLEAR ALL GRP TLV Received  0
MVPN BIDIR CLEAR RP GRP TLV Received   0
MVPN BIDIR CLEAR ALL DF TLV Received   0
MVPN BIDIR CLEAR RP DF TLV Received    0
MVPN BIDIR CLEAR ALL RP TLV Received   0
MVPN BIDIR NONDF INSTALL TLV Received  0

INSTALL TLV Ack Sent                   0
SELECTIVE DELETE TLV Ack Sent          0
GROUP DELETE TLV Ack Sent              0
UPDATE TLV Ack Sent                    0
INPUT VLAN DELETE TLV Ack Sent         0
OUTPUT VLAN DELETE TLV Ack Sent        0
GLOBAL DELETE TLV Ack Sent             0
MFD INSTALL TLV Ack Sent               0
MFD DELETE TLV Ack Sent                0
MFD GLOBAL DELETE Ack Sent             0
NRPF MFD INSTALL TLV Ack Sent          0
NRPF MFD DELETE TLV Ack Sent           0
SUBNET INSTALL TLV Ack Sent            15
SUBNET DELETE TLV Ack Sent             0
MVPN INSTALL TLV Ack Sent              0
MVPN SELECTIVE DELETE TLV Ack Sent     0
MVPN UPDATE TLV Ack Sent               0
MVPN GROUP DELETE TLV Ack Sent         0
MVPN MFD INSTALL TLV Ack Sent          0
MVPN MFD DELETE TLV Ack Sent           0
MVPN BIDIR RPDF UPDATE TLV Ack Sent    0
MVPN BIDIR RP UPDATE TLV Ack Sent      0
MVPN BIDIR CLEAR ALL GRP TLV Ack Sent  1
MVPN BIDIR CLEAR RP GRP TLV Ack Sent   0
MVPN BIDIR CLEAR ALL DF TLV Ack Sent   0
MVPN BIDIR CLEAR RP DF TLV Ack Sent    0
MVPN BIDIR CLEAR ALL RP TLV Ack Sent   0
MVPN BIDIR NONDF INSTALL TLV Ack Sent  0

TLV Error Statistics
-----+-----
Generic error                          0
L3 entry exist error                    0
Hash collision error                    0
L3 entry not found                      0
MFD exist error                         0
MFD not found error                     0
Invalid subnet error                    0
Bidir-RP not found error                 0
Bidir-DF partial fail error             0
Bidir-DF Table full error               0

```

■ show mmls msc

```
TLV Debug Statistics
-----+-----+
Non RPF L3 failure          0
Bidir DF install           0
Bidir DF failure           0
Bidir NDF install          0
Bidir NDF failure         0
Bidir DF err-tlv sent      0
Bidir GRP err-tlv sent    0
Switch-sp#
```

show mobility

レイヤ 3 モビリティおよびワイヤレス ネットワークに関する情報を表示するには、**show mobility** コマンドを使用します。

```
show mobility {{ap [ipaddr]} | {mn [ip ipaddr]} | {mac mac-addr} | {network network-id}
              | status}
```

シンタックスの説明

ap	アクセス ポイントに関する情報を表示します。
<i>ipaddr</i>	(任意) IP アドレス
mn	モバイル ノードに関する情報を表示します。
ip ipaddr	(任意) IP データベース スレッドに関する情報を表示します。
mac mac-addr	(任意) MAC データベース スレッドに関する情報を表示します。
network network-id	特定のワイヤレス ネットワーク ID に関する情報を表示します。
status	ステータス情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、WLSM が搭載された Catalyst 6500 シリーズ スイッチだけでサポートされます。

例

次に、アクセス ポイントに関する情報を表示する例を示します。

```
Router# show mobility ap
AP IP Address   AP Mac Address Wireless Network-ID
-----
148.1.1.2 000d.29a2.a852 101 102 109 103
Router#
```

次に、特定のネットワーク ID のアクセス ポイントに関する情報を表示する例を示します。

```
Router# show mobility ap 148.1.1.2 detail
IP Address : 148.1.1.2
MAC Address : 000d.29a2.a852
Participating Wireless Tunnels: 101, 102, 109, 103

Registered Mobile Nodes on AP {148.1.1.2, 000d.29a2.a852} :
MN Mac Address MN IP Address AP IP Address Wireless Network-ID
-----
000a.8afa.85c9 10.1.3.11 148.1.1.2 103
000d.bdb7.83f7 10.1.2.11 148.1.1.2 102
```

show mobility

```

000d.bdb7.83fb 10.1.1.11 148.1.1.2 101
Router#

Router# show mobility network-id 101
Wireless Network ID : 101
Wireless Tunnel Source IP Address : 1.1.1.1
Wireless Network Properties : Trusted
Wireless Network State : Up

Registered Access Point on Wireless Network 101:
AP IP Address AP Mac Address Wireless Network-ID
-----
148.1.1.2 000d.29a2.a852 101 102 109 103

Registered Mobile Nodes on Wireless Network 101:
MN Mac Address MN IP Address AP IP Address Wireless Network-ID
-----
000d.bdb7.83fb 10.1.1.11 148.1.1.2 101
Router#

Router# show mobility status
WLAN Module is located in Slot: 4 (HSRP State: Active) LCP
Communication status      : up
MAC address used for Proxy ARP: 0030.a349.d800
Number of Wireless Tunnels      : 1
Number of Access Points        : 2
Number of Mobile Nodes         : 0
Wireless Tunnel Bindings:
Src IP Address   Wireless Network-ID   Flags
-----
1.1.1.1         101                               B
Flags: T=Trusted, B=IP Broadcast enabled, A=TCP Adjust-mss enabled
Router#

```

関連コマンド

コマンド	説明
mobility	ワイヤレス mGRE トンネルを設定します。

show module

モジュールのステータスと情報を表示するには、**show module** コマンドを使用します。

show module [*mod-num* | **all** | **power** | **provision** | **version**]

シンタックスの説明

mod-num	(任意) モジュール番号
all	(任意) すべてのモジュールの情報を表示します。
power	(任意) 管理ステータスと動作ステータスを表示します。
provision	(任意) モジュール プロビジョニングに関するステータスを表示します。
version	(任意) バージョン情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

show module コマンド出力の Mod Sub-Module フィールドには、スーパーバイザ エンジン番号に、アップリンク ドータ カードのモジュール タイプおよび情報が付加されて表示されます。

引数を指定しないで **show module** コマンドを入力すると、**show module all** コマンドを入力した場合と同じになります。

例

次に、Supervisor Engine 720 が搭載された Catalyst 6500 シリーズ スイッチのすべてのモジュールに関する情報を表示する例を示します。

```
Router# show module
Mod Ports Card Type                               Model                               Serial No.
-----
  5      2 Supervisor Engine 720 (Active)          WS-SUP720-BASE                     SAD0644030K
  8     48 aCEF720 48 port 10/100/1000 Ethernet   WS-X6748-GE-TX                     SAD07010045
  9     32 dCEF720 32 port Gigabit Ethernet      WS-X6832-SFP                       SAD07010045

Mod MAC addresses                               Hw   Fw       Sw       Status
-----
  5 00e0.aabb.cc00 to 00e0.aabb.cc3f           1.0  12.2(2003012 12.2(2003012 Ok
  8 0005.9a3b.d8c4 to 0005.9a3b.d8c7           0.705 7.1(0.12-Eng 12.2(2003012 Ok
  9 00e0.b0ff.f0f4 to 00e0.b0ff.f0f5           0.207 12.2(2002082 12.2(2003012 Ok

Mod Sub-Module                               Model                               Serial                               Hw   Status
-----
  5 Policy Feature Card 3                      WS-F6K-PFC3                        SAD0644031P                       0.302 Ok
  5 PISA Daughtercard                          WS-SUP720                           SAD06460172                       0.701

Mod Online Diag Status
```

show module

```

-----
 5 Not Available
 7 Bypass
 8 Bypass
 9 Bypass
Router#

```

次に、特定のモジュールの情報を表示する例を示します。

```

Router# show module 2
Mod Ports Card Type                               Model                               Serial No.
-----
 5      2 Supervisor Engine 720 (Active)         WS-SUP720-BASE                     SAD0644030K

Mod MAC addresses                               Hw   Fw           Sw           Status
-----
 5 00e0.aabb.cc00 to 00e0.aabb.cc3f  1.0  12.2(2003012 12.2(2003012 Ok

Mod Sub-Module                               Model                               Serial                               Hw   Status
-----
 5 Policy Feature Card 3                     WS-F6K-PFC3                       SAD0644031P                       0.302 Ok
 5 PISA Daughtercard                         WS-SUP720                          SAD06460172                       0.701

Mod Online Diag Status
-----
 5 Not Available
Router#

```

次に、バージョン情報を表示する例を示します。

```

Router# show module version
Mod Port Model                               Serial #   Versions
-----
 2 0      WS-X6182-2PA                               Hw : 1.0
                                     Fw : 12.2(20030125:231135)
                                     Sw : 12.2(20030125:231135)
 4 16    WS-X6816-GBIC                         SAD04400CEE Hw : 0.205
 6 2     WS-X6K-SUP3-BASE                     SAD064300GU Hw : 0.705
                                     Fw : 7.1(0.12-Eng-02)TAM
                                     Sw : 12.2(20030125:231135)
                                     Sw1: 8.1(0.45)KIS
      WS-X6K-SUP3-PFC3                       SAD064200VR Hw : 0.701
                                     Fw : 12.2(20021016:001154)
                                     Sw : 12.2(20030125:231135)
      WS-F6K-PFC3                           SAD064300M7 Hw : 0.301
 9 48    WS-X6548-RJ-45                       SAD04490BAC Hw : 0.301
                                     Fw : 6.3(1)
                                     Sw : 7.5(0.30)CFW11

Router#

```

次に、モジュールの管理ステータスと動作ステータスを表示する例を示します。

```

Router# show module power
Mod Card Type                               Admin Status Oper Status
-----
 1 SFM-capable 48-port 10/100 Mbps RJ45     on           on
 4 SFM-capable 16 port 1000mb GBIC         on           on
 5 Supervisor Engine 720 (Active)         on           on

Router#

```

次に、モジュール プロビジョニング情報を表示する例を示します。

```
Router# show module provision
Module Provision
 1    dynamic
 2    dynamic
 3    dynamic
 4    dynamic
 5    dynamic
 6    dynamic
 7    dynamic
 8    dynamic
 9    dynamic
10    dynamic
11    dynamic
12    dynamic
13    dynamic
Router#
```

show monitor permit-list

設定されている許可リストの状態とインターフェイスを表示するには、**show monitor permit-list** コマンドを使用します。

show monitor permit-list

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、設定済みの許可リストの状態とインターフェイスを表示する例を示します。

```
Router# show monitor permit-list
SPAN Permit-list      :Admin Enabled
Permit-list ports     :Gi5/1-4,Gi6/1
Router(config)#
```

関連コマンド

コマンド	説明
monitor permit-list	宛先ポート許可リストを設定するか、既存の宛先ポート許可リストに追加します。

show monitor session

ERSPAN、SPAN、および RSPAN セッションに関する情報を表示するには、**show monitor session** コマンドを使用します。

show monitor session [*{range session-range}*] | **local** | **remote** | **all** | *session*]

show monitor session [*erspan-destination* | *erspan-source*] [**detail**]

シンタックスの説明

range session-range	(任意) セッションの範囲を表示します。有効値は 1 ~ 66 です。詳細については、「使用上のガイドライン」を参照してください。
local	(任意) ローカル SPAN セッションだけを表示します。
remote	(任意) RSPAN の送信元および宛先セッションを両方とも表示します。
all	(任意) すべてのセッションを表示します。
<i>session</i>	(任意) セッション番号。有効値は 1 ~ 66 です。
erspan-destination	(任意) 宛先 ERSPAN セッションに関する情報だけを表示します。
erspan-source	(任意) 送信元 ERSPAN セッションに関する情報だけを表示します。
detail	(任意) 詳細なセッション情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

セッション範囲を入力する場合は、ダッシュ (-) を使用して範囲を指定するか、またはカンマ (,) を使用して複数のエントリを区切ります。カンマまたはダッシュの前後にスペースを入力しないでください。複数の範囲を入力するには、範囲をカンマで区切ります。

セッションを指定しないで **show monitor session** コマンドを入力すると、すべてのセッションの情報が表示されます。

例

次に、特定のセッションに関するモニタ設定の保存済みバージョンを表示する例を示します。

```
Router# show monitor session 2
Session 2
-----
Type : Remote Source Session
Source Ports:
    RX Only:      Fa1/1-3
Dest RSPAN VLAN: 901
Router#
```

show monitor session

次に、特定のセッションに関するモニタ設定の保存済みバージョンの詳細情報を表示する例を示します。

```
Router# show monitor session 2 detail
Session 2
-----
Type : Remote Source Session

Source Ports:
  RX Only:      Fa1/1-3
  TX Only:      None
  Both:         None
Source VLANs:
  RX Only:      None
  TX Only:      None
  Both:         None
Source RSPAN VLAN: None
Destination Ports: None
Filter VLANs:   None
Dest RSPAN VLAN: 901
Router#
```

次に、宛先 ERSPAN セッションに関する情報だけを表示する例を示します。

```
Router# show monitor session erspan-destination
Session 2
-----
Type      : ERSPAN Destination Session
Status    : Admin Disabled
Router#
```

次に、宛先 ERSPAN セッションに関する詳細情報だけを表示する例を示します。

```
Router# show monitor session erspan-destination detail
Session 2
-----
Type      : ERSPAN Destination Session
Status    : Admin Disabled
Description : -
Source Ports :
  RX Only  : None
  TX Only  : None
  Both     : None
Source VLANs :
  RX Only  : None
  TX Only  : None
  Both     : None
Source RSPAN VLAN : None
Destination Ports : None
Filter VLANs : None
Destination RSPAN VLAN : None
Source IP Address : None
Source IP VRF     : None
Source ERSPAN ID  : None
Destination IP Address : None
Destination IP VRF : None
Destination ERSPAN ID : None
Origin IP Address : None
IP QOS PREC      : 0
IP TTL           : 255
Router#
```

次に、送信元 ERSPAN セッションに関する情報だけを表示する例を示します。

```
Router# show monitor session erspan-source
Session 1
```

```

-----
Type                : ERSPAN Source Session
Status              : Admin Disabled
Session 3
-----
Type                : ERSPAN Source Session
Status              : Admin Disabled
Router#

```

次に、送信元 ERSPAN セッションに関する詳細情報だけを表示する例を示します。

```
Router# show monitor session erspan-source detail
```

```

Session 1
-----
Type                : ERSPAN Source Session
Status              : Admin Disabled
Description         : -
Source Ports       :
    RX Only        : None
    TX Only        : None
    Both           : None
Source VLANs      :
    RX Only        : None
    TX Only        : None
    Both           : None
Source RSPAN VLAN : None
Destination Ports : None
Filter VLANs      : None
Destination RSPAN VLAN : None
Source IP Address : None
Source IP VRF     : None
Source ERSPAN ID  : None
Destination IP Address : None
Destination IP VRF : None
Destination ERSPAN ID : None
Origin IP Address : None
IP QOS PREC      : 0
IP TTL           : 255

Session 3
-----
Type                : ERSPAN Source Session
Status              : Admin Disabled
Description         : -
Source Ports       :
    RX Only        : None
    TX Only        : None
    Both           : None
Source VLANs      :
    RX Only        : None
    TX Only        : None
    Both           : None
Source RSPAN VLAN : None
Destination Ports : None
Filter VLANs      : None
Destination RSPAN VLAN : None
Source IP Address : None
Source IP VRF     : None
Source ERSPAN ID  : None
Destination IP Address : None
Destination IP VRF : None
Destination ERSPAN ID : None
Origin IP Address : None
IP QOS PREC      : 0

```

■ show monitor session

```
IP TTL                : 255
Router#
```

関連コマンド

コマンド	説明
monitor session	新規 ERSPAN、SPAN または RSPAN セッションの開始、既存セッションに対するインターフェイスまたは VLAN の追加や削除、特定の VLAN への ERSPAN、SPAN、または RSPAN トラフィックのフィルタリング、セッションの削除を行います。
monitor session type	ERSPAN 送信元セッション番号を作成するか、セッションに対して ERSPAN セッション コンフィギュレーション モードを開始します。
remote-span	VLAN を RSPAN VLAN として設定します。

show mpls l2transport vc

ルータ上の仮想回線のステータスを表示するには、**show mpls l2transport vc** コマンドを使用します。

show mpls l2transport vc [detail] [[vc-id] | [vc-id-min] vc-id-max] | [summary]

シンタックスの説明

detail	(任意) PE ルータ上の仮想回線に関する詳細情報を表示します。
vc-id	(任意) 仮想回線 ID
vc-id-min	(任意) 表示する仮想回線 ID の範囲を指定します。有効値は 0 ~ 429,467,295 です。
vc-id-max	(任意) 仮想回線 ID の範囲。有効値は 0 ~ 429,467,295 です。
summary	(任意) PE ルータの MPLS インターフェイス上のアクティブ仮想回線のサマリーを表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、スイッチ上の仮想回線のステータスを表示する例を示します。

```
Router# show mpls l2transport vc
Transport Client      VC      Local      Remote      Tunnel
VC ID      Intf      State    VC Label    VC Label    Label
4          V14      UP      23          21          77
101       V1101    UP      24          22          77
Router#
```

次に、**summary** キーワードの出力例を示します。

```
Router# show mpls l2transport vc summary
MPLS interface VC summary:
  interface: Gi8/1, programmed imposition vcs: 1
  interface: Gi8/3, programmed imposition vcs: 1

VC summary (active/non-active) by destination:
  destination: 13.0.0.1, Number of locally configured vc(s): 2
Router#
```

次に、スイッチ インターフェイス上で現在ルーティングされている仮想回線について、詳細情報を表示する例を示します。

```
Router# show mpls l2transport vc detail
VC ID: 111, Local Group ID: 5, Remote Group ID: 2 (VC is up)
Client Intf: Gi1/0.1 is up, Destination: 2.2.2.2, Peer LDP Ident: 2.2.2.2:0
Local VC Label: 17, Remote VC Label: 17, Tunnel Label: 16
Outgoing Interface: Gi0/0, Next Hop: 12.1.1.3
```

show mpls l2transport vc

```

Local MTU: 1500, Remote MTU: 1500
Remote interface description: GigabitEthernet0/0.1
Imposition: LC Programmed
Current Imposition/Last Disposition Slot: 1/255
Packet Totals(in/out): 0/0
Byte totals(in/out): 0/0

VC ID: 123, Local Group ID: 6, Remote Group ID: 3 (VC is up)
Client Intf: Gi1/0.2 is up, Destination: 2.2.2.2, Peer LDP Ident: 2.2.2.2:0
Local VC Label: 18, Remote VC Label: 19, Tunnel Label: 16
Outgoing Interface: Gi0/0, Next Hop: 12.1.1.3
Local MTU: 1500, Remote MTU: 1500
Remote interface description: GigabitEthernet0/0.2
Imposition: LC Programmed
Current Imposition/Last Disposition Slot: 1/255
Packet Totals(in/out): 0/0
Byte totals(in/out): 0/0
Router#
    
```

次に、指定された仮想回線に関する詳細仮想回線情報を表示する例を示します。

Router# **show mpls l2transport vc 111 detail**

```

VC ID: 111, Local Group ID: 5, Remote Group ID: 2 (VC is up)
Client Intf: Gi1/0.1 is up, Destination: 2.2.2.2, Peer LDP Ident: 2.2.2.2:0
Local VC Label: 17, Remote VC Label: 17, Tunnel Label: 16
Outgoing Interface: Gi0/0, Next Hop: 12.1.1.3
Local MTU: 1500, Remote MTU: 1500
Remote interface description: GigabitEthernet0/0.1
Imposition: LC Programmed
Current Imposition/Last Disposition Slot: 1/255
Packet Totals(in/out): 0/0
Byte totals(in/out): 0/0
Router#
    
```

表 2-83 に、この例で表示されるフィールドについて説明します。

表 2-83 show mpls l2transport vc コマンドのフィールドの説明

フィールド	説明
Transport VC ID	スイッチ上のインターフェイスのいずれかに割り当てられた仮想回線識別子
Client Intf	レイヤ 2 VLAN パケットが通過する入力または出力インターフェイス
VC State	仮想回線のステータス。ステータスは、次のいずれかになります。 <ul style="list-style-type: none"> UP : 仮想回線は、2 つの仮想回線エンドポイント間でトラフィックを送送できる状態です。インポジションおよびディスポジションインターフェイスが両方ともプログラムされている場合に、仮想回線は有効です。 ディスポジション インターフェイスは、仮想回線が設定されていて、クライアント インターフェイスが起動している場合にプログラムされます。 インポジション インターフェイスは、ディスポジション インターフェイスがプログラムされていて、リモート仮想回線ラベルおよび IGP ラベルが設定されている場合にプログラムされます。バックツーバック設定では、IGP ラベルは暗黙的にヌルに設定できます (IGP ラベルは、ピアに対する LSP が存在することを意味します)。 DOWN : VC は、2 つの仮想回線エンドポイント間でトラフィックを送送する準備ができていません。

表 2-83 show mpls l2transport vc コマンドのフィールドの説明 (続き)

フィールド	説明
Local VC Label	ルータがピア ルータに送信する仮想回線ラベル。ピア ルータがインポジション中に使用します。ローカル仮想回線ラベルは、ディスポジション ラベルで、MPLS バックボーンから着信するパケットの出力インターフェイスを判別します。
Remote VC Label	リモート ピア ルータのディスポジション仮想回線ラベル
Tunnel Label	MPLS バックボーンを介して、出力インターフェイスを搭載した宛先ルータにパケットをルーティングするために使用される IGP ラベル
VC ID	ルータ上のインターフェイスのいずれかに割り当てられた仮想回線識別子
Local Group ID	仮想回線をローカルにグループ化するために使用される ID。MPLS 上のイーサネットは、ハードウェア ポート (ルータのポートごとに一意) 別に仮想回線をグループ化します。
Remote Group ID	複数の仮想回線をグループ化するためにピアで使用される ID
Client	レイヤ 2 VLAN パケットが通過する入力または出力インターフェイス
Destination	この仮想回線に指定された宛先。宛先 IP アドレスは mpls l2transport route vc コマンド内で指定します。
Peer LDP ID	目的のピアの LDP IP アドレス
Outgoing Interface	仮想回線の出力インターフェイス
Next Hop	ネクスト ホップの IP アドレス
Local MTU	クライアント インターフェイスに指定された最大伝送ユニット
Remote MTU	リモートルータのクライアント インターフェイスに指定された最大伝送ユニット
Imposition	モジュールのステータス
LC programmed	プログラムされていない LC
Current Imposition/ Last Disposition Slot	現行インポジションは、インポジションに使用される発信インターフェイスです。最終ディスポジション スロットは、この仮想回線のパケットが着信するインターフェイスです。
Packet Totals (in/out)	各方向に転送されるパケットの総数
Byte Totals (in/out)	各方向に転送される合計バイト数

関連コマンド

コマンド	説明
mpls l2transport route	MPLS 上のレイヤ 2 パケットのルーティングをイネーブルにします。

show mpls platform

プラットフォーム固有の情報を表示するには、**show mpls platform** コマンドを使用します。

show mpls platform { **common** | **eompls** | **gbte-tunnels** | **reserved-vlans vlan** *vlan-id* | **statistics** [**reset**] } | **vpn-vlan-mapping** }

シンタックスの説明

common	LAN および WAN インターフェイス間の共有コードのカウンタを表示します。
eompls	EoMPLS 対応インターフェイスに関する情報を表示します。
gbte-tunnels	MMLS GBTE トンネルに関する情報を表示します。
reserved-vlans vlan <i>vlan-id</i>	RP 予約済み VLAN show コマンドを表示します。有効値は 0 ~ 4095 です。
statistics	RP コントロールプレーン統計情報を表示します。
reset	(任意) 統計カウンタをリセットします。
vpn-vlan-mapping	VPN/VLAN マッピング テーブルに関する情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、LAN および WAN インターフェイス間の共有コードのカウンタを表示する例を示します。

```
Router# show mpls platform common
Common MPLS counters for LAN and WAN
-----

No. of MPLS configured LAN interfaces          = 12
No. of cross-connect configured VLAN interfaces = 0
Router#
```

次に、EoMPLS 対応インターフェイスの情報を表示する例を示します。

```
Router# show mpls platform eompls
Interface      VLAN
GigabitEthernet 101
FastEthernet6/1 2022
Router#
```

次に、GBTE トンネル情報を表示する例を示します。

```
Router# show mpls platform gbte-tunnels
To           From           InLbl  I/I/F kbps      Kbits      H/W Info
Router#
```

次に、RP 予約済み VLAN show コマンドを表示する例を示します。

```
Router# show mpls platform reserved-vlans vlan 1005
Router#
```



(注) この例は、設定されている予約済み VLAN がない場合の出力を示しています。

次に、RP コントロールプレーン統計に関する情報を表示する例を示します。

```
Router# show mpls platform statistics
RP MPLS Control Plane Statistics:
=====
Reserved VLAN creates                0000000001
Reserved VLAN frees                  0000000000
Reserved VLAN creation failures     0000000000
Aggregate Label adds                 0000000001
Aggregate Label frees                0000000000
Aggregate Labels in Superman         0000000001
Feature Rsvd VLAN Reqs               0000000000
Feature Gen Rsvd VLAN Reqs           0000000000
Feature Rsvd VLAN Free Reqs         0000000000
EoMPLS VPN# Msgs                     0000000009
EoMPLS VPN# Msg Failures             0000000000
EoMPLS VPN# Msg Rsp Failures         0000000000
EoMPLS VPN# Set Reqs                 0000000010
EoMPLS VPN# Reset Reqs               0000000008
FIDB mallocs                         0000000000
FIDB malloc failures                 0000000000
FIDB frees                           0000000000
EoMPLS Req mallocs                   0000000018
EoMPLS Req malloc failures           0000000000
EoMPLS Req frees                     0000000018
EoMPLS VPN# allocs                   0000000010
EoMPLS VPN# frees                     0000000008
EoMPLS VPN# alloc failures           0000000000
GB TE tunnel additions               0000000000
GB TE tunnel label resolves           0000000000
GB TE tunnel deletions               0000000000
GB TE tunnel changes                 0000000000
GB TE tunnel heads skips             0000000000
gb_flow allocs                       0000000000
gb_flow frees                         0000000000
rsvp req creats                      0000000000
rsvp req frees                       0000000000
rsvp req malloc failures              0000000000
gb_flow malloc failures               0000000000
psb search failures                  0000000000
GB TE tunnel deleton w/o gb_flow     0000000000
errors finding slot number            0000000000
Router#
```

次に、RP コントロールプレーン統計カウンタをリセットする例を示します。

```
Router# show mpls platform statistics reset
Resetting Const RP MPLS control plane software statistics ...
GB TE tunnel additions                0000000000
GB TE tunnel label resolves            0000000000
GB TE tunnel deletions                 0000000000
GB TE tunnel changes                   0000000000
GB TE tunnel heads skips               0000000000
gb_flow allocs                         0000000000
gb_flow frees                          0000000000
```

■ show mpls platform

```
rsvp req creates                0000000000
rsvp req frees                  0000000000
rsvp req malloc failures        0000000000
gb_flow malloc failures         0000000000
psb search failures             0000000000
GB TE tunnel deleton w/o gb_flow 0000000000
errors finding slot number      0000000000
Router#
```

次に、VPN/VLAN マッピング テーブルに関する情報を表示する例を示します。

```
Router# show mpls platform vpn-vlan-mapping
VPN#  Rsvd Vlan  IDB Created  Feature  Has agg label  In superman  EoM data
0     1025      Yes         No       No             No           No
1     0         No          No       Yes            Yes          No
Router#
```

show mpls ttfib

MPLS TTFIB テーブルに関する情報を表示するには、**show mpls ttfib** コマンドを使用します。

show mpls ttfib [{detail [hardware]}] | {vrf instance [detail]}

シンタックスの説明	detail	(任意) 詳細情報を表示します。
	hardware	(任意) ハードウェアの詳細情報を表示します。
	vrf instance	(任意) 指定された VPN ルーティング/転送インスタンスのエントリを表示します。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、MPLS TTFIB テーブルに関する情報を表示する例を示します。

```
Router# show mpls ttfib
Local  Outgoing  Packets Tag          LTL  Dest.  Destination  Outgoing
Tag    Tag or VC   Switched          Index Vlanid  Mac Address  Interface
4116   21          0                 0xE0  1020   0000.0400.0000 PO4/1*
        34          0                 0x132 1019   00d0.040d.380a GE5/3
        45          0                 0xE3  4031   0000.0430.0000 PO4/4
4117   16          0                 0x132 1019   00d0.040d.380a GE5/3*
        17          0                 0xE0  1020   0000.0400.0000 PO4/1
        18          0                 0xE3  4031   0000.0430.0000 PO4/4
4118   21          0                 0xE0  1020   0000.0400.0000 PO4/1*
        56          0                 0xE3  4031   0000.0430.0000 PO4/4
4119   35          0                 0xE3  4031   0000.0430.0000 PO4/4*
        47          0                 0xE0  1020   0000.0400.0000 PO4/1
```

show pagp

ポート チャネル情報を表示するには、**show pagp** コマンドを使用します。

show pagp [*group-number*] {**counters** | **internal** | **neighbor** | **pgroup**}

シンタックスの説明

group-number	(任意) チャネル グループ番号を指定します。有効値は 1 ~ 282 の最大 64 個の値です。
counters	トラフィック情報を表示します。
internal	内部情報を表示します。
neighbor	ネイバ情報を表示します。
pgroup	アクティブなポート チャネルを表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

show pagp コマンドを入力すると、アクティブ ポートチャネルの情報が表示されます。非アクティブなポートチャネルの情報を表示するには、グループを指定して **show pagp** コマンドを入力します。

257 ~ 282 の **port-channel number** 値は、CSM および FWSM だけでサポートされています。

例

次に、PAgP カウンタに関する情報を表示する例を示します。

```
Router# show pagp counters
          Information          Flush
Port      Sent   Recv      Sent   Recv
-----
Channel group: 1
  Fa5/4    2660   2452      0      0
  Fa5/5    2676   2453      0      0
Channel group: 2
  Fa5/6    289    261      0      0
  Fa5/7    290    261      0      0
Channel group: 1023
  Fa5/9     0      0        0      0
Channel group: 1024
  Fa5/8     0      0        0      0
Router#
```

次に、PAgP 内部情報を表示する例を示します。

```
Router# show pagp 1 internal
Flags: S - Device is sending Slow hello. C - Device is in Consistent state.
      A - Device is in Auto mode.
Timers: H - Hello timer is running. Q - Quit timer is running.
       S - Switching timer is running. I - Interface timer is running.

Channel group 1

Port      Flags State  Timers  Hello  Partner  PAgP  Learning
Fa5/4     SC   U6/S7  30s     30s    1        128   Any
Fa5/5     SC   U6/S7  30s     30s    1        128   Any
Router#
```

次に、すべてのネイバの PAgP ネイバ情報を表示する例を示します。

```
Router# show pagp neighbor
Flags: S - Device is sending Slow hello. C - Device is in Consistent state.
      A - Device is in Auto mode. P - Device learns on physical port.

Channel group 1 neighbors

Partner
Port      Name          Partner Device ID      Partner Port      Age  Flags  Cap.
Fa5/4     JAB031301    0050.0f10.230c 2/45           2s  SAC   2D
Fa5/5     JAB031301    0050.0f10.230c 2/46           27s SAC   2D

Channel group 2 neighbors

Partner
Port      Name          Partner Device ID      Partner Port      Age  Flags  Cap.
Fa5/6     JAB031301    0050.0f10.230c 2/47           10s SAC   2F
Fa5/7     JAB031301    0050.0f10.230c 2/48           11s SAC   2F

Channel group 1023 neighbors

Partner
Port      Name          Partner Device ID      Partner Port      Age  Flags  Cap.

Channel group 1024 neighbors

Partner
Port      Name          Partner Device ID      Partner Port      Age  Flags  Cap.
Router#
```

関連コマンド

コマンド	説明
pagp learn-method	着信パケットの入力インターフェイスを学習します。
pagp port-priority	ホットスタンバイモードのポートを選択します。

show platform

プラットフォーム情報を表示するには、**show platform** コマンドを使用します。

```
show platform {buffers | eeprom | fault | {hardware capacity} | {hardware pfc mode} |
internal-vlan | netint | {software ipv6-multicast connected} | {tech-support
ipmulticast group-ip-addr src-ip-addr} | tlb}
```

シンタックスの説明

buffers	バッファ割り当て情報を表示します。
eeprom	CPU EEPROM 情報を表示します。
fault	障害日付を表示します。
hardware capacity	ハードウェア リソースの容量と利用率を表示します。 show platform hardware capacity コマンドを参照してください。
hardware pfc mode	装着されている PFC のタイプを表示します。
internal-vlan	内部 VLAN を表示します。
netint	プラットフォームのネットワーク割り込み情報を表示します。
software ipv6-multicast connected	ルートプロセッサ上のすべての IPv6 サブネットの ACL エントリを表示します。 show platform software ipv6-multicast コマンドを参照してください。
tech-support ipmulticast	TAC 用の IP マルチキャスト関連情報を表示します。
<i>group-ip-addr</i>	グループ IP アドレス。
<i>src-ip-addr</i>	送信元 IP アドレス。
tlb	TLB レジスタに関する情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、バッファ割り当て情報を表示する例を示します。

```
Router# show platform buffers
Reg. set  Min    Max
TX                640
ABQ          640 16384
0              0     40
1          6715 8192
2              0     0
3              0     0
4              0     0
5              0     0
6              0     0
7              0     0
```

```
Threshold = 8192
```

```
Vlan Sel Min Max Cnt Rsvd
1019 1 6715 8192 0 0
Router#
```

次に、CPU EEPROM 情報を表示する例を示します。

```
Router# show platform eeprom
PISA CPU IDPROM:
IDPROM image:

IDPROM image block #0:
hexadecimal contents of block:
00: AB AB 02 9C 13 5B 02 00 00 02 60 03 03 E9 43 69 .....[....`...Ci
10: 73 63 6F 20 53 79 73 74 65 6D 73 00 00 00 00 00 sco Systems.....
20: 00 00 57 53 2D 58 36 4B 2D 53 55 50 33 2D 50 46 ..WS-X6K-SUP3-PF
30: 43 33 00 00 00 00 53 41 44 30 36 34 34 30 31 57 C3....SAD064401W
40: 4C 00 00 00 00 00 00 00 00 00 37 33 2D 37 34 30 L.....73-740
50: 34 2D 30 37 00 00 00 00 00 30 35 00 00 00 00 00 4-07.....05....
60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
70: 00 00 00 00 02 BD 00 00 00 00 00 09 00 05 00 01 .....
80: 00 03 00 01 00 01 00 02 03 E9 00 00 00 00 00 00 .....
90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

block-signature = 0xABAB, block-version = 2,
block-length = 156, block-checksum = 4955

*** common-block ***
IDPROM capacity (bytes) = 512 IDPROM block-count = 2
FRU type = (0x6003,1001)
OEM String = 'Cisco Systems'
Product Number = 'WS-X6K-SUP3-PFC3'
Serial Number = 'SAD064401WL'
Manufacturing Assembly Number = '73-7404-07'
Manufacturing Assembly Revision = '05'
Hardware Revision = 0.701
Manufacturing bits = 0x0 Engineering bits = 0x0
SNMP OID = 9.5.1.3.1.1.2.1001
Power Consumption = 0 centiamperes RMA failure code = 0-0-0-0
CLEI =
*** end of common block ***

IDPROM image block #1:
hexadecimal contents of block:
00: 60 03 02 67 0C 24 00 00 00 00 00 00 00 00 00 00 `..g.$.....
10: 00 00 00 00 00 00 00 00 51 00 05 9A 3A 7E 9C 00 00 .....Q...:~...
20: 02 02 00 01 00 01 00 00 00 00 00 00 00 00 00 00 .....
30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
40: 14 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
50: 00 00 81 81 81 81 80 80 80 80 80 80 80 80 80 80 .....
60: 80 80 06 72 00 46 37 .....r.F7

block-signature = 0x6003, block-version = 2,
block-length = 103, block-checksum = 3108

*** linecard specific block ***
feature-bits = 00000000 00000000
hardware-changes-bits = 00000000 00000000
card index = 81
mac base = 0005.9A3A.7E9C
mac_len = 0
num_processors = 2
epld_num = 2
```

show platform

```

epld_versions = 0001 0001 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
port numbers:
  pair #0: type=14, count=01
  pair #1: type=00, count=00
  pair #2: type=00, count=00
  pair #3: type=00, count=00
  pair #4: type=00, count=00
  pair #5: type=00, count=00
  pair #6: type=00, count=00
  pair #7: type=00, count=00
sram_size = 0
sensor_thresholds =
  sensor #0: critical = -127 oC (sensor present but ignored), warning = -127 oC (sensor
present but ignored)
  sensor #1: critical = -127 oC (sensor present but ignored), warning = -127 oC (sensor
present but ignored)
  sensor #2: critical = -128 oC (sensor not present), warning = -128 oC (sensor not
present)
  sensor #3: critical = -128 oC (sensor not present), warning = -128 oC (sensor not
present)
  sensor #4: critical = -128 oC (sensor not present), warning = -128 oC (sensor not
present)
  sensor #5: critical = -128 oC (sensor not present), warning = -128 oC (sensor not
present)
  sensor #6: critical = -128 oC (sensor not present), warning = -128 oC (sensor not
present)
  sensor #7: critical = -128 oC (sensor not present), warning = -128 oC (sensor not
present)
max_connector_power = 1650
cooling_requirement = 70
ambient_temp = 55
*** end of linecard specific block ***
Router#

```

次に、障害日付情報を表示する例を示します。

```

Router# show platform fault
Fault History Buffer:
s72033_rp Software (s72033_rp-JSV-M), Experimental Version 12.2(20030331:071521)
[kkuttuva-CSCea55513-const2 120]
Compiled Mon 31-Mar-03 21:58 by kkuttuva
Signal = 10, Code = 0x1C, Uptime 00:01:14
$0 : 00000000, AT : 00000000, v0 : 00000000, v1 : 00000000
a0 : 00000000, a1 : 10050000, a2 : 00000000, a3 : 43F4B614
t0 : 50A19548, t1 : 10048000, t2 : 10040000, t3 : 10050000
t4 : 43F515A8, t5 : 43F515A4, t6 : 43F515A0, t7 : 43F5159C
s0 : 50A19548, s1 : 00000000, s2 : 50A19548, s3 : 10030100
s4 : 10030000, s5 : 41700000, s6 : 43F4B614, s7 : 41DB0000
t8 : 43F51614, t9 : 00000000, k0 : 5032D19C, k1 : 40231598
gp : 41F96960, sp : 50A19508, s8 : 422183A0, ra : 4027FB50
EPC : 4027FB84, SREG : 3401F103, Cause : 8000001C
Router#

```

次に、PFC 動作モードを表示する例を示します。

```

Router# show platform hardware pfc mode
PFC operating mode : PFC3A
Router#

```

次に、プラットフォームのネット割り込み情報を表示する例を示します。

```

Router# show platform netint
Network IO Interrupt Throttling:
throttle count=0, timer count=0

```

```

active=0, configured=1
netint usec=3999, netint mask usec=800
inband_throttle_mask_hi = 0x0
inband_throttle_mask_lo = 0x800000
Router#

```

次に、TLB レジスタ情報を表示する例を示します。

```
Router# show platform tlb
```

```

Mistral revision 5
TLB entries : 42
Virt Address range      Phy Address range      Attributes
0x10000000:0x1001FFFF  0x010000000:0x01001FFFF  CacheMode=2, RW, Valid
0x10020000:0x1003FFFF  0x010020000:0x01003FFFF  CacheMode=2, RW, Valid
0x10040000:0x1005FFFF  0x010040000:0x01005FFFF  CacheMode=2, RW, Valid
0x10060000:0x1007FFFF  0x010060000:0x01007FFFF  CacheMode=2, RW, Valid
0x10080000:0x10087FFF  0x010080000:0x010087FFF  CacheMode=2, RW, Valid
0x10088000:0x1008FFFF  0x010088000:0x01008FFFF  CacheMode=2, RW, Valid
0x18000000:0x1801FFFF  0x010000000:0x01001FFFF  CacheMode=0, RW, Valid
0x19000000:0x1901FFFF  0x010000000:0x01001FFFF  CacheMode=7, RW, Valid
0x1E000000:0x1E1FFFFF  0x01E000000:0x01E1FFFFF  CacheMode=2, RW, Valid
0x1E880000:0x1E89FFFF  0x01E880000:0x01E89FFFF  CacheMode=2, RW, Valid
0x1FC00000:0x1FC7FFFF  0x01FC00000:0x01FC7FFFF  CacheMode=2, RO, Valid
0x30000000:0x3001FFFF  0x070000000:0x07001FFFF  CacheMode=2, RW, Valid
0x40000000:0x407FFFFF  0x000000000:0x0007FFFFF  CacheMode=3, RO, Valid
.
.
.
0x58000000:0x59FFFFFF  0x088000000:0x089FFFFFF  CacheMode=3, RW, Valid
0x5A000000:0x5BFFFFFF  0x08A000000:0x08BFFFFFF  CacheMode=3, RW, Valid
0x5C000000:0x5DFFFFFF  0x08C000000:0x08DFFFFFF  CacheMode=3, RW, Valid
0x5E000000:0x5FFFFFFF  0x08E000000:0x08FFFFFFF  CacheMode=3, RW, Valid
Router#

```

show platform hardware capacity

ハードウェア リソースの容量と利用率を表示するには、**show platform hardware capacity** コマンドを使用します。

show platform hardware capacity [*resource-type*]

シンタックスの説明	<i>resource-type</i>	(任意) ハードウェア リソース タイプ。有効値については、「使用上のガイドライン」を参照してください。
------------------	----------------------	--

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン *resource-type* の有効値は次のとおりです。

- **acl** : ACL/QoS TCAM リソースの容量と利用率を表示します。
- **cpu** : CPU リソースの容量と利用率を表示します。
- **eobc** : EOBC リソースの容量と利用率を表示します。
- **flash** : フラッシュ /NVRAM リソースの容量と利用率を表示します。
- **forwarding** : レイヤ 2 およびレイヤ 3 転送リソースの容量と利用率を表示します。
- **interface** : インターフェイス リソースの容量と利用率を表示します。
- **monitor** : SPAN リソースの容量と利用率を表示します。
- **multicast** : レイヤ 3 マルチキャスト リソースの容量と利用率を表示します。
- **netflow** : NetFlow リソースの容量と利用率を表示します。
- **pfc** : レイヤ 2 転送、レイヤ 3 転送、NetFlow、CPU レート リミッタ、および ACL/QoS TCAM リソースを含むすべての PFC リソースの容量と利用率を表示します。
- **power** : パワー リソースの容量と利用率を表示します。
- **qos** : QoS ポリサー リソースの容量と利用率を表示します。
- **rate-limiter** : CPU レート リミッタ リソースの容量と利用率を表示します。
- **system** : システム リソースの容量と利用率を表示します。
- **vlan** : VLAN リソースの容量と利用率を表示します。

show platform hardware capacity cpu コマンドは、次の情報を表示します。

- 最後の 5 秒間の CPU 利用率 (ビジー時間および中断時間)、最後の 1 分の平均的なビジー時間の割合、および最後の 5 分の平均的なビジー時間の割合
- プロセッサ メモリの使用可能な合計バイト、使用バイト、および利用率
- I/O メモリの使用可能な合計バイト、使用バイト、および利用率

show platform hardware capacity eobc コマンドは、次の情報を表示します。

- 送信および受信レート
- 受信および送信されたパケット
- 廃棄された受信パケットおよび廃棄された送信パケット

show platform hardware capacity forwarding コマンドは、次の情報を表示します。

- MAC テーブルの使用可能な合計エントリ、使用エントリ、および利用率
- FIB TCAM テーブルの使用可能な合計エントリ、使用エントリ、および利用率。プロトコル単位で表示されます。
- 隣接テーブルの使用可能な合計エントリ、使用エントリ、および利用率。隣接テーブルが分割されるリージョンごとに表示されます。
- NetFlow TCAM および ICAM テーブルで作成されたエントリ、失敗したエントリ、およびリソースの使用率
- ACL/QoS TCAM テーブルの使用可能な合計エントリおよびマスク、使用エントリおよびマスク、予約済みエントリおよびマスク、エントリおよびマスクの使用率。出力は、ラベルの使用可能な容量、使用容量、予約済み容量、および利用率を表示します。ACL/QoS TCAM に関連する他のハードウェア リソースのリソースも表示されます (LOU、ANDOR、および ORAND の使用可能な容量、使用容量、予約済み容量、および利用率など)。
- CPU レート リミッタの使用可能な容量、使用容量、予約済み容量、および利用率

show platform hardware capacity interface コマンドは、次の情報を表示します。

- Tx/Rx drops : 各オンライン モジュール (すべてのポートを集約) の送信および受信の廃棄カウンタの合計を表示し、モジュールで最も高い廃棄カウントを持つポート番号を表示します。
- Tx/Rx per port buffer size : バッファ サイズが一貫しているモジュールのモジュール単位のポート バッファ サイズをまとめます。

show platform hardware capacity monitor コマンドは、次の SPAN 情報を表示します。

- 最大ローカル SPAN セッション、最大 RSPAN セッション、最大 ERSPAN セッション、および最大サービス モジュール セッション
- ローカル SPAN セッション、RSPAN セッション、ERSPAN セッション、およびサービス モジュール セッションの使用容量および使用可能な容量

show platform hardware capacity multicast コマンドは、次の情報を表示します。

- マルチキャスト レプリケーション モード (入力および出力の IPv4 および IPv6 モード)
- システム内の各モジュールの合計使用容量および利用率を示す MET テーブルの使用状況
- 合計使用容量および利用率を示す双方向 PIM DF テーブルの使用状況

show platform hardware capacity

show platform hardware capacity system コマンドは、次の情報を表示します。

- PFC 動作モード (PFC バージョン)
- スーパーバイザの冗長モード (RPR、SSO、none など)
- 次の内容が含まれるモジュール固有のスイッチング情報
 - 製品番号 (WS-SUP720-BASE および WS-X6548-RJ-45 など)
 - シリーズ (スーパーバイザ エンジン)
 - CEF モード (central CEF および dCEF)

show platform hardware capacity vlan コマンドは、次の VLAN 情報を表示します。

- 合計 VLAN
- 使用 VTP VLAN
- 使用外部 VLAN
- 使用内部 VLAN
- 未使用 VLAN

例

次に、Catalyst 6500 シリーズ スイッチのルート プロセッサ、スイッチ プロセッサ、および LAN モジュールの CPU 容量と利用率の情報を表示する例を示します。

```
Router# show platform hardware capacity cpu
CPU Resources
  CPU utilization: Module           5 seconds      1 minute      5 minutes
                   1 RP             0% / 0%        1%            1%
                   1 SP             5% / 0%        5%            4%
                   7                 69% / 0%      69%           69%
                   8                 78% / 0%      74%           74%
  Processor memory: Module  Bytes:      Total          Used           %Used
                   1 RP             176730048     51774704      29%
                   1 SP             192825092     51978936      27%
                   7                 195111584     35769704      18%
                   8                 195111584     35798632      18%
  I/O memory: Module  Bytes:      Total          Used           %Used
                   1 RP             35651584      12226672      34%
                   1 SP             35651584      9747952       27%
                   7                 35651584      9616816       27%
                   8                 35651584      9616816       27%
```

次に、ルート プロセッサ、スイッチ プロセッサの EOBC 関連の統計情報を表示する例を示します。

```
Router# show platform hardware capacity eobc
EOBC Resources
Module           Packets/sec      Total packets    Dropped packets
  1 RP           Rx:              61              108982           0
                  Tx:              37              77298            0
  1 SP           Rx:              34              101627           0
                  Tx:              39              115417           0
  7              Rx:              5               10358            0
                  Tx:              8               18543            0
  8              Rx:              5               12130            0
                  Tx:              10              20317            0
```

次に、システム内にあるフラッシュ /NVRAM リソースで使用される合計容量、使用バイト、および利用率に関する情報を表示する例を示します。

```
Router# show platform hardware capacity flash
Flash/NVRAM Resources
Usage: Module Device          Bytes:      Total          Used          %Used
      1 RP bootflash:          31981568    15688048      49%
      1 SP disk0:              128577536   105621504     82%
      1 SP sup-bootflash:      31981568    29700644     93%
      1 SP const_nvram:        129004      856           1%
      1 SP nvram:              391160      22065         6%
```

Router#

次に、システム内の EARL の容量と利用率を表示する例を示します。

```
Router# show platform hardware capacity forwarding
L2 Forwarding Resources
      MAC Table usage:  Module Collisions Total          Used          %Used
                        6          0  65536          11           1%

      VPN CAM usage:              Total          Used          %Used
                                512           0           0%

L3 Forwarding Resources
      FIB TCAM usage:              Total          Used          %Used
      72 bits (IPv4, MPLS, EoM)    196608         36           1%
      144 bits (IP mcast, IPv6)    32768          7           1%

      detail:      Protocol          Used          %Used
                  IPv4              36           1%
                  MPLS              0           0%
                  EoM              0           0%

                  IPv6              4           1%
                  IPv4 mcast        3           1%
                  IPv6 mcast        0           0%

      Adjacency usage:              Total          Used          %Used
                                1048576        175          1%

Forwarding engine load:
      Module          pps  peak-pps          peak-time
      6                8    1972  02:02:17 UTC Thu Apr 21 2005

Netflow Resources
      TCAM utilization:  Module          Created          Failed          %Used
                        6                1                0                0%

      ICAM utilization:  Module          Created          Failed          %Used
                        6                0                0                0%

      Flowmasks:  Mask#  Type          Features
      IPv4:        0    reserved     none
      IPv4:        1    Intf FulNAT_INGRESS NAT_EGRESS FM_GUARDIAN
      IPv4:        2    unused      none
      IPv4:        3    reserved     none

      IPv6:        0    reserved     none
      IPv6:        1    unused      none
      IPv6:        2    unused      none
      IPv6:        3    reserved     none

CPU Rate Limiters Resources
      Rate limiters:  Total          Used          Reserved          %Used
      Layer 3         9                4                1                44%
      Layer 2         4                2                2                50%

ACL/QoS TCAM Resources
Key: ACLent - ACL TCAM entries, ACLmsk - ACL TCAM masks, AND - ANDOR,
     QoSent - QoS TCAM entries, QOSmsk - QoS TCAM masks, OR - ORAND,
```

show platform hardware capacity

Lbl-in - ingress label, Lbl-eg - egress label, LOUsrc - LOU source,
 LOUdst - LOU destination, ADJ - ACL adjacency

Module	ACLent	ACLmsk	QoSent	QoSmsk	Lbl-in	Lbl-eg	LOUsrc	LOUdst	AND	OR	ADJ
6	1%	1%	1%	1%	1%	1%	0%	0%	0%	0%	1%

Router#

次に、インターフェイス リソースを表示する例を示します。

```
Router# show platform hardware capacity interface
Interface Resources
Interface drops:
  Module      Total drops:    Tx          Rx          Highest drop port:  Tx  Rx
  9           0                0           2           0      48

Interface buffer sizes:
  Module      Bytes:          Tx buffer      Rx buffer
  1           12345           12345          12345
  5           12345           12345          12345
```

Router#

次に、SPAN 情報を表示する例を示します。

```
Router# show platform hardware capacity monitor
SPAN Resources
Source sessions: 2 maximum, 0 used
  Type          Used
  Local         0
  RSPAN source  0
  ERSPAN source 0
  Service module 0
Destination sessions: 64 maximum, 0 used
  Type          Used
  RSPAN destination 0
  ERSPAN destination (max 24) 0
```

Router#

次に、レイヤ 3 マルチキャスト機能のリソースの容量と利用率を表示する例を示します。

```
Router# show platform hardware capacity multicast
L3 Multicast Resources
IPv4 replication mode: ingress
IPv6 replication mode: ingress
Bi-directional PIM Designated Forwarder Table usage: 4 total, 0 (0%) used
Replication capability: Module          IPv4          IPv6
                          5                egress       egress
                          9                ingress       ingress
MET table Entries: Module          Total    Used    %Used
                          5                65526     6      0%
```

Router#

次に、システム電力の容量と利用率に関する情報を表示する例を示します。

```
Router# show platform hardware capacity power
Power Resources
Power supply redundancy mode: administratively combined
                              operationally combined
System power: 1922W, 0W (0%) inline, 1289W (67%) total allocated
Powered devices: 0 total
```

Router#

次に、Catalyst 6500 シリーズ スイッチ内の EARL 単位の QoS ポリサー リソースの容量と利用率を表示する例を示します。

```
Router# show platform hardware capacity qos
QoS Policer Resources
Aggregate policers: Module          Total      Used      %Used
                        1             1024      102       10%
                        5             1024        1         1%
Microflow policer configurations: Module Total      Used      %Used
                        1             64        32        50%
                        5             64         1         1%
Router#
```

次に、主要なシステム リソースに関する情報を表示する例を示します。

```
Router# show platform hardware capacity systems
System Resources
PFC operating mode: PFC3BXL
Supervisor redundancy mode: administratively rpr-plus, operationally rpr-plus
Switching Resources: Module  Part number      Series      CEF mode
                        5      WS-SUP720-BASE  supervisor  CEF
                        9      WS-X6548-RJ-45  CEF256     CEF
Router#
```

次に、VLAN 情報を表示する例を示します。

```
Router# show platform hardware capacity vlan
VLAN Resources
VLANs: 4094 total, 10 VTP, 0 extended, 0 internal, 4084 free
Router#
```

show platform pisa np

Supervisor Engine 32 PISA 固有の情報を表示するには、**show platform pisa np** コマンドを使用します。

show platform pisa np counter

シンタックスの説明

<i>counter</i>	カウンタ情報。有効値については、「使用上のガイドライン」を参照してください。
----------------	--

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

counter 引数の有効値は次のとおりです。

- **me num counters** : マイクロエンジン情報を表示します。有効値は 0 ~ 15 です。
- **acl counters** : ACL カウンタ情報を表示します。
- **all counters** : Supervisor Engine 32 PISA 固有カウンタをすべて表示します。
- **all pps counters** : すべての Supervisor Engine 32 PISA 固有カウンタの 1 秒あたりのパケット数を表示します。
- **fpm counters** : フレキシブル パケット マッチング (FPM) カウンタ情報を表示します。
- **mqc counters** : モジュラ QoS CLI 情報を表示します。
- **nbar counters** : Network-Based Application Recognition (NBAR) カウンタ情報を表示します。
- **rx counters** : 受信エンジン カウンタ情報を表示します。
- **tx counters** : 送信エンジン カウンタ情報を表示します。

例

次に、ACL カウンタの情報を表示する例を示します。

```
Router# show platform pisa np acl counters
```

```
ACL Statistics
-----
ACL Pkts Received      : 0
ACL Pkts Forwarded    : 0
ACL Unknown Msg       : 0
Router#
```

次に、すべての Supervisor Engine 32 PISA 固有カウンタを表示する例を示します。

```
Router# show platform pisa np all counters
```

```
NP ENGINE STATISTICS:
-----
RX Statistics
-----
Idle: 0
Frames Received: 162
Control Frames Received: 0
Forward RBUF: 0
Forward RBUF+DRAM: 162
Forward Buffered: 0
Post stalls: 0
Error: 0
Error(bad sop): 0
Error(missing sop): 0
Error(data buf alloc fail): 0
Error(control buf alloc fail): 0
Error(packet too big): 0
Error(packet length mismatch): 0

NBAR Statistics
-----
NBAR Pkts Received : 0
NBAR Pkts Classified: 0
PD Pkts Received : 0
NBAR Pkts Out : 0
NBAR Debug 0 : 0
NBAR Debug 1 : 0
NBAR Debug 2 : 0
NBAR Debug 3 : 0

FPM Statistics
-----
FPM Config Stamp : 0
FPM Pkts Received : 0
FPM Pkts Forwarded : 0
FPM Pkts Dropped : 0
FPM Unknown Msg : 0
FPM Error : 0
FPM Cache Misses : 0

ACL Statistics
-----
ACL Pkts Received : 0
ACL Pkts Forwarded : 0
ACL Unknown Msg : 0

MQC Statistics
-----
MQC Pkts Received : 0
MQC Pkts Transmitted : 0
MQC Unknown : 0
MQC Error : 0
MQC Pkts marked DSCP : 0
MQC Policer Conformed: 0
MQC Policer Exceeded : 0
MQC Pkts Dropped : 0

TX Statistics
-----
Errors: 0
```

show platform pisa np

```
Fastpath RBUFs received: 162
Fastpath pkt received: 0
FastTX receive: 0
SlowTX receive: 162
Packets transmitted (loopback): 162
Packets transmit to hyperion: 162
Packets punt to CP: 0
Packets punt to Nitrox: 0
Packets forward to CM: 0
Packets forward to TCP: 0
Packets forward to Reassembly: 0
Packets forward to Fragmentation: 0
Packets forward to XScale: 162
Packets IPCP forward: 0
WARN: TX Packet too small: 0
DROP: Packet too big error: 0
DROP: Connection Route: 0
DROP: Connection Miss: 0
DROP: Bad connection route: 162
DROP: RX Interface miss: 0
DROP: Out of buffers: 0
DROP: Unknown Msg received: 0
DROP: Bandwidth rate policed: 0
Close request Sent: 0
```

```
Stubs Statistics for ME: 2
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0
```

```
Stubs Statistics for ME: 3
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0
```

```
Stubs Statistics for ME: 4
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0
```

```
Stubs Statistics for ME: 5
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
```

```
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0
```

```
Stubs Statistics for ME: 6
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0
```

```
Stubs Statistics for ME: 7
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0
```

```
Stubs Statistics for ME: 8
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0
```

```
Stubs Statistics for ME: 9
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0
```

```
Stubs Statistics for ME: 10
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0
```

```
Stubs Statistics for ME: 11
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
```

■ show platform pisa np

```

SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0

Stubs Statistics for ME: 12
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0

Stubs Statistics for ME: 13
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0

Stubs Statistics for ME: 14
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0

Stubs Statistics for ME: 15
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0

```

次に、すべての Supervisor Engine 32 PISA 固有カウンタの 1 秒あたりのパケット数を表示する例を示します。

```
Router# show platform pisa np all pps
```

```

Throughput in packets-per-sec (pps) within 5 secs interval:
-----
Rx   Ingress PPS 0
Rx   Egress  PPS 0
NBAR Ingress PPS 0
NBAR Egress  PPS 0
FPM  Ingress PPS 0
FPM  Egress  PPS 0

```

```
ACL Ingress PPS 0
ACL Egress PPS 0
MQC Ingress PPS 0
MQC Egress PPS 0
Tx Ingress PPS 0
Tx Egress PPS 0
Router#
```

次に、FPM カウンタ情報を表示する例を示します。

```
Router# show platform pisa np fpm counters
```

```
FPM Statistics
-----
FPM Config Stamp      : 0
FPM Pkts Received    : 0
FPM Pkts Forwarded   : 0
FPM Pkts Dropped     : 0
FPM Unknown Msg      : 0
FPM Error             : 0
FPM Cache Misses     : 0
Router#
```

次に、特定の ME に関する ME カウンタ情報を表示する例を示します。

```
Router# show platform pisa np me 0 counters
```

```
Stubs Statistics for ME: 0
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0
Router#
```

次に、モジュラ QoS CLI 情報を表示する例を示します。

```
Router# show platform pisa np mqc counters
```

```
MQC Statistics
-----
MQC Pkts Received      : 0
MQC Pkts Transmitted   : 0
MQC Unknown            : 0
MQC Error               : 0
MQC Pkts marked DSCP   : 0
MQC Policer Conformed: 0
MQC Policer Exceeded  : 0
MQC Pkts Dropped       : 0
Router#
```

次に、Network-Based Application Recognition カウンタ情報を表示する例を示します。

```
Router# show platform pisa np nbar counters
```

```
NBAR Statistics
-----
NBAR Pkts Received : 0
NBAR Pkts Classified: 0
PD Pkts Received : 0
NBAR Pkts Out      : 0
```

■ show platform pisa np

```
NBAR Debug 0      : 0
NBAR Debug 1      : 0
NBAR Debug 2      : 0
NBAR Debug 3      : 0
```

次に、受信エンジンのカウンタ情報を表示する例を示します。

```
Router# show platform pisa np rx counters
```

```
RX Statistics
-----
Idle: 0
Frames Received: 159
Control Frames Received: 0
Forward RBUF: 0
Forward RBUF+DRAM: 159
Forward Buffered: 0
Post stalls: 0
Error: 0
Error(bad sop): 0
Error(missing sop): 0
Error(data buf alloc fail): 0
Error(control buf alloc fail): 0
Error(packet too big): 0
Error(packet length mismatch): 0
Router#
```

次に、送信エンジンのカウンタ情報を表示する例を示します。

```
Router# show platform pisa np tx counters
```

```
TX Statistics
-----
Errors: 0
Fastpath RBUFs received: 159
Fastpath pkt received: 0
FastTX receive: 0
SlowTX receive: 159
Packets transmitted (loopback): 159
Packets transmit to hyperion: 159
Packets punt to CP: 0
Packets punt to Nitrox: 0
Packets forward to CM: 0
Packets forward to TCP: 0
Packets forward to Reassembly: 0
Packets forward to Fragmentation: 0
Packets forward to XScale: 159
Packets IPCP forward: 0
WARN: TX Packet too small: 0
DROP: Packet too big error: 0
DROP: Connection Route: 0
DROP: Connection Miss: 0
DROP: Bad connection route: 159
DROP: RX Interface miss: 0
DROP: Out of buffers: 0
DROP: Unknown Msg received: 0
DROP: Bandwidth rate policed: 0
Close request Sent: 0
Router#
```

show platform software ipv6-multicast

プラットフォーム ソフトウェア IPv6 マルチキャストに関する情報を表示するには、show platform software ipv6-multicast コマンドを使用します。

show platform software ipv6-multicast {acl-exception | acl-table | capability | connected | shared-adjacencies | statistics | summary}

シンタックスの説明

acl-exception	ACL 例外のためにソフトウェアでスイッチングされた IPv6 マルチキャスト エントリを表示します。
acl-table	IPv6 マルチキャスト ACL 要求テーブル エントリを表示します。
capability	ハードウェア容量を表示します。
connected	IPv6 マルチキャスト サブネット/接続済みハードウェア エントリを表示します。
shared-adjacencies	IPv6 マルチキャスト共有の隣接関係を表示します。
statistics	内部ソフトウェア ベースの統計を表示します。
summary	IPv6 マルチキャスト ハードウェア ショートカット数を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、IPv6 ハードウェア容量を表示する例を示します。

```
Router# show platform software ipv6-multicast capability
Hardware switching for ipv6 is Enabled
(S,G) forwarding for ipv6 supported using Netflow
(*,G) bridging for ipv6 is supported using Fib
Directly-connected entries for IPv6 is supported using ACL-TCAM.

Current System HW Replication Mode : Egress
Auto-detection of Replication Mode : ON

Slot Replication-Capability Replication-Mode
  2 Egress                      Egress
  5 Egress                      Egress
Router#
```

次に、IPv6 マルチキャスト サブネット/接続済みハードウェア エントリを表示する例を示します。

```
Router# show platform software ipv6-multicast connected

IPv6 Multicast Subnet entries
Flags : H - Installed in ACL-TCAM
        X - Not installed in ACL-TCAM due to
```

show platform software ipv6-multicast

```

label-full exception

Interface: Vlan40 [ H ]
    S:40::1 G:FF00::
    S:0:5000::2 G:FF00::
    S:5000::2 G:FF00::
Interface: Vlan30 [ H ]
    S:30::1 G:FF00::
Interface: Vlan20 [ H ]
    S:20::1 G:FF00::
Interface: Vlan10 [ H ]
    S:10::1 G:FF00::
Router#

```

次に、IPv6 マルチキャスト共有隣接情報を表示する例を示します。

```
Router# show platform software ipv6-multicast shared-adjacencies
```

```
---- SLOT [7] ----
```

Shared IPv6 Mcast Adjacencies	Index	Packets	Bytes
Subnet bridge adjacency	0x7F802	0	0
Control bridge adjacency	0x7	0	0
StarG_M bridge adjacency	0x8	0	0
S_G bridge adjacency	0x9	0	0
Default drop adjacency	0xA	0	0
StarG (spt == INF) adjacency	0xB	0	0
StarG (spt != INF) adjacency	0xC	0	0

```
Router#
```

次に、IPv6 マルチキャスト統計情報を表示する例を示します。

```
Router# show platform software ipv6-multicast statistics
```

```

IPv6 Multicast HW-switching Status           : Enabled
IPv6 Multicast (*,G) HW-switching Status    : Disabled
IPv6 Multicast Subnet-entries Status        : Enabled
Default MFIB IPv6-table                     : 0x5108F770
(S,G,C) flowmask index                      : 3
(*,G,C) flowmask index                      : 65535

```

```
General Counters
```

```

-----+-----+
Mfib-hw-entries count                        0
Mfib-add count                               4
Mfib-modify count                            2
Mfib-delete count                           2
Mfib-NP-entries count                       0
Mfib-D-entries count                        0
Mfib-IC-entries count                       0
Error Counters

```

```

-----+-----+
ACL flowmask err count                       0
ACL TCAM exptn count                         0
ACL renewable count                          0
Idb Null error                               0
Router#

```

次に、IPv6 マルチキャストハードウェアショートカット数を表示する例を示します。

```
Router# show platform software ipv6-multicast summary
```

```

IPv6 Multicast Netflow SC summary on Slot[7]:
Shortcut Type          Shortcut count
-----+-----+

```

```
(S, G)                                0

IPv6 Multicast FIB SC summary on Slot[7]:
Shortcut Type                          Shortcut count
-----+-----
(*, G/128)                              0
(*, G/m)                                0

Router#
```

関連コマンド

コマンド	説明
ipv6 mfib hardware-switching	IPv6 マルチキャストパケットのグローバル単位でのハードウェアスイッチングを設定します。

show platform software pisa fm interface

インターフェイスの PISA 機能マネージャ データを表示するには、**show platform software pisa fm interface** コマンドを使用します。

```
show platform software pisa fm interface {all | {interface-type interface-number} |
{port-channel number} | {vlan vlan-id}}
```

シンタックスの説明

all	PISA 機能マネージャ データを、すべてのインターフェイスについて表示します。
<i>interface-type</i>	インターフェイス タイプ。有効値は fastethernet 、 gigabitethernet 、および tengigabitethernet です。
<i>interface-number</i>	モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
port-channel number	チャンネル インターフェイスを指定します。有効値は 1 ~ 282 の範囲の最大 64 個の値です。257 ~ 282 の値は、CSM および FWSM だけでサポートされています。
vlan vlan-id	VLAN を指定します。有効値は 1 ~ 4094 です。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZYA1	このコマンドのサポートが追加されました。

使用上のガイドライン

interface-number 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

例

次に、VLAN 10 の PISA 機能マネージャ データを表示する例を示します。このデータは、**reverse-only** キーワードでは設定されていません。

```
Router> show platform software pisa fm interface vlan 10
```

```
PISA FM Interface type/properties
=====
Interface Type    = L3
Trunk              = False
Ether Channel     = False

PISA FM FDB DUMP
```

```

=====
Interface Vlan10

ACL name 112
ACL direction input
ACL reverse only False

Direction-less features:
-----
Feature-QOS      : NONE
Feature-ACL      : NONE
Feature-PD       : SF-INS
Feature-URLF     : NONE
Feature-TAGGING  : NONE

Ingress features:
-----
Feature-QOS      : NONE
Feature-ACL      : NONE
Feature-PD       : NONE
Feature-URLF     : NONE
Feature-TAGGING  : NONE

Egress features:
-----
Feature-QOS      : NONE
Feature-ACL      : NONE
Feature-PD       : NONE
Feature-URLF     : NONE
Feature-TAGGING  : NONE

Action flags:  INGRESS INGRESS-ACL-RDT-SEL EGRESS-ACL-CAP-SEL
=====

```

次に、**reverse-only** キーワードで設定されない場合の、ギガビットイーサネットポート 4/25 の PISA 機能マネージャ データを表示する例を示します。

```

Router> show platform software pisa fm interface gigabitethernet 4/25
pisa_fm_ec_cap_enabled 1
IDB = 0x271885C0
PISA_SB = 0x27660AC0
PISA_FDB = 0x27181500

PISA FM Interface type/properties
=====
Interface Type      = L2
Trunk               = True
Ether Channel      = False

PISA FM FDB DUMP
=====
Interface GigabitEthernet4/25

ACL name 101
ACL direction input
ACL reverse only False

Direction-less features:
-----
Feature-QOS      : NONE
Feature-ACL      : NONE
Feature-PD       : SF-INS
Feature-URLF     : NONE
Feature-TAGGING  : NONE

```

■ show platform software pisa fm interface

```
Ingress features:
```

```
-----
```

```
Feature-QOS      : NONE
Feature-ACL      : NONE
Feature-PD       : NONE
Feature-URLF     : NONE
Feature-TAGGING  : NONE
```

```
Egress features:
```

```
-----
```

```
Feature-QOS      : NONE
Feature-ACL      : NONE
Feature-PD       : NONE
Feature-URLF     : NONE
Feature-TAGGING  : NONE
```

```
Action flags:  INGRESS-ACL-CAP-SEL  EGRESS-COPY
```

```
=====
```

次に、**reverse-only** キーワードで設定される場合の、ギガビットイーサネットポート 4/25 の PISA 機能マネージャ データを表示する例を示します。

```
Router> show platform software pisa fm interface gigabitethernet 4/25
```

```
pisa_fm_ec_cap_enabled 0
```

```
IDB = 0x271885C0
```

```
PISA_SB = 0x27660AC0
```

```
PISA FDB = 0x27181500
```

```
PISA FM Interface type/properties
```

```
=====
```

```
Interface Type   = L2
Trunk             = True
Ether Channel    = False
```

```
PISA FM FDB DUMP
```

```
=====
```

```
Interface GigabitEthernet4/25
```

```
ACL name 101
```

```
ACL direction input
```

```
ACL reverse only True
```

```
Direction-less features:
```

```
-----
```

```
Feature-QOS      : NONE
Feature-ACL      : NONE
Feature-PD       : SF-INS
Feature-URLF     : NONE
Feature-TAGGING  : NONE
```

```
Ingress features:
```

```
-----
```

```
Feature-QOS      : NONE
Feature-ACL      : NONE
Feature-PD       : NONE
Feature-URLF     : NONE
Feature-TAGGING  : NONE
```

```
Egress features:
```

```
-----
```

```
Feature-QOS      : NONE
Feature-ACL      : NONE
Feature-PD       : NONE
```

```
Feature-URLF      : NONE
Feature-TAGGING   : NONE
```

```
Action flags:  INGRESS EGRESS-COPY
=====
```



(注) **show platform software pisa fm interface all** コマンドは、すべてのインターフェイスのすべてのデータを順番に表示します。

関連コマンド

コマンド	説明
platform ip features pisa	Intelligent Traffic Redirect (ITR) 機能を設定します。

show platform software pisa split-vlan

PISA 上で分割された VLAN を表示するには **show platform software pisa split-vlan** コマンドを、特権 EXEC モードで実行します。

show platform software pisa split-vlan {*interface interface-type* | *range* | *summary*}

シンタックスの説明

interface <i>interface-type</i>	指定されたインターフェイスを含むエントリだけを表示します。有効値は、Fast Ethernet、Gigabit Ethernet、port channel、および VLAN です。
<i>range</i>	インターフェイス、ポート チャネル、または VLAN の範囲を表示します。有効なインターフェイス範囲は 1 ~ 6、VLAN 範囲は 1 ~ 4094 です。
summary	既存の PISA VLAN の数を表示します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(18)ZYA1	このコマンドのサポートが追加されました。

例

次に、Fast Ethernet ポート 1/48 上の PISA 分割済み VLAN 情報を表示する例を示します。

```
Router# show platform software pisa split-vlan interface fas 1/48

Codes: P - NBAR PD, N - NBAR, F - FPM, U - URLF, 0x380 - RP, 0x340 - IXP
Interface          Vlan      PISA Vlan  InFeat  OutFeat
DestIndex State
-----
FastEthernet1/48   1019      1023       F        F
0x340              down
Router#
```

次に、PISA 分割済み VLAN のサマリーを表示する例を示します。

```
Router# show platform software pisa split-vlan summary
PISA Vlan Usage
-----
1019      FastEthernet1/46.1
1023      FastEthernet1/48
Router#
```

関連コマンド

コマンド	説明
show platform	プラットフォーム情報を表示します。

show policy-map

ポリシー マップに関する情報を表示するには、**show policy-map** コマンドを使用します。

show policy-map [*policy-map-name*]

シンタックスの説明	<i>policy-map-name</i> (任意) ポリシー マップの名前
------------------	---

コマンドのデフォルト	このコマンドにはデフォルト設定がありません。
-------------------	------------------------

コマンドモード	EXEC (>)
----------------	----------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例	次に、すべてのポリシー マップに関する情報を表示する例を示します。
----------	-----------------------------------

```
Router# show policy-map
  Policy Map simple
  Policy Map max-pol-ipp5
  class ipp5

  class ipp5
    police flow 10000000 10000 conform-action set-prec-transmit 6 exceed-action
  policed-dscp-transmit trust precedence police 2000000000 2000000 2000000 co
  nform-action set-prec-transmit 6exceed-action policed-dscp-transmit
Router#
```

次に、特定のポリシー マップの情報を表示する例を示します。

```
Router# show policy-map max-pol-ipp5
  Policy Map max-pol-ipp5
  class ipp5

  class ipp5
    police flow 10000000 10000 conform-action set-prec-transmit 6 exceed-action
  policed-dscp-transmit trust precedence police 2000000000 2000000 2000000 co
  nform-action set-prec-transmit 6exceed-action policed-dscp-transmit
Router#
```

関連コマンド	コマンド	説明
	class-map	QoS クラス マップを設定するための QoS クラス マップ コンフィギュレーション モードにアクセスします。
	policy-map	QoS ポリシー マップを設定するための QoS ポリシー マップ コンフィギュレーション モードにアクセスします。

■ show policy-map

コマンド	説明
show class-map	クラス マップ情報を表示します。
show policy-map interface	インターフェイスに対応付けられた入力および出力ポリシーの統計情報およびコンフィギュレーションを表示します。

show policy-map control-plane

コントロールプレーンのポリシーマップの 1 つのクラスまたはすべてのクラスの設定を表示するには、**show policy-map control-plane** コマンドを使用します。

```
show policy-map control-plane [all] [input [class class-name] | output | [class
class-name]]
```

シンタックスの説明

all	(任意) すべてのコントロールプレーン インターフェイスの情報を表示します。
input	(任意) 付加された入力ポリシーの統計を表示します。
class <i>class-name</i>	(任意) クラスの名前を表示します。
output	(任意) 付加された出力ポリシーの統計を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC (#)

コマンドの履歴

使用上のガイドライン

show policy-map control-plane コマンドは、プロセス レベルに入るパケットの数やレートを制御する集約コントロールプレーン サービスの情報を表示します。

例

次に、コントロールプレーンに関連するポリシー マップ TEST の例を示します。このポリシー マップは、クラス マップ TEST に一致するトラフィックをポリシングし、(クラス マップ **class-default** に一致する) 他のすべてのトラフィックはそのまま通過できます。表 2-84 に、この出力で表示されるフィールドについて説明します。

```
Router# show policy-map control-plane

Control Plane

Service-policy input:TEST

Class-map:TEST (match-all)
  20 packets, 11280 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:access-group 101
  police:
    8000 bps, 1500 limit, 1500 extended limit
    conformed 15 packets, 6210 bytes; action:transmit
    exceeded 5 packets, 5070 bytes; action:drop
    violated 0 packets, 0 bytes; action:drop
    conformed 0 bps, exceed 0 bps, violate 0 bps

Class-map:class-default (match-any)
  105325 packets, 11415151 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:any
```

表 2-84 show policy-map control-plane のフィールドの説明

フィールド	説明
クラスまたはサービス ポリシーに関連するフィールド	
Service-policy input	コントロールプレーンに適用される入力サービス ポリシーの名前。(設定済みの場合、このフィールドには出力サービス ポリシーも表示されます)
Class-map	表示されるトラフィックのクラス。トラフィックは、設定済みのクラスごとに表示されます。トラフィック クラスの次に、クラス一致の実装の選択 (match-all または match-any など) も表示されます。
offered rate	パケットがクラスに着信するレート (kbps)
drop rate	パケットがクラスから廃棄されるレート (kbps)。廃棄レートは、与えられたレートから正常に送信されたパケット数を引いて計算されます。
Match	指定されたトラフィック クラスの一致条件 (注) 使用可能な一致条件オプションの詳細については、『Cisco IOS Quality of Service Solutions Configuration Guide』の「Configuring the Modular Quality of Service Command-Line Interface」を参照してください。
トラフィック ポリシングに関連するフィールド	
police	トラフィック ポリシングをイネーブルするように police コマンドが設定されています。
conformed	指定されたレートに一致するパケットに対して実行されるアクション。アクションが実行されたパケット数とバイト数を表示します。
exceeded	指定されたレートを越えたパケットに対して実行されるアクション。アクションが実行されたパケット数とバイト数を表示します。
violated	指定されたレートに違反するパケットに対して実行されるアクション。アクションが実行されたパケット数とバイト数を表示します。

関連コマンド

コマンド	説明
control-plane	コントロールプレーン コンフィギュレーション モードを開始します。
service-policy (control-plane)	集約コントロールプレーン サービスのコントロールプレーンにポリシー マップを付加します。

show policy-map interface

インターフェイスに対応付けられた入力および出力ポリシーの統計情報およびコンフィギュレーションを表示するには、**show policy-map interface** コマンドを使用します。

show policy-map interface [*{interface interface-number}*] [*{null interface-number}*] [*{vlan vlan-id}*] [**input** | **output**]

シンタックスの説明

<i>interface</i>	(任意) インターフェイス タイプ。有効値は、 ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 atm 、および ge-wan です。
<i>interface-number</i>	モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
null <i>interface-number</i>	(任意) マル インターフェイスを指定します。有効値は 0 です。
vlan <i>vlan-id</i>	(任意) VLAN ID を指定します。有効値は 1 ~ 4094 です。
input	(任意) 入力ポリシーだけを指定します。
output	(任意) 出力ポリシーだけを指定します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

output キーワードはサポートされていません。

Supervisor Engine 32 PISA が搭載された Catalyst 6500 シリーズ スイッチでは、バイト カウンタが表示されます。

ポリシング済みカウンタ情報は出力されないで、代わりに **0** が表示されます (**0** パケット、**0** バイトなど)。廃棄および転送されたポリシング済みカウンタ情報を表示するには、**show mls qos ip** コマンドを入力します。

interface-number 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

例

次に、インターフェイスに対応付けられているすべての入力および出力ポリシーの統計情報およびコンフィギュレーションを表示する例を示します。

```
Router# show policy-map interface
FastEthernet5/36
```

■ show policy-map interface

```

service-policy input: max-pol-ipp5
  class-map: ipp5 (match-all)
    0 packets, 0 bytes
    5 minute rate 0 bps
    match: ip precedence 5
  class ipp5
    police 2000000000 2000000 conform-action set-prec-transmit 6 exceed-action p
policed-dscp-transmit
Router#

```

次に、特定のインターフェイスの入力ポリシー統計情報およびコンフィギュレーションを表示する例を示します。

```

Router# show policy-map interface fastethernet 5/36 input
FastEthernet5/36
  service-policy input: max-pol-ipp5
    class-map: ipp5 (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 5
    class ipp5
      police 2000000000 2000000 conform-action set-prec-transmit 6 exceed-action p
policed-dscp-transmit
Router#

```

関連コマンド

コマンド	説明
class-map	QoS クラス マップを設定するための QoS クラス マップ コンフィギュレーション モードにアクセスします。
policy-map	QoS ポリシー マップを設定するための QoS ポリシー マップ コンフィギュレーション モードにアクセスします。
show class-map	クラス マップ情報を表示します。
show mls qos	MLS QoS 情報を表示します。

show port-security

ポートセキュリティ設定に関する情報を表示するには、**show port-security** コマンドを使用します。

show port-security [*interface interface interface-number*]

show port-security [*interface interface interface-number*] {*address* | *vlan*}

シンタックスの説明	
interface interface	(任意) インターフェイス タイプを指定します。有効値は ethernet 、 fastethernet 、 gigabitethernet 、および tengigabitethernet です。
address	すべてのスイッチ インターフェイスまたは指定されたインターフェイスに設定されたすべてのセキュア MAC アドレス、および各アドレスのエイジング情報を表示します。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン **vlan** キーワードは、トランク ポートだけでサポートされ、トランク ポートに対して設定された VLAN あたりの最大数を表示します。

interface-number 引数はモジュールおよびポート番号を指定します。**interface-number** の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

例 次に、オプションを指定しなかった場合の **show port-security** コマンドの出力例を示します。

```
Router# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security
Action
                (Count)          (Count)      (Count)
-----
Fa5/1            11              11           0                  Shutdown
Fa5/5            15              5            0                  Restrict
Fa5/11           5               4            0                  Protect
-----

Total Addresses in System: 21
Max Addresses limit in System: 128
Router#
```

■ show port-security

次に、指定されたインターフェイスのポートセキュリティ情報を表示する例を示します。

```
Router# show port-security interface fastethernet 5/1
Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 11
Total MAC Addresses: 11
Configured MAC Addresses: 3
Aging time: 20 mins
Aging type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0
Router#
```

次に、すべてのスイッチ インターフェイスまたは指定されたインターフェイスに設定されたすべてのセキュア MAC アドレス、および各アドレスのエージング情報を表示する例を示します。

```
Router# show port-security address
Default maximum: 10
VLAN Maximum Current
1    5    3
2    4    4
3    6    4
Router#
```

■ 関連コマンド

コマンド	説明
clear port-security	MAC アドレス テーブルからセキュア MAC アドレスおよびスティッキ MAC アドレスを削除します。

show power

パワー ステータスに関する情報を表示するには、**show power** コマンドを使用します。

```
show power [{available | redundancy-mode | {status {all | {module num}}}} |
           {power-supply number} | total | used | inline [{interface number} | {module num}]]
```

シンタックスの説明

available	(任意) 使用可能なシステム電力 (マージン) を表示します。
redundancy-mode	(任意) 電源装置の冗長モードを表示します。
status	(任意) パワー ステータスを表示します。
all	すべての FRU タイプを表示します。
module num	特定のモジュールのパワー ステータスを表示します。
power-supply number	特定の電源装置のパワー ステータスを表示します。有効値は 1 および 2 です。
total	(任意) 電源装置で使用可能な総電力を表示します。
used	(任意) 電源がオンの機器に関するパワー バジレットの合計を表示します。
inline	(任意) インライン パワー ステータスを表示します。
interface number	(任意) インターフェイス タイプを指定します。指定できる有効値は ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 null 、 port-channel 、および vlan です。詳細については、「 使用上のガイドライン 」を参照してください。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

Catalyst 6500 シリーズ スイッチは、使用しているスーパーバイザ エンジンの種類に関係なく、冗長スーパーバイザ エンジン構成を想定して、2 番めのスーパーバイザ エンジン スロットに電力を供給します。この機能は停止できません。

2 台めのスーパーバイザ エンジンを設置しない場合は、電力を最大限に利用できるように、電力消費の大きいモジュールを 2 番めのスーパーバイザ エンジン スロットに組み込むことを推奨します。

interface-number 引数はモジュールおよびポート番号を指定します。**interface-number** の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビットイーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

show power

vlan-id の有効値は 1 ~ 4094 です。

show power コマンド出力の **Inline power** フィールドには、モジュールで消費されるインライン パワーが表示されます。たとえば、次の例は、モジュール 9 で 0.300 A のインライン パワーが消費されることを示します。

```
Inline power # current
module      9  0.300A
```

例

次に、使用可能なシステム電力を表示する例を示します。

```
Router> show power available
system power available = 20.470A
Router>
```

次に、電源装置の冗長モードを表示する例を示します。

```
Router# show power redundancy-mode
system power redundancy mode = redundant
Router#
```

次に、システム パワー ステータスを表示する例を示します。

```
Router> show power
system power redundancy mode = combined
system power total =      3984.12 Watts (94.86 Amps @ 42V)
system power used =      1104.18 Watts (26.29 Amps @ 42V)
system power available = 2879.94 Watts (68.57 Amps @ 42V)
Power-Capacity PS-Fan Output Oper
PS  Type                Watts  A @42V Status Status State
-----
1   WS-CAC-3000W         2830.80 67.40 OK      OK      on
2   WS-CAC-1300W         1153.32 27.46 OK      OK      on
Note: PS2 capacity is limited to 2940.00 Watts (70.00 Amps @ 42V)
when PS1 is not present
Pwr-Allocated Oper
Fan  Type                Watts  A @42V State
-----
1   FAN-MOD-9             241.50 5.75 OK
2   FAN-MOD-9             241.50 5.75 failed
Pwr-Requested Pwr-Allocated Admin Oper
Slot Card-Type        Watts  A @42V Watts  A @42V State State
-----
1   WS-X6K-SUP2-2GE      145.32 3.46 145.32 3.46 on  on
2   WS-X6K-SUP2-2GE      -      - 145.32 3.46 -  -
3   WS-X6516-GBIC        118.02 2.81 118.02 2.81 on  on
5   WS-C6500-SFM         117.18 2.79 117.18 2.79 on  on
7   WS-X6516A-GBIC       214.20 5.10 -      - on  off (insuff cooling capacity)
8   WS-X6516-GE-TX       178.50 4.25 178.50 4.25 on  on
9   WS-X6816-GBIC        733.98 17.48 -      - on  off (connector rating
exceeded)
Router>
```

次に、すべての FRU タイプのパワー ステータスを表示する例を示します。

```
Router# show power status all
FRU-type # current admin state oper
power-supply 1 27.460A on on
module 1 4.300A on on
module 2 4.300A - - (reserved)
module 5 2.690A on on
Router#
```

次に、特定のモジュールのパワー ステータスを表示する例を示します。

```
Router# show power status module 1
FRU-type      #      current  admin state oper
module        1      -4.300A  on      on
Router#
```

次に、特定の電源装置のパワー ステータスを表示する例を示します。

```
Router# show power status power-supply 1
FRU-type      #      current  admin state oper
power-supply  1      27.460A  on      on
Router#
```

次に、大容量の電源装置に関する情報を表示する例を示します。

```
Router# show power status power-supply 2
Power-Capacity PS-Fan Output Oper
PS   Type      Watts   A @42V Status Status State
-----
1    WS-CAC-6000W 2672.04 63.62 OK    OK    on
2    WS-CAC-9000W-E 2773.68 66.04 OK    OK    on
Router#
```

次に、電源装置で使用可能な総電力を表示する例を示します。

```
Router# show power total
system power total = 27.460A
Router#
```

次に、電源がオンの機器に関するパワー バジレットの合計を表示する例を示します。

```
Router# show power used
system power used = -6.990A
Router#
```

次に、インターフェイスのインライン パワー ステータスを表示する例を示します。

```
Router# show power inline
Interface      Admin   Oper   Power ( mWatt )  Device
-----
FastEthernet9/1  auto  on      6300              Cisco 6500 IP Phone
FastEthernet9/2  auto  on      6300              Cisco 6500 IP Phone
.
.
. <Output truncated>
```

次に、特定のモジュールのインライン パワー ステータスを表示する例を示します。

```
Router# show power inline mod 7
Interface  Admin   Oper   Power      Device      Class
          (Watts)
-----
Gi7/1     auto   on      6.3        Cisco IP Phone 7960 n/a
Gi7/2     static power-deny  0          Ieee PD      3
.
.
. <Output truncated>
```

show power**関連コマンド**

コマンド	説明
power enable	モジュールに電源を投入します。
power redundancy-mode	電源装置の冗長モードを設定します。

show qdm status

Catalyst 6500 シリーズスイッチに接続された、現在アクティブな QDM クライアントのステータスに関する情報を表示するには、**show qdm status** コマンドを使用します。

show qdm status

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドを使用すると、Catalyst 6500 シリーズスイッチに接続された各 QDM クライアントに割り当てられた一意のクライアント ID を表示できます。出力では次の情報が表示されます。

- Catalyst 6500 シリーズスイッチに現在接続されている QDM クライアント数
- QDM クライアントのバージョン
- クライアント名および IP アドレス
- クライアント ID
- 接続期間

例 次に、現在アクティブな QDM Web ベースクライアントのステータスに関する情報を表示する例を示します。

```
Router# show qdm status
Number of QDM Clients : 2
QDM Client v2.1(0.7)-_picard_2 @ 10.34.8.92 (id:5)
    connected since 07:50:00 UTC Sat Aug 11 1917

QDM Client v2.1(0.7)-_janeway_2 @ 171.69.49.14 (id:4)
    connected since 07:49:39 UTC Sat Aug 11 1917
Router#
```

関連コマンド	コマンド	説明
	disconnect qdm	QDM セッションを切断します。

show qm-sp port-data

QoS マネージャ スイッチ プロセッサに関する情報を表示するには、**show qm-sp port-data** コマンドを使用します。

```
show qm-sp port-data {mod port}
```

シンタックスの説明

<i>mod port</i>	モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
-----------------	---

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

スイッチ コマンド— 特権 EXEC (Switch-sp#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、スーパーバイザ エンジンだけでサポートされています。このコマンドを入力できるのは、Catalyst 6500 シリーズ スイッチ コンソールからだけです (**remote login** コマンドを参照)。

mod port 引数は、モジュールおよびポート番号を指定します。有効値は、使用するシャーシおよびモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 です。

ハードウェアにプログラミングされた値を確認するには、**show qm-sp port-data** コマンドを入力します。

例 次に、QoS マネージャに関する情報を表示する例を示します。

```
Switch-sp# show qm-sp port-data 1 2
-----
* Type: Tx[1p2q2t] Rx[1p1q4t] [0] Pinnacle
* Per-Port: [Untrusted] Default COS[0] force[0] [VLAN based]
-----
* COSMAP(C[Q/T]) TX: 0[1/1] 1[1/1] 2[1/2] 3[1/2] 4[2/1] 5[3/1] 6[2/1] 7[2/2]
                  RX: 0[1/1] 1[1/1] 2[1/2] 3[1/2] 4[1/3] 5[2/1] 6[1/3] 7[1/4]
-----
* WRR bandwidth: [7168 18432]
* TX queue limit(size): [311296 65536 65536]
* WRED queue[1]: failed (0x82)
                  queue[2]: failed (0x82)
```

```

-----
* TX drop thr queue[1]: type[2 QOS_SCP_2_THR] dropThr[311104 311104]
      queue[2]: type[2 QOS_SCP_2_THR] dropThr[61504 61504]
* RX drop threshold:   type[4 QOS_SCP_4_THR] dropThr[62259 62259 62259 62259]
* RXOvr drop threshold: type[0 UNSUPPORTED] dropThr[16843009 131589 61504 61504]
* TXOvr drop threshold: type[0 UNSUPPORTED] dropThr[67174656 260 16843009 131589]
Switch-sp#

```

関連コマンド

コマンド	説明
rcv-queue queue-limit	完全優先キューと標準受信キューの間のサイズ比を設定します。
remote login	Catalyst 6500 シリーズ スイッチ コンソールまたは特定のモジュールにアクセスします。
wrr-queue	標準送信キュー間の帯域幅を割り当てます。
wrr-queue queue-limit	インターフェイス上の送信キュー サイズ比を設定します。
wrr-queue threshold	1q4t および 2q2t インターフェイス上の標準受信キューおよび標準送信キューの廃棄しきい値パーセントを設定します。

■ show qm-sp port-data

show queueing interface

キューイング情報を表示するには、**show queueing interface** コマンドを使用します。

show queueing interface *{ {interface interface-number} | {null interface-number} | {vlan vlan-id} }*

シンタックスの説明	パラメータ	説明
<i>interface</i>		インターフェイス タイプ。有効値は ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 atm 、および ge-wan です。
<i>interface-number</i>		モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
null <i>interface-number</i>		ヌル インターフェイスを指定します。有効値は 0 です。
vlan <i>vlan-id</i>		VLAN ID を指定します。有効値は 1 ~ 4094 です。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン *interface-number* 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

show queueing interface コマンドは、ハードウェアにプログラミングされた絶対値を表示しません。ハードウェアにプログラミングされた値を確認するには、**show qm-sp port-data** コマンドを入力します。

例 次に、キューイング情報を表示する例を示します。

```
Router# show queueing interface fastethernet 5/1
Interface FastEthernet5/1 queueing strategy: Weighted Round-Robin
Port QoS is enabled
Port is untrusted
Extend trust state: trusted
Default COS is 0
Transmit queues [type = 2q2t]:
  Queue Id      Scheduling  Num of thresholds
  -----
    1           WRR low      2
    2           WRR high      2

WRR bandwidth ratios: 100[queue 1] 255[queue 2]
```

■ show queueing interface

```
queue-limit ratios:      70[queue 1] 30[queue 2]
```

```
queue tail-drop-thresholds
```

```
-----
```

```
1      80[1] 100[2]
```

```
2      80[1] 100[2]
```

```
queue thresh cos-map
```

```
-----
```

```
1      1      0 1
```

```
1      2      2 3
```

```
Router#
```

show redundancy

RF 情報を表示するには、**show redundancy** コマンドを使用します。

show redundancy {clients | counters | history | states | switchover}

シンタックスの説明	clients	RF クライアントに関する情報を表示します。
	counters	RF カウンタに関する情報を表示します。
	history	RF の過去のステータス ログを表示します。
	states	RF ステートに関する情報を表示します。
	switchover	スイッチオーバー数、アクティブになってからのアップタイム、およびシステム アップタイプの合計を表示します。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンド モード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、RF クライアントに関する情報を表示する例を示します。

```
Router# show redundancy clients
clientID = 0      clientSeq = 0      RF_INTERNAL_MSG
clientID = 25     clientSeq = 130    CHKPT RF
clientID = 5026   clientSeq = 130    CHKPT RF
clientID = 5029   clientSeq = 135    Redundancy Mode RF
clientID = 5006   clientSeq = 170    RFS client
clientID = 6      clientSeq = 180    Const OIR Client
clientID = 7      clientSeq = 190    PF Client
clientID = 5008   clientSeq = 190    PF Client
clientID = 28     clientSeq = 330    Const Startup Config
clientID = 29     clientSeq = 340    Const IDPROM Client
clientID = 65000  clientSeq = 65000  RF_LAST_CLIENT
Router#
```

出力では次の情報が表示されます。

- **clientID** : クライアントの ID 番号を表示します。
- **clientSeq** : クライアントの通知シーケンス番号を表示します。
- 現在の RF ステート

■ show redundancy

次に、RF カウンタに関する情報を表示する例を示します。

```
Router# show redundancy counters
Redundancy Facility OMs
    comm link up = 0
    comm link down down = 0

    invalid client tx = 0
    null tx by client = 0
    tx failures = 0
    tx msg length invalid = 0

    client not rxing msgs = 0
rx peer msg routing errors = 0
    null peer msg rx = 0
    errored peer msg rx = 0

    buffers tx = 0
tx buffers unavailable = 0
    buffers rx = 0
    buffer release errors = 0

duplicate client registers = 0
    failed to register client = 0
    Invalid client syncs = 0
Router#
```

次に、RF 履歴に関する情報を表示する例を示します。

```
Router# show redundancy history
00:00:00 client added: RF_INTERNAL_MSG(0) seq=0
00:00:00 client added: RF_LAST_CLIENT(65000) seq=65000
00:00:02 client added: Const Startup Config Sync Clie(28) seq=330
00:00:02 client added: CHKPT RF(25) seq=130
00:00:02 client added: PF Client(7) seq=190
00:00:02 client added: Const OIR Client(6) seq=180
00:00:02 client added: Const IDPROM Client(29) seq=340
00:00:02 *my state = INITIALIZATION(2) *peer state = DISABLED(1)
00:00:02 RF_PROG_INITIALIZATION(100) RF_INTERNAL_MSG(0) op=0 rc=11
00:00:02 RF_PROG_INITIALIZATION(100) CHKPT RF(25) op=0 rc=11
00:00:02 RF_PROG_INITIALIZATION(100) Const OIR Client(6) op=0 rc=11
00:00:02 RF_PROG_INITIALIZATION(100) PF Client(7) op=0 rc=11
.
.
.
```

次に、RF ステータスに関する情報を表示する例を示します。

```
Router# show redundancy states
my state = 13 -ACTIVE
peer state = 1 -DISABLED
Mode = Simplex
Unit = Primary
Unit ID = 1

Redundancy Mode (Operational) = Route Processor Redundancy
Redundancy Mode (Configured) = Route Processor Redundancy
Split Mode = Disabled
Manual Swact = Disabled Reason: Simplex mode
Communications = Down Reason: Simplex mode
```

```

client count = 11
client_notification_TMR = 30000 milliseconds
  keep_alive TMR = 4000 milliseconds
  keep_alive count = 0
  keep_alive threshold = 7
  RF debug mask = 0x0

```

Router#

SSO を設定して **show redundancy states** コマンドを入力した場合、Redundancy Mode (Operational) フィールドおよび Redundancy Mode (Configured) フィールドに Stateful Switchover が表示されます。

次に、スイッチオーバー数、アクティブになってからのアップタイム、およびシステム アップタイプの合計を表示する例を示します。

```

Router# show redundancy switchover
Switchovers this system has experienced      : 1
Uptime since this supervisor switched to active : 1 minute
Total system uptime from reload              : 2 hours, 47 minutes

```

Router#

関連コマンド

コマンド	説明
mode	冗長モードを設定します。
redundancy	冗長コンフィギュレーション モードを開始します。
redundancy force-switchover	アクティブ スーパーバイザ エンジンからスタンバイ スーパーバイザ エンジンへのスイッチオーバーを強制します。

show rom-monitor

ROMMON ステータスを表示するには、**show rom-monitor** コマンドを使用します。

show rom-monitor {slot num} {sp | rp}

シンタックスの説明

slot num	表示する ROMMON のスロット番号を指定します。
sp	スイッチ プロセッサの ROMMON ステータスを表示します。
rp	ルート プロセッサの ROMMON ステータスを表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

show rom-monitor コマンドを入力すると、次の出力が表示されます。

- リージョン region1 および region2 : ROMMON イメージのステータス、および region1 または region2 イメージを起動する優先順位を表示します。ROMMON イメージのステータス値は次のとおりです。
 - First run : 新規イメージのチェックが実行中です。
 - Invalid : 新規イメージのチェックが完了し、アップグレードプロセスが開始しています。
 - Approved : ROMMON フィールドのアップグレードプロセスが完了しています。
- Currently running : 現在稼働中のイメージおよびリージョンを表示します。

sp または **rp** キーワードが必須となるのは、指定されたスロットにスーパーバイザ エンジンが搭載されている場合だけです。

例

次に、ROMMON 情報を表示する例を示します。

```
Router# show rom-monitor slot 1 sp
Region F1:APPROVED
Region F2:FIRST_RUN, preferred
Currently running ROMMON from F1 region
Router#
```

関連コマンド

コマンド	説明
upgrade rom-monitor	ROMMON に関して実行優先順位を設定します。

show rpc

RPC 情報を表示するには、**show rpc** コマンドを使用します。

show rpc {applications | counters | status}

シンタックスの説明

applications	RPC アプリケーションに関する情報を表示します。
counters	RPC カウンタを表示します。
status	RPC ステータスを表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、RPC アプリケーションを表示する例を示します。

```
Router# show rpc applications
ID Dest Callback Application
 1 0011 <remote> rpc-master
 2 0011 <remote> cygnus-oir
 3 0021 60201708 rpc-slave-33
 4 0021 6022A514 idprom-MP
 5 0021 60204420 msfc-oir
 6 0011 <remote> Nipcon-SP
 7 0011 <remote> sw_vlan_sp
 8 0011 <remote> stp_switch_api
 9 0011 <remote> pagp_rpc
10 0011 <remote> span_switch_rpc
11 0011 <remote> pf_rp_rpc
13 0011 <remote> mapping_sp
14 0011 <remote> logger-sp
17 0011 <remote> c6k_power_sp
18 0011 <remote> c6k_sp_environmental
19 0011 <remote> pagp_switch_rpc
20 0011 <remote> pm-cp
21 0021 602675B0 Nipcon-RP
22 0021 602283B0 pm-mp
23 0021 601F2538 sw_vlan_rp
24 0021 601F77D0 span_switch_sp_rpc
25 0021 601F7950 idbman_fec
26 0021 601F7F30 logger-rp
27 0021 601F80D8 pagp_switch_l3_split
28 0021 601F81C0 pagp_switch_sp2mp
29 0021 6026F190 c6k_rp_environmental
Router#
```

次に、RPC カウンタに関する情報を表示する例を示します。

■ show rpc

```
Router# show rpc counters
ID Dest Rcv-req Xmt-req Q size Application
1 0011 0 26 0 rpc-master
2 0011 0 6221 0 cygnus-oir
4 0021 15 0 0 idprom-MP
5 0021 6222 0 0 msfc-oir
7 0011 0 2024 0 sw_vlan_sp
8 0011 0 3 0 stp_switch_api
9 0011 0 188 0 pagp_rpc
11 0011 0 4 0 pf_rp_rpc
13 0011 0 2 0 mapping_sp
14 0011 0 3 0 logger-sp
17 0011 0 2 0 c6k_power_sp
18 0011 0 66 0 c6k_sp_environmental
19 0011 0 109 0 pagp_switch_rpc
20 0011 0 33 0 pm-cp
22 0021 126 0 0 pm-mp
23 0021 5 0 0 sw_vlan_rp
24 0021 14 0 0 span_switch_sp_rpc
25 0021 22 0 0 idbman_fec
26 0021 8 0 0 logger-rp
27 0021 3 0 0 pagp_switch_l3_split
28 0021 3 0 0 pagp_switch_sp2mp
Router#
```

show running-config

モジュール、レイヤ 2 VLAN、またはインターフェイスのステータスおよび設定を表示するには、**show running-config** コマンドを使用します。

```
show running-config [ {interface interface } | {module number} | {vlan vlan-id} ]
```

シンタックスの説明

interface interface	(任意) インターフェイス タイプを指定します。有効値は ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 atm 、および ge-wan です。
module number	(任意) モジュール番号を指定します。
vlan vlan-id	(任意) 情報表示する VLAN を指定します。有効値は 1 ~ 4094 です。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

場合によっては、**show interfaces** コマンドと **show running-config** コマンドで表示されるデュプレックス モードが異なる場合があります。この場合は、**show interfaces** コマンドで表示されるデュプレックス モードが、インターフェイスが実際に実行しているデュプレックス モードです。**show interfaces** コマンドは、インターフェイスの動作モードを表示しますが、**show running-config** コマンドは、インターフェイスに設定されているモードを表示します。

特定のインターフェイスに **show running-config** コマンドを使用した場合は、デュプレックス モード設定が表示されているにもかかわらず、速度設定が表示されないことがあります。この出力は、インターフェイス速度が **auto** に設定されており、速度を **auto** 以外に設定すると表示されているデュプレックス モードが動作設定になることを示します。このような設定の場合、このインターフェイスで動作中のデュプレックス モードは、**show running-config** コマンドで表示されるデュプレックス モードと一致しません。

例

次に、すべてのモジュールのモジュール設定およびステータス設定を表示する例を示します。

```
Router# show running-config
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug datetime localtime
service timestamps log datetime localtime
no service password-encryption
!
hostname Router
```

■ show running-config

```
!  
boot buffersize 126968  
boot system flash slot0:halley  
boot bootldr bootflash:c6msfc-boot-mz.120-6.5T.XE1.0.83.bin  
enable password lab  
!  
clock timezone Pacific -8  
clock summer-time Daylight recurring  
redundancy  
  main-cpu  
  auto-sync standard  
!  
ip subnet-zero  
!  
ip multicast-routing  
ip dvmrp route-limit 20000  
ip cef  
mls flow ip destination  
mls flow ipx destination  
cns event-service server  
!  
spanning-tree portfast bpdu-guard  
spanning-tree uplinkfast  
spanning-tree vlan 200 forward-time 21  
port-channel load-balance sdip  
!  
!  
!  
  shutdown  
!  
!  
.  
.  
.
```

show scp

SCP 情報を表示するには、**show scp** コマンドを使用します。

```
show scp {accounting | counters | {{mcast [group group-id] | inst}} | {process id} |
status}
```

シンタックスの説明

accounting	SCP アカウンティングに関する情報を表示します。
counters	SCP カウンタに関する情報を表示します。
mcast	SCP マルチキャストに関する情報を表示します。
group group-id	(任意) 特定のグループおよびグループ ID の情報を表示します。有効値は 1 ~ 127 です。
inst	(任意) インスタンスに関する情報を表示します。
process id	(任意) SAP を SCP に登録したすべてのプロセスを表示します。
status	ローカル SCP サーバのステータス情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、SAP を SCP に登録したすべてのプロセスを表示する例を示します。

```
Router# show scp process
Sap Pid Name
==== == =====
0 180 CWAN-RP SCP Input Process
18 42 itasca
20 3 Exec
21 3 Exec
22 180 CWAN-RP SCP Input Process
Total number of SAP registered = 5
Router#
```

show snmp mib ifmib ifindex

すべてのシステム インターフェイスまたは指定したシステム インターフェイスについて、SNMP インターフェイス インデックス識別番号 (ifIndex 値) を表示するには、**show snmp mib ifmib ifindex** コマンドを使用します。

```
show snmp mib ifmib ifindex [interface
                             interface-number][:subinterface][.subinterface][port]
```

シンタックスの説明

<i>interface</i>	(任意) インターフェイス タイプ。有効値は ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 atm 、および ge-wan です。
<i>interface-number</i>	モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
<i>:subinterface</i>	(任意) サブインターフェイス番号。有効値は 0 です。
<i>.subinterface</i>	(任意) サブインターフェイス番号。有効値は 0 ~ 4,294,967,295 です。
<i>port</i>	(任意) インターフェイス番号

コマンドのデフォルト

すべてのインターフェイスの ifIndex 値が表示されます。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

show snmp mib ifmib ifindex コマンドでは、CLI を使用してインターフェイスおよびサブインターフェイスに割り当てられた SNMP インターフェイス インデックス識別番号 (ifIndex 値) を表示できます。このコマンドを使用すると、ネットワーク管理ステーションを使用しなくても、これらの値を表示できます。

オプションの *interface-type*、*slot*、*port-adaptor*、および *port* 引数を使用して特定のインターフェイスを指定しなかった場合は、システム上に存在するすべてのインターフェイスとサブインターフェイスの ifDescr と ifIndex のペアが表示されます。

システム上で使用可能なオプションを調べるには、**show snmp mib ifmib ifindex ?** コマンドを使用します。一般的な *interface-types* 値は、**async**、**dialer**、**ethernet**、**fastEthernet**、および **serial** です。

例

次に、特定のインターフェイスの ifIndex を表示する例を示します。

```
Router# show snmp mib ifmib ifIndex Ethernet2/0
Ethernet2/0: Ifindex = 2
```

次に、すべてのインターフェイスの ifIndex を表示する例を示します。

```
Router# show snmp mib ifmib ifindex
ATM1/0: Ifindex = 1
```

```

ATM1/0-aal5 layer: Ifindex = 12
ATM1/0-atm layer: Ifindex = 10
ATM1/0.0-aal5 layer: Ifindex = 13
ATM1/0.0-atm subif: Ifindex = 11
ATM1/0.9-aal5 layer: Ifindex = 32
ATM1/0.9-atm subif: Ifindex = 31
ATM1/0.99-aal5 layer: Ifindex = 36
ATM1/0.99-atm subif: Ifindex = 35
Ethernet2/0: Ifindex = 2
Ethernet2/1: Ifindex = 3
Ethernet2/2: Ifindex = 4
Ethernet2/3: Ifindex = 5
Null0: Ifindex = 14
Serial3/0: Ifindex = 6
Serial3/1: Ifindex = 7
Serial3/2: Ifindex = 8
Serial3/3: Ifindex = 9
    
```

関連コマンド

コマンド	説明
snmp ifindex persist	再起動後も保持される Interfaces MIB (IF-MIB) 内の ifIndex 値 (ifIndex 永続性) を特定のインターフェイス上だけでイネーブルにします。
snmp-server ifindex persist	ifIndex 値を、SNMP で使用するために再起動後も一定となるようにグローバルにイネーブル化します。

show spanning-tree

スパニングツリー ステートに関する情報を表示するには、**show spanning-tree** コマンドを使用します。

```
show spanning-tree [bridge-group | active | backbonefast | {bridge [id]} | detail |
inconsistentports | {interface interface interface-number} | root | summary [total] |
uplinkfast | {vlan vlan-id} | {port-channel number} | pathcost-method]
```

シンタックスの説明

<i>bridge-group</i>	(任意) ブリッジグループの番号。有効値は 1 ~ 255 です。
active	(任意) アクティブ インターフェイスに関するスパニングツリー情報だけを表示します。
backbonefast	(任意) スパニングツリー BackboneFast ステータスに関する情報を表示します。
bridge	(任意) ブリッジのステータスおよびコンフィギュレーションに関する情報を表示します。
id	(任意) ブリッジ ID を表示します。
detail	(任意) スパニングツリー ステートに関する詳細情報を表示します。
inconsistentports	(任意) ルート不一致ステートに関する情報を表示します。
interface interface	(任意) インターフェイス タイプと番号を表示します。タイプの有効値は ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 atm 、および ge-wan です。
<i>interface-number</i>	(任意) モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
root	(任意) ルート ブリッジのステータスおよびコンフィギュレーションを表示します。
summary	(任意) ポート ステートのサマリーを表示します。
total	(任意) スパニングツリー ステート セクションのすべての行を表示します。
uplinkfast	(任意) スパニングツリー UplinkFast ステータスを表示します。
vlan vlan-id	(任意) VLAN ID を指定します。有効値は 1 ~ 4094 です。
port-channel number	(任意) チャンネル インターフェイスを指定します。有効値は 1 ~ 282 の範囲の最大 64 個の値です。
pathcost-method	(任意) 使用されているデフォルト パス コスト計算方式を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

pos、**atm**、および **ge-wan** キーワードは、Supervisor Engine 2 が搭載された Catalyst 6500 シリーズスイッチだけでサポートされています。

257 ~ 282 の **port-channel number** 値は、CSM および FWSM だけでサポートされています。

interface-number 引数はモジュールおよびポート番号を指定します。**interface-number** の有効値は、指定されたインターフェイスタイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロットシャーシに 48 ポート 10/100BASE-T イーサネットモジュールが搭載されている場合に、ギガビットイーサネットインターフェイスを指定すると、モジュール番号の有効値は 2 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

スパニングツリーのアクティブステータスをチェックする場合に多数の VLAN が存在するときには、**show spanning-tree summary total** コマンドを入力します。VLAN の一覧をスクロールしなくても VLAN の総数を表示できます。

例

次に、インターフェイス情報のサマリーを表示する例を示します。

```
Router# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    4097
            Address    0004.9b78.0800
            This bridge is the root
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4097  (priority 4096 sys-id-ext 1)
            Address    0004.9b78.0800
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  15

Interface          Port ID          Designated          Port ID
Name               Prio.Nbr         Cost Sts             Cost Bridge ID       Prio.Nbr
-----
Gi2/1              128.65           4 LIS              0 4097 0004.9b78.0800 128.65
Gi2/2              128.66           4 LIS              0 4097 0004.9b78.0800 128.66
Fa4/3              128.195          19 LIS             0 4097 0004.9b78.0800 128.195
Fa4/4              128.196          19 BLK             0 4097 0004.9b78.0800 128.195

Router#
```

表 2-85 に、この例で表示されるフィールドについて説明します。

表 2-85 show spanning-tree コマンドの出カフィールド

フィールド	定義
Port ID Prio.Nbr	ポート ID およびプライオリティ番号
Cost	ポート コスト
Sts	ステータス情報

次に、アクティブ インターフェイスのスパニングツリー情報だけを表示する例を示します。

```
Router# show spanning-tree active
UplinkFast is disabled
BackboneFast is disabled

VLAN1 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address 0050.3e8d.6401
```

■ show spanning-tree

```

Configured hello time 2, max age 20, forward delay 15
Current root has priority 16384, address 0060.704c.7000
Root port is 265 (FastEthernet5/9), cost of root path is 38
Topology change flag not set, detected flag not set
Number of topology changes 0 last change occurred 18:13:54 ago
Times: hold 1, topology change 24, notification 2
      hello 2, max age 14, forward delay 10
Timers: hello 0, topology change 0, notification 0
.
.
.
Router#

```

次に、スパニングツリー **BackboneFast** ステータスを表示する例を示します。

```

Router# show spanning-tree backbonefast
BackboneFast is enabled

BackboneFast statistics
-----
Number of transition via backboneFast (all VLANs) : 0
Number of inferior BPDUs received (all VLANs)    : 0
Number of RLQ request PDUs received (all VLANs)  : 0
Number of RLQ response PDUs received (all VLANs) : 0
Number of RLQ request PDUs sent (all VLANs)      : 0
Number of RLQ response PDUs sent (all VLANs)     : 0
Router#

```

次に、現在のブリッジのスパニングツリー情報だけを表示する例を示します。

```

Router# show spanning-tree bridge
VLAN1
  Bridge ID   Priority    32768
             Address    0050.3e8d.6401
             Hello Time  2 sec   Max Age 20 sec   Forward Delay 15 sec
.
.
.
Router#

```

次に、インターフェイスに関する詳細情報を表示する例を示します。

```

Router# show spanning-tree detail

VLAN1 is executing the ieee compatible Spanning Tree protocol
Bridge Identifier has priority 4096, address 00d0.00b8.1401
Configured hello time 2, max age 20, forward delay 15
We are the root of the spanning tree
Topology change flag not set, detected flag not set
Number of topology changes 9 last change occurred 02:41:34 ago
from FastEthernet4/21
Times: hold 1, topology change 35, notification 2
hello 2, max age 20, forward delay 15
Timers: hello 1, topology change 0, notification 0, aging 300

Port 213 (FastEthernet4/21) of VLAN1 is forwarding
Port path cost 19, Port priority 128, Port Identifier 128.213.
Designated root has priority 4096, address 00d0.00b8.1401
Designated bridge has priority 4096, address 00d0.00b8.1401
Designated port id is 128.213, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
BPDUs: sent 4845, received 1
Router#

```

次に、特定のインターフェイスのスパニングツリーに関する情報を表示する例を示します。

```
Router# show spanning-tree interface fastethernet 5/9
Interface Fa0/10 (port 23) in Spanning tree 1 is ROOT-INCONSISTENT
Port path cost 100, Port priority 128
Designated root has priority 8192, address 0090.0c71.a400
Designated bridge has priority 32768, address 00e0.1e9f.8940
.
.
.
```

次に、特定のブリッジグループのスパニングツリーに関する情報を表示する例を示します。

```
Router# show spanning-tree 1
UplinkFast is disabled
BackboneFast is disabled

Bridge group 1 is executing the ieee compatible Spanning Tree protocol
Bridge Identifier has priority 32768, address 00d0.d39c.004d
Configured hello time 2, max age 20, forward delay 15
Current root has priority 32768, address 00d0.d39b.fddd
Root port is 7 (FastEthernet2/2), cost of root path is 19
Topology change flag set, detected flag not set
Number of topology changes 3 last change occurred 00:00:01 ago
    from FastEthernet2/2
Times: hold 1, topology change 35, notification 2
    hello 2, max age 20, forward delay 15
Timers: hello 0, topology change 0, notification 0 bridge aging time 15

Port 2 (Ethernet0/1/0) of Bridge group 1 is down

Port path cost 100, Port priority 128
Designated root has priority 32768, address 0050.0bab.1808
Designated bridge has priority 32768, address 0050.0bab.1808
Designated port is 2, path cost 0
Timers: message age 0, forward delay 0, hold 0
BPDU: sent 0, received 0

Router#
```

次に、ポートステータスのサマリーを表示する例を示します。

```
Router# show spanning-tree summary
Root bridge for: Bridge group 1, VLAN0001, VLAN0004-VLAN1005
VLAN1013-VLAN1499, VLAN2001-VLAN4094
EtherChannel misconfiguration guard is enabled
Extended system ID is enabled
Portfast is enabled by default
PortFast BPDU Guard is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard is disabled by default
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is long
Name                Blocking Listening Learning Forwarding STP Active
-----
1 bridge            0          0          0          1          1
3584 vlans 3584 0 0 7168 10752
                Blocking Listening Learning Forwarding STP Active
-----
Total                3584          0          0          7169          10753
Router#
```

show spanning-tree

次に、スパニングツリー ステート セクションのすべての行を表示する例を示します。

```
Router# show spanning-tree summary total
Root bridge for:Bridge group 10, VLAN1, VLAN6, VLAN1000.
Extended system ID is enabled.
PortFast BPDU Guard is disabled
EtherChannel misconfiguration guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Default pathcost method used is long

Name                Blocking Listening Learning Forwarding STP Active
-----
105 VLANs 3433      0          0          105      3538

BackboneFast statistics
-----
Number of transition via backboneFast (all VLANs) :0
Number of inferior BPDUs received (all VLANs)    :0
Number of RLQ request PDUs received (all VLANs)  :0
Number of RLQ response PDUs received (all VLANs) :0
Number of RLQ request PDUs sent (all VLANs)      :0
Number of RLQ response PDUs sent (all VLANs)     :0
Router#
```

次に、特定の VLAN のスパニングツリーに関する情報を表示する例を示します。

```
Router# show spanning-tree vlan 200
VLAN0200
Spanning tree enabled protocol ieee
Root ID Priority 32768
  Address 00d0.00b8.14c8
  This bridge is the root
  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 32768
  Address 00d0.00b8.14c8
  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
  Aging Time 300
Interface Role Sts Cost Prio.Nbr Status
-----
Fa4/4 Desg FWD 200000 128.196 P2p
Fa4/5 Back BLK 200000 128.197 P2p
Router#
```

表 2-86 に、この例で表示されるフィールドについて説明します。

表 2-86 show spanning-tree vlan コマンドの出カフィールド

フィールド	定義
Role	現在の 802.1w ロール。有効値は、Boun (boundary)、Desg (designated)、Root、Altn (alternate)、および Back (backup) です。
Sts	スパニング ツリー状態。有効値は、BKN* (broken) ¹ 、BLK (blocking)、DWN (down)、LTN (listening)、LBK (loopback)、LRN (learning)、および FWD (forwarding) です。
Cost	ポート コスト

表 2-86 show spanning-tree vlan コマンドの出力フィールド (続き)

フィールド	定義
Prio.Nbr	ポート優先順位とポート番号で構成されるポート ID
Status	ステータス情報。有効値は次のとおりです。 <ul style="list-style-type: none"> • P2p/Shr : インターフェイスは、スパンニング ツリーによってポイント ツー ポイント (それぞれ共有される) インターフェイスと見なされます。 • Edge : PortFast が設定され (default コマンドをグローバルに使用するか、または直接インターフェイス上で)、BPDU は受信されていません。 • *ROOT_Inc、*LOOP_Inc、*PVID_Inc、および *TYPE_Inc : ポートは不整合のため故障状態 (BKN*) です。ポートはルート不整合、ループ ガード不整合、PVID (ポート VLAN ID) 不整合、またはタイプ不整合です。 • Bound(type) : MST モードで、境界ポートを識別し、ネイバのタイプ (STP、RSTP、または PVST) を示します。 • Peer(STP) : PVRST rapid-pvst モードで、前のバージョンの 802.1D ブリッジに接続されているポートを識別します。

1. * については、Status フィールドの定義を参照してください。

次に、root inconsistent ステートのポートがあるかどうかを判別する例を示します。

```
Router# show spanning-tree inconsistentports
```

```
Name                Interface          Inconsistency
-----
VLAN1                FastEthernet3/1   Root Inconsistent
```

```
Number of inconsistent ports (segments) in the system : 1
```

```
Router#
```

関連コマンド

コマンド	説明
spanning-tree backbonefast	すべてのイーサネット VLAN で BackboneFast をイネーブルにします。
spanning-tree cost	STP 計算に使用するインターフェイスのパス コストを設定します。
spanning-tree guard	ガード モードをイネーブルまたはディセーブルにします。
spanning-tree pathcost method	デフォルトのパス コスト計算方式を設定します。
spanning-tree portfast (interface configuration mode)	PortFast モードをイネーブルにします。
spanning-tree portfast bpdupfilter default	すべての PortFast ポートで、BPDU フィルタリングをデフォルトでイネーブルにします。
spanning-tree portfast bpduguard default	すべての PortFast ポートで、BPDU ガードをデフォルトでイネーブルにします。
spanning-tree port-priority	2つのブリッジがルートブリッジとなるために競合している場合に、インターフェイスに優先順位を設定します。
spanning-tree uplinkfast	UplinkFast をイネーブルにします。
spanning-tree vlan	VLAN 単位で STP を設定します。

show spanning-tree mst

MST プロトコルに関する情報を表示するには、**show spanning-tree mst** コマンドを使用します。

show spanning-tree mst [configuration [digest]]

show spanning-tree mst [instance-id] [detail]

show spanning-tree mst [instance-id] interface interface [detail]

シンタックスの説明

configuration	(任意) リージョン コンフィギュレーション情報を表示します。
digest	(任意) 現在の MSTCI に含まれている MD5 ダイジェストに関する情報を表示します。
<i>instance-id</i>	(任意) インスタンス ID 番号を指定します。有効値は 0 ~ 4094 です。
detail	(任意) MST プロトコルに関する詳細情報を表示します。
interface interface	(任意) インターフェイス タイプと番号を表示します。タイプの有効値は ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 atm 、 ge-wan 、 port-channel 、および vlan です。有効値については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

interface の有効値は、指定したインターフェイス タイプおよび使用されているシャーシおよびモジュールによって決まります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 2 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

port-channel number の有効値は、1 ~ 282 の範囲の最大 64 の値です。257 ~ 282 の **port-channel number** 値は、CSM および FWSM だけでサポートされています。

vlan の有効値は 1 ~ 4094 です。

instance-id の有効値は 0 ~ 4094 です。

show spanning-tree mst configuration コマンドの出力表示に、警告メッセージが表示されることがあります。セカンダリ VLAN が、対応付けられたプライマリ VLAN と同じインスタンスにマッピングされていない場合に、このメッセージが表示されます。出力には、対応付けられたプライマリ VLAN と同じインスタンスにマッピングされていないセカンダリ VLAN のリストが含まれます。警告メッセージは次のとおりです。

These secondary vlans are not mapped to the same instance as their primary:
-> 3

出力がポート単位で同時に標準ブリッジと先行標準ブリッジの両方に適用される場合、**show spanning-tree mst configuration digest** コマンドの出力表示に、2 つの異なるダイジェストが表示されます。

先行標準の BPDU だけを送信するようにポートを設定する場合、先行標準フラグが **show spanning-tree** コマンドに表示されます。先行標準フラグの種類は次のとおりです。

- **Pre-STD** または **prestandard** (長形式) : ポートが先行標準 BPDU を送信するように設定されている場合、およびこのインターフェイス上で先行標準ネイバブリッジが検出された場合に、このフラグが表示されます。
- **Pre-STD-Cf** または **prestandard (config)** (長形式) : 先行標準 BPDU を送信するようにポートを設定し、そのポートで先行標準 BPDU が受信されない場合、自動検出メカニズムが失敗した場合、または先行標準ネイバが存在しない場合に設定が間違っている場合、このフラグが表示されます。
- **Pre-STD-Rx** または **prestandard (rcvd)** (長形式) : 先行標準 BPDU がポートで受信され、先行標準 BPDU を送信するようにポートを設定していない場合に、このフラグが表示されます。ポートは先行標準 BPDU を送信しますが、先行標準ネイバとのやりとりを自動検出メカニズムだけに依存しないようにポートの設定を変更することを推奨します。

設定が先行標準に適合していない場合 (たとえば、単一の MST インスタンス ID が 16 以上の場合)、先行標準ダイジェストは計算されず、次の出力が表示されます。

```
Router# show spanning-tree mst configuration digest
Name          [region1]
Revision 2      Instances configured 3
Digest        0x3C60DBF24B03EBF09C5922F456D18A03
Pre-std Digest N/A, configuration not pre-standard compatible
Router#
```

MST BPDU には、リージョン名、リージョン レビジョン、および MST コンフィギュレーションの VLAN と インスタンス間のマッピングの MD5 ダイジェストで構成される MSTCI が含まれます。

出力の定義については、**show spanning-tree** コマンドを参照してください。

例

次に、リージョン設定に関する情報を表示する例を示します。

```
Router> show spanning-tree mst configuration
Name          [leo]
Revision 2702
Instance Vlans mapped
-----
```

```
0          1-9,11-19,21-29,31-39,41-4094
1          10,20,30,40
-----
```

次に、追加の MST プロトコル値を表示する例を示します。

```
Router# show spanning-tree mst 3 detail
##### MST03 vlans mapped: 3,3000-3999
Bridge address 0002.172c.f400 priority 32771 (32768 sysid 3)
Root this switch for MST03
```

```
GigabitEthernet1/1 of MST03 is boundary forwarding
Port info port id 128.1 priority 128
cost 20000
Designated root address 0002.172c.f400 priority 32771
cost 0
Designated bridge address 0002.172c.f400 priority 32771 port
```

■ show spanning-tree mst

```

id 128.1
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 4, received 0

FastEthernet4/1 of MST03 is designated forwarding
Port info port id 128.193 priority 128 cost
200000
Designated root address 0002.172c.f400 priority 32771
cost 0
Designated bridge address 0002.172c.f400 priority 32771 port id
128.193
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 254, received 1

FastEthernet4/2 of MST03 is backup blocking
Port info port id 128.194 priority 128 cost
200000
Designated root address 0002.172c.f400 priority 32771
cost 0
Designated bridge address 0002.172c.f400 priority 32771 port id
128.193
Timers: message expires in 2 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 3, received 252
Router#

```

次に、特定のインターフェイスの MST 情報を表示する例を示します。

```

Router# show spanning-tree mst 0 interface fastethernet 4/1 detail
Edge port: no (trunk) port guard : none
(default)
Link type: point-to-point (point-to-point) bpdu filter: disable
(default)
Boundary : internal bpdu guard : disable
(default)
FastEthernet4/1 of MST00 is designated forwarding
Vlans mapped to MST00 1-2,4-2999,4000-4094
Port info port id 128.193 priority 128 cost
200000
Designated root address 0050.3e66.d000 priority 8193
cost 20004
Designated ist master address 0002.172c.f400 priority 49152
cost 0
Designated bridge address 0002.172c.f400 priority 49152 port id
128.193
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus sent 492, received 3
Router#

```

次に、現在の MSTCI に含まれている MD5 ダイジェストを表示する例を示します。

```

Router# show spanning-tree mst configuration digest
Name          [mst-config]
Revision 10    Instances configured 25
Digest        0x40D5ECA178C657835C83BBCB16723192
Pre-std Digest 0x27BF112A75B72781ED928D9EC5BB4251
Router#

```

次に、CIST ルートポートであるポート上のリージョンの境界にある、すべての MST インスタンスに対する新規のマスター ロールを表示する例を示します。

```

Router# show spanning-tree mst interface fastethernet4/9

FastEthernet4/9 of MST00 is root forwarding
Edge port: no                (default)                port guard : none                (default)

```

```

Link type: point-to-point (auto)          bpdu filter: disable      (default)
Boundary : boundary (RSTP)              bpdu guard : disable     (default)
Bpdus sent 3428, received 6771

```

```

Instance Role Sts Cost          Prio.Nbr Vlans mapped
-----
0          Root FWD 200000    128.201 2-7,10,12-99,101-999,2001-3999,4001-4094
8          Mstr FWD 200000    128.201 8,4000
9          Mstr FWD 200000    128.201 1,9,100
11         Mstr FWD 200000    128.201 11,1000-2000
Router#

```

関連コマンド

コマンド	説明
spanning-tree mst	任意の MST インスタンスのパス コストおよびポート プライオリティ パラメータを設定します。
spanning-tree mst forward-time	Catalyst 6500 シリーズスイッチ上のすべてのインスタンスに対して転送遅延タイマーを設定します。
spanning-tree mst hello-time	Catalyst 6500 シリーズスイッチ上のすべてのインスタンスに対して hello タイム遅延タイマーを設定します。
spanning-tree mst max-hops	BPDU が廃棄されるまでのリージョンの最大ホップ数を指定します。
spanning-tree mst root	インスタンスのプライマリ ルートとセカンダリ ルートを指定したり、ブリッジプライオリティ、およびタイマー値を設定したりします。

show standby delay

遅延期間に関する HSRP 情報を表示するには、**show standby delay** コマンドを使用します。

show standby delay [*type number*]

シンタックスの説明

type number (任意) 出力を表示するインターフェイスのタイプおよび番号

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、遅延期間に関する情報を表示する例を示します。

```
Router# show standby delay

Interface           Minimum Reload
Ethernet0/3         1           5
Router#
```

関連コマンド

コマンド	説明
standby delay	HSRP グループを初期化するまでの遅延期間を設定します。
minimum reload	

show sup-bootflash

sup-bootflash ファイル システムに関する情報を表示するには、**show sup-bootflash** コマンドを使用します。

show sup-bootflash [all | chips | filesys]

シンタックスの説明

all	(任意) 使用可能なすべてのフラッシュの情報を表示します。
chips	(任意) フラッシュ チップに関する情報を表示します。
filesys	(任意) ファイル システムに関する情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、ブートフラッシュ情報のサマリーを表示する例を示します。

```
Router# show sup-bootflash
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
1  .. image   EBC8FC4D A7487C   6 10700796 Nov 19 1999 07:07:37 halley
2  .. unknown C7EB077D EE2620   25 4644130 Nov 19 1999 07:50:44 cat6000-sup_
5-3-3-CSX.bin

645600 bytes available (15345184 bytes used)
Router#
```

次に、すべてのブートフラッシュ情報を表示する例を示します。

```
Router# show sup-bootflash all
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
1  .. image   EBC8FC4D A7487C   6 10700796 Nov 19 1999 07:07:37 halley
2  .. unknown C7EB077D EE2620   25 4644130 Nov 19 1999 07:50:44 cat6000-sup_
5-3-3-CSX.bin

645600 bytes available (15345184 bytes used)

----- F I L E   S Y S T E M   S T A T U S -----
Device Number = 2
DEVICE INFO BLOCK: bootflash
Magic Number      = 6887635   File System Vers = 10000   (1.0)
Length            = 1000000   Sector Size     = 40000
Programming Algorithm = 19       Erased State    = FFFFFFFF
File System Offset = 40000    Length         = F40000
MONLIB Offset     = 100      Length         = F568
Bad Sector Map Offset = 3FFF8    Length         = 8
Squeeze Log Offset = F80000   Length         = 40000
Squeeze Buffer Offset = FC0000   Length         = 40000
```

show sup-bootflash

```

    Num Spare Sectors      = 0
      Spares:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  No Unrecovered Errors
  No Squeeze in progress
USAGE INFO:
  Bytes Used      = EA2620  Bytes Available = 9D9E0
  Bad Sectors     = 0       Spared Sectors = 0
  OK Files        = 2       Bytes = EA2520
  Deleted Files   = 0       Bytes = 0
  Files w/Errors  = 0       Bytes = 0

***** Intel SCS Status/Register Dump *****

COMMON MEMORY REGISTERS: Bank 0
  Intelligent ID Code : 890089
  Compatible Status Reg: 800080

DEVICE TYPE:
  Layout              : Paired x16 Mode
  Write Queue Size    : 64
  Queued Erase Supported : No

Router#
```

次に、フラッシュ チップに関する情報を表示する例を示します。

```

Router# show sup-bootflash chips

***** Intel SCS Status/Register Dump *****

COMMON MEMORY REGISTERS: Bank 0
  Intelligent ID Code : 890089
  Compatible Status Reg: 800080

DEVICE TYPE:
  Layout              : Paired x16 Mode
  Write Queue Size    : 64
  Queued Erase Supported : No

Router#
```

次に、ファイル システムに関する情報を表示する例を示します。

```

Router# show sup-bootflash filesys

----- F I L E   S Y S T E M   S T A T U S -----
  Device Number = 2
DEVICE INFO BLOCK: bootflash
  Magic Number      = 6887635  File System Vers = 10000  (1.0)
  Length            = 1000000  Sector Size      = 40000
  Programming Algorithm = 19    Erased State     = FFFFFFFF
  File System Offset = 40000    Length = F40000
  MONLIB Offset     = 100      Length = F568
  Bad Sector Map Offset = 3FFF8  Length = 8
  Squeeze Log Offset = F80000  Length = 40000
  Squeeze Buffer Offset = FC0000  Length = 40000
  Num Spare Sectors = 0
    Spares:
STATUS INFO:
  Writable
```

```
NO File Open for Write
Complete Stats
No Unrecovered Errors
No Squeeze in progress
USAGE INFO:
Bytes Used      = EA2620 Bytes Available = 9D9E0
Bad Sectors    = 0       Spared Sectors = 0
OK Files       = 2       Bytes = EA2520
Deleted Files  = 0       Bytes = 0
Files w/Errors = 0       Bytes = 0
```

```
Router#
```

show system jumbomtu

グローバル MTU 設定を表示するには、**show system jumbomtu** コマンドを使用します。

show system jumbomtu

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード 特権 EXEC (#)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、グローバル MTU 設定を表示する例を示します。

```
Router# show system jumbomtu
Global Ethernet MTU is 1550 bytes.
Router#
```

関連コマンド	コマンド	説明
	system jumbomtu	レイヤ 2 およびレイヤ 3 パケットの最大サイズを設定します。

show tcam counts

Ternary Content Addressable Memory (TCAM) 統計情報を表示するには、**show tcam counts** コマンドを使用します。

show tcam counts [*module number*]

シンタックスの説明	module number	(任意) モジュール番号を指定します。有効値については、「使用上のガイドライン」を参照してください。
------------------	----------------------	--

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン **module number** キーワードおよび引数は、モジュールおよびポート番号を指定します。*number* の有効値は、使用するシャーシおよびモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合、モジュール番号の有効値は 2 ~ 13、ポート番号の有効値は 1 ~ 48 です。

例 次に、TCAM の統計情報を表示する例を示します。

```
Router# show tcam counts
          Used      Free      Percent Used      Reserved
          ----      -
Labels:      8        504             1
ACL_TCAM
-----
Masks:      6        4090             0             0
Entries:    37        32731            0             0
QOS_TCAM
-----
Masks:      3        4093             0             0
Entries:    20        32748            0             0
LOU:        0         128              0
ANDOR:      0          16               0
ORAND:      0          16               0
ADJ:        1        2047             0
Router#
```

表 2-87 に、この例で表示されるフィールドについて説明します。

表 2-87 show tcam counts コマンドの出力フィールド

フィールド	説明
Labels Used	使用されているラベル数 (最大 512 個)
Labels Free	残りの空きラベル数
Labels Percent Used	使用されているラベルの割合 (パーセント)
Masks Used	使用されているマスク数 (最大 4096 個)
Masks Free	残りの空きマスク数
Masks Percent Used	使用されているマスクの割合 (パーセント)
Entries Used	使用されているエントリ数 (最大 32,767 個)
Entries Free	残りの空きエントリ数
Entries Percent Used	使用されているエントリの割合 (パーセント)

show tcam interface

インターフェイス ベースの TCAM 情報を表示するには、**show tcam interface** コマンドを使用します。

```
show tcam interface {interface interface-number} | {null interface-number} |
    {vlan vlan-id} {acl {in | out}} | {qos {type1 | type2}} type [detail | module number]
```

シンタックスの説明	
<i>interface</i>	(任意) インターフェイス タイプ。有効値は、 ethernet 、 fastethernet 、 gigabitethernet 、 tengigabitethernet 、 pos 、 atm 、および ge-wan です。
<i>interface-number</i>	(任意) モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
null interface-number	(任意) ヌル インターフェイスを指定します。有効値は 0 です。
vlan vlan-id	(任意) VLAN を指定します。有効値については、「使用上のガイドライン」を参照してください。
acl in	(任意) ACL ベースの着信パケットを表示します。
acl out	(任意) ACL ベースの発信パケットを表示します。
qos type1	(任意) QoS ベースのタイプ 1 パケットを表示します。
qos type2	(任意) QoS ベースのタイプ 2 パケットを表示します。
<i>type</i>	表示するプロトコル タイプ。有効値は arp 、 ipv4 、 ipv6 、 mpls 、および other です。
detail	(任意) 詳細情報を表示します。
module number	(任意) モジュール番号を指定します。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード EXEC (>)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン TCAM ACL 一致カウンタをクリアするには、**clear mls acl counters** コマンドを使用します。

例 次に、インターフェイス ベースの TCAM 情報を表示する例を示します。

```
Router# show tcam interface vlan 7 acl in ip
deny ip any any
permit ip 20.20.0.0 0.0.255.255 22.22.0.0 0.0.255.255
redirect ip 20.21.0.0 0.0.255.255 22.23.0.0 0.0.255.255
permit tcp 24.24.0.0 0.0.255.255 30.30.0.0 0.0.255.255
Fragments (1 match)
permit tcp 25.25.0.0 0.0.255.255 31.31.0.0 0.0.255.255
fragments
```

show tcam interface

```

permit tcp 25.25.0.0 0.0.255.255 range 30000 30020 31.31.0.0
0.0.255.255 range 10000 10010 (102 matches)
permit tcp 24.24.0.0 0.0.255.255 eq 9000 30.30.0.0 0.0.255.255
eq telnet
deny ip any any
deny ip any any
Router#
    
```

次に、TCAM の詳細情報を表示する例を示します。

Router# **show tcam interface fa5/2 acl in ip detail**

```

-----
DPort - Destination Port   SPort - Source Port       TCP-F - U -URG
Pro   - Protocol
I     - Inverted LOU       TOS   - TOS Value           - A -ACK
rtr   - Router
MRFM  - M -MPLS Packet     TN    - T -Tcp Control         - P -PSH
COD   - C -Bank Care Flag - R -Recirc. Flag        - N -Non-cachable       - R -RST
      - I -OrdIndep. Flag - F -Fragment Flag     CAP  - Capture Flag         - S -SYN
      - D -Dynamic Flag   - M -More Fragments    F-P  - FlowMask-Prior.      - F -FIN
T     - V(Value)/M(Mask)/R(Result)
X     - XTAG                (*)  - Bank Priority
-----

Interface: 1018  label: 1  lookup_type: 0
protocol: IP  packet-type: 0

+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|T|Index| Dest Ip Addr | Source Ip Addr|   DPort   |   SPort   | TCP-F
|Pro|MRFM|X|TOS|TN|COD|F-P|
+-----+-----+-----+-----+-----+-----+-----+
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
V 18396      0.0.0.0      0.0.0.0      P=0          P=0          -----
  0 ---- 0  0 -- --- 0-0
M 18404      0.0.0.0      0.0.0.0      0            0
  0 ---- 0  0
R rslt: L3_DENY_RESULT          rtr_rslt: L3_DENY_RESULT

V 36828      0.0.0.0      0.0.0.0      P=0          P=0          -----
  0 ---- 0  0 -- --- 0-0
M 36836      0.0.0.0      0.0.0.0      0            0
  0 ---- 0  0
R rslt: L3_DENY_RESULT (*)      rtr_rslt: L3_DENY_RESULT (*)
Router#
    
```

関連コマンド

コマンド	説明
clear mls acl counters	MLS ACL カウンタをクリアします。

show tech-support

問題を報告するときに Cisco TAC にとって役立つ情報を表示するには、**show tech-support** コマンドを使用します。

```
show tech-support [cef | ipmulticast [vrf instance-number] | isis | password [page] |
platform | page | rsvp]
```

シンタックスの説明

cef	(任意) CEF 関連 TAC 情報を表示します。
ipmulticast	(任意) IP マルチキャスト関連 TAC 情報を表示します。
vrf <i>instance-number</i>	(任意) VRF インスタンス番号を指定します。
isis	(任意) CLNS および ISIS 関連 TAC 情報を表示します。
password	(任意) 出力からパスワードおよびその他のセキュリティ情報が除外されます。
page	(任意) 一度に情報を 1 ページ分出力します。
platform	(任意) プラットフォーム固有の TAC 情報を表示します。
rsvp	(任意) IP RSVP 関連 TAC 情報を表示します。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- 出力は改ページなしで表示されます。
- パスワードおよび他のセキュリティ情報は出力から除かれます。

コマンド モード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

show tech-support 出力を中断および終了するには、**CTRL**、**ALT**、および **6** のキーを同時に押して離します。

次の出力行を表示するには、**Return** キーを押します。次の情報ページを表示するには、**Space** キーを押します。**page** キーワードを入力しない場合は、出力がスクロールします (改ページで停止しません)。

password キーワードを入力しなかった場合、出力内のパスワードおよびその他のセキュリティ依存情報は、ラベル [removed] で置き換えられます。

show tech-support コマンドは、複数の **show** コマンドが組み合わされたものであり、出力が長くなる場合があります。**show tech-support** コマンドの出力例については、一覧表示されている各 **show** コマンドを参照してください。

引数を指定しないで **show tech-support** コマンドを入力すると、出力には次の **show** コマンドと同等な結果が表示されます (ただし、これらに限定されません)。

■ show tech-support

- **show version**
- **show running-config**
- **show stacks**
- **show interfaces**
- **show controllers**
- **show process memory**
- **show process cpu**
- **show buffers**
- **show logging**
- **show module**
- **show power**
- **show environment**
- **show interfaces switchport**
- **show interfaces trunk**
- **show vlan**
- **show mac-address-table**
- **show spanning-tree**

ipmulticast キーワードを入力した場合、出力には次の **show** コマンドの結果が表示されます（ただし、これらに限定されません）。

- **show ip pim interface**
- **show ip pim interface count**
- **show ip pim interface df**
- **show ip pim mdt**
- **show ip pim mdt bgp**
- **show ip pim neighbor**
- **show ip pim rp**
- **show ip pim rp metric**
- **show ip igmp groups**
- **show ip igmp interface**
- **show mls ip multicast rp-mapping gm-cache**
- **show ip mroute count**
- **show ip mroute**
- **show ip mcache**
- **show ip dvmrp route**
- **show mmls msc rpdf-cache**
- **show mmls gc process**

isis キーワードを入力した場合、出力には **show isis** コマンドと同等な結果が表示されます。

rsvp キーワードを入力した場合、出力には **show ip rsvp** コマンドと同等な結果が表示されます。

例 **show tech-support** コマンドの出力例については、「使用上のガイドライン」に一覧表示されているコマンドを参照してください。

show top counters interface report

TopN レポートと情報を表示するには、**show top counters interface report** コマンドを使用します。

show top counters interface report [*number*]

シンタックスの説明

<i>number</i>	(任意) 表示するレポートの数。有効値は、1 ~ 5 です。
---------------	--------------------------------

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、ファスト イーサネット、ギガビット イーサネット、および 10 ギガビット イーサネットのポートだけでサポートされます。

TopN 要求を入力すると、一連のポーリングが実行され、Catalyst 6500 シリーズ スイッチ内の適用可能なポートすべてのカウンタが読み取られ、情報が保存されます。その後、TopN プロセスは指定されたインターバルの間スリープ状態になります。ウェイクアップ後、もう一度ポーリングが実行され、ポートからカウンタ情報が読み取られます。2 組のデータの差異が格納されます。次にポートがソートされ、ポートは 7 種類の統計情報の 1 つを選択し、TopN レポートが生成されます。

次の場合、ポート統計は表示されません。

- 最初のポーリングの際にポートが存在しなかった場合
- 2 度めのポーリングの際にポートが存在しなかった場合
- ポーリング インターバル中にポートの速度またはデュプレックスが変更された場合
- ポーリング インターバル中に、ポートのタイプがレイヤ 2 からレイヤ 3 へ、またはレイヤ 3 からレイヤ 2 へ変更された場合



(注)

レポート表示フォーマットについては、1 行 80 文字という制限により、Tx/Rx-okts、Tx/Rx-bcst、および Tx/Rx-mcst カラム用に確保されるのは 10 スペースだけです。これらのカラムが 10 桁より大きい場合、表示は次の行にラップされます。

TopN プロセスを Telnet セッションから開始して、TopN プロセスが完了する前に Telnet セッションが終了した場合、すべてのバックグラウンド TopN プロセスが実行して、TopN レポートを生成しますが、フォアグラウンドの TopN プロセスは Telnet セッションが終了すると終了します。

非常に短いインターバル (10 秒) で多数のポート (13 スロット × 96 ポート/スロットなど) の TopN レポートを生成する場合、最初のポーリングと 2 回目のポーリングの間の実際のインターバル時間は、ポーリングの所要時間のために、指定されたインターバル時間より長くなる場合があります。

例

次に、TopN レポートと情報を表示する例を示します。

```
Router# show top counters interface report
Id Start Time                Int N   Sort-By   Status  Owner
-----
1  08:18:25 UTC Tue Nov 23 2004 76 20  util    done   console
2  08:19:54 UTC Tue Nov 23 2004 76 20  util    done   console
3  08:21:34 UTC Tue Nov 23 2004 76 20  util    done   console
4  08:26:50 UTC Tue Nov 23 2004 90 20  util    done   bambam onvty0 (9.10.69.13)
Router#
```

次に、特定のレポートについて TopN レポートと情報を表示する例を示します。

```
Router# show top counters interface report 1
Started By      : console
Start Time     : 08:18:25 UTC Tue Nov 23 2004
End Time       : 08:19:42 UTC Tue Nov 23 2004
Port Type      : All
Sort By        : util
Interval       : 76 seconds
Port   Band  Util Bytes      Packets      Broadcast  Multicast  In-  Buf-
      width  (Tx + Rx)  (Tx + Rx)    (Tx + Rx)  (Tx + Rx)  err  ovflw
-----
Fa2/5  100   50  726047564  11344488    11344487    1          0    0
Fa2/48 100   35  508018905  7937789     0           43         0    0
Fa2/46 100   25  362860697  5669693     0           43         0    0
Fa2/47 100   22  323852889  4762539     4762495     43         0    0
Fa2/6  100   15  217815835  3403372     0           39         21   0
Fa2/44 100   10  145146009  2267900     0           43         0    0
Gi4/15 1000  0    0           0           0           0         0    0
Gi4/14 1000  0    0           0           0           0         0    0
Gi4/13 1000  0    0           0           0           0         0    0
Gi4/12 1000  0    0           0           0           0         0    0
Gi4/11 1000  0    0           0           0           0         0    0
Gi4/10 1000  0    0           0           0           0         0    0
Gi4/9  1000  0    0           0           0           0         0    0
Gi4/8  1000  0   776         2           0           2         0    0
Gi4/7  1000  0    0           0           0           0         0    0
Gi4/6  1000  0    0           0           0           0         0    0
Gi4/5  1000  0    0           0           0           0         0    0
Gi4/4  1000  0    0           0           0           0         0    0
Gi4/3  1000  0   776         2           0           2         0    0
Gi4/2  1000  0    0           0           0           0         0    0
Router#
```

次に、保留中ステータスの TopN レポートを要求した場合の表示例を示します。

```
Router# show top counters interface report 4
Id  Start time                Int N   Sort-by   Status  Owner (type/machine/user)
-----
4  1/24/2004,11:34:26  30  20  In-Errors  pending  Console//
Router#
```

関連コマンド

コマンド	説明
clear top counters interface report	TopN レポートをクリアします。
collect top counters interface	TopN プロセスおよび特定の TopN レポートを表示します。

show udld

管理および動作上の UDLD ステータスを表示するには、**show udld** コマンドを使用します。

show udld [*interface-id* | **neighbors**]

シンタックスの説明

interface-id (任意) インターフェイス名を指定します。

neighbors (任意) ネイバ情報だけを表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース

変更内容

12.2(18)ZY このコマンドのサポートが追加されました。

使用上のガイドライン

interface-id 値を入力しなかった場合は、すべてのインターフェイスの管理および動作上の UDLD ステータスが表示されます。

例

次に、単一のインターフェイスの UDLD ステートを表示する例を示します。

```
Router# show udld gigabitethernet2/2

Interface Gi2/2
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement
Message interval: 60
Time out interval: 5
No multiple neighbors detected
  Entry 1
  ---
  Expiration time: 146
  Device ID: 1
  Current neighbor state: Bidirectional
  Device name: 0050e2826000
  Port ID: 2/1
  Neighbor echo 1 device: SAD03160954
  Neighbor echo 1 port: Gi1/1

  Message interval: 5
  CDP Device name: 066527791
Router#
```

次に、ネイバ情報だけを表示する例を示します。

```

Router# show udld neighbors
Port      Device Name          Device ID  Port-ID OperState
-----
Gi3/1     SAL0734K5R2         1         Gi4/1   Bidirectional
Gi4/1     SAL0734K5R2         1         Gi3/1   Bidirectional
Router#

```

関連コマンド

コマンド	説明
udld	アグレッシブ モード UDLD または標準モード UDLD をイネーブルにしたり、設定可能なメッセージ時間を設定したりします。
udld port	インターフェイス上で UDLD をイネーブルにしたり、インターフェイス上でアグレッシブ モード UDLD をイネーブルにしたりします。

show version

システム ハードウェアの設定、ソフトウェア バージョン、コンフィギュレーション ファイル名や送信元、およびブート イメージを表示するには、**show version** コマンドを使用します。

show version

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、システム ハードウェアの設定、ソフトウェア バージョン、コンフィギュレーション ファイル名や送信元、およびブート イメージを表示する例を示します。

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) c6sup2_rp Software (c6sup2_rp-JSV-M), Version 12.1(nightly.E020626) NIG
HTLY BUILD
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Wed 26-Jun-02 06:20 by
Image text-base: 0x40008BF0, data-base: 0x419BA000

ROM: System Bootstrap, Version 12.1(11r)E1, RELEASE SOFTWARE (fc1)

Router uptime is 2 weeks, 8 hours, 48 minutes
Time since Router switched to active is 1 minute
System returned to ROM by power-on (SP by power-on)
System image file is "sup-bootflash:c6sup22-jsv-mz"

cisco Catalyst 6000 (R7000) processor with 112640K/18432K bytes of memory.
Processor board ID SAD06210067
R7000 CPU at 300Mhz, Implementation 39, Rev 3.3, 256KB L2, 1024KB L3 Cache
Last reset from power-on
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
3 Virtual Ethernet/IEEE 802.3 interface(s)
48 FastEthernet/IEEE 802.3 interface(s)
381K bytes of non-volatile configuration memory.

16384K bytes of Flash internal SIMM (Sector size 512K).
Configuration register is 0x2102
Router#
```

表 2-88 に、この例で表示されるフィールドについて説明します。

表 2-88 show version のフィールドの説明

フィールド	説明
IOS (tm) c6sup2_rp Software (c6sup2_rp-JSV-M), Version 12.1(nightly.E020626) NIGHTLY BUILD	バージョン番号です。可能性のあるソフトウェア問題を報告する場合は、必ず完全なバージョン番号を指定してください。出力例では、バージョン番号は 12.1 です。
ROM: System Bootstrap, Version 12.1(11r)E1, RELEASE SOFTWARE (fc1)	ブートストラップ バージョン スtring
BOOTFLASH: 7200 Software (C7200-BOOT-M), Version 11.1(472), RELEASE SOFTWARE	ブート バージョン スtring
Router uptime is	システムが起動してから、稼動している時間
Time since Router switched to active	スイッチオーバーが発生してからの時間
System restarted by	システムが最後に起動したときの方法（通常のシステム起動およびシステム エラー）のログです。たとえば、以下のように、存在しないアドレスへのアクセスを試みた場合に通常発生するバス エラーを示す情報が表示されることがあります。 System restarted by bus error at PC 0xC4CA, address 0x210C0C0
System image file is	ソフトウェアがネットワークを介して起動された場合、ブートホストのインターネット アドレスが表示されます。ソフトウェアがオンボード ROM からロードされた場合は、この行に [running default software] と表示されます。
cisco Catalyst 6000 (R7000) processor with 112640K/18432K bytes of memory.	ハードウェア設定オプションおよび非標準ソフトウェア オプションを表示する、それぞれの残りの出力
Configuration register is	16 進表記で表示されたコンフィギュレーション レジスタの内容

show version EXEC コマンドの出力には、バス エラー メッセージなどの特定のメッセージが含まれることがあります。このようなエラー メッセージが表示された場合は、テクニカル サポート担当者にこのメッセージの全文を報告してください。

show vlan

VLAN 情報を表示するには、**show vlan** コマンドを使用します。

```
show vlan [{brief | {id vlan-id} | {name name} [ifindex]} | ifindex]
```

シンタックスの説明

brief	(任意) VLAN ごとに、VLAN 名、ステータス、およびポートを 1 行で表示します。
id vlan-id	(任意) VLAN ID 番号によって識別される単一 VLAN に関する情報を表示します。有効値は 1 ~ 4094 です。
name name	(任意) VLAN 名によって識別される単一 VLAN に関する情報を表示します。有効値は 1 ~ 32 文字の ASCII 文字列です。
ifindex	(任意) VLAN の ifIndex 番号を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

各イーサネット スイッチ ポートおよびイーサネット リピータ グループが属するのは、1 つの VLAN だけです。トランク ポートは複数の VLAN に属することができます。

state suspend または **state active** コマンドを使用して VLAN をシャットダウンした場合、次の値が Status フィールドに表示されます。

- **suspended** : VLAN は一時停止です。
- **active** : VLAN はアクティブです。

shutdown コマンドを使用して VLAN をシャットダウンした場合、次の値が Status フィールドに表示されます。

- **act/lshut** : VLAN ステータスはアクティブですが、ローカルにシャットダウンされています。
- **sus/lshut** : VLAN ステータスは一時停止ですが、ローカルにシャットダウンされています。

VLAN が内部的にシャットダウンされている場合、次の値が Status フィールドに表示されます。

- **act/ishut** : VLAN ステータスはアクティブですが、内部的にシャットダウンされています。
- **sus/ishut** : VLAN ステータスは一時停止ですが、内部的にシャットダウンされています。

VLAN がローカルかつ内部的にシャットダウンされている場合、Status フィールドに表示される値は **act/ishut** または **sus/ishut** です。VLAN がローカルだけでシャットダウンされている場合、Status フィールドに表示される値は **act/lshut** または **sus/lshut** です。

VLAN 範囲はハイフンで区切り、複数の VLAN はカンマで区切ります。間にスペースは入れません。たとえば、次のように入力します。

```
Router# show vlan id 1-4,3,7,5-20
```

例

次に、アクティブで内部的にシャットダウンされている VLAN (VLAN0002) の出力例を示します。

```
Router# show vlan
VLAN Name                Status    Ports
-----
1    default                 active    Fa5/9
2    VLAN0002                act/ishut Fa5/9
<...Output truncated...>
```

次に、アクティブでローカルにシャットダウンされている VLAN (VLAN0002) の出力例を示します。

```
Router# show vlan
VLAN Name                Status    Ports
-----
1    default                 active    Fa5/9
2    VLAN0002                act/lshut Fa5/9
<...Output truncated...>
```

次に、管理ドメイン内のすべての VLAN に関する VLAN パラメータを表示する例を示します。

```
Router# show vlan
VLAN Name                Status    Ports
-----
1    default                 active    Fa5/9
2    VLAN0002                active    Fa5/9
3    VLAN0003                active    Fa5/9
4    VLAN0004                active    Fa5/9
5    VLAN0005                active    Fa5/9
6    VLAN0006                active    Fa5/9
<...Output truncated...>
```

```
1004 fddinet-default        active    Fa5/9
1005 trbrf-default        active    Fa5/9

VLAN Type SAID      MTU    Parent RingNo BridgeNo Stp    BrgdMode Trans1 Trans2
-----
1    enet  100001   1500  -      -      -      -      -      0      0
2    enet  100002   1500  -      -      -      -      -      0      0
3    enet  100003   1500  -      -      -      -      -      303    0
4    enet  100004   1500  -      -      -      -      -      304    0
5    enet  100005   1500  -      -      -      -      -      305    0
6    enet  100006   1500  -      -      -      -      -      0      0
10   enet  100010   1500  -      -      -      -      -      0      0
<...Output truncated...>
```

```
Remote SPAN VLANs
-----
2, 20
```

```
Primary Secondary Type          Ports
-----
Router#
```

次に、VLAN 名、ステータス、および対応付けられたポートだけを表示する例を示します。

```
Router# show vlan brief
VLAN Name                Status    Ports
-----
1    default                 active    Fa5/9
2    VLAN0002                active    Fa5/9
```

show vlan

```

3    VLAN0003                act/lshut Fa5/9
4    VLAN0004                act/lshut Fa5/9
5    VLAN0005                active    Fa5/9
10   VLAN0010                active    Fa5/9
.
.
.
999  VLAN0999                active    Fa5/9
1002 fddi-default            active    Fa5/9
1003 trcrf-default           active    Fa5/9
1004 fddinet-default         active    Fa5/9
1005 trbrf-default           active    Fa5/9
Router#

```

次に、複数の VLAN の VLAN パラメータを表示する例を示します。

Router# **show vlan id 1-4,3,7,5-20**

VLAN Name	Status	Ports
1 default	active	Fa5/7, Fa5/12
2 VLAN0002	active	
3 VLAN0003	act/lshut	
4 VLAN0004	act/lshut	
5 VLAN0005	active	
6 VLAN0006	active	
10 VLAN0010	active	
20 VLAN0020	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
2	enet	100002	1500	-	-	-	-	-	0	0
3	enet	100003	1500	-	-	-	-	-	303	0
4	enet	100004	1500	-	-	-	-	-	304	0
5	enet	100005	1500	-	-	-	-	-	305	0
6	enet	100006	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0

Remote SPAN VLANs

Primary	Secondary	Type	Ports
-----	-----	-----	-----

Router#

次に、VLAN 10 の ifIndex 番号だけを表示する例を示します。

Router# **show vlan id 10 ifindex**

```

VLAN Ifindex
-----
10    37
Router#

```

表 2-89 に、この例で表示されるフィールドについて説明します。

表 2-89 show vlan コマンドの出力フィールド

フィールド	説明
VLAN	VLAN 番号
Name	VLAN 名 (設定されている場合)
Status	VLAN のステータス (active または suspend、act/lshut または sus/lshut、act/ishut または sus/ishut)
Ports	VLAN に属するポート
Type	VLAN のメディア タイプ
SAID	VLAN のセキュリティ アソシエーション ID
MTU	VLAN の最大伝送ユニット サイズ
Parent	親 VLAN (存在する場合)
RingNo	VLAN のリング番号 (該当する場合)
BrdgNo	VLAN のブリッジ番号 (該当する場合)
Stp	VLAN で使用されるスパニングツリー プロトコル タイプ
BrdgMode	この VLAN のブリッジング モード: 可能な値は Source-Route Bridging (SRB; ソースルートブリッジング) および Source-Route Transparent (SRT; ソースルートトランスペアレント) で、デフォルトは SRB です。
AREHops	All-Routes Explorer フレームの最大ホップ数: 可能な値は 1 ~ 13、デフォルトは 7 です。
STEHops	Spanning-Tree Explorer フレームの最大ホップ数: 可能な値は 1 ~ 13、デフォルトは 7 です。
Backup CRF	Token Ring Concentrator Relay Function (TrCRF; トークンリング コンセントレータリレー機能) がトラフィックのバックアップパスであるかどうかを示すステータス
Ifindex	ifIndex の番号
Remote SPAN VLAN	RSPAN のステータス
Primary	プライマリ VLAN の番号
Secondary	セカンダリ VLAN の番号
Ports	VLAN 内のポートを指定します。
Type	VLAN のタイプ: 可能な値は primary、isolated、community、non_operation、または normal です。

関連コマンド

コマンド	説明
show vlan private-vlan	PVLAN 情報を表示します。
vlan (config-VLAN submode)	特定の VLAN を設定します。
vtp	グローバル VTP ステートを設定します。

show vlan access-log

設定されたロギング プロパティ、フロー テーブルの内容、統計情報などの VACL ロギングに関する情報を表示するには、**show vlan access-log** コマンドを使用します。

show vlan access-log config

```
show vlan access-log flow protocol {{src-addr src-mask} | any | {host {hostname | host-ip}}}} {{dst-addr dst-mask} | any | {host {hostname | host-ip}}}} [vlan vlan-id]
```

show vlan access-log statistics

シンタックスの説明

config	設定された VACL ロギング プロパティを表示します。
flow	VACL フロー テーブルの内容を表示します。
<i>protocol</i>	プロトコル名または番号。有効値は icmp 、 igmp 、 ip 、 tcp 、 udp 、またはプロトコルを指定する 0 ~ 255 の番号です。
<i>src-addr src-mask</i>	送信元のアドレスおよびマスク
any	任意のホストに関する情報を表示します。
host hostname	ホスト名の情報を表示します。
host host-ip	IP アドレスに関する情報を表示します。
<i>dst-addr dst-mask</i>	宛先のアドレスおよびマスク
vlan vlan-id	(任意) 特定の VLAN に関する情報を表示します。有効値は 1 ~ 4094 です。
statistics	パケット数、メッセージ数などの統計情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、設定された VACL ロギング プロパティを表示する例を示します。

```
Router# show vlan access-log config
VACL Logging Configuration:
  max log table size      :500
  log threshold           :4000
  rate limiter            :3000
Router#
```

次に、VACL の統計情報を表示する例を示します。

```
Router# show vlan access-log statistics
VACL Logging Statistics:
  total packets      :0
  logged             :0
  dropped            :0
Dropped Packets Statistics:
  unsupported protocol :0
  no packet buffer    :0
  hash queue full    :0
  flow table full     :0
Misc Information:
  VACL Logging LTL Index :0x7E02
  free packet buffers   :8192
  log messages sent     :0
  log table size        :0
Router#
```

関連コマンド

コマンド	説明
vlan access-log	ログ テーブル サイズ、リダイレクト パケット レート、ロギングしきい値などの VACL ロギング プロパティを設定します。

show vlan access-map

VLAN アクセス マップの内容を表示するには、**show vlan access-map** コマンドを使用します。

show vlan access-map [*map-name*]

シンタックスの説明

<i>map-name</i>	(任意) VLAN アクセス マップ名
-----------------	---------------------

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、VLAN アクセス マップの内容を表示する例を示します。

```
Router# show vlan access-map mordred
Vlan access-map "mordred" 1
    match: ip address 13
    action: forward capture
Router#
show vlan counters
```

関連コマンド

コマンド	説明
action	パケットの action 句を設定します。
match	VLAN アクセス マップ シーケンスの ACL を 1 つまたは複数選択して、match 句を指定します。
vlan access-map	VLAN アクセス マップを作成するか、VLAN アクセス マップ コマンドモードを開始します。

show vlan counters

ソフトウェア キャッシュ カウンタ値を表示するには、**show vlan counters** コマンドを使用します。

show vlan [id *vlanid*] counters

シンタックスの説明	id <i>vlanid</i> (任意) 特定の VLAN のソフトウェアキャッシュ カウンタ値を表示します。有効値は 1 ~ 4094 です。
------------------	--

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード 特権 EXEC (#)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン **show vlan id counters** コマンドは SVI ではサポートされていません。
レイヤ 2 およびレイヤ 3 VLAN インターフェイスおよびルータ ポートの場合、インターフェイス単位のスイッチング統計情報および VLAN カウンタ情報が、約 3 分間隔で PISA にエクスポートされます。
引数を指定しないで **show vlan counters** コマンドを入力した場合は、すべての VLAN のソフトウェア キャッシュ カウンタ値が表示されます。

例 次に、特定の VLAN のソフトウェアキャッシュ カウンタ値を表示する例を示します。

```
Router> show vlan id 205 counters
VLAN vlanid 205
L2-Unicast-Pkts      10
L3-In-Unicast-Pkts   0
L3-Out-Unicast-Pkts  0
L2-NonUnicast-Pkts + L3-In-NonUnicast-Pkts  5
L3-Out-NonUnicast-Pkts  6
L2-Unicast-Octets    6
L3-In-Unicast-Octets  6
L3-Out-Unicast-Octets  6
L2-NonUnicast-Octets + L3-In-NonUnicast-Octets  6
L3-Out-NonUnicast-Octets  6
```

関連コマンド	コマンド	説明
	clear vlan counters	指定された VLAN または既存のすべての VLAN でソフトウェア キャッシュされたカウンタ値をゼロにクリアします。

show vlan dot1q tag native

ネイティブ VLAN のタグging情報を表示するには、**show vlan dot1q tag native** コマンドを使用します。

show vlan dot1q tag native

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、ネイティブ VLAN タグging情報を表示する例を示します。

```
Router# show vlan dot1q tag native
dot1q native vlan tagging is enabled
Internal dot1q native vlan: 1015
```

```
Router#
```

関連コマンド

コマンド	説明
vlan dot1q tag native	トランク内のすべての VLAN の 802.1Q タグgingをイネーブルにします。

show vlan filter

VLAN フィルタに関する情報を表示するには、**show vlan filter** コマンドを使用します。

```
show vlan filter [{access-map map-name} | {vlan vlan-id} | {interface interface
interface-number}]
```

シンタックスの説明

access-map <i>map-name</i>	(任意) 指定されたマップでフィルタリングされた VLAN を表示します。
vlan <i>vlan-id</i>	(任意) 指定された VLAN のフィルタを表示します。有効値は 1 ~ 4094 です。
interface <i>interface</i>	インターフェイス タイプを指定します。有効値は pos 、 atm 、または serial です。詳細については、「使用上のガイドライン」を参照してください。
<i>interface-number</i>	インターフェイス番号。詳細については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

show vlan filter map-name interface コマンドが対応しているのは、ATM、POS、またはシリアル インターフェイス タイプだけです。システムにこれらのインターフェイス タイプが装備されていない場合は、**interface interface interface-number** キーワードおよび引数を使用できません。

interface-number 引数はモジュールおよびポート番号を指定します。*interface-number* の有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 2 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

オプションのキーワードおよび引数を指定しなければ、すべてのマッピングが表示されます。

access-map map_name を入力した場合は、指定されたマップに対応付けられたすべての VLAN および インターフェイスが表示されます。**vlan vlan-id** または **interface interface interface-number** を入力した場合は、対応付けられたアクセス マップ (存在する場合) が表示されます。

VLAN の VACL に対する出力の意味は、次のとおりです。

- Configured on VLANs : ユーザにより設定済み
- Active on VLANs : VACL がアクティブである VLAN リスト

■ show vlan filter

例

次に、VACL と VLAN 間、VACL とインターフェイス間のマッピングを表示する例を示します。

```
Router# show vlan filter
VLAN Map mordred:
  Configured on VLANs: 2,4-6
  Active on VLANs: 2,4-6
Router#
```

関連コマンド

コマンド	説明
vlan access-map	VLAN アクセス マップを作成するか、VLAN アクセス マップ コマンド モードを開始します。
vlan filter	VLAN アクセス マップを適用します。

show vlan internal usage

内部 VLAN 割り当てに関する情報を表示するには、**show vlan internal usage** コマンドを使用します。

show vlan [id vlan-id] internal usage

シンタックスの説明	id vlan-id (任意) 指定された VLAN の内部 VLAN 割り当て情報を表示します。有効値は 1 ~ 4094 です。
------------------	---

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドのデフォルト 特権 EXEC (#)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン 場合により、出力には次のものが表示されます。

workaround vlan

ワークアラウンド VLAN は、PFC ベースのポリシングを PWAN1 メイン インターフェイス上でイネーブル化するために使用します。ワークアラウンド VLAN を使用しなければ、パケットは PWAN1 について PFC ポリサーを 2 回ヒットします。パケットが PXF 処理の前後にローカルバスを通過する際、同じ VLAN が使用されるからです。

使用上のガイドライン **show vlan internal usage** コマンドを入力すると、イーサネット インターフェイスが表示されます。

例 次に、現在の内部 VLAN 割り当てを表示する例を示します。

```
Router# show vlan internal usage
```

```
VLAN Usage
-----
1025 -
1026 -
1027 -
1028 -
1029 Port-channel6
1030 GigabitEthernet1/2
1032 FastEthernet3/20
1033 FastEthernet3/21
1129 -
```

次に、特定の VLAN の内部 VLAN 割り当てを表示する例を示します。

```
Router# show vlan id 1030 internal usage
```

```
VLAN Usage
```

■ show vlan internal usage

```
-----  
1030 GigabitEthernet1/2
```

show vlan mapping

802.1Q VLAN と ISL VLAN のマッピングを登録するには、**show vlan mapping** コマンドを使用します。

show vlan mapping

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード 特権 EXEC (#)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、802.1Q VLAN と ISL VLAN のマップのリストを表示する例を示します。

```
Router# show vlan mapping
802.1Q Trunk Remapped VLANs:
802.1Q VLAN ISL VLAN
-----
101          202
200          330
Router#
```

関連コマンド	コマンド	説明
	show interfaces vlan mapping	ポート上の VLAN マッピングのステータスを表示します。
	switchport vlan mapping enable	スイッチ ポート単位で VLAN マッピングをイネーブルにします。

show vlan private-vlan

PVLAN 情報を表示するには、**show vlan private-vlan** コマンドを使用します。

show vlan private-vlan [type]

シンタックスの説明

type (任意) PVLAN タイプ (isolated、community、または primary) を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

show vlan private-vlan type コマンドの出力に、タイプとして [normal] が表示されている場合は、PVLAN に通常の VLAN が設定されています。[normal] が表示されている場合は、タイプを設定する前に 2 つの VLAN が対応付けられていて、PVLAN が動作していません。この情報は、デバッグ時に役立ちます。

例

次に、現在設定されているすべての PVLAN に関する情報を表示する例を示します。

```
Router# show vlan private-vlan
```

```

Primary Secondary Type           Ports
-----
2         301      community      Fa5/3, Fa5/25
2         302      community
                10          community
100      101      isolated
150      151      non-operational
                202        community
                303        community
401      402      non-operational
Router#
```

次に、現在設定されているすべての PVLAN タイプに関する情報を表示する例を示します。

```
Router# show vlan private-vlan type
```

```

Vlan Type
-----
202 primary
303 community
304 community
305 community
306 community
307 community
```

```

308 normal
309 community
440 isolated
Router#

```

表 2-90 に、この例で表示されるフィールドについて説明します。

表 2-90 show vlan private-vlan コマンドの出カフィールド

フィールド	説明
Primary	プライマリ VLAN の番号
Secondary	セカンダリ VLAN の番号
Secondary-Type	セカンダリ VLAN タイプ：可能な値は isolated または community です。
Ports	VLAN 内のポートを指定します。
Type	VLAN のタイプ：可能な値は primary、isolated、community、non_operation、または normal です。

関連コマンド

コマンド	説明
private-vlan mapping	プライマリ VLAN とセカンダリ VLAN のマッピングを作成して、両方の VLAN で同じプライマリ VLAN SVI を共有できるようにします。
private-vlan	PVLAN、および PVLAN とセカンダリ VLAN とのアソシエーションを設定します。

show vlan remote-span

RSPAN VLAN のリストを表示するには、**show vlan remote-span** を使用します。

show vlan remote-span

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、RSPAN VLAN のリストを表示する例を示します。

```
Router# show vlan remote-span
Remote SPAN VLANs
-----
2,20
```

関連コマンド

コマンド	説明
remote-span	VLAN を RSPAN VLAN として設定します。
vlan (config-VLAN submode)	特定の VLAN を設定します。

show vlans

Cisco IOS VLAN サブインターフェイスに関する情報を表示するには、**show vlans** コマンドを使用します。

show vlans [*vlan*]

シンタックスの説明

vlan (任意) VLAN ID 番号を指定します。有効値は 1 ~ 4094 です。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

EXEC モードで **show vlan** コマンドを使用すると、レイヤ 2 VLAN に関する情報が表示されます。特権 EXEC モードで **show vlans** コマンドを使用すると、レイヤ 3 の VLAN サブインターフェイス情報が表示されます。

show vlans コマンドを入力する場合は、**vlans** キーワードの短縮形を使用できません。

例

次に、Cisco IOS VLAN サブインターフェイスに関する情報を表示する例を示します。

```
Router# show vlans
Virtual LAN ID: 122 (Inter Switch Link Encapsulation)
VLAN Trunk Interface: GE-WAN9/1.1
Protocols Configured: Address: Received: Transmitted:
IP 10.122.0.2 18 16
Virtual LAN ID: 123 (Inter Switch Link Encapsulation)
VLAN Trunk Interface: GE-WAN9/1.2
Protocols Configured: Address: Received: Transmitted:
IP 10.123.0.2 13 16
Virtual LAN ID: 124 (Inter Switch Link Encapsulation)
VLAN Trunk Interface: GE-WAN9/1.3
Protocols Configured: Address: Received: Transmitted:
IP 10.124.0.2 0 17
Virtual LAN ID: 133 (Inter Switch Link Encapsulation)
VLAN Trunk Interface: GE-WAN9/3.1
Protocols Configured: Address: Received: Transmitted:
IP 11.133.0.1 0 1
Virtual LAN ID: 134 (Inter Switch Link Encapsulation)
VLAN Trunk Interface: GE-WAN9/3.2
Protocols Configured: Address: Received: Transmitted:
IP 11.134.0.1 0 1
Router#
```

表 2-91 に、この例で表示されるフィールドについて説明します。

表 2-91 show vlans コマンドの出力フィールド

フィールド	説明
Virtual LAN ID	VLAN のドメイン番号
VLAN Trunk Interface	VLAN トラフィックを伝送するサブインターフェイス
Protocols Configured	VLAN に設定されたプロトコル
Address	ネットワーク アドレス
Received	受信されたパケット数
Transmitted	送信されたパケット数

show vlan virtual-port

必要な論理仮想ポート数を表示するには、**show vlan virtual-port** コマンドを使用します。

show vlan virtual-port [slot num]

シンタックスの説明

slot num (任意) ステータスを表示するスロット番号を指定します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、指定されたスロットに必要な論理仮想ポート数を表示する例を示します。

```
Router# show vlan virtual-port slot 3
Slot 3
Port          Virtual-ports
-----
Fa3/1          1
Fa3/2          1
Fa3/3          1
Fa3/4          1
Fa3/5          1
Fa3/6          1
Fa3/7          1
Fa3/8          1
Fa3/11         1
Fa3/12         1
Fa3/13         1
.
.
.
Fa3/33         4
Fa3/34         4
Fa3/35         4
Fa3/36         4
Fa3/37         4
Fa3/38         4
Fa3/39         4
Fa3/40         4
Total virtual ports:82
Router#
```

次にすべてのスロットに必要な論理仮想ポート数を表示する例を示します。

```
Router# show vlan virtual-port
Slot 1
-----
Total slot virtual ports 1
```

■ show vlan virtual-port

```
Slot 3
-----
Total slot virtual ports 82
Slot 4
-----
Total slot virtual ports 4
Total chassis virtual ports 87
Router#
```

show vtp

VTP 統計情報とドメイン情報を表示するには、**show vtp** コマンドを使用します。

```
show vtp {counters | status}
```

シンタックスの説明

counters	VTP 統計に関する情報を表示します。
status	VTP ドメイン ステータスに関する情報を表示します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC (>)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

show vtp status コマンドの出力では、最後に変更した時間が修飾子自身の時間になります。たとえば、「Configuration last modified by 7.0.22.11 at 5-5-06 05:51:49」の行に表示される時間は、修飾子 (7.0.22.11) が最後に VLAN 設定を変更した時間です。

例

次に、VTP の統計情報を表示する例を示します。

```
Router# show vtp counters
VTP statistics:
Summary advertisements received      : 1
Subset advertisements received      : 1
Request advertisements received     : 0
Summary advertisements transmitted  : 31
Subset advertisements transmitted   : 1
Request advertisements transmitted   : 0
Number of config revision errors    : 0
Number of config digest errors      : 0
Number of V1 summary errors         : 0

VTP pruning statistics:

Trunk          Join Transmitted Join Received  Summary advts received from
-----
Fa5/9          1555             1564             0
Router#
```

次に、VTP ドメインのステータスを表示する例を示します。

```
Router# show vtp status
VTP Version          : 2
Configuration Revision : 250
Maximum VLANs supported locally : 1005
```

show vtp

```

Number of existing VLANs      : 33
VTP Operating Mode           : Server
VTP Domain Name              : Lab_Network
VTP Pruning Mode             : Enabled
VTP V2 Mode                  : Enabled
VTP Traps Generation         : Disabled
MD5 digest                   : 0xE6 0xF8 0x3E 0xDD 0xA4 0xF5 0xC2 0x0E
Configuration last modified by 172.20.52.18 at 9-22-99 11:18:20
Local updater ID is 172.20.52.18 on interface V11 (lowest numbered VLAN interface found)
Router#
    
```

次に、**show vtp** 出力内に、**Summary** という語を含む行だけを表示する例を示します。

```

Router# show vtp counters | include Summary
Summary advertisements received      : 1
Summary advertisements transmitted : 32
Trunk          Join Transmitted Join Received      Summary advts received from
Router#
    
```

表 2-92 に、この例で表示されるフィールドについて説明します。

表 2-92 show vtp コマンドの出力フィールド

フィールド	説明
Summary advts received	受信されたサマリー アドバタイズの総数
Subset advts received	受信されたサブセット アドバタイズの総数
Request advts received	受信されたリクエスト アドバタイズの総数
Summary advts transmitted	送信されたサマリー アドバタイズの総数
Subset advts transmitted	送信されたサブセット アドバタイズの総数
Request advts transmitted	送信されたリクエスト アドバタイズの総数
No of config revision errors	コンフィギュレーション リビジョン エラーの数
No of config digest errors	コンフィギュレーション ダイジェスト エラーの数
Trunk	VTP プルーニングに参加するトランク ポート
Join Transmitted	送信された VTP プルーニング join の数
Join Received	受信された VTP プルーニング join の数
Summary advts received from non-pruning-capable device	プルーニング非対応装置から受信されたサマリー アドバタイズの数
Number of existing VLANs	ドメイン内の VLAN の総数
Configuration Revision	VLAN 情報を交換するために使用される VTP リビジョン番号
Maximum VLANs supported locally	装置で許可されている VLAN の最大数
Number of existing VLANs	既存の VLAN 数
VTP Operating Mode	VTP がイネーブルとディセーブルのいずれに設定されているかを示すステータス
VTP Domain Name	VTP ドメイン名
VTP Pruning Mode	VTP プルーニングがイネーブルとディセーブルのどちらに設定されているかを示すステータス
VTP V2 Mode	VTP V2 モードのステータス (server、client、または transparent)

表 2-92 show vtp コマンドの出力フィールド (続き)

フィールド	説明
VTP Traps Generation	VTP トラップ生成モードがイネーブルとディセーブルのいずれに設定されているかを示すステータス
MD5 digest	チェックサム値

関連コマンド

コマンド	説明
vtp	グローバル VTP ステートを設定します。

■ show vtp

shutdown vlan

指定された VLAN 上でローカルトラフィックを遮断するには、**shutdown vlan** コマンドを使用します。VLAN のローカルトラフィックを再開するには、このコマンドの **no** 形式を使用します。

shutdown vlan *vlan-id*

no shutdown vlan *vlan-id*

シンタックスの説明	<i>vlan-id</i> ローカルに遮断する VLAN の VLAN 番号。有効値は 2 ～ 1001 です。
-----------	---

コマンドのデフォルト	このコマンドにはデフォルト設定がありません。
------------	------------------------

コマンドモード	グローバル コンフィギュレーション (config)
---------	----------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン	このコマンドは、拡張範囲 VLAN をサポートしません。
------------	------------------------------

例	次に、VLAN 2 でトラフィックを遮断する例を示します。
---	-------------------------------

```
Router(config)# shutdown vlan 2
Router(config)#
```

snmp ifindex clear

特定のインターフェイスに対して実行された設定済みの **snmp ifindex** コマンドをクリアするには、**snmp ifindex clear** コマンドを使用します。

snmp ifindex clear

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

IF-MIB の ifIndex 値が再起動後も保持され、SNMP を使用することにより特定のインターフェイスを一貫して識別できる場合は、インターフェイス インデックスの永続性が確保されます。

特定のインターフェイスで ifIndex 永続性に関するグローバル コンフィギュレーション設定を使用する場合は、このインターフェイス上で **snmp ifindex clear** コマンドを使用します。このコマンドは、特定のインターフェイスに入力されたすべての ifIndex コンフィギュレーション コマンドを削除します。

ifIndex 設定を削除した場合、グローバル コンフィギュレーション モードで **snmp-server ifindex persist** コマンドによって指定したように、ifIndex 永続性がすべてのインターフェイスについてイネーブル化されます。

例

次に、すべてのインターフェイスの ifIndex 永続性をイネーブルにする例を示します。

```
Router(config)# snmp ifindex persist
```

次に、イーサネット 0/1 の IfIndex 永続性だけをディセーブルにする例を示します。

```
Router(config)# interface ethernet 0/1
Router(config-if)# no snmp ifindex persist
Router(config-if)# exit
```

次に、イーサネット 0/1 設定から ifIndex 設定を削除する例を示します。

```
Router(config)# interface ethernet 0/1
Router(config-if)# snmp ifindex clear
Router(config-if)# exit
```

関連コマンド

コマンド	説明
snmp ifindex persist	再起動後も保持される Interfaces MIB (IF-MIB) 内の ifIndex 値 (ifIndex 永続性) を特定のインターフェイス上だけでイネーブルにします。
snmp-server ifindex persist	ifIndex 値を、SNMP で使用するために再起動後も一定となるようにグローバルにイネーブル化します。

snmp ifindex persist

再起動後も保持される Interfaces MIB (IF-MIB) 内の ifIndex 値 (ifIndex 永続性) を特定のインターフェイス上だけでイネーブルにするには、**snmp ifindex persist** コマンドを使用します。ifIndex 永続性を特定のインターフェイス上だけでディセーブルにするには、このコマンドの **no** 形式を使用します。

snmp ifindex persist

no snmp ifindex persist

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

IF-MIB の ifIndex 値が再起動後も保持され、SNMP) を使用することにより特定のインターフェイスを一貫して識別できる場合は、インターフェイス インデックスの永続性が確保されます。

snmp ifindex persist コマンドをインターフェイス コンフィギュレーション モードで使用すると、IF-MIB の ifIndex テーブル内のエントリ (各インターフェイスに対応するエントリ) ごとに、ifIndex 永続性をイネーブルにしたり、ディセーブルにしたりすることができます。

snmp-server ifindex persist コマンドをグローバル コンフィギュレーション モードで使用すると、ルーティング装置のすべてのインターフェイスに対して、ifIndex 永続性をイネーブルにしたり、ディセーブルにしたりできます。このアクションは、IF-MIB の ifIndex テーブル内に ifDescr および ifIndex エントリがあるインターフェイスにだけ適用されます。

特定のインターフェイスに設定した ifIndex コマンドは、そのインターフェイスのすべてのサブインターフェイスに適用されます。

例

次に、インターフェイス イーサネット 0/1 の ifIndex 永続性だけをイネーブルにする例を示します。

```
Router(config)# interface ethernet 0/1
Router(config-if)# snmp ifindex persist
Router(config-if)# exit
```

次に、すべてのインターフェイスの ifIndex 永続性をイネーブルにし、インターフェイス イーサネット 0/1 の ifIndex 永続性だけをディセーブルにする例を示します。

```
Router(config)# snmp ifindex persist
Router(config)# interface ethernet 0/1
Router(config-if)# no snmp ifindex persist
Router(config-if)# exit
```

関連コマンド

コマンド	説明
snmp ifindex clear	特定のインターフェイスに対して実行された設定済みの snmp ifindex コマンドをクリアします。
snmp-server ifindex persist	ifIndex 値を、SNMP で使用するために再起動後も一定となるようにグローバルにイネーブル化します。

snmp-server enable traps

システムで使用できる SNMP) 通知 (トラップまたはインフォーム) をイネーブルにするには、**snmp-server enable traps** コマンドを使用します。使用できるすべての SNMP 通知をディセーブルにするには、このコマンドの **no** 形式を使用します。

snmp-server enable traps [*notification-type*]

no snmp-server enable traps [*notification-type*]

シンタックスの説明

notification-type (任意) イネーブルまたはディセーブルにする通知 (トラップまたはインフォーム) のタイプです。タイプを指定しなければ、装置で使用可能なすべての通知がイネーブルまたはディセーブルになります。有効値については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

このコマンドは、デフォルトではディセーブルです。ほとんどの通知タイプはディセーブルです。しかし、一部の通知タイプはこのコマンドでは制御できません。

このコマンドを *notification-type* の指定なしで入力すると、このコマンドで制御されるすべての通知タイプがイネーブルになります。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

他の通知タイプについては、『Cisco IOS Release 12.2 Command Reference』を参照してください。

SNMP 通知は、トラップまたはインフォーム要求として送信できます。このコマンドはトラップおよびインフォーム要求の両方を、指定された通知タイプについてイネーブル化します。送信される通知がトラップかインフォームかを指定するには、**snmp-server host [traps | informs]** コマンドを使用します。

snmp-server enable traps コマンドを入力しなければ、このコマンドで制御される通知は送信されません。これらの SNMP 通知を送信するようにルータを設定するには、少なくとも 1 回 **snmp-server enable traps** コマンドを入力する必要があります。このコマンドをキーワードなしで入力すると、すべての通知タイプがイネーブルになります。このコマンドをキーワード付きで入力すると、そのキーワードに関係する通知タイプだけがイネーブルになります。複数の通知タイプをイネーブルにするには、**snmp-server enable traps** コマンドを各通知タイプおよび通知オプションについて別々に実行する必要があります。

snmp-server enable traps コマンドは、**snmp-server host** コマンドとともに使用します。**snmp-server host** コマンドは、SNMP 通知を受信するホストの指定に使用します。通知を送信するためには、少なくとも 1 回 **snmp-server host** コマンドを設定する必要があります。

トラップに使用される MIB の一覧を示します。

- **chassis** : CISCO-STACK-MIB からの chassisAlarm トラップを制御します。
- **flash** : CISCO-FLASH-MIB からの SNMP Flash トラップを制御します。

- **insertion** : SNMP Flash 挿入トラップ通知を制御します。
- **removal** : SNMP Flash 削除トラップ通知を制御します。
- **fru-ctrl** : CISCO-ENTITY-FRU-CONTROL-MIB からの FRU 制御トラップを制御します。
- **module** : CISCO-STACK-MIB からの SNMP モジュール トラップを制御します。
- **stpx** : CISCO-STP-EXTENSIONS-MIB からのすべてのトラップを制御します。
- **vlancreate** : SNMP VLAN 作成トラップ通知を制御します。
- **vlandelete** : SNMP VLAN 削除トラップ通知を制御します。
- **vtp** : CISCO-VTP-MIB からの VTP トラップを制御します。

次の SNMP サーバ対応トラップがサポートされています。

- **bridge** : STP Bridge MIB トラップを制御します。
- **c6kxbar** : c6kxbar intbus-crcexcd intbus-crcrcvrd swbus トラップを制御します。
- **csg** : CSG エージェントクォータ データベース トラップを制御します。
- **flex-links** : フレックスリンクス ステータス トラップを制御します。
- **mac-notification** : MAC-Notification 移動しきい値トラップを制御します。
- **stpx** : STPX 不一致/ルート不一致/ループ不一致 トラップを制御します。
- **vlan-mac-limit** : レイヤ 2 制御 VLAN MAC 制限通知トラップを制御します。

例

次に、**public** と定義されたコミュニティストリングを使用して、名前 **myhost.cisco.com** で指定されたホストにすべてのトラップを送信する例を示します。

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com public
```

snmp-server enable traps transceiver type all

すべてのトランシーバタイプでサポートされているすべての SNMP トランシーバトラップをイネーブルにするには、**snmp-server enable traps transceiver type all** コマンドを使用します。トランシーバの SNMP トラップ通知をディセーブルにするには、このコマンドの **no** 形式を使用します。

snmp-server enable traps transceiver type all

no snmp-server enable traps transceiver type all

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

ディセーブル

コマンドモード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

snmp-server enable traps コマンドは、**snmp-server host** コマンドとともに使用します。**snmp-server host** コマンドは、SNMP 通知を受信するホストの指定に使用します。通知を送信するためには、少なくとも 1 回 **snmp-server host** コマンドを設定する必要があります。

例

次に、すべてのトランシーバタイプでサポートされているすべての SNMP トランシーバトラップをイネーブルにする例を示します。

```
Router(config)# snmp-server enable traps transceiver type all
Router(config)#
```

関連コマンド

コマンド	説明
show interfaces transceiver	DOM がイネーブルになっているオプティカル トランシーバに関する情報を表示します。

snmp-server ifindex persist

ifIndex 値を、SNMP) で使用するために再起動後も一定となるようにグローバルにイネーブル化するには、**snmp-server ifindex persist** コマンドを使用します。ifIndex 永続性をグローバルにディセーブルにするには、このコマンドの **no** 形式を使用します。

snmp-server ifindex persist

no snmp-server ifindex persist

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト ディセーブル

コマンド モード グローバル コンフィギュレーション (config)

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン IF-MIB の ifIndex 値が再起動後も保持され、SNMP を使用することにより特定のインターフェイスを一貫して識別できる場合は、インターフェイス インデックスの永続性が確保されます。

グローバル コンフィギュレーション モードの **snmp-server ifindex persist** コマンドは、インターフェイス固有の設定を上書きしません。ifIndex 永続性に関するインターフェイス固有の設定を上書きするには、**[no] snmp ifindex persist** および **snmp ifindex clear** コマンドをインターフェイス コンフィギュレーション モードで入力します。

[no] snmp-server ifindex persist コマンドをグローバル コンフィギュレーション モードで入力すると、IF-MIB の ifIndex テーブル内の ifDescr および ifIndex エントリを使用するルーティング装置のすべてのインターフェイスで、ifIndex 永続性をイネーブルにしたり、ディセーブルにできます。

例 次に、すべてのインターフェイスの ifIndex 永続性をイネーブルにする例を示します。

```
Router (config) # snmp-server ifindex persist
Router (config) #
```



(注)

この例は、**no snmp ifindex persist** コマンドをインターフェイス コンフィギュレーション モードで使用して特定のインターフェイスで ifIndex 永続性がディセーブル化されている場合に、ifIndex 永続性はこのインターフェイス上でディセーブルのまま保持されることを示します。グローバル ifIndex コマンドは、インターフェイス固有のコマンドを上書きしません。

関連コマンド

コマンド	説明
snmp ifindex clear	特定のインターフェイスに対して実行された設定済みの snmp ifindex コマンドをクリアします。
snmp ifindex persist	再起動後も保持される Interfaces MIB (IF-MIB) 内の ifIndex 値 (ifIndex 永続性) を特定のインターフェイス上だけでイネーブルにします。

snmp-server source-interface

SNMP トラップがインフォームやトラップの送信元とするインターフェイスを指定するには、**snmp-server source-interface** コマンドを使用します。送信元指定を削除するには、このコマンドの **no** 形式を使用します。

snmp-server source-interface {traps | informs} *interface*

no snmp-server source-interface {traps | informs} [*interface*]

シンタックスの説明

traps	SNMP トラップを指定します。
informs	SNMP インフォームを指定します。
<i>interface</i>	送信元インターフェイスのインターフェイス タイプ、およびモジュールとポート番号を指定します。

コマンドのデフォルト

インターフェイスは指定されません。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

送信元インターフェイスには IP アドレスが設定されている必要があります。

interface-type/module/port のフォーマットで、*interface* 引数を入力します。

Cisco SNMP サーバから送信された SNMP トラップまたはインフォームには、その時点で送出されたインターフェイスの通知 IP アドレスが設定されています。特定のインターフェイスからの通知をモニタするには、このコマンドを使用します。

例

次に、インターフェイス `gigabitethernet5/2` をすべてのインフォームの送信元として指定する例を示します。

```
Router(config)# snmp-server source-interface informs gigabitethernet5/2
Router(config)#
```

次に、インターフェイス `gigabitethernet5/3` をすべてのトラップの送信元として指定する例を示します。

```
Router(config)# snmp-server source-interface traps gigabitethernet5/3
Router(config)#
```

次に、特定のインターフェイスの全トラップの送信元指定を削除する例を示します。

```
Router(config)# no snmp-server source-interface traps gigabitethernet5/3
Router(config)#
```

■ snmp-server source-interface

関連コマンド

コマンド	説明
snmp-server trap-source interface	SNMP トラップの送信元とするインターフェイスを指定します。このコマンドが、 snmp-server source-interface コマンドに置き換えられました。
snmp-server enable traps	ルータからの SNMP トラップおよびインフォームの送信をイネーブルにします。
snmp-server host	SNMP 通知動作の受信者を指定します。

snmp-server trap authentication unknown-context

不明なコンテキスト エラー発生時の許可失敗トラップをイネーブルにするには、**snmp-server trap authentication unknown-context** コマンドを使用します。許可失敗トラップをディセーブルにするには、このコマンドの **no** 形式を使用します。

snmp-server trap authentication unknown-context

no snmp-server trap authentication unknown-context

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト authFail トラップは生成されません。

コマンド モード グローバル コンフィギュレーション (config)

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、不明なコンテキスト エラー発生時の許可失敗トラップをイネーブルにする例を示します。

```
Router(config)# snmp-server trap authentication unknown-context
Router(config)#
```

次に、不明なコンテキスト エラー発生時の許可失敗トラップをディセーブルにする例を示します。

```
Router(config)# no snmp-server trap authentication unknown-context
Router(config)#
```

snmp-server trap link switchover

スイッチ フェールオーバー時に、リンクアップ トラップによって引き継がれるリンクダウン トラップの送信をスイッチのすべてのインターフェイスでイネーブルにするには、**snmp-server trap link switchover** コマンドを使用します。スイッチ フェールオーバー時のリンクダウンをディセーブルにするには、このコマンドの **no** 形式を使用します。

snmp-server trap link switchover

no snmp-server trap link switchover

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト イネーブル

コマンド モード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン デフォルトでは、スイッチオーバー時にリンク トラップが生成されません。

例 次に、デフォルト設定に戻す例を示します。

```
Router(config)# snmp-server trap link switchover
Router(config)#
```

次に、スイッチ フェールオーバー時に、リンクアップ トラップによって引き継がれるリンクダウンをスイッチのすべてのインターフェイスでディセーブルにする例を示します。

```
Router(config)# no snmp-server trap link switchover
Router(config)#
```

spanning-tree backbonefast

すべてのイーサネット VLAN 上で BackboneFast 機能をイネーブルにするには、**spanning-tree backbonefast** コマンドを使用します。BackboneFast をディセーブルにするには、このコマンドの **no** 形式を使用します。

spanning-tree backbonefast

no spanning-tree backbonefast

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト BackboneFast はディセーブルです。

コマンド モード グローバル コンフィギュレーション (config)

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン 間接リンク障害の検出を可能にして、スパニングツリーをより短時間で再設定できるようにするには、すべての Catalyst 6500 シリーズスイッチ上で BackboneFast をイネーブルにします。

例 次に、すべてのイーサネット VLAN で BackboneFast をイネーブルにする例を示します。

```
Router(config)# spanning-tree backbonefast  
Router(config)#
```

コマンド	説明
show spanning-tree	スパニングツリー ステートに関する情報を表示します。

spanning-tree bpdudfilter

インターフェイス上で BPDU フィルタリングをイネーブルにするには、**spanning-tree bpdudfilter** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree bpdudfilter {enable | disable}

no spanning-tree bpdudfilter

シンタックスの説明

enable	現在のインターフェイス上で BPDU フィルタリングをイネーブルにします。
disable	現在のインターフェイス上で BPDU フィルタリングをディセーブルにします。

コマンドのデフォルト

spanning-tree portfast bpdudfilter default コマンドの入力時に設定された設定です。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



注意

spanning-tree bpdudfilter enable コマンドを入力する場合は、慎重に行ってください。インターフェイス上で BPDU フィルタリングをイネーブルにすることは、このインターフェイスのスパニングツリーをディセーブルにすることと類似しています。このコマンドを正しく使用しない場合、ブリッジンググループが発生する可能性があります。

spanning-tree bpdudfilter enable コマンドを入力して BPDU フィルタリングをイネーブルにすると、PortFast 設定が無効になります。

すべてのサービス プロバイダー エッジ スイッチにレイヤ 2 プロトコル トンネリングを設定する場合は、**spanning-tree bpdudfilter enable** コマンドを入力して、802.1Q トンネル ポート上でスパニングツリー BPDU フィルタリングをイネーブルにする必要があります。

BPDU フィルタリングにより、ポートは BPDU を送受信できなくなります。その設定は、トランキンクであるかどうかに関係なく、インターフェイス全体に適用されます。このコマンドには、3 つの状態があります。

- **spanning-tree bpdudfilter enable** : インターフェイス上で BPDU フィルタリングが無条件にイネーブルになります。
- **spanning-tree bpdudfilter disable** : インターフェイス上で BPDU フィルタリングが無条件にディセーブルになります。
- **no spanning-tree bpdudfilter** : インターフェイスが PortFast 動作ステートにある場合、および **spanning-tree portfast bpdudfilter default** コマンドを設定する場合、インターフェイス上で BPDU フィルタリングがイネーブルになります。

PortFast 用に設定済みのすべてのポートで BPDU フィルタリングをイネーブルにするには、**spanning-tree portfast bpdufilter default** コマンドを使用します。

例

次に、現在のインターフェイス上で BPDU フィルタリングをイネーブルにする例を示します。

```
Router(config-if)# spanning-tree bpdufilter enable  
Router(config-if)#
```

関連コマンド

コマンド	説明
show spanning-tree	スパニングツリー ステートに関する情報を表示します。
spanning-tree portfast bpdufilter default	すべての PortFast ポートで、BPDU フィルタリングをデフォルトでイネーブルにします。

spanning-tree bpduguard

インターフェイス上で BPDU ガードをイネーブルにするには、**spanning-tree bpduguard** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree bpduguard {enable | disable}

no spanning-tree bpduguard

シンタックスの説明

enable	現在のインターフェイス上で BPDU ガードをイネーブルにします。
disable	現在のインターフェイス上で BPDU ガードをディセーブルにします。

コマンドのデフォルト

spanning-tree portfast bpduguard default コマンドの入力時に設定された設定です。

コマンドのデフォルト

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

BPDU ガードを使用すると、ポートは BPDU を受信できなくなります。通常、この機能はサービス プロバイダー環境で使用されます。ネットワーク管理者はこの機能を使用して、アクセス ポートがスパニングツリーに参加しないようにできます。この機能を使用してもポートが BPDU を受信する場合は、その対策として、ポートは errdisable ステートになります。このコマンドには、3 つの状態があります。

- **spanning-tree bpduguard enable** : インターフェイス上で BPDU ガードが無条件にイネーブルになります。
- **spanning-tree bpduguard disable** : インターフェイス上で BPDU ガードが無条件にディセーブルになります。
- **no spanning-tree bpduguard** : インターフェイスが PortFast 動作ステートにある場合、および **spanning-tree portfast bpduguard default** コマンドが設定されている場合、インターフェイス上で BPDU ガードがイネーブルになります。

例

次に、現在のインターフェイス上で BPDU ガードをイネーブルにする例を示します。

```
Router(config-if)# spanning-tree bpduguard enable
Router(config-if)#
```

関連コマンド

コマンド	説明
show spanning-tree	スパニングツリー ステートに関する情報を表示します。
spanning-tree portfast bpduguard default	すべての PortFast ポートで、BPDU ガードをデフォルトでイネーブルにします。

spanning-tree cost

STP 計算に使用するインターフェイスのパス コストを設定するには、**spanning-tree cost** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree cost *cost*

no spanning-tree cost

シンタックスの説明

cost パス コスト。有効値は 1 ~ 200,000,000 です。

コマンドのデフォルト

デフォルト パス コストは、インターフェイスの帯域幅設定から計算されます。デフォルト パス コストは次のとおりです。

- イーサネット : 100
- 16 Mb トークンリング : 62
- FDDI : 10
- FastEthernet : 10
- ATM 155 : 6
- GigabitEthernet : 1
- 10 ギガビット イーサネット : 2
- HSSI : 647

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

cost を設定する場合は、値が大きいほどコストが高くなります。指定されたプロトコル タイプに関係なく、この値が適用されます。

例

次に、インターフェイスにアクセスし、このインターフェイスに対応付けられたスパンニングツリー VLAN にパス コスト値 250 を設定する例を示します。

```
Router(config)# interface ethernet 2/0
Router(config-if)# spanning-tree cost 250
Router(config-if)#
```

関連コマンド

コマンド	説明
show spanning-tree	スパンニングツリー ステートに関する情報を表示します。

spanning-tree etherchannel guard misconfig

チャンネルの設定ミスによるループが検出された場合に、エラー メッセージを表示するには、**spanning-tree etherchannel guard misconfig** コマンドを使用します。エラー メッセージをディセーブルにするには、このコマンドの **no** 形式を使用します。

spanning-tree etherchannel guard misconfig

no spanning-tree etherchannel guard misconfig

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト イネーブル

コマンド モード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン EtherChannel は PAgP または LACP を使用し、インターフェイスの EtherChannel モードが **channel-group group-number mode on** コマンドを使用してイネーブル化されている場合は機能しません。

EtherChannel ガードの設定ミスが検出されると、次のエラー メッセージが表示されます。

```
msgdef(CHNL_MISCFG, SPANTREE, LOG_CRIT, 0, "Detected loop due to etherchannel  
misconfiguration of %s %s")
```

設定ミスに関連するローカル ポートを判別するには、**show interfaces status err-disabled** コマンドを入力します。リモート装置の EtherChannel 設定を調べるには、リモート装置上で **show etherchannel summary** コマンドを入力します。

設定を訂正したら、対応付けられたポート チャンネル インターフェイス上で **shutdown** および **no shutdown** コマンドを入力します。

例 次に、EtherChannel ガードの設定ミス機能をイネーブルにする例を示します。

```
Router(config)# spanning-tree etherchannel guard misconfig  
Router(config)#
```

関連コマンド

コマンド	説明
show etherchannel summary	チャンネルの EtherChannel 情報を表示します。
show interfaces status err-disabled	インターフェイス ステータスを表示したり、LAN ポートで errdisable ステートにあるインターフェイスだけのリストを表示したりします。
shutdown	インターフェイスをディセーブルにします。

spanning-tree extend system-id

1024 個の MAC アドレスをサポートするシャーシ上で拡張システム ID 機能をイネーブルにするには、**spanning-tree extend system-id** コマンドを使用します。拡張システム ID をディセーブルにするには、このコマンドの **no** 形式を使用します。

spanning-tree extend system-id

no spanning-tree extend system-id

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

1024 個の MAC アドレスをサポートしないシステム上でイネーブルです。

コマンドのデフォルト

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

Catalyst 6500 シリーズ スイッチは、64 または最大 1024 個の MAC アドレスをサポートできます。64 個の MAC アドレスを持つ Catalyst 6500 シリーズ スイッチの場合、STP は拡張システム ID と MAC アドレスを使用して、VLAN ごとに一意のブリッジ ID を作成します。

64 個の MAC アドレスをサポートする Catalyst 6500 シリーズ スイッチでは、拡張システム ID をディセーブルにできません。

拡張システム ID をイネーブルまたはディセーブルにすると、すべてのアクティブな STP インスタンスのブリッジ ID が更新されるため、これによってスパニングツリー トポロジィが変更される場合があります。

例

次に、拡張システム ID をイネーブルにする例を示します。

```
Router(config)# spanning-tree extend system-id  
Router(config)#
```

関連コマンド

コマンド	説明
show spanning-tree	スパニングツリー ステートに関する情報を表示します。

spanning-tree guard

ガード モードをイネーブルまたはディセーブルにするには、**spanning-tree guard** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
spanning-tree guard {loop | root | none}
```

```
no spanning-tree guard
```

シンタックスの説明

loop	インターフェイスでループ ガード モードをイネーブルにします。
root	インターフェイスでルートガード モードをイネーブルにします。
none	ガード モードをなしに設定します。

コマンドのデフォルト

ガード モードはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、ルート ガードをイネーブルにする例を示します。

```
Router(config-if)# spanning-tree guard root
Router(config-if)#
```

関連コマンド

コマンド	説明
show spanning-tree	スパンニングツリー ステートに関する情報を表示します。
spanning-tree loopguard default	所定のブリッジのすべてのポート上でデフォルトとしてループ ガードをイネーブルにします。

spanning-tree link-type

リンク タイプをポートに設定するには、**spanning-tree link-type** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree link-type {point-to-point | shared}

no spanning-tree link-type

シンタックスの説明

point-to-point	インターフェイスがポイントツーポイント リンクとなるように指定します。
shared	インターフェイスが共有メディアとなるように指定します。

コマンドのデフォルト

リンク タイプは、明示的に設定しなければ、デュプレックス設定から自動的に生成されます。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

RSTP+ 高速トランジションが機能するのは、2 つのブリッジ間のポイントツーポイント リンク上だけです。

デフォルトでは、ポートのリンク タイプはデュプレックス モードから取得されます。つまり、全二重ポートはポイントツーポイント リンクであると見なされ、半二重コンフィギュレーションは共有リンクであると見なされます。

ポートを共有リンクに指定した場合は、デュプレックス設定に関係なく、RSTP+ 高速トランジションを使用できません。

例

次に、ポートを共有リンクとして設定する例を示します。

```
Router(config-if)# spanning-tree link-type shared  
Router(config-if)#
```

関連コマンド

コマンド	説明
show spanning-tree interface	スパニングツリー ステートに関する情報を表示します。

spanning-tree loopguard default

指定されたブリッジのすべてのポート上でループ ガードをデフォルトでイネーブルにするには、**spanning-tree loopguard default** コマンドを使用します。ループ ガードをディセーブルにするには、このコマンドの **no** 形式を使用します。

spanning-tree loopguard default

no spanning-tree loopguard default

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト ループ ガードはディセーブルです。

コマンド モード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン ループ ガードを使用すると、ブリッジ ネットワークのセキュリティが向上します。また、単一方向リンクの原因となる障害によって代替ポートまたはルート ポートが指定ポートとして使用されることがなくなります。

ループ ガードが動作するのは、スパニングツリーがポイントツーポイントと見なすポート上だけです。ループガード ポートを個別に設定すると、このコマンドが上書きされます。

例 次に、ループ ガードをイネーブルにする例を示します。

```
Router(config)# spanning-tree loopguard default  
Router(config)#
```

関連コマンド	コマンド	説明
	show spanning-tree	スパニングツリー ステートに関する情報を表示します。
	spanning-tree guard	ガード モードをイネーブルまたはディセーブルにします。

spanning-tree mode

PVST+、高速 PVST+、MST モードを切り替えるには、**spanning-tree mode** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mode [pvst | mst | rapid-pvst]

no spanning-tree mode

シンタックスの説明

pvst	(任意) PVST+ モード
mst	(任意) MST モード
rapid-pvst	(任意) 高速 PVST+ モード

コマンドのデフォルト

pvst

コマンドのデフォルト

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



注意

spanning-tree mode コマンドを使用して PVST+、高速 PVST+、および MST モードを切り替える場合は、慎重に行ってください。このコマンドを入力すると、以前のモードのスパニングツリー インスタンスはすべて停止し、新しいモードで再開されます。このコマンドを使用すると、ユーザ トラフィックが中断することがあります。

例

次に、MST モードに切り替える例を示します。

```
Router(config)# spanning-tree mode mst
Router(config)#
```

次に、デフォルト モード (PVST+) に戻す例を示します。

```
Router(config)# no spanning-tree mode
Router(config)#
```

関連コマンド

コマンド	説明
show spanning-tree mst	MST プロトコルに関する情報を表示します。

spanning-tree mst

任意の MST インスタンス（インスタンス ID 0 の CIST を含む）のパス コストおよびポート プライオリティ パラメータを設定するには、**spanning-tree mst** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
spanning-tree mst instance-id {cost cost} | {port-priority prio}
```

```
no spanning-tree mst instance-id {cost | port-priority}
```

シンタックスの説明

instance-id	インスタンス ID 番号を指定します。有効値は 0 ~ 15 です。
cost cost	(任意) インスタンスのパス コストを指定します。有効値は 1 ~ 200,000,000 です。
port-priority prio	(任意) インスタンスのポート プライオリティを指定します。有効値は 0 ~ 240 で、16 ずつ増分します。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- *cost* は、ポート速度に応じて変わります。インターフェイス速度が速いほどコストは小さくなります。MST は常に **long** のパス コストを使用します。
- *prio* は **128** です。

コマンドのデフォルト

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

cost cost の値が大きいほど、コストは高くなります。*cost* 値を入力する場合は、エントリにカンマを含めないでください。たとえば、**1,000** ではなく、**1000** と入力します。

port-priority prio 値が高いほど、プライオリティは小さくなります。

例

次に、インターフェイスのパス コストを設定する例を示します。

```
Router(config-if)# spanning-tree mst 0 cost 17031970
Router(config-if)#
```

次に、インターフェイスのプライオリティを設定する例を示します。

```
Router(config-if)# spanning-tree mst 0 port-priority 64
Router(config-if)#
```

関連コマンド

コマンド	説明
show spanning-tree mst	MST プロトコルに関する情報を表示します。
spanning-tree port-priority	2 つのブリッジがルートブリッジとなるために競合している場合に、インターフェイスにプライオリティを設定します。

spanning-tree mst configuration

MST コンフィギュレーション サブモードを開始するには、**spanning-tree mst configuration** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst configuration

no spanning-tree mst configuration

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

デフォルトでは、MST の設定値がすべてのパラメータのデフォルト値になります。

- VLAN はどの MST インスタンスにもマッピングされません (すべての VLAN は CIST インスタンスにマッピングされます)。
- リージョン名は空のストリングです。
- リビジョン番号は 0 です。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

MST の設定には、3 つの主要パラメータが使用されます。

- インスタンス VLAN マッピング : **instance** コマンドを参照してください。
- リージョン名 : **name (MST configuration submode)** コマンドを参照してください。
- コンフィギュレーション リビジョン番号 : **revision** コマンドを参照してください。

abort および **exit** コマンドを使用すると、MST コンフィギュレーション サブモードを終了できます。2 つのコマンドの違いは、変更内容を保存するかどうかです。

exit コマンドは、MST コンフィギュレーション サブモードが終了する前に、すべての変更を実行します。セカンダリ VLAN が、対応付けられたプライマリ VLAN と同じインスタンスにマッピングされていない場合に、MST コンフィギュレーション サブモードを終了すると、警告メッセージが表示され、対応付けられたプライマリ VLAN と同じインスタンスにマッピングされていないセカンダリ VLAN が一覧表示されます。警告メッセージは次のとおりです。

```
These secondary vlans are not mapped to the same instance as their primary:  
-> 3
```

abort コマンドは、変更を実行しないで、MST コンフィギュレーション サブモードを終了します。

MST コンフィギュレーションサブモードパラメータを変更すると、接続損失が発生する可能性があります。サービスの中断を減らすには、MST コンフィギュレーションサブモードを開始する場合、現在の MST コンフィギュレーションのコピーを変更します。コンフィギュレーションの編集が終了したら、**exit** キーワードを使用して、すべての変更を一度に適用するか、または **abort** キーワードを使用して、コンフィギュレーションへの変更を実行しないで終了できます。

2 名のユーザがまったく同時に新しいコンフィギュレーションを実行することは通常ありませんが、その場合は次の警告メッセージが表示されます。

```
% MST CFG:Configuration change lost because of concurrent access
```

例

次に、MST コンフィギュレーションサブモードを開始する例を示します。

```
Router(config)# spanning-tree mst configuration
Router(config-mst)#
```

次に、MST コンフィギュレーションをデフォルト設定に戻す例を示します。

```
Router(config)# no spanning-tree mst configuration
Router(config)#
```

関連コマンド

コマンド	説明
instance	1 つまたは一連の VLAN を MST インスタンスにマッピングします。
name (MST configuration submode)	MST リージョン名を設定します。
revision	MST コンフィギュレーションのレビジョン番号を設定します。
show	MST の設定を確認します。
show spanning-tree mst	MST プロトコルに関する情報を表示します。

spanning-tree mst forward-time

転送遅延タイマーを Catalyst 6500 シリーズスイッチ上のすべてのインスタンスに設定するには、**spanning-tree mst forward-time** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst forward-time *seconds*

no spanning-tree mst forward-time

シンタックスの説明

<i>seconds</i>	Catalyst 6500 シリーズスイッチのすべてのインスタンスの転送遅延タイマーの設定秒数。有効値は、4 ~ 30 秒です。
----------------	--

コマンドのデフォルト

seconds は 15 です。

コマンドモード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、転送遅延タイマーを設定する例を示します。

```
Router(config)# spanning-tree mst forward-time 20
Router(config)#
```

関連コマンド

コマンド	説明
show spanning-tree mst	MST プロトコルに関する情報を表示します。

spanning-tree mst hello-time

hello タイム遅延タイマーを Catalyst 6500 シリーズ スイッチ上のすべてのインスタンスに設定するには、**spanning-tree mst hello-time** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst hello-time *seconds*

no spanning-tree mst hello-time

シンタックスの説明	<i>seconds</i>	Catalyst 6500 シリーズ スイッチのすべてのインスタンスの hello タイム遅延タイマーの設定秒数。有効値は、1 ~ 10 秒です。
------------------	----------------	---

コマンドのデフォルト	2 秒
-------------------	-----

コマンドのデフォルト	グローバル コンフィギュレーション (config)
-------------------	----------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン	<i>hello-time</i> 値を指定しない場合、この値はネットワークの直径から計算されます。
-------------------	--

例 次に、hello タイム遅延タイマーを設定する例を示します。

```
Router(config)# spanning-tree mst hello-time 3
Router(config)#
```

関連コマンド	コマンド	説明
	show spanning-tree mst	MST プロトコルに関する情報を表示します。

spanning-tree mst max-age

有効期限タイマーを Catalyst 6500 シリーズ スイッチ上のすべてのインスタンスに設定するには、**spanning-tree mst max-age** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst max-age *seconds*

no spanning-tree mst max-age

シンタックスの説明	<i>seconds</i>	Catalyst 6500 シリーズ スイッチのすべてのインスタンスの有効期限タイマーの設定秒数。有効値は、6 ~ 40 秒です。
-----------	----------------	---

コマンドのデフォルト	20 秒
------------	------

コマンド モード	グローバル コンフィギュレーション (config)
----------	----------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例	次に、有効期限タイマーを設定する例を示します。 Router(config)# spanning-tree mst max-age 40 Router(config)#
---	---

関連コマンド	コマンド	説明
	show spanning-tree mst	MST プロトコルに関する情報を表示します。

spanning-tree mst max-hops

BPDU が廃棄されるまでのリージョンの最大ホップ数を指定するには、**spanning-tree mst max-hops** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst max-hops *hopnumber*

no spanning-tree mst max-hops

シンタックスの説明	<i>hopnumber</i>	BPDU が廃棄されるまでのリージョンの最大ホップ数を指定します。有効値は、1 ~ 255 ホップです。
------------------	------------------	--

コマンドのデフォルト	20 ホップ
-------------------	--------

コマンドのデフォルト	グローバル コンフィギュレーション (config)
-------------------	----------------------------

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、最大ホップ数を設定する例を示します。

```
Router(config)# spanning-tree mst max-hops 25
Router(config)#
```

関連コマンド	コマンド	説明
	show spanning-tree mst	MST プロトコルに関する情報を表示します。

spanning-tree mst pre-standard

先行標準の BPDU だけを送信するようにポートを設定するには、**spanning-tree mst pre-standard** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst pre-standard

no spanning-tree mst pre-standard

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

デフォルトでは、先行標準ネイバを自動的に検出します。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

デフォルト設定であっても、ポートは先行標準および標準 BPDU の両方を受信できます。

先行標準 BPDU は、IEEE 標準が完成する前に作成された Cisco IOS MST 実装に基づいています。標準 BPDU は、最終 IEEE 標準に基づいています。

先行標準の BPDU だけを送信するようにポートを設定する場合、先行標準フラグが **show spanning-tree** コマンドに表示されます。先行標準フラグの種類は次のとおりです。

- Pre-STD または **prestandard** (長形式) : ポートが先行標準 BPDU を送信するように設定されている場合、およびこのインターフェイス上で先行標準ネイバ ブリッジが検出された場合に、このフラグが表示されます。
- Pre-STD-Cf または **prestandard (config)** (長形式) : 先行標準 BPDU を送信するようにポートを設定し、そのポートで先行標準 BPDU が受信されない場合、自動検出メカニズムが失敗した場合、または先行標準ネイバが存在しない場合に設定が間違っている場合、このフラグが表示されます。
- Pre-STD-Rx または **prestandard (rcvd)** (長形式) : 先行標準 BPDU がポートで受信され、先行標準 BPDU を送信するようにポートを設定していない場合に、このフラグが表示されます。ポートは先行標準 BPDU を送信しますが、先行標準ネイバとのやりとりを自動検出メカニズムだけに依存しないようにポートの設定を変更することを推奨します。

MST の設定が先行標準に適合しない場合 (インスタンス ID が 15 より大きい場合)、ポート上の STP の設定に関係なく、標準 MST BPDU だけが送信されます。

例 次に、先行標準 BPDU だけを送信するようにポートを設定する例を示します。

```
Router(config-if) # spanning-tree mst pre-standard  
Router(config-if) #
```

関連コマンド

コマンド	説明
show spanning-tree mst	MST プロトコルに関する情報を表示します。

spanning-tree mst root

インスタンスのプライマリ ルートとセカンダリ ルートを指定したり、ブリッジプライオリティ、およびタイマー値を設定したりするには、**spanning-tree mst root** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst *instance-id* root **{primary | secondary}** **{priority *prio*}** [**diameter *dia*** [**hello-time *hello-time***]]

no spanning-tree mst root

シンタックスの説明

<i>instance-id</i>	インスタンス ID 番号を指定します。有効値は 1 ~ 15 です。
primary	スパニングツリー インスタンスのブリッジ ルートを作成するために必要なプライオリティ (小さな値) を指定します。
secondary	プライマリ ルートに障害が発生した場合に、セカンダリ ルートとして機能させるスイッチを指定します。
priority <i>prio</i>	ブリッジプライオリティを指定します。有効値および詳細については、「使用上のガイドライン」を参照してください。
diameter <i>dia</i>	(任意) ネットワーク直径に基づくブリッジのタイマー値を指定します。有効値は、1 ~ 7 です。
hello-time <i>hello-time</i>	(任意) ルート スイッチがコンフィギュレーション メッセージを生成する間隔を指定します。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- **spanning-tree mst root** にはデフォルト設定がありません。
- *prio* は **32768** です。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ブリッジプライオリティは、4096 ずつ増分して設定できます。プライオリティを設定する場合、有効値は **0**、**4096**、**8192**、**12288**、**16384**、**20480**、**24576**、**28672**、**32768**、**36864**、**40960**、**45056**、**49152**、**53248**、**57344**、および **61440** です。

スイッチをルートにする場合は、*prio* を **0** に設定します。

instance-id は、単一インスタンスまたはインスタンス範囲 (0-3,5,7-9 など) として入力できます。

spanning-tree root secondary のブリッジプライオリティ値は 16384 です。

diameter *dia* および **hello-time *hello-time*** キーワードおよび引数は、インスタンス **0** だけに使用できます。

hello-time 引数を指定しない場合、この引数はネットワークの直径から計算されます。

例

次に、ブリッジプライオリティを設定する例を示します。

```
Router(config)# spanning-tree mst 0 root priority 4096
Router(config)#
```

次に、ブリッジのプライオリティおよびタイマー値を設定する例を示します。

```
Router(config)# spanning-tree mst 0 root primary diameter 7 hello-time 2
Router(config)# spanning-tree mst 5 root primary
Router(config)#
```

関連コマンド

コマンド	説明
show spanning-tree mst	MST プロトコルに関する情報を表示します。

spanning-tree pathcost method

デフォルトのパス コスト計算方式を設定するには、**spanning-tree pathcost method** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree pathcost method {long | short}

no spanning-tree pathcost method

シンタックスの説明

long	デフォルト ポート パス コスト用の 32 ビット ベース値を指定します。
short	デフォルト ポート パス コスト用の 16 ビット ベース値を指定します。

コマンドのデフォルト

short

コマンドのデフォルト

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、Catalyst 6500 シリーズ スイッチのすべてのスパニングツリー インスタンスに適用されます。

long パス コスト計算方式では、パス コスト計算に 32 ビットをすべて利用して、1 ~ 200,000,000 の値を生成します。

short パス コスト計算方式 (16 ビット) では、1 ~ 65,535 の値が生成されます。

例

次に、デフォルトのパス コスト計算方式を long に設定する例を示します。

```
Router(config)# spanning-tree pathcost method long
Router(config)#
```

次に、デフォルトのパス コスト計算方式を short に設定する例を示します。

```
Router(config)# spanning-tree pathcost method short
Router(config)#
```

関連コマンド

コマンド	説明
show spanning-tree	スパニングツリー ステートに関する情報を表示します。

spanning-tree portfast (interface configuration mode)

リンクがアップした時点で、インターフェイスがタイマーの経過を待たずにただちにフォワーディングステートに移行した場合に、PortFast モードをイネーブルにするには、**spanning-tree portfast** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree portfast

spanning-tree portfast {disable | trunk}

no spanning-tree portfast

シンタックスの説明

disable	インターフェイスの PortFast をディセーブルにします。
trunk	トランク モードの場合でも、インターフェイスの PortFast をイネーブルにします。

コマンドのデフォルト

spanning-tree portfast default コマンドによって設定される設定値

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、エンドステーションに接続されているインターフェイスだけに使用してください。偶発的なトポロジーループが原因でデータパケットループが発生し、Catalyst 6500 シリーズスイッチおよびネットワークの動作が妨げられることがあります。

リンクがアップすると、PortFast モードがイネーブルに設定されたインターフェイスは標準の転送遅延時間の経過を待たずに、ただちにスパニングツリーフォワーディングステートに移行します。

no spanning-tree portfast コマンドは、慎重に使用してください。このコマンドは、**spanning-tree portfast default** コマンドがイネーブルの場合は、PortFast をディセーブルにしません。

このコマンドには、4つの状態があります。

- **spanning-tree portfast** : 所定のポートで、PortFast を無条件にイネーブルにします。
- **spanning-tree portfast disable** : 所定のポートで、PortFast を明示的にディセーブルにします。このコンフィギュレーション行はデフォルトでないため、実行コンフィギュレーションに含まれます。
- **spanning-tree portfast trunk** : トランクポートに PortFast を設定できます。



(注) **spanning-tree portfast trunk** コマンドを入力すると、アクセスモードの場合でも、ポートは PortFast に対応するように設定されます。

spanning-tree portfast (interface configuration mode)

- **no spanning-tree portfast** : **spanning-tree portfast default** コマンドをグローバル コンフィギュレーション モードで定義する場合、およびポートがトランク ポートでない場合に、PortFast を自動的にイネーブルにします。PortFast をグローバルに設定しない場合、**no spanning-tree portfast** コマンドは **spanning-tree portfast disable** コマンドと同様に機能します。

例

次に、PortFast モードをイネーブルにする例を示します。

```
Router(config-if)# spanning-tree portfast
Router(config-if)#
```

関連コマンド

コマンド	説明
show spanning-tree	スパンニングツリー ステートに関する情報を表示します。
spanning-tree portfast default	すべてのアクセス ポートで、PortFast をデフォルトでイネーブルにします。

spanning-tree portfast bpdudfilter default

すべての PortFast ポートで、BPDU フィルタリングをデフォルトでイネーブルにするには、**spanning-tree portfast bpdudfilter default** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree portfast bpdudfilter default

no spanning-tree portfast bpdudfilter default

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト デイセーブル

コマンド モード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン **spanning-tree portfast bpdudfilter** コマンドは、PortFast ポートで BPDU フィルタリングをグローバルにイネーブルにします。BPDU フィルタリングにより、ポートはすべての BPDU を送受信できなくなります。

portfast bpdudfilter default コマンドを無効にするには、インターフェイスごとに BPDU フィルタリングを設定します。



(注) BPDU フィルタリングをイネーブルにする場合は、慎重に行ってください。ポート単位でイネーブルにする場合とグローバルにイネーブルする場合では、機能が異なります。グローバルにイネーブル化された BPDU フィルタリングは、PortFast 動作ステータスのポートだけに適用されます。リンクがアップすると、ポートは BPDU をいくつか送信してから、発信 BPDU を効率的にフィルタリングします。エッジポートに着信した BPDU は、ただちに PortFast 動作ステータスを失い、BPDU フィルタリングがデイセーブルになります。

BPDU フィルタリングがポート上でローカルにイネーブル化されている場合、Catalyst 6500 シリーズスイッチはこのポート上で BPDU を送受信できません。



注意 このコマンドは、慎重に使用してください。このコマンドを誤って使用すると、ブリッジンググループを発生させる可能性があります。

■ **spanning-tree portfast bpdudfilter default**

次に、BPDU フィルタリングをデフォルトでイネーブルにする例を示します。

```
Router(config)# spanning-tree portfast bpdudfilter default  
Router(config)#
```

関連コマンド

コマンド	説明
show spanning-tree mst	MST プロトコルに関する情報を表示します。
spanning-tree bpdudfilter	インターフェイス上で BPDU フィルタリングをイネーブルにします。

spanning-tree portfast bpduguard default

すべての PortFast ポートで、BPDU ガードをデフォルトでイネーブルにするには、**spanning-tree portfast bpduguard default** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree portfast bpduguard default

no spanning-tree portfast bpduguard default

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト ディセーブル

コマンド モード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



注意

このコマンドは、慎重に使用してください。このコマンドは、エンドステーションに接続されているインターフェイスだけに使用してください。偶発的なトポロジー ループが原因でデータ パケット ループが発生し、Catalyst 6500 シリーズ スイッチおよびネットワークの動作が妨げられることがあります。

BPDU ガードは、BPDU を受信したポートをディセーブルにします。BPDU ガードが適用されるのは、PortFast がイネーブルに設定されていて、PortFast 動作ステートになっているポートだけです。

例 次に、BPDU ガードをデフォルトでイネーブルにする例を示します。

```
Router(config)# spanning-tree portfast bpduguard default  
Router(config)#
```

関連コマンド	コマンド	説明
	show spanning-tree mst	MST プロトコルに関する情報を表示します。
	spanning-tree portfast bpduguard default	インターフェイス上で BPDU ガードをイネーブルにします。

spanning-tree portfast default

すべてのアクセス ポートで、PortFast をデフォルトでイネーブルにするには、**spanning-tree portfast default** コマンドを使用します。すべてのアクセス ポートで、PortFast をデフォルトでディセーブルにするには、このコマンドの **no** 形式を使用します。

spanning-tree portfast default

no spanning-tree portfast default

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



注意

このコマンドは、慎重に使用してください。このコマンドは、エンドステーションに接続されているインターフェイスだけに使用してください。偶発的なトポロジー ループが原因でデータ パケット ループが発生し、Catalyst 6500 シリーズ スイッチおよびネットワークの動作が妨げられることがあります。

リンクがアップすると、PortFast モードがイネーブルに設定されたインターフェイスは標準の転送遅延時間の経過を待たずに、ただちにスパンニングツリー フォワーディング ステートに移行します。

インターフェイスごとに個別に PortFast モードをイネーブルにするには、**spanning-tree portfast (interface configuration mode)** コマンドを使用します。

例

次に、すべてのアクセス ポートで、PortFast をデフォルトでイネーブルにする例を示します。

```
Router(config)# spanning-tree portfast default
Router(config)#
```

関連コマンド

コマンド	説明
show spanning-tree	スパンニングツリー ステートに関する情報を表示します。
spanning-tree portfast (interface configuration mode)	PortFast モードをイネーブルにします。

spanning-tree port-priority

2つのブリッジがルートブリッジとなるために競合している場合に、インターフェイスにプライオリティを設定するには、**spanning-tree port-priority** コマンドを使用します。設定されたプライオリティによって、差が生じます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree port-priority *port-priority*

no spanning-tree port-priority

シンタックスの説明 *port-priority* ポートのプライオリティ。有効値は 2 ~ 255 です。

コマンドのデフォルト *port-priority* は **128** です。

コマンドモード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

例 次に、イーサネット インターフェイス 2/0 のルートブリッジとしてスパンニングツリー インスタンス 20 が選択される可能性を高める例を示します。

```
Router(config-if)# spanning-tree port-priority 0
Router(config-if)#
```

関連コマンド	コマンド	説明
	show spanning-tree	スパンニングツリー ステートに関する情報を表示します。
	spanning-tree mst	任意の MST インスタンス (インスタンス ID 0 の CIST を含む) のパス コストおよびポートプライオリティパラメータを設定します。
	spanning-tree vlan	VLAN 単位で STP を設定します。

spanning-tree transmit hold-count

送信ホールド カウントを指定するには、**spanning-tree transmit hold-count** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree transmit hold-count *value*

no spanning-tree transmit hold-count

シンタックスの説明

<i>value</i>	一時停止するまで 1 秒間に送信される BPDU の数。有効値は、1 ~ 20 です。
--------------	---

コマンドのデフォルト

value は **6** です。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、すべてのスパンニングツリー モードでサポートされています。送信ホールド カウントは、一時停止するまで 1 秒間に送信される BPDU の数を決定します。



(注)

このパラメータをより高い値に変更すると、特に高速 PVST モードで、CPU 利用率に重大な影響を与える可能性があります。このパラメータを低い値に設定すると、一部のシナリオでコンバージェンスが低速になる可能性があります。デフォルト設定から値を変更しないことを推奨します。

value 設定を変更する場合は、**show running-config** コマンドを入力して、変更内容を確認します。コマンドを削除する場合は、**show spanning-tree mst** コマンドを使用して、削除内容を確認します。

例

次に、送信ホールド カウントを指定する例を示します。

```
Router(config)# spanning-tree transmit hold-count 8
Router(config)#
```

関連コマンド

コマンド	説明
show running-config	モジュールまたはレイヤ 2 VLAN のステータスおよび設定を表示します。
show spanning-tree mst	MST プロトコルに関する情報を表示します。

spanning-tree uplinkfast

UplinkFast をイネーブルにするには、**spanning-tree uplinkfast** コマンドを使用します。UplinkFast をディセーブルにするには、このコマンドの **no** 形式を使用します。

spanning-tree uplinkfast [**max-update-rate** *packets-per-second*]

no spanning-tree uplinkfast [**max-update-rate**]

シンタックスの説明

max-update-rate	(任意) 更新パケットの最大送信速度 (パケット/秒) を指定します。
<i>packets-per-second</i>	有効値は 0 ~ 65,535 です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- UplinkFast はディセーブルです。
- *packets-per-second* は 150 パケット/秒です。

コマンドのデフォルト

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドはアクセス スイッチだけで使用します。

UplinkFast が設定されている場合、このスイッチがルートとして選択されないように、ブリッジプライオリティは 49,152 に変更されます。指定されたスパニングツリー インスタンスに属するすべてのスパニングツリー インターフェイスのインターフェイス パス コストも、すべて 3000 ずつ増分します。

ルート インターフェイスの障害がスパニングツリーで検出されると、UplinkFast 機能はただちに代替ルート インターフェイスに切り替えて、新しいルート インターフェイスを直接フォワーディング ステートに移行させます。この間、トポロジー変更通知が送信されます。トポロジーの変更による中断を最小限にするため、元のルート インターフェイスに対応付けられたアドレスを除き、転送元ブリッジのステーション アドレスごとに、マルチキャスト パケットが 01-00-0C-CD-CD-CD に送信されます。

spanning-tree uplinkfast max-update-rate コマンドを使用すると、UplinkFast がイネーブルになり (まだイネーブルでない場合)、更新パケットの送信速度が変更されます。デフォルトの速度に戻すには、このコマンドの **no** 形式を使用します。

例

次に、UplinkFast をイネーブルにして、最大速度を 200 パケット/秒に設定する例を示します。

```
Router(config)# spanning-tree uplinkfast max-update-rate 200
Router(config)#
```

関連コマンド

コマンド	説明
show spanning-tree	スパニングツリー ステートに関する情報を表示します。

spanning-tree vlan

VLAN 単位で STP を設定するには、**spanning-tree vlan** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
spanning-tree vlan vlan-id [forward-time seconds | hello-time hello-time | max-age
seconds | priority priority | protocol protocol | {root {primary | secondary} [diameter
net-diameter [hello-time hello-time]}]
```

```
no spanning-tree vlan vlan-id [forward-time | hello-time | max-age | priority | protocol |
root]
```

シンタックスの説明

vlan-id	VLAN ID 番号。有効値は 1 ~ 4094 です。
forward-time <i>seconds</i>	(任意) STP 転送遅延時間を指定します。有効値は 4 ~ 30 秒です。
hello-time <i>hello-time</i>	(任意) ルート スイッチで生成されるコンフィギュレーション メッセージの間隔 (秒数) を指定します。有効値は 1 ~ 10 秒です。
max-age <i>seconds</i>	(任意) BPDU 内の情報が有効である最大期間 (秒数) を指定します。有効値は 6 ~ 40 秒です。
priority <i>priority</i>	(任意) STP ブリッジプライオリティを指定します。有効値は 0 ~ 65,535 です。
protocol <i>protocol</i>	(任意) STP を指定します。有効値については、「使用上のガイドライン」を参照してください。
root primary	(任意) このスイッチを強制的にルート ブリッジに設定します。
root secondary	(任意) プライマリ ルートに障害が発生した場合に、このスイッチをルート スイッチとして機能させます。
diameter <i>net-diameter</i>	(任意) エンドステーション間の 2 つの接続ポイント間に存在するブリッジの最大数を指定します。有効値は 2 ~ 7 です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- **forward-time** : 15 秒
- **hello-time** : 2 秒
- **max-age** : 20 秒
- **priority** : IEEE STP がイネーブルの場合のデフォルトは 32768、STP がイネーブルの場合のデフォルトは 128
- **protocol** : IEEE
- **root** : STP ルートなし

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



注意

no spanning-tree vlan *vlan-id* コマンドを使用して、VLAN 上でスパニングツリーをディセーブルにする場合は、VLAN 内のすべてのスイッチおよびブリッジでスパニングツリーがディセーブルであることを確認してください。スパニングツリーがイネーブルとなっているスイッチおよびブリッジは、ネットワークの物理トポロジーに関して不完全な情報しか持たないため、同一 VLAN 内の一部のスイッチおよびブリッジでスパニングツリーをディセーブルにし、他のスイッチおよびブリッジでイネーブルにしておくことはできません。



注意

物理的なループがないトポロジー内であっても、スパニングツリーをディセーブルにしないことを推奨します。スパニングツリーは設定ミスやケーブル障害を防ぎます。VLAN 内に物理的なループがないことが確認されるまで、VLAN 内のスパニングツリーをディセーブルにしないでください。

max-age seconds が設定されている場合に、ブリッジが指定インターバル内にルートブリッジから BPDU を受信しない場合は、ネットワークが変更されていると見なされ、スパニングツリートポロジーが再計算されます。

protocol の有効値は **dec** (Digital STP)、**ibm** (IBM STP)、**ieee** (IEEE Ethernet STP)、および **vlan-bridge** (VLAN Bridge STP) です。

spanning-tree root primary コマンドを入力すると、スイッチのブリッジプライオリティが 8192 に変更されます。**spanning-tree root primary** コマンドを入力したにもかかわらず、スイッチがルートにならなかった場合は、このスイッチのブリッジプライオリティが現在のブリッジのブリッジプライオリティよりも 100 だけ小さな値に変更されます。スイッチがルートにならない場合は、エラーが発生します。

spanning-tree root secondary コマンドを入力すると、スイッチのブリッジプライオリティが 16384 に変更されます。ルートスイッチに障害が発生した場合は、このスイッチが次のルートスイッチになります。

spanning-tree root コマンドは、バックボーンスイッチだけで使用してください。

例

次に、VLAN 200 でスパニングツリーをイネーブルにする例を示します。

```
Router(config)# spanning-tree vlan 200
Router(config)#
```

次に、スイッチを VLAN 10 のルートスイッチとして設定し、ネットワーク直径を 4 に設定する例を示します。

```
Router(config)# spanning-tree vlan 10 root primary diameter 4
Router(config)#
```

次に、スイッチを VLAN 10 のセカンダリルートスイッチとして設定し、ネットワーク直径を 4 に設定する例を示します。

```
Router(config)# spanning-tree vlan 10 root secondary diameter 4
Router(config)#
```

関連コマンド

コマンド	説明
show spanning-tree	スパニングツリーステートに関する情報を表示します。

speed

イーサネット インターフェイスのポート速度を設定するには、**speed** コマンドを使用します。速度設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

speed {**10** | **100** | **1000**}

speed auto [*speed-list*]

speed [**1000** | **nonegotiate**]

no speed

シンタックスの説明

10	インターフェイスの伝送を 10 Mbps に指定します。
100	インターフェイスの伝送を 100 Mbps に指定します。
1000	(任意) インターフェイスの伝送を 1000 Mbps に指定します。
auto	自動ネゴシエーション機能をイネーブルにします。
<i>speed-list</i>	(任意) 特定の速度に対する速度の自動ネゴシエーション機能。有効値については、「使用上のガイドライン」を参照してください。
nonegotiate	(任意) ギガビット イーサネット ポート上でリンク ネゴシエーション プロトコルをイネーブルまたはディセーブルにします。

コマンドのデフォルト

デフォルト設定のリストについては、表 2-93 を参照してください。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

10/100 ポートには **speed** [**10** | **100**] コマンド、10/100/1000 ポートには **speed auto** [**10** **100** [**1000**]] コマンド、ギガビット イーサネット ポートには **speed** [**1000** | **nonegotiate**] コマンドを使用します。

speed-list の入力値はスペースで区切ります。

次の *speed-list* 設定がサポートされています。

- **speed auto** : すべての速度をネゴシエーションします。
- **speed auto 10 100** : 10 および 100 の速度だけをネゴシエーションします。
- **speed auto 10 100 1000** : すべての速度をネゴシエーションします。

リンク ネゴシエーションがイネーブルの場合は、2 つのギガビット イーサネット ポート間の速度、デュプレックス、フロー制御、およびクロッキングのネゴシエーションが自動的にイネーブルになります。

表 2-93 に、サポートされているコマンド オプションをインターフェイス別に示します。

表 2-93 サポートされている speed コマンド オプション

インターフェイスタイプ	サポートされている構文	デフォルト設定	使用上のガイドライン
10/100 Mbps モジュール	<code>speed [10 100]</code> <code>speed auto [10 100]</code>	auto	速度が auto に設定されている場合は、 duplex を設定できません。 速度が 10 または 100 に設定されている場合に、デュプレックスを設定しないと、デュプレックスは half に設定されます。
10/100/1000 Mbps インターフェイス	<code>speed auto [{10 100} [1000]]</code>	auto	速度が auto に設定されている場合は、 duplex を設定できません。 速度が 10 または 100 に設定されている場合に、デュプレックスを設定しないと、デュプレックスはデフォルトで half に設定されます。 速度が 10 または 100 に設定されている場合に、インターフェイスはデフォルトで強制的に半二重に設定されません。
100 Mbps ファイバモジュール	出荷時の設定	該当なし	
ギガビットイーサネット モジュール	<code>speed [1000 nonegotiate]</code>	速度が 1000 であるか、またはネゴシエーションがイネーブルです。	速度、デュプレックス、フロー制御、およびクロッキングのネゴシエーションがイネーブルです。
10 Mbps ポート	出荷時の設定	該当なし	

インターフェイスの `speed` および `duplex` コマンドを手動で設定し、**speed auto** 以外の値（10 または 100 Mbps など）を入力する場合は、接続先インターフェイスの `speed` コマンドを適合する速度に設定してください。ただし、**auto** キーワードは使用しないでください。

10/100 Mbps または 10/100/1000 Mbps イーサネット インターフェイスでイーサネット インターフェイス速度を **auto** に設定すると、速度およびデュプレックスが両方とも自動ネゴシエーションされます。

ギガビット イーサネット インターフェイスは全二重通信専用です。ギガビット イーサネット インターフェイス、またはギガビット イーサネット用に設定された 10/100/1000 Mps インターフェイス上では、デュプレックス モードを変更できません。

インターフェイス速度を手動で 10 または 100 Mbps に設定すると、インターフェイスのデュプレックス モードを設定するように指示するプロンプトが表示されます。



(注)

Catalyst 6500 シリーズスイッチは、いずれかの接続先インターフェイスが **auto** 以外の値に設定されている場合、インターフェイスの速度およびデュプレックス モードを自動ネゴシエーションできません。

**注意**

インターフェイス速度およびデュプレックス モードを変更すると、インターフェイスがシャットダウンされてから再設定時に再びイネーブルになる場合があります。

ポート速度が 1000 に設定されている場合は、デュプレックス モードを **half** に設定できません。同様に、モードが半二重に設定されている場合は、ポート速度を **1000** に設定できません。また、ポート速度が **auto** に設定されている場合は、**duplex** コマンドは拒否されます。

表 2-94 で、**duplex** コマンドおよび **speed** コマンド間の関係を説明します。

表 2-94 duplex コマンドと speed コマンドの関係

duplex コマンド	speed コマンド	システム アクション
duplex half または duplex full	speed auto	速度とデュプレックス モードの両方を自動ネゴシエーションします。
duplex half	speed 10	強制的に 10 Mbps および半二重になります。
duplex full	speed 10	強制的に 10 Mbps および全二重になります。
duplex half	speed 100	強制的に 100 Mbps および半二重になります。
duplex full	speed 100	強制的に 100 Mbps および全二重になります。
duplex full	speed 1000	強制的に 1000 Mbps および全二重になります。

例

次に、100 Mbps で伝送するようにインターフェイスを設定する例を示します。

```
Router(config-if)# speed 100
Router(config-if)#
```

関連コマンド

コマンド	説明
duplex	インターフェイス上でデュプレックス操作を設定します。
interface	設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
show interfaces	特定のインターフェイスで認識されるトラフィックを表示します。

squeeze

フラッシュ ファイル システムをスクイーズしてフラッシュ ファイルを永続的に削除するには、**squeeze** コマンドを使用します。

squeeze filesystem:

シンタックスの説明	filesystem: フラッシュ ファイル システムを指定します。有効値は bootflash: および flash: です。
------------------	---

コマンドのデフォルト	このコマンドにはデフォルト設定がありません。
-------------------	------------------------

コマンドモード	特権 EXEC
----------------	---------

コマンドの履歴	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>12.2(18)ZY</td> <td>このコマンドのサポートが追加されました。</td> </tr> </tbody> </table>	リリース	変更内容	12.2(18)ZY	このコマンドのサポートが追加されました。
リリース	変更内容				
12.2(18)ZY	このコマンドのサポートが追加されました。				

使用上のガイドライン	フラッシュ メモリが満杯の場合は、[deleted] とマークされたファイルによって使用されているスペースを再利用できるように、ファイルを再配置する必要があります。
-------------------	--

squeeze コマンドを入力すると、すべての有効なファイルはフラッシュ メモリの先頭にコピーされ、[deleted] とマークされたファイルは全部消去されます。削除されたファイルの回復はできませんが、再利用されるフラッシュ メモリ スペースに書き込むことはできます。

squeeze コマンドを使用すると、削除されたファイルを消去するだけでなく、[error] とマークされたすべてのファイルを消去することもできます。エラー ファイルは、ファイル書き込みに失敗した場合（装置がいっぱいの場合など）に作成されます。エラー ファイルを消去するには、**squeeze** コマンドを使用する必要があります。スクイーズ動作は、フラッシュ メモリ スペースのほぼ全体で消去および書き込みが行われるため、数分間かかることがあります。

filesystem を入力するときは、コロンが必要です。

例	次に、[deleted] とマークされたファイルをフラッシュ メモリから永続的に消去する例を示します。
----------	---

```
Router # squeeze flash:
Router #
```

関連コマンド	<table border="1"> <thead> <tr> <th>コマンド</th> <th>説明</th> </tr> </thead> <tbody> <tr> <td>delete</td> <td>フラッシュ メモリ デバイスまたは NVRAM からファイルを削除します。</td> </tr> <tr> <td>dir</td> <td>ファイル システムのファイル リストを表示します。</td> </tr> <tr> <td>undelete</td> <td>フラッシュ ファイル システムで [delete] マークが付いたファイルを回復します。</td> </tr> </tbody> </table>	コマンド	説明	delete	フラッシュ メモリ デバイスまたは NVRAM からファイルを削除します。	dir	ファイル システムのファイル リストを表示します。	undelete	フラッシュ ファイル システムで [delete] マークが付いたファイルを回復します。
コマンド	説明								
delete	フラッシュ メモリ デバイスまたは NVRAM からファイルを削除します。								
dir	ファイル システムのファイル リストを表示します。								
undelete	フラッシュ ファイル システムで [delete] マークが付いたファイルを回復します。								

stack-mib portname

ポートに名前文字列を指定するには、**stack-mib portname** コマンドを使用します。

stack-mib portname portname

シンタックスの説明

<i>portname</i>	ポートの名前
-----------------	--------

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

stack-mib コマンドを使用してポートに名前文字列を設定する処理は、CISCO-STACK-MIB の portTable 内の portName MIB オブジェクトに対応します。portName は CISCO-STACK-MIB の portTable 内の MIB オブジェクトです。このオブジェクトは、インターフェイスの機能を示す説明文として設定できます。

例

次に、ポートに名前を設定する例を示します。

```
Router(config-if)# stack-mib portname portal_to_paradise  
Router(config-if)#
```

standby delay minimum reload

HSRP グループを初期化するまでの遅延期間を設定するには、**standby delay minimum reload** コマンドを使用します。遅延期間をディセーブルにするには、このコマンドの **no** 形式を使用します。

standby delay minimum [*min-delay*] **reload** [*reload-delay*]

no standby delay minimum [*min-delay*] **reload** [*reload-delay*]

シンタックスの説明	
<i>min-delay</i>	(任意) インターフェイスの起動後に HSRP グループの初期化を遅らせる最小時間 (秒数)。この最小遅延期間は、以降のすべてのインターフェイス イベントに適用されます。
<i>reload-delay</i>	(任意) ルータのリロード後の遅延時間 (秒数)。この遅延時間は、ルータのリロード後の最初のインターフェイス起動イベントだけに適用されます。

コマンドのデフォルト デフォルト設定は次のとおりです。

- *min-delay* は **1** 秒です。
- *reload-delay* は **5** 秒です。

コマンド モード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン アクティブ ルータに障害が発生するか、またはネットワークから取り除かれた場合は、スタンバイ ルータが自動的に新規のアクティブ ルータになります。元のアクティブ ルータがオンライン状態に戻った場合は、**standby preempt** コマンドを使用して、このルータにアクティブ ルータとしての機能を引き継がせるかどうかを制御できます。

ただし、**standby preempt** コマンドが設定されていない場合でも、元のアクティブ ルータをリロードしてオンライン状態に戻すと、このルータはアクティブ ルータとしての機能を再開します。HSRP グループの初期化の遅延期間を設定するには、**standby delay minimum reload** コマンドを使用します。このコマンドを使用すると、ルータがアクティブな機能を再開するまで、パケットの通過を許可する時間を設定できます。

standby timers コマンドがミリ秒単位で設定されている場合、またはスイッチの特定の VLAN インターフェイスに HSRP が設定されている場合は、**standby delay minimum reload** コマンドを使用することを推奨します。

ほとんどの設定では、デフォルト値により、パケットが通過する十分な期間が設定されます。これより長い遅延期間を設定する必要はありません。

HSRP パケットがインターフェイスに着信すると、遅延はキャンセルされます。

■ standby delay minimum reload

例

次に、最小遅延期間を 30 秒に、最初のリロード後の遅延期間を 120 秒に設定する例を示します。

```
Router(config-if) # standby delay minimum 30 reload 120  
Router(config-if) #
```

関連コマンド

コマンド	説明
show standby delay	遅延期間に関する HSRP 情報を表示します。
standby preempt	HSRP プリエンプションおよびプリエンプション遅延を設定します。
standby timers	hello パケットの間隔と、他のルータがアクティブ ホット スタンバイまたはスタンバイ ルータの終了を宣言するまでの時間を設定します。

standby track

他のインターフェイスの利用状況に基づいてホットスタンバイプライオリティが変更されるようにインターフェイスを設定するには、**standby track** コマンドを使用します。グループのすべてのトラッキング設定を削除するには、このコマンドの **no** 形式を使用します。

```
standby [group-number] track {interface-type interface-number | designated-router}
[priority-decrement]
```

```
no standby group-number track
```

シンタックスの説明

<i>group-number</i>	(任意) トラッキングが適用されるインターフェイス上のグループ番号。有効値は、0 ~ 255 です。
<i>interface-type</i> <i>interface-number</i>	トラッキングするインターフェイス タイプおよび番号
designated-router	指定ルータの指定が解除された場合に、アクティブ HSRP ルータが指定ルータになるように指定します。
<i>priority-decrement</i>	(任意) インターフェイスがダウン (または回復) したときに、ルータのホットスタンバイプライオリティを減分 (または増分) する値

コマンドのデフォルト

デフォルト設定は次のとおりです。

- *group* は **0** です。
- *priority-decrement* は **10** です。
- **designated-router** キーワードはディセーブルです。

コマンドモード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

designated-router キーワードを入力する前に、新規の指定ルータが引き継ぐ現行の指定ルータより高い HSRP プライオリティを保有していることを確認する必要があります。

トラッキングされたインターフェイスがダウンすると、ホットスタンバイプライオリティが *priority-decrement* 引数によって指定された数だけ減分します。インターフェイスがトラッキングされていなければ、ステートが変化した場合でもホットスタンバイプライオリティに影響することはありません。ホットスタンバイに設定された各インターフェイスには、トラッキングするインターフェイスのリストを別々に設定できます。

トラッキングされたインターフェイスが複数ダウンした場合、*priority-decrement* 値が設定されているかどうかに関係なく、減分值が下がっていきます。

インターフェイスで IP アドレスがディセーブルに設定されていると、トラッキングされたインターフェイスはダウンしていると見なされます。

このコマンドの **no** 形式を使用する場合は、*group-number* を入力する必要があります。

インターフェイスをトラッキングするのに HSRP を設定し、そのインターフェイスが OIR 動作に備えて物理的に削除されている場合、HSRP はインターフェイスが常にダウンしていると見なします。

HSRP インターフェイス トラッキング設定は削除できません。この状態を防ぐには、インターフェイスを物理的に削除する前に **no standby track interface-type interface-number** コマンドを使用します。

group-number に **0** を入力する場合、NVRAM にはグループ番号が書き込まれず、下位互換性が提供されます。

例

次に、特定のインターフェイス上でグループ 1 をトラッキングする HSRP をイネーブルにする例を示します。

```
Router(config-if)# standby 1 track Ethernet0/2
Router(config-if)#
```

次に、指定ルータの指定が解除された場合に、アクティブ HSRP ルータが指定ルータになるように指定する例を示します。

```
Router(config-if)# standby 1 track designated-router 15
Router(config-if)#
```

関連コマンド

コマンド	説明
show standby	HSRP 情報を表示します。

standby use-bia

割り当て済みの MAC アドレス（イーサネットおよび FDDI 上）または機能アドレス（トークンリング上）の代わりに、インターフェイスの Burned-In Address を仮想 MAC アドレスとして使用するよう HSRP を設定するには、**standby use-bia** コマンドを使用します。デフォルトの仮想 MAC アドレスに戻すには、このコマンドの **no** 形式を使用します。

standby use-bia [scope interface]

no standby use-bia

シンタックスの説明

scope interface (任意) 主要インターフェイスの代わりに入力されたサブインターフェイスに対して、このコマンドを設定します。

コマンドのデフォルト

HSRP は、イーサネットおよび FDDI では割り当て済みの MAC アドレスを、トークンリングでは機能アドレスを使用します。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、PFC 2 が搭載された Catalyst 6500 シリーズ スイッチではサポートされていません。PFC2 は、最大 16 の一意の HSRP グループ番号をサポートします。異なる VLAN 上で同じ HSRP グループ番号を使用できます。17 個以上の HSRP グループを設定する場合、この制約により、VLAN 番号を HSRP グループ番号としては使用できません。



(注)

同じ番号の HSRP グループは、同じ仮想 MAC アドレスを使用するため、ブリッジグループを設定する場合にエラーが発生することがあります。

ハードウェア レイヤ 3 スイッチングは、次の入力および出力カプセル化をサポートします。

- イーサネット V2.0 (ARPA)
- 1 バイト コントロールを使用する 802.2 対応の 802.3 (SAP1)
- 802.2 対応の 802.3 および SNAP

ハードウェア レイヤ 3 スイッチングは永続的にイネーブルです。したがって設定作業は不要です。

例

次に、仮想 IP アドレスにマッピングされる仮想 MAC アドレスとして、インターフェイスの Burned-In Address を使用するよう HSRP を設定する例を示します。

```
Router(config-if) # standby use-bia
Router(config-if) #
```

storm-control level

抑制レベルを設定するには、**storm-control level** コマンドを使用します。抑制モードをオフにするには、このコマンドの **no** 形式を使用します。

```
storm-control {broadcast | multicast | unicast} level level[.level]
```

```
no storm-control {broadcast | multicast | unicast} level
```

シンタックスの説明

broadcast	ブロードキャスト トラフィックを指定します。
multicast	マルチキャスト トラフィックを指定します。
unicast	ユニキャスト トラフィックを指定します。
<i>level</i>	整数の抑制レベル。有効値は 0 ~ 100% です。
<i>.level</i>	(任意) フラクショナル抑制レベル。有効値は 0 ~ 99 です。

コマンドのデフォルト

すべてのパケットが通過します。

コマンドモード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、スイッチ ポートおよびルータ ポートに入力できます。

インターフェイス上でトラフィック ストーム制御をイネーブルにし、トラフィック ストーム制御レベルを設定し、インターフェイス上でイネーブル化されたすべてのトラフィック ストーム制御モードにトラフィック ストーム制御レベルを適用するには、**storm-control level** コマンドを入力します。

3 つの抑制モードすべてで共有される抑制レベルは、1 つだけです。たとえば、ブロードキャスト レベルを 30 に設定し、マルチキャスト レベルを 40 に設定した場合は、両方のレベルがイネーブルになり、それぞれ 40 に設定されます。

Catalyst 6500 シリーズ スイッチは、ギガビットおよび 10 ギガビット イーサネット LAN ポート上だけでマルチキャストおよびユニキャスト トラフィックのストーム制御をサポートします。ブロードキャスト トラフィックのストーム制御はすべての LAN ポート上でサポートされます。

multicast および **unicast** キーワードは、ギガビットおよび 10 ギガビット イーサネット LAN ポートだけでサポートされます。ユニキャストおよびマルチキャスト抑制は、WS-X6148A-RJ-45 および WS-X6148-SFP モジュールでもサポートされています。

フラクショナル抑制レベルを入力するときは、ピリオドが必要です。

抑制レベルは、合計帯域幅に対するパーセントとして入力します。しきい値が 100% であれば、トラフィックに対して制限が課せられていないことになります。しきい値が 0 または 0.0 (フラクショナル) % であれば、指定されたすべてのトラフィックは、ポート上でブロックされることになります。次の注意事項を参照してください。

- フラクショナル レベルの値が 0.33 以下の場合、次のモジュール上では 0.0 の場合と同様になります。
 - WS-X6704-10GE
 - WS-X6748-SFP
 - WS-X6724-SFP
 - WS-X6748-GE-TX
- ポート上の指定されたすべてのトラフィックをブロックするには、その他すべてのモジュールで 0 を入力します。

廃棄数を表示するには、**show interfaces counters broadcast** コマンドを入力します。

イネーブル化された抑制モードおよびレベル設定を表示するには、**show running-config** コマンドを入力します。

指定されたトラフィック タイプの抑制をオフにするには、次のいずれかを実行します。

- 指定されたトラフィック タイプの *level* を 100% に設定します。
- このコマンドの **no** 形式を使用します。

例

次に、抑制モードをイネーブルにして、抑制レベルを設定する例を示します。

```
Router(config-if)# storm-control broadcast level 30
Router(config-if)#
```

次に、抑制モードをディセーブルにする例を示します。

```
Router(config-if)# no storm-control multicast level
Router(config-if)#
```

関連コマンド

コマンド	説明
show interfaces counters	物理インターフェイスで認識されるトラフィックを表示します。
show running-config	モジュールまたはレイヤ 2 VLAN のステータスおよび設定を表示します。

switchport

レイヤ 2 スイッチド インターフェイスのスイッチング特性を変更するには、**switchport** コマンドを使用します (パラメータを指定しません)。インターフェイスをルーテッドインターフェイス ステータスに戻して、すべてのレイヤ 2 コンフィギュレーションを消去するには、このコマンドの **no** 形式を使用します (パラメータを指定しません)。スイッチング特性を設定するには、**switchport** コマンドを使用します (パラメータを指定します)。

switchport

switchport {host | nonegotiate}

no switchport

no switchport nonegotiate

シンタックスの説明

host	ホスト接続用にポート設定を最適化します。
nonegotiate	装置がこのインターフェイスのネゴシエーション プロトコルに関係しないように指定します。

コマンドのデフォルト

プラットフォームまたはインターフェイス ハードウェアに対応するデフォルト VLAN は、デフォルトのアクセス VLAN およびトランク インターフェイス ネイティブ VLAN です。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

LAN インターフェイスをレイヤ 2 インターフェイスとして設定するには、キーワードを指定しないで **switchport** コマンドを入力してから、キーワードを指定してさらに **switchport** コマンドを入力する必要があります。この処理は、インターフェイスに対して **switchport** コマンドをまだ入力していない場合だけ必要となります。

no switchport コマンドを入力すると、ポートはシャットダウンされてから再びイネーブルになります。この処理により、ポートに接続された装置上でメッセージが生成されることがあります。

ポート設定を最適化するには、**switchport host** コマンドを入力して、スイッチ ポート モードを **access** に設定し、スパニングツリーの **PortFast** をイネーブルにし、チャンネルのグループ化をディセーブルにします。この設定を実行できるのは、エンドステーション上だけです。

スパニングツリー **PortFast** がイネーブルであるため、単一ホストに接続されたポートだけに、**switchport host** コマンドを入力する必要があります。他の Catalyst 6500 シリーズ スイッチ、ハブ、コンセントレータ、スイッチ、およびブリッジを高速起動ポートに接続すると、一時的にスパニングツリー ループが発生することがあります。

パケット転送を開始するまでの期間を短縮するには、**switchport host** コマンドをイネーブルにします。

switchport nonegotiate コマンドの **no** 形式を使用すると、**nonegotiate** ステータスが削除されます。

nonegotiate キーワードを使用した場合は、インターフェイス上で DISL/DTP ネゴシエーション パケットが送信されません。装置は、指定された **access** または **trunk** の **mode** パラメータによって、トランキングされるかどうかが決まります。**dynamic (auto または desirable)** モードでこのコマンドを実行しようとする、エラーが戻されます。

ポートを SPAN 宛先ポートとして設定するには、ポートを強制的にトランキングさせる必要があります。ポートを強制的にトランキングさせるには、**switchport nonegotiate** コマンドを使用します。

例

次に、ポート インターフェイスがシスコ ルーテッド ポートとしての動作を停止して、レイヤ 2 スイッチド インターフェイスに変換されるように設定する例を示します。

```
Router(config-if)# switchport
Router(config-if)#
```



(注)

シスコ ルーテッド ポートをサポートしないプラットフォームでは、**switchport** コマンドを使用できません。このようなプラットフォームのすべての物理ポートは、レイヤ 2 スイッチド インターフェイスと見なされます。

次に、ホスト接続用にポート設定を最適化する例を示します。

```
Router(config-if)# switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
Router(config-if)#
```

次に、スイッチド インターフェイスとして設定されたポート インターフェイスが、トランキング モードをネゴシエーションしないように制限し、(**mode** の設定に応じて) トランクまたはアクセス ポートとして動作するように設定する例を示します。

```
Router(config-if)# switchport nonegotiate
Router(config-if)#
```

関連コマンド

コマンド	説明
show interfaces switchport	スイッチング (非ルーティング) ポートの管理ステータスおよび動作ステータスを表示します。

switchport access vlan

インターフェイスがアクセス モードのときに VLAN を設定するには、**switchport access vlan** コマンドを使用します。アクセス モード VLAN をデバイスの適切なデフォルト VLAN にリセットするには、このコマンドの **no** 形式を使用します。

switchport access vlan *vlan-id*

no switchport access vlan

シンタックスの説明

<i>vlan-id</i>	インターフェイスがアクセス モードの場合の VLAN を指定します。有効値は 1 ~ 4094 です。
----------------	---

コマンドのデフォルト

デフォルト設定は次のとおりです。

- アクセス VLAN およびトランク インターフェイス ネイティブ VLAN が、プラットフォームまたはインターフェイス ハードウェアに対応するデフォルト VLAN です。
- すべての VLAN リストは VLAN をすべて含みます。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

LAN インターフェイスをレイヤ 2 インターフェイスとして設定するには、キーワードを指定しないで **switchport** コマンドを入力してから、**switchport access vlan** コマンドを入力する必要があります。この処理は、インターフェイスに対して **switchport** コマンドをまだ入力していない場合だけ必要となります。

no switchport コマンドを入力すると、ポートはシャットダウンされてから再びイネーブルになります。この処理により、ポートに接続された装置上でメッセージが生成されることがあります。

アクセス モード VLAN をデバイスに適したデフォルト VLAN にリセットするには、**switchport access vlan** コマンドの **no** 形式を使用します。

例

次に、ポート インターフェイスがシスコルーテッド ポートとしての動作を停止して、レイヤ 2 スイッチド インターフェイスに変換されるように設定する例を示します。

```
Router(config-if)# switchport
Router(config-if)#
```



(注)

シスコルーテッド ポートをサポートしないプラットフォームでは、**switchport** コマンドを使用できません。このようなプラットフォームのすべての物理ポートは、レイヤ 2 スイッチド インターフェイスと見なされます。

次に、すでにスイッチド インターフェイスとして設定されたポート インターフェイスが、インターフェイス コンフィギュレーション モードで、プラットフォームのデフォルト VLAN ではなく VLAN 2 で動作するように設定する例を示します。

```
Router(config-if)# switchport access vlan 2
Router(config-if)#
```

関連コマンド

コマンド	説明
show interfaces	スイッチング（非ルーティング）ポートの管理ステータスおよび動作ステータスを表示します。
switchport	

switchport autostate exclude

VLAN インターフェイスのリンクアップ計算からポートを除くには、**switchport autostate exclude** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport autostate exclude

no switchport autostate exclude

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

すべてのポートが VLAN インターフェイスのリンクアップ計算に含まれます。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

LAN インターフェイスをレイヤ 2 インターフェイスとして設定するには、キーワードを指定しないで **switchport** コマンドを入力してから、さらに **switchport autostate exclude** コマンドを入力する必要があります。この処理は、インターフェイスに対して **switchport** コマンドをまだ入力していない場合だけ必要となります。



(注)

シスコ ルーテッド ポートをサポートしないプラットフォームでは、**switchport** コマンドを使用できません。このようなプラットフォームのすべての物理ポートは、レイヤ 2 スイッチド インターフェイス と見なされます。

PISA 上に設定された VLAN インターフェイスは、関連付けられた VLAN で転送しているポートがある場合に、アップの状態と見なされます。VLAN 上のすべてのポートがダウンまたはブロックしている場合は、PISA 上の VLAN インターフェイスはダウンしていると思なされます。アップの状態と考えられる VLAN インターフェイスについては、VLAN 内のすべてのポートがアップ状態で、転送している必要があります。**switchport autostate exclude** コマンドを入力すれば、VLAN インターフェイスのリンクアップ計算からポートを除くことができます。

switchport autostate exclude コマンドは、複数のポートが VLAN にある場合に、VLAN インターフェイスのリンクアップ計算から除くポートをマークします。

show interface interface switchport コマンドは、モードが設定されている場合に、自動ステート モードを表示します。モードが設定されていないと、自動ステート モードが表示されません。

例 次に、VLAN インターフェイスのリンクアップ計算からポートを除く例を示します。

```
Router(config-if)# switchport autostate exclude  
Router(config-if)#
```

次に、VLAN インターフェイスのリンクアップ計算にポートを加える例を示します。

```
Router(config-if)# no switchport autostate exclude  
Router(config-if)#
```

関連コマンド

コマンド	説明
show interfaces switchport	スイッチング（非ルーティング）ポートの管理ステータスおよび動作ステータスを表示します。

switchport backup

Flexlink バックアップ インターフェイスとしてインターフェイスを設定するには、**switchport backup** コマンドを使用します。Flexlink をディセーブルにするには、このコマンドの **no** 形式を使用します。

switchport backup interface interface-type interface-number

no switchport backup interface interface-type interface-number

シンタックスの説明

interface interface-type interface-number Flexlink バックアップ インターフェイスとして設定するインターフェイスタイプ、およびモジュールとポート番号を指定します。

コマンドのデフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

Flexlink をイネーブルにする場合、アクティブ リンクおよびスタンバイ リンクの両方が物理的にアップの状態になり、相互のバックアップが提供されます。

Flexlink はレイヤ 2 インターフェイスだけでサポートされ、ルーテッド ポートをサポートしません。

Flexlink は、復旧後に元のアクティブ インターフェイスに切り替わりません。

interface-number はモジュールおよびポート番号を指定します。有効値は、使用するシャーシおよびモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合、スロット番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 です。

Flexlink は、簡易アクセス トポロジー（リーフ ノードからの 2 つのアップリンク）用に設計されています。配線クローゼットとディストリビューション/コア ネットワーク間にループが存在しないようにし、Flexlink が正常に動作するようにする必要があります。

Flexlink は、直接接続されたリンク障害に対してだけ高速コンバージェンスを提供します。他のネットワーク障害は、Flexlink 高速コンバージェンスで改善されません。

LAN インターフェイスをレイヤ 2 インターフェイスとして設定するには、キーワードを指定しないで **switchport** コマンドを入力してから、さらに **switchport autostate exclude** コマンドを入力する必要があります。この処理は、インターフェイスに対して **switchport** コマンドをまだ入力していない場合だけ必要となります。



(注)

シスコルーテッド ポートをサポートしないプラットフォームでは、**switchport** コマンドを使用できません。このようなプラットフォームのすべての物理ポートは、レイヤ 2 スイッチド インターフェイスと見なされます。

例

次に、インターフェイス上で Flexlink をイネーブルにする例を示します。

```
Router(config-if)# switchport backup interface fastethernet 4/1  
Router(config-if)#
```

次に、インターフェイス上で Flexlink をディセーブルにする例を示します。

```
Router(config-if)# switchport backup interface fastethernet 4/1  
Router(config-if)#
```

関連コマンド

コマンド	説明
show interfaces	Flexlink ペアを表示します。
switchport backup	

switchport block unicast

未知のユニキャスト パケットの転送を禁止するには、**switchport block unicast** コマンドを使用します。未知のユニキャスト パケットの転送を許可するには、このコマンドの **no** 形式を使用します。

switchport block unicast

no switchport block unicast

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- 未知のユニキャスト トラフィックはブロックされません。
- 未知の MAC アドレスを持つすべてのトラフィックがすべてのポートに送信されます。

コマンドのデフォルト

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

スイッチ ポート上で未知のユニキャスト トラフィックをブロックできます。

未知のユニキャスト トラフィックのブロッキングは、スイッチ ポート上で自動的にイネーブルにはなりません。明示的に設定する必要があります。



(注)

パケットのブロッキングの詳細については、『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*』を参照してください。

設定を確認するには、**show interfaces interface-id switchport** コマンドを入力します。

例

次に、インターフェイス上で未知のユニキャスト トラフィックをブロックする例を示します。

```
Router(config-if)# switchport block unicast
Router(config-if)#
```

関連コマンド

コマンド	説明
show interfaces switchport	スイッチング (非ルーティング) ポートの管理ステータスおよび動作ステータスを表示します。

switchport capture

VACL でフィルタリングされたトラフィックをキャプチャするようにポートを設定するには、**switchport capture** コマンドを使用します。ポート上でキャプチャ モードをディセーブルにするには、このコマンドの **no** 形式を使用します。

switchport capture

no switchport capture

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト ディセーブル

コマンド モード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

LAN インターフェイスをレイヤ 2 スイッチド インターフェイスとして設定するには、キーワードを指定しないで **switchport** コマンドを入力してから、キーワードを指定してさらに **switchport** コマンドを入力する必要があります。この処理は、インターフェイスに対して **switchport** コマンドをまだ入力していない場合だけ必要となります。

NAM の VACL キャプチャ機能は Supervisor Engine 720 上でサポートされますが、IDS-M-2 ではサポートされません。

switchport capture コマンドはレイヤ 2 スイッチド インターフェイスだけに適用されます。

WAN インターフェイスは、VACL のキャプチャ機能だけをサポートします。

no switchport コマンドを入力すると、ポートはシャットダウンされてから再びイネーブルになります。この処理により、ポートに接続された装置上でメッセージが生成されることがあります。

switchport capture コマンドを入力するとインターフェイスにキャプチャ機能が設定され、キャプチャ ビットが設定されたパケットがインターフェイスで受信されるようになります。

switchport capture および **switchport capture allowed vlan** コマンドの入力順に制約はありません。ポートをキャプチャ ポートに設定するには、**switchport capture** コマンドを（引数の指定をせずに）入力する必要があります。

キャプチャ ポートでは、キャプチャされたパケットの宛先 VLAN を許可する必要があります。キャプチャ ポートをイネーブルにすると、デフォルトですべての VLAN からのパケットが許可されます。キャプチャ ポートに本来設定されていたモードが解除され、キャプチャ モードからモニタ モードに変わります。モニタ モードでは、キャプチャ ポートは以下ようになります。

- 以前に属していた VLAN に属しません。
- 着信トラフィックを許可しません。

switchport capture

- トランキング カプセル化が ISL または 802.1Q であった場合に、トランク ポートからキャプチャ ポートをイネーブルにすると、キャプチャ ポートのカプセル化が保護されます。キャプチャされた パケットは、対応するカプセル化タイプによってカプセル化されます。アクセス ポートからキャプチャ ポートをイネーブルにした場合は、キャプチャされたパケットはカプセル化されません。
- **no switchport capture** コマンドを入力してキャプチャ機能をディセーブルにすると、ポートは以前に設定されていたモード（アクセスまたはトランク）に戻ります。
- パケットがキャプチャされるのは、宛先 VLAN がキャプチャ ポート上で許可されている場合だけです。

例

次に、VACL でフィルタリングされたトラフィックをキャプチャするようにインターフェイスを設定する例を示します。

```
Router(config-if)# switchport capture
Router(config-if)#
```

関連コマンド

コマンド	説明
show interfaces switchport	スイッチング（非ルーティング）ポートの管理ステータスおよび動作ステータスを表示します。
switchport capture allowed vlan	VACL でフィルタリングされたトラフィックの宛先 VLAN を指定します。

switchport capture allowed vlan

VACL でフィルタリングされたトラフィックの宛先 VLAN を指定するには、**switchport capture allowed vlan** コマンドを使用します。設定された宛先 VLAN リストを消去して、デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
switchport capture allowed vlan {add | all | except | remove} vlan-id
[,vlan-id[,vlan-id[,...]]
```

```
no switchport capture allowed vlan
```

シンタックスの説明

add	現在のリストに指定された VLAN を追加します。
all	現在のリストにすべての VLAN を追加します。
except	指定された VLAN を除くすべての VLAN を追加します。
remove	現在のリストから指定された VLAN を削除します。
<i>vlan-id</i>	ポートがキャプチャ モードの場合の許可 VLAN の VLAN ID。有効値は 1 ～ 4094 です。

コマンドのデフォルト

all

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

LAN インターフェイスをレイヤ 2 スイッチド インターフェイスとして設定するには、キーワードを指定しないで **switchport** コマンドを入力してから、キーワードを指定してさらに **switchport** コマンドを入力する必要があります。この処理は、インターフェイスに対して **switchport** コマンドをまだ入力していない場合だけ必要となります。

switchport capture allowed vlan コマンドはレイヤ 2 スイッチド インターフェイスだけに適用されます。

no switchport コマンドを入力すると、ポートはシャットダウンされてから再びイネーブルになります。この処理により、ポートに接続された装置上でメッセージが生成されることがあります。

vlan-id は、単一の VLAN、VLAN グループ、またはその両方として入力できます。たとえば、**switchport capture allowed vlan 1-1000, 2000, 3000-3100** のようになります。

switchport capture および **switchport capture allowed vlan** コマンドの入力順に制約はありません。ポートをキャプチャ ポートに設定するには、**switchport capture** コマンドを（引数の指定をせずに）入力する必要があります。

WAN インターフェイスは、VACL のキャプチャ機能だけをサポートします。

switchport capture allowed vlan

例

次に、指定された VLAN を追加して、VACL でフィルタリングされたトラフィックをキャプチャする例を示します。

```
Router(config-if)# switchport capture allowed vlan add 100  
Router(config-if)#
```

関連コマンド

コマンド	説明
show interfaces switchport	スイッチング（非ルーティング）ポートの管理ステータスおよび動作ステータスを表示します。

switchport dot1q ethertype

インターフェイスにプログラミングする EtherType 値を指定するには、**switchport dot1q ethertype** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport dot1q ethertype value

シンタックスの説明 *value* 802.1Q カプセル化の EtherType 値。有効値は 0x600 ~ 0xFFFF です。

コマンドのデフォルト *value* は 0x8100 です。

コマンドモード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン カスタム EtherType フィールド値をトランク ポートおよびアクセス ポートで設定できます。各ポートがサポートする EtherType フィールド値は 1 つだけです。カスタム EtherType フィールド値で設定されたポートは、他の EtherType フィールド値を持つフレームをタグ付きフレームとして認識しません。



注意

カスタム EtherType フィールド値で設定されたポートは、他の EtherType フィールド値を持つフレームをタグなしフレームとして認識します。カスタム EtherType フィールド値で設定されたトランク ポートは、他の EtherType フィールド値でタグ付けされたフレームをネイティブ VLAN 内に入れます。カスタム EtherType フィールド値で設定されたアクセス ポートまたはトンネル ポートは、他の EtherType フィールド値でタグ付けされたフレームをアクセス VLAN 内に入れます。

カスタム EtherType フィールド値は、次のモジュールで設定できます。

- スーパーバイザ エンジン
- WS-X6516A-GBIC
- WS-X6516-GBIC



(注) WS-X6516A-GBIC および WS-X6516-GBIC モジュールは、設定されたカスタム EtherType フィールド値を、各ポート ASIC によりサポートされるすべてのポートに適用します (1 ~ 8 および 9 ~ 16)。

- WS-X6516-GE-TX

カスタム EtherType フィールド値は、EtherChannel 内のポートでは設定できません。

EtherChannel は、カスタム EtherType フィールド値で設定されたポートから構成することはできません。

■ switchport dot1q ethertype

例

次に、インターフェイスでプログラミングされる EtherType 値を設定する例を示します。

```
Router (config-if)# switchport dot1q ethertype 1234  
Router (config-if)#
```

関連コマンド

コマンド	説明
show interfaces	スイッチング（非ルーティング）ポートの管理ステータスおよび動作ステータスを表示します。
switchport	

switchport mode

インターフェイス タイプを設定するには、**switchport mode** コマンドを使用します。モードを、デバイスに適したデフォルト モードにリセットするには、このコマンドの **no** 形式を使用します。

switchport mode {access | trunk | {dynamic {auto | desirable}} | dot1q-tunnel}

switchport mode private-vlan {host | promiscuous}

no switchport mode

no switchport mode private-vlan

シンタックスの説明

access	単一の非トランキング、タグなし VLAN レイヤ 2 インターフェイスを指定します。
trunk	レイヤ 2 のトランキング VLAN インターフェイスを指定します。
dynamic auto	リンクからトランク リンクに変換されるインターフェイスを指定します。
dynamic desirable	リンクからトランク リンクへの変換を積極的に試行するインターフェイスを指定します。
dot1q-tunnel	802.1Q トンネリング インターフェイスを指定します。
private-vlan host	アクティブ ホストの PVLAN ポートになる PVLAN とのアソシエーションが有効であるポートを指定します。
private-vlan promiscuous	アクティブ混合モード ポートになる PVLAN とのマッピングが有効であるポートを指定します。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- モードはプラットフォームごとに異なります。配線クローゼット用のプラットフォームでは **dynamic auto** に、バックボーン スイッチ用のプラットフォームでは **dynamic desirable** になります。
- PVLAN ポートに設定されたモードはありません。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

access モードを開始した場合、インターフェイスは永続的な非トランキング モードになり、近接インターフェイスがリンクから非トランク リンクへの変換に合意しない場合でも、この変換を行うようにネゴシエートします。

trunk モードを開始した場合、インターフェイスは永続的なトランキング モードになり、近接インターフェイスがリンクからトランク リンクへの変換に合意しない場合でも、この変換を行うようにネゴシエートします。

dynamic auto モードを開始した場合に、近接インターフェイスが **trunk** または **desirable** モードに設定されると、インターフェイスはリンクをトランク リンクに変換します。

dynamic desirable モードを開始した場合に、近接インターフェイスが **trunk**、**desirable**、または **auto** モードに設定されると、インターフェイスはトランク インターフェイスになります。

ポートが混合モード ポートまたはホスト PVLAN ポートとして設定されていて、次のいずれかの条件が適用される場合、ポートは非アクティブになります。

- ポートに PVLAN との有効なアソシエーションがない、またはマッピングが設定されていない。
- ポートが SPAN 宛先である。

プライベート ポートの PVLAN とのアソシエーションまたはマッピングを削除するか、またはプライベート ポートを SPAN 宛先として設定した場合、削除されたプライベート ポートの PVLAN とのアソシエーションやマッピング、または SPAN 宛先として設定されたプライベート ポートは非アクティブになります。

dot1q-tunnel モードを開始した場合、プロトコル トンネリング インターフェイス上で BPDU フィルタリングがイネーブルになり、CDP がディセーブルになります。

例

次に、インターフェイスを **dynamic desirable** モードに設定する例を示します。

```
Router(config-if)# switchport mode dynamic desirable
Router(config-if)#
```

次に、ポートを PVLAN ホスト モードに設定する例を示します。

```
Router(config-if)# switchport mode private-vlan host
Router(config-if)#
```

次に、ポートを PVLAN 混合 モードに設定する例を示します。

```
Router(config-if)# switchport mode private-vlan promiscuous
Router(config-if)#
```

関連コマンド

コマンド	説明
show dot1q-tunnel	802.1Q トンネル対応ポートのリストを表示します。
show interfaces switchport	スイッチング (非ルーティング) ポートの管理ステータスおよび動作ステータスを表示します。
switchport	レイヤ 2 スイッチド インターフェイスのスイッチング特性を変更します。
switchport private-vlan host-association	レイヤ 2 スイッチド インターフェイスのスイッチング特性を変更します。
switchport private-vlan mapping	混合モード ポートの PVLAN マッピングを定義します。

switchport port-security

ポート セキュリティをインターフェイスでイネーブルにするには、**switchport port-security** コマンドを使用します。ポート セキュリティをディセーブルにするには、このコマンドの **no** 形式を使用します。

switchport port-security

no switchport port-security

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト ディセーブル

コマンド モード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン ポート セキュリティを設定する場合は、次の注意事項に従ってください。

- ポート セキュリティはトランク上でサポートされています。
- ポート セキュリティは 802.1Q トンネル ポート上でサポートされています。
- セキュア ポートは、Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) の宛先ポートにできません。
- セキュア ポートは、EtherChannel に所属できません。
- セキュア ポートはトランク ポートにできません。
- セキュア ポートは、802.1X ポートにできません。セキュア ポートで 802.1X をイネーブルにしようとする、エラー メッセージが表示され、802.1X はイネーブルになりません。802.1X 対応ポートをセキュア ポートに変更しようとする、エラー メッセージが表示され、セキュリティ設定は変更されません。

例 次に、ポート セキュリティをイネーブルにする例を示します。

```
Router(config-if)# switchport port-security  
Router(config-if)#
```

次に、ポート セキュリティをディセーブルにする例を示します。

```
Router(config-if)# no switchport port-security  
Router(config-if)#
```

■ switchport port-security

関連コマンド

コマンド	説明
show port-security	ポート セキュリティ設定に関する情報を表示します。

switchport port-security aging

ポート セキュリティ エージングを設定するには、**switchport port-security aging** コマンドを使用します。エージングをディセーブルにするには、このコマンドの **no** 形式を使用します。

switchport port-security aging **{time time}** | **{type {absolute | inactivity}}**

シンタックスの説明	パラメータ	説明
	time time	すべてのアドレスが保護される期間を設定します。有効値は 1 ~ 1440 分です。
	type	エージングのタイプを指定します。
	absolute	絶対エージングを指定します。詳細については、「使用上のガイドライン」を参照してください。
	inactivity	トラフィックがないときだけタイマーの実行を開始することを指定します。詳細については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト デフォルト設定は次のとおりです。

- ディセーブル
- イネーブルの場合、デフォルトは次のとおりです。
 - *time* は 0 です。
 - *type* は **absolute** です。

コマンドのデフォルト インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン ポート セキュリティを設定する場合は、次の注意事項に従ってください。

- ポート セキュリティはトランク上でサポートされています。
- ポート セキュリティは 802.1Q トンネル ポート上でサポートされています。
- セキュア ポート上で自動的に学習されたアドレスについては、2 つのタイプのエージングのいずれかを適用できます。
- 絶対エージングでは、トラフィック パターンに関係なく、エージング タイムを超えると MAC アドレスがタイムアウトになります。このデフォルトはすべてのセキュア ポートに適用され、エージング タイムは 0 に設定されます。
- 非アクティビティ エージングでは、対応するホストからの非アクティビティがエージング タイムを超えると、MAC アドレスがタイムアウトになります。

例 次に、エージング タイムを 2 時間に設定する例を示します。

```
Router(config-if)# switchport port-security aging time 120
Router(config-if)#
```

■ switchport port-security aging

次に、エージング タイムを 2 分に設定する例を示します。

```
Router(config-if)# switchport port-security aging time 2
Router(config-if)#
```

次に、ポートのエージング タイプを絶対エージングに設定する例を示します。

```
Router(config-if) switchport port-security aging type absolute
Router(config-if)#
```

次に、ポートのエージング タイプを非アクティビティに設定する例を示します。

```
Router(config-if) switchport port-security aging type inactivity
Router(config-if)#
```

関連コマンド

コマンド	説明
show port-security	ポート セキュリティ設定に関する情報を表示します。

switchport port-security mac-address

セキュア MAC アドレスのリストに MAC アドレスを追加するには、**switchport port-security mac-address** コマンドを使用します。セキュア MAC アドレス リストから MAC アドレスを削除するには、このコマンドの **no** 形式を使用します。

```
switchport port-security mac-address {mac-addr | {sticky [mac-addr]} [vlan vlan |
vlan-list | {voice | access}]}
```

```
no switchport port-security mac-address {mac-addr | {sticky [mac-addr]} [vlan vlan |
vlan-list | {voice | access}]}
```

シンタックスの説明

mac-addr	インターフェイスの MAC アドレス。有効値は 1 ～ 1024 です。
sticky	インターフェイス上でダイナミック MAC アドレスをスティッキーとして設定します。
vlan vlan vlan-list	(任意) VLAN または VLAN の範囲を指定します。詳細については、「使用上のガイドライン」を参照してください。
access	(任意) アクセス VLAN の MAC アドレスを構成します。
voice	(任意) 音声 VLAN の MAC アドレスを構成します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。
12.2(18)ZYA1	access キーワードおよび voice キーワードが追加されました。

使用上のガイドライン

すべてのインターフェイスのセキュア MAC アドレスの最大数より少ないセキュア MAC アドレスを設定した場合、残りの MAC アドレスはダイナミックに学習されます。

複数の MAC アドレスを削除するには、削除する MAC アドレスごとに、このコマンドの **no** 形式を 1 回ずつ入力する必要があります。

vlan-list 引数は、ポートが設定され、トランクとして動作可能な場合だけ使用できます。**switchport mode trunk** コマンドを入力してから、**switchport nonegotiate** コマンドを入力してください。

sticky キーワードは、インターフェイス上でダイナミック MAC アドレスをスティッキーとして設定します。スティッキー MAC アドレスは、スタティック レイヤ 2 エントリを特定のインターフェイスに固定されるように設定します。この機能により、MAC の移動を防止したり、エントリが別のインターフェイスで学習されるのを防いだりすることができます。

インターフェイス上でポート セキュリティ機能がイネーブルになっていないときでも、スティッキー機能を設定することができます。インターフェイス上でポート セキュリティがイネーブルになると動作可能になります。



(注)

switchport port-security mac-address sticky コマンドは、インターフェイス上でスティッキ機能がイネーブルになっている場合だけ入力することができます。

ポートセキュリティがイネーブルのとき、スティッキ機能をディセーブルにすると、設定済みの学習されたスティッキ アドレスのすべてが設定から削除されて、ダイナミック セキュア アドレスに変換されます。

ポートセキュリティがディセーブルのとき、スティッキ機能をディセーブルにすると、設定済みの学習されたスティッキ アドレスのすべてが設定から削除されます。

Cisco IOS Release 12.2(18)ZYA1 では、**access** キーワードおよび **voice** キーワード導入されており、ポートが構成されている場合で、アクセス ポートとして動作可能な場合だけに、使用可能です。

例

次に、セキュア MAC アドレスを設定する例を示します。

```
Router(config-if)# switchport port-security mac-address 1000.2000.3000
```

次に、アドレス テーブルからセキュア MAC アドレスを削除する例を示します。

```
Router(config-if)# no switchport port-security mac-address 1000.2000.3000
```

次に、Cisco IOS Release 12.2(18)ZYA1 において、音声 VLAN でセキュア MAC アドレスを設定する例を示します。

```
Router(config-if)# switchport port-security mac-address 1000.2000.3000 vlan voice
```

次に、インターフェイスでスティッキ機能をイネーブルにする例を示します。

```
Router(config-if)# switchport port-security mac-address sticky
```

次に、インターフェイスでスティッキ機能をディセーブルにする例を示します。

```
Router(config-if)# no switchport port-security mac-address sticky
```

次に、特定の MAC アドレスをスティッキ アドレスにする例を示します。

```
Router(config-if)# switchport port-security mac-address sticky 0000.0000.0001
```

次に、特定のスティッキ アドレスを削除する例を示します。

```
Router(config-if)# no switchport port-security mac-address sticky 0000.0000.0001
```

次に、インターフェイスに設定されているすべてのスティッキ アドレスとスタティック アドレスを削除する例を示します。

```
Router(config-if)# no switchport port-security mac-address
```

関連コマンド

コマンド	説明
clear port-security	MAC アドレス テーブルからセキュア MAC アドレスおよびスティッキ MAC アドレスを削除します。
show port-security	ポートセキュリティ設定に関する情報を表示します。
switchport mode trunk	ポートをトランク メンバー として設定します。
switchport nonegotiate	LAN ポートを永続的なトランッキング モード として設定します。

switchport port-security maximum

ポート上のセキュア MAC アドレスの最大数を設定するには、**switchport port-security maximum** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport port-security maximum *maximum* [*vlan vlan* | *vlan-list*]

no switchport port-security maximum

シンタックスの説明	
<i>maximum</i>	インターフェイスのセキュア MAC アドレスの最大数を指定します。有効値は 1 ~ 4097 です。
vlan <i>vlan</i> <i>vlan-list</i>	(任意) VLAN または VLAN の範囲を指定します。詳細については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト *vlan* は 1 です。

コマンドモード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドを複数回入力した場合は、2 回目以降の入力によって以前の *maximum* の値が上書きされます。新しい *maximum* 引数がこのポートの現在のセキュアアドレス数よりも大きい場合、*maximum* 値が単に増加するだけです。

新しい *maximum* が元の *maximum* よりも小さく、元の *maximum* 上により多くのセキュアアドレスが存在する場合、コマンドは拒否されます。

ポートのセキュア MAC アドレスの最大数より少ないセキュア MAC アドレスを設定した場合、残りの MAC アドレスはダイナミックに学習されます。

ポートのセキュア MAC アドレスが最大数に達すると、VLAN ポート単位の最大数が集約最大数と違う場合でも、そのポートではそれ以上のアドレスは学習されません。

特定の VLAN について、ポートのセキュア MAC アドレスの最大数を上書きするには、**switchport port-security maximum** *maximum* *vlan vlan* | *vlan-list* コマンドを入力します。

vlan-list 引数には、1,7,9-15,17 など、範囲、カンマ、および区切られたエントリを入力できます。

vlan-list 引数は、ポートが設定され、トランクとして動作可能な場合だけ使用できます。**switchport mode trunk** コマンドを入力してから、**switchport nonegotiate** コマンドを入力してください。

例 次に、このポートで許可されているセキュア MAC アドレスの最大数を設定する例を示します。

```
Router(config-if)# switchport port-security maximum 5
Router(config-if)#
```

次に、特定の VLAN について設定されている最大数を上書きするコマンドの例を示します。

■ switchport port-security maximum

```
Router(config-if)# switchport port-security maximum 3 vlan 102
Router(config-if)#
```

関連コマンド

コマンド	説明
show port-security	ポート セキュリティ設定に関する情報を表示します。

switchport port-security violation

セキュリティ違反が検出された場合に行うアクションを設定するには、**switchport port-security violation** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport port-security violation {shutdown | restrict | protect}

シンタックスの説明	shutdow	restrict	protect
	セキュリティ違反がある場合、ポートをシャットダウンします。	ポートセキュリティ プロセス レベルの非セキュア ホストからのすべてのパケットを廃棄して、セキュリティ違反数を増加させます。	ポートセキュリティ プロセス レベルの非セキュア ホストからのすべてのパケットを廃棄しますが、セキュリティ違反数は増加させません。

コマンドのデフォルト **shutdown**

コマンド モード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ポートセキュリティ違反は、次のいずれかの理由で発生します。

- インターフェイスが認識している送信元 MAC アドレスの数がポートセキュリティの制限を超えている場合
- 1 つのポートの送信元 MAC セキュア アドレスが別のセキュア ポートに表示される場合。この状況では、restrict/protect モードでソフトウェアが違反トラフィックにヒットするため、違反が発生します。**mls rate-limit layer2 port-security** コマンドを使用して、この状態からソフトウェアを保護できます。

セキュリティ違反が検出されると、次のアクションのいずれかが発生します。

- **protect** : ポートのセキュア MAC アドレスの数がポートで許可されている最大限度に達すると、十分な数のセキュア MAC アドレスを削除しない限り、送信元が不明なアドレスを持つパケットは廃棄されます。
- **restrict** : ポートのセキュリティ違反が発生すると、データが制限され、SecurityViolation カウンタの値が増加します。
- **shutdown** : セキュリティ違反が発生すると、インターフェイスが **errdisable** になります。



(注)

セキュア ポートが **errdisable** ステートの場合、**errdisable recovery cause psecure-violation** グローバル コンフィギュレーション コマンドを入力してこのステートを解除したり、**shutdown** および **no shutdown** コマンドをインターフェイス コンフィギュレーション モードで入力して手動で再イネーブル化したりすることができます。

■ switchport port-security violation

例

次に、セキュリティ違反が検出された場合に実行するアクションを設定する例を示します。

```
Router(config-if)# switchport port-security violation restrict
Router(config-if)#
```

関連コマンド

コマンド	説明
show port-security	ポートセキュリティ設定に関する情報を表示します。

switchport private-vlan host-association

隔離ポートまたはコミュニティポートの PVLAN アソシエーションを定義するには、**switchport private-vlan host-association** コマンドを使用します。ポートから PVLAN マッピングを削除するには、このコマンドの **no** 形式を使用します。

switchport private-vlan host-association {*primary-vlan-id*} {*secondary-vlan-id*}

no switchport private-vlan host-association

シンタックスの説明	
<i>primary-vlan-id</i>	PVLAN 関係におけるプライマリ VLAN の番号を指定します。有効値は 1 ~ 4094 です。
<i>secondary-vlan-id</i>	PVLAN 関係におけるセカンダリ VLAN の番号を指定します。有効値は 1 ~ 4094 です。

コマンドのデフォルト PVLAN は設定されていません。

コマンドモード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン PVLAN ホストモードでないポート上では、実行しても効果がありません。ポートが PVLAN ホストモードであっても VLAN が存在しない場合は、コマンドを使用できますが、このポートは非アクティブになります。

セカンダリ VLAN は隔離またはコミュニティ VLAN になる場合があります。

例 次に、プライマリ VLAN (VLAN 18) およびセカンダリ VLAN (VLAN 20) をポートに設定する例を示します。

```
Router(config-if)# switchport private-vlan host-association 18 20
Router(config-if)#
```

次に、ポートから PVLAN アソシエーションを削除する例を示します。

```
Router(config-if)# no switchport private-vlan host-association
Router(config-if)#
```

関連コマンド	コマンド	説明
	show interfaces switchport	スイッチング (非ルーティング) ポートの管理ステータスおよび動作ステータスを表示します。
	switchport mode	このコマンドのインターフェイスタイプを設定します。

switchport private-vlan mapping

混合モード ポートの PVLAN マッピングを定義するには、**switchport private-vlan mapping** コマンドを使用します。プライマリ VLAN からすべてのマッピングを削除するには、このコマンドの **no** 形式を使用します。

```
switchport private-vlan mapping {primary-vlan-id} {secondary-vlan-list} |
  {add secondary-vlan-list} | {remove secondary-vlan-list}
```

```
no switchport private-vlan mapping
```

シンタックスの説明

<i>primary-vlan-id</i>	PVLAN 関係におけるプライマリ VLAN の番号を指定します。有効値は 1 ~ 4094 です。
<i>secondary-vlan-id</i>	PVLAN 関係におけるセカンダリ VLAN の番号を指定します。有効値は 1 ~ 4094 です。
add	セカンダリ VLAN をプライマリ VLAN にマッピングします。
remove	セカンダリ VLAN とプライマリ VLAN のマッピングを消去します。

コマンドのデフォルト

PVLAN マッピングは設定されていません。

コマンドモード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

PVLAN 混合モードでないポート上では、実行しても効果がありません。ポートが PVLAN 混合モードであっても VLAN が存在しない場合は、コマンドを使用できますが、このポートは非アクティブになります。

セカンダリ VLAN は隔離またはコミュニティ VLAN になる場合があります。

例 次に、プライマリ VLAN 18 とセカンダリ隔離 VLAN 20 のマッピングをポートに設定する例を示します。

```
Router(config-if) # switchport private-vlan mapping 18 20  
Router(config-if) #
```

次に、マッピングに VLAN を追加する例を示します。

```
Router(config-if) # switchport private-vlan mapping 18 add 21  
Router(config-if) #
```

次に、ポートから PVLAN マッピングを削除する例を示します。

```
Router(config-if) # no switchport private-vlan mapping  
Router(config-if) #
```

関連コマンド

コマンド	説明
show interfaces private-vlan mapping	VLAN SVI の PVLAN マッピングに関する情報を表示します。

switchport trunk

インターフェイスがトランキング モードの場合にトランクの特性を設定するには、**switchport trunk** コマンドを使用します。すべてのトランキング特性をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

switchport trunk encapsulation {isl | {dot1q [ethertype value]} | negotiate}

switchport trunk native vlan *vlan-id*

switchport trunk allowed vlan *vlan-list*

switchport trunk pruning vlan *vlan-list*

no switchport trunk {encapsulation {isl | dot1q | negotiate}} | {native vlan} | {allowed vlan} | {pruning vlan}

シンタックスの説明

encapsulation isl	トランクのカプセル化形式を ISL に設定します。
encapsulation dot1q	スイッチ ポートのカプセル化形式を 802.1Q に設定します。
ethertype <i>value</i>	EtherType 値を設定します。有効値は 0x0 ~ 0x5EF-0xFFFF です。
encapsulation negotiate	DISL および DTP ネゴシエーションでカプセル化形式が解決されない場合に、ISL がカプセル化形式として選択されるように指定します。
native vlan <i>vlan-id</i>	ネイティブ VLAN を 802.1Q トランキング モードでトランク用に設定します。有効値は 1 ~ 4094 です。
allowed vlan <i>vlan-list</i>	トランキング モードにおいて、このインターフェイスをタグ付きフォーマットで伝送する許可 VLAN です。有効値は 1 ~ 4094 です。
pruning vlan <i>vlan-list</i>	トランキング モードにおいて、VTP プルーニング用にイネーブル化される VLAN のリストです。有効値は 1 ~ 4094 です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- カプセル化タイプは、プラットフォームまたはインターフェイス ハードウェアによって決まります。
- アクセス VLAN およびトランク インターフェイス ネイティブ VLAN が、プラットフォームまたはインターフェイス ハードウェアに対応するデフォルト VLAN です。
- すべての VLAN リストは VLAN をすべて含みます。
- 802.1Q カプセル化用の **ethertype value** は 0x8100 です。

コマンドのデフォルト

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、GE レイヤ 2 WAN ポートではサポートされていません。

switchport trunk encapsulation コマンドがサポートされるのは、ISL と 802.1Q の両方の形式をサポートするプラットフォームおよびインターフェイス ハードウェアに対してだけです。

switchport trunk encapsulation isl コマンドを、ISL トランク カプセル化をサポートしないインターフェイスを含むポート チャンネルで入力した場合、コマンドは拒否されます。

SPAN 宛先ポートがトランクまたはアクセス ポートであるインターフェイスで **switchport trunk allowed vlan** コマンドを入力できます。



(注) **switchport trunk pruning vlan *vlan-list*** コマンドは拡張範囲 VLAN をサポートしません。*vlan-list* の有効値は 1 ~ 1005 です。

dot1q ethertype *value* キーワードおよび引数は、ポート チャンネル インターフェイスではサポートされていません。このコマンドは、個々のポート インターフェイスだけで実行できます。また、チャンネルグループ内のポートは、異なる EtherType 設定を持つように設定できます。



注意

カスタム EtherType 値をポートで設定する場合は注意が必要です。**negotiate** キーワードを入力した場合、DISL および DTP ネゴシエーションでカプセル化形式が解決されなければ、ISL がカプセル化形式として選択され、セキュリティ リスクが生じることがあります。トランクのカプセル化形式をデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

ネイティブ モード VLAN を装置に適したデフォルト VLAN にリセットするには、**native vlan** コマンドの **no** 形式を使用します。

リストをデフォルトリスト (すべての VLAN を許可) にリセットするには、**allowed vlan** コマンドの **no** 形式を使用します。

リストをデフォルトリスト (すべての VLAN に VTP プルーニングを許可) にリセットするには、**pruning vlan** コマンドの **no** 形式を使用します。

dot1q ethertype *value* コマンドの **no** 形式は、リストをデフォルト値にリセットします。

vlan-list の形式は、**all | none | add | remove | except *vlan-list*[,*vlan-list*...]** です (以下を参照)。

- **all** : 適切な VLAN をすべて指定します。このキーワードは、**switchport trunk pruning vlan** コマンドではサポートされません。
- **none** : 空のリストを意味します。このキーワードは、**switchport trunk allowed vlan** コマンドではサポートされません。
- **add** : 現在設定されている VLAN リストを置き換えしないで、定義済み VLAN リストを追加します。
- **remove** : 現在設定されている VLAN リストを置き換えしないで、リストから定義済み VLAN リストを削除します。VLAN 1 は削除できません。トランクから VLAN 1 を削除した場合も、トランク インターフェイスは VLAN 1 の管理トラフィック (CDP3、VTP、PAGP4、DTP など) の送受信を継続します。



(注) トランクから任意のデフォルト VLAN (1002 ~ 1005) を削除できます。この処理は以前のリリースでは実行できません。

- **except** : 定義済み VLAN リストを反転して、計算する必要がある VLAN を一覧表示します。
- *vlan-list* は、1 ~ 4094 の単一の VLAN 番号、または 2 つの VLAN 番号で表される連続した VLAN 範囲です。小さい番号をハイフンで区切って最初に置きます。これは、このポートがトランッキング モードにある場合の許可 VLAN の VLAN ID を表します。

switchport trunk

スーパーバイザ エンジンと PISA の両方で Cisco IOS ソフトウェアが実行されている Catalyst 6500 シリーズスイッチを、Catalyst オペレーティングシステムが実行されている Catalyst 6500 シリーズスイッチに接続する場合は、トランク上で予約されている VLAN 範囲 (1006 ~ 1024) をイネーブルにしないでください。これらの VLAN は、Catalyst オペレーティングシステムを実行する Catalyst 6500 シリーズスイッチ専用です。これらをイネーブルにすると、Catalyst オペレーティングシステムを実行する Catalyst 6500 シリーズスイッチ間にトランキングチャンネルが存在する場合に、ポートが errdisable ステートになる場合があります。

例

次に、スイッチドインターフェイスとして設定されたポートインターフェイスが、トランキングモードのデフォルトのトランキング形式に関係なく、802.1Q トランキング形式でカプセル化されるように設定する例を示します。

```
Router(config-if)# switchport trunk encapsulation dot1q
Router(config-if)#
```

関連コマンド

コマンド	説明
show interfaces switchport	スイッチング (非ルーティング) ポートの管理ステータスおよび動作ステータスを表示します。

switchport vlan mapping

VLAN *original-vlan-id* に着信するトラフィックを VLAN *translated-vlan-id* にマッピングし、内部的に VLAN *translated-vlan-id* でタグ付けされたトラフィックに、ポートから出力される前に VLAN *original-vlan-id* でタグ付けするには、**switchport vlan mapping** コマンドを使用します。VLAN ペアのマッピングをクリアしたり、スイッチポートに設定されているすべてのマッピングをクリアしたりするには、このコマンドの **no** 形式を使用します。

switchport vlan mapping *original-vlan-id translated-vlan-id*

no switchport vlan mapping {*original-vlan-id translated-vlan-id*} | **all**}

シンタックスの説明

<i>original-vlan-id</i>	変換前の VLAN 番号。有効値は 1～4094 です。
<i>translated-vlan-id</i>	変換後の VLAN 番号。有効値は 1～4094 です。
all	スイッチポートに設定されているすべてのマッピングをクリアします。

コマンドのデフォルト

スイッチポートにはマッピングが設定されていません。

コマンドモード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、GE レイヤ 2 WAN ポートではサポートされていません。

VLAN 変換を機能させたい場合は、ポートの VLAN 変換をイネーブルにする必要があります。VLAN 変換をイネーブルにするには、**switchport vlan mapping enable** コマンドを使用します。

トランクから変換される VLAN を削除しないでください。VLAN をマッピングする場合、両方の VLAN がトラフィックを伝送するトランクで許可されていることを確認します。

表 2-95 に、VLAN 変換、サポートする VLAN 変換のタイプ、ポートグループ単位で設定可能なポート数、VLAN 変換をサポートする各モジュールでのトランクタイプを一覧表示します。

表 2-95 VLAN 変換をサポートするモジュール

製品番号	VLAN 変換サポートタイプ	ポートグループ数	ポートグループ単位のポート範囲	ポートグループ単位の交換数	サポートする VLAN 変換トランクタイプ
WS-SUP720	ポートグループ単位	1	1-2	32	802.1Q
WS-X6501-10GEX4	ポート単位	1	1 グループ内に 1 ポート	32	802.1Q
WS-X6502-10GE	ポート単位	1	1 グループ内に 1 ポート	32	802.1Q
WS-X6516A-GBIC	ポートグループ単位	2	1-8, 9-16	32	802.1Q

表 2-95 VLAN 変換をサポートするモジュール (続き)

製品番号	VLAN 変換サポートタイプ	ポートグループ数	ポートグループ単位のポート範囲	ポートグループ単位の交換数	サポートする VLAN 変換トランクタイプ
WS-X6516-GBIC	ポートグループ単位	2	1-8, 9-16	32	802.1Q
WS-X6516-GE-TX	ポートグループ単位	2	1-8, 9-16	32	802.1Q
WS-X6524-100FX-MM	ポートグループ単位	1	1-24	32	ISL および 802.1Q
WS-X6548-RJ-45	ポートグループ単位	1	1-48	32	ISL および 802.1Q
WS-X6548-RJ-21	ポートグループ単位	1	1-48	32	ISL および 802.1Q

switchport vlan mapping コマンドを使用して設定されたマッピングは、スイッチ ポートが動作トランク ポートになるまで有効になりません。

ポートに設定された VLAN マッピングは、同一 ASIC にある他のすべてのポートに適用されます。場合によっては、ASIC のあるポートに設定されたマッピングが同一 ASIC 内にある別のポートに設定済みのマッピングを上書きする場合があります。

ポート VLAN マッピングは、ASIC がポート単位の VLAN マッピングをサポートしない場合、ポート ASIC のすべてのポートに適用されます。

ルータ ポートであるポート ASIC の VLAN マッピングを設定した場合、ポートがスイッチ ポートになるまでポート VLAN マッピングは有効になりません。

VLAN を伝送するトランクタイプにかかわらず、2 つの VLAN をマッピングできます。

例

次に、変換前の VLAN に変換後の VLAN をマッピングする例を示します。

```
Router(config-if)# switchport vlan mapping 100 201
Router(config-if)#
```

次に、VLAN ペア間のマッピングをクリアする例を示します。

```
Router(config-if)# no switchport vlan mapping 100 201
Router(config-if)#
```

次に、スイッチ ポートに設定されているすべてのマッピングをクリアする例を示します。

```
Router(config-if)# no switchport vlan mapping 100 201
Router(config-if)#
```

関連コマンド

コマンド	説明
show interfaces vlan mapping	ポート上の VLAN マッピングのステータスを表示します。
show vlan mapping	802.1Q VLAN と ISL VLAN のマッピングを登録します。
switchport vlan mapping enable	スイッチ ポート単位で VLAN マッピングをイネーブルにします。

switchport vlan mapping enable

スイッチ ポート単位で VLAN マッピングをイネーブルにするには、**switchport vlan mapping enable** コマンドを使用します。スイッチ ポート単位の VLAN マッピングをディセーブルにするには、このコマンドの **no** 形式を使用します。

switchport vlan mapping enable

no switchport vlan mapping enable

コマンドのデフォルト VLAN マッピングはすべてのスイッチ ポートでディセーブルです。

コマンドのデフォルト インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



(注) マッピングを実行させるポートに、**switchport vlan mapping enable** コマンドを入力する必要があります。

このコマンドをサポートするモジュールのリストについては、表 2-95 を参照してください。

マッピングがグローバル VLAN マッピング コマンドで設定されているか、スイッチポート VLAN マッピング コマンドで設定されているかにかかわらず、**switchport vlan mapping enable** コマンドは、ハードウェアの VLAN マッピング ルックアップをイネーブルまたはディセーブルにします。

同じポート ASIC に接続されているポート上で選択的に VLAN 変換をオンまたはオフにできるため、このコマンドは、ASIC 単位で VLAN マッピングをサポートしているハードウェアだけで役に立ちます。

例 次に、スイッチ ポート単位で VLAN マッピングをイネーブルにする例を示します。

```
Router(config-if)# switchport vlan mapping enable  
Router(config-if)#
```

次に、スイッチ ポート単位で VLAN マッピングをディセーブルにする例を示します。

```
Router(config-if)# no switchport vlan mapping enable  
Router(config-if)#
```

関連コマンド

コマンド	説明
show interfaces vlan mapping	ポート上の VLAN マッピングのステータスを表示します。
show vlan mapping	802.1Q VLAN と ISL VLAN のマッピングを登録します。
switchport vlan mapping	VLAN <i>original-vlan-id</i> に着信するトラフィックを VLAN <i>translated-vlan-id</i> にマッピングし、内部的に VLAN <i>translated-vlan-id</i> でタグ付けされたトラフィックに、ポートから出力される前に VLAN <i>original-vlan-id</i> でタグ付けします。

switchport voice vlan

複数の VLAN アクセス ポートに音声 VLAN を設定するには、**switchport voice vlan** コマンドを使用します。スイッチ ポートから音声 VLAN を削除するには、このコマンドの **no** 形式を使用します。

switchport voice vlan {dot1p | none | untagged | vvid}

no switchport voice vlan

シンタックスの説明	dot1p	レイヤ 2 CoS 値がタグ付けされた 802.1p フレームに音声トラフィックを格納して、デフォルト VLAN 内で伝送するように IP 電話を設定する CDP パケットを送信します。
	none	IP 電話がデフォルト VLAN 内で独自の設定を使用し、タグなし音声トラフィックを伝送できるようにします。
	untagged	デフォルト VLAN 内でタグなし音声トラフィックを伝送するように IP 電話を設定する CDP パケットを送信します。
	vvid	音声 VLAN ID。有効値は 1 ~ 4094 です。レイヤ 2 CoS 値がタグ付けされた 802.1Q フレームに音声トラフィックを格納して、音声 VLAN 内で伝送するように IP 電話を設定する CDP パケットを送信します。

コマンド モード **none**

コマンド モード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン デフォルトのレイヤ 2 CoS は 5 です。デフォルトのレイヤ 3 IP precedence は 5 です。

このコマンドは、音声 VLAN を作成しません。VLAN コンフィギュレーション モードで音声 VLAN を作成するには、**vlan (global configuration mode)** コマンドを入力します。VLAN データベースにネイティブ VLAN と音声 VLAN を両方とも設定して、スイッチ ポートを複数の VLAN アクセス モードに設定すると、このコマンドはスイッチ ポートを動作上の起動状態にします。

dot1p を入力した場合、スイッチ ポートは 802.1p パケットだけを受信できます。

none を入力した場合、スイッチ ポートは VVID TLV を含む CDP パケットを送信しません。

untagged を入力した場合、スイッチ ポートはタグなしパケットだけを受信できます。

vvid を入力すると、スイッチ ポートは指定された **vvid** がタグ付けされたパケットを受信します。

例 次に、動作する複数の VLAN アクセス ポートを作成する例を示します。

```
Router(config-if)# switchport
Router(config-if)# switchport mode access
Router(config-if)# switchport access vlan 100
```

■ **switchport voice vlan**

```
Router(config-if)# switchport voice vlan 101  
Router(config-if)
```

次に、複数の VLAN アクセス モードを標準アクセス ポートに変更する例を示します。

```
Router(config-if)# interface fastethernet5/1  
Router(config-if)# no switchport voice vlan  
Router(config-if)
```

■ **関連コマンド**

コマンド	説明
switchport access vlan	インターフェイスがアクセス モードのときに VLAN を設定します。
switchport mode	インターフェイス タイプを設定します。

sync-restart-delay

正確なステータス報告が行われるように同期再起動遅延タイマーを設定するには、**sync-restart-delay** コマンドを使用します。

sync-restart-delay timer

シンタックスの説明	<i>timer</i> ステータス レジスタのリセット間隔を指定します。有効値は 200 ~ 60,000 ミリ秒です。
------------------	---

コマンドのデフォルト *timer* は **210** ミリ秒です。

コマンドモード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドは、ギガビット イーサネット ファイバ ポートだけでサポートされます。ステータス レジスタには、リンク パートナーの現在のステータスが記録されます。

例 次に、ギガビット イーサネットの同期再起動遅延タイマーを設定する例を示します。

```
Router(config-if)# sync-restart-delay 2000
Router(config-if)#
```

関連コマンド	コマンド	説明
	show running-config	モジュールまたはレイヤ 2 VLAN のステータスおよび設定を表示します。

system flowcontrol bus

First-in first-out (FIFO; 先入れ先出し) オーバーフロー エラー カウントを設定するには、**system flowcontrol bus** コマンドを使用します。元の FIFO しきい値設定に戻すには、このコマンドの **no** 形式を使用します。

[default] system flowcontrol bus {auto | on}

no system flowcontrol bus

シンタックスの説明

default	(任意) デフォルト設定を指定します。
auto	FIFO オーバーフロー エラー カウントが 5 秒間隔で設定されたエラーしきい値を超過した場合に、FIFO オーバーフロー エラー カウントをモニタし、警告メッセージを送信します。
on	(任意) 元の FIFO しきい値設定を指定します。

コマンドのデフォルト

auto

コマンドのデフォルト

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



(注)

システムのフロー制御を **auto** モードのままにし、Cisco TAC からの指示があった場合にだけ他のモードを使用することを推奨します。

例

次に、FIFO オーバーフロー エラー カウントが 5 秒間隔で設定されたエラーしきい値を超過した場合に、FIFO オーバーフロー エラー カウントをモニタし、警告メッセージを送信する例を示します。

```
Router(config)# system flowcontrol bus auto
Router(config)#
```

次に、元の FIFO しきい値設定を指定する例を示します。

```
Router(config)# system flowcontrol bus on
Router(config)#
```

system jumbomtu

レイヤ 2 およびレイヤ 3 パケットの最大サイズを設定するには、**system jumbo mtu** コマンドを使用します。デフォルトの MTU 設定に戻すには、このコマンドの **no** 形式を使用します。

system jumbomtu mtu-size

no system jumbomtu

シンタックスの説明	<i>mtu-size</i>	レイヤ 2 およびレイヤ 3 パケットの最大サイズ。有効値は 1500 ~ 9216 バイトです。
-----------	-----------------	---

コマンドのデフォルト *mtu-size* は **9216** バイトです。

コマンド モード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン *mtu-size* パラメータが指定するのはイーサネット パケットのサイズであり、イーサネット フレーム全体のサイズではありません。レイヤ 3 MTU は、**system jumbomtu** コマンドを入力すると変化します。

system jumbomtu コマンドは、ポート ASIC のグローバル MTU をイネーブルにします。ポート ASIC 上でジャンボ フレームをイネーブルにすると、入力側では任意のサイズのパケットが許可され、出力側では発信パケットがチェックされます。グローバル MTU を超える出力側のパケットは、ポート ASIC で廃棄されます。

たとえば、VLAN 1 のポート A および VLAN 2 のポート B が存在する場合に、VLAN 1 および VLAN 2 を **mtu 9216** に設定し、**system jumbomtu 4000** コマンドを入力すると、4000 バイトを超えるパケットは発信されなくなります。ポート B および A では、4000 バイトを超えるパケットが廃棄されるためです。

例 次に、グローバル MTU サイズを 1550 バイトに設定する例を示します。

```
Router(config)# system jumbomtu 1550
Router(config)# end
Router#
```

次に、MTU のデフォルト設定に戻す例を示します。

```
Router(config)# no system jumbomtu
Router(config)#
```

■ system jumbomtu

関連コマンド

コマンド	説明
mtu	最大パケット サイズまたは MTU サイズを調整します。
show interfaces	特定のインターフェイスで認識されるトラフィックを表示します。
show system jumbomtu	グローバル MTU 設定を表示します。

tcam priority

TCAM の入力時、またはラベルが枯渇した場合に、ソフトウェア転送用のインターフェイスのプライオリティを設定するには、**tcam priority** コマンドを使用します。

tcam priority {high | normal | low}

シンタックスの説明	high	プライオリティを高く設定します。
	normal	プライオリティを標準に設定します。
	low	プライオリティを低く設定します。

コマンドのデフォルト **normal**

コマンドモード インターフェイス コンフィギュレーション (config-if)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

インターフェイスは次の順序で選択されます。

1. VACL およびマルチキャストが設定されていないロー プライオリティ インターフェイス
2. VACL が設定されていない、マルチキャストによる承認済みのロー プライオリティ インターフェイス
3. VACL が設定されている、マルチキャストによる承認済みのロー プライオリティ インターフェイス
4. ロー プライオリティ インターフェイス (マルチキャストによって承認されていない)
5. VACL およびマルチキャストが設定されていない標準プライオリティ インターフェイス
6. VACL が設定されていない、マルチキャストによる承認済みの標準プライオリティ インターフェイス
7. VACL が設定されている、マルチキャストによる承認済みの標準プライオリティ インターフェイス
8. 標準プライオリティ インターフェイス (マルチキャストによって承認されていない)
9. VACL およびマルチキャストが設定されていないハイ プライオリティ インターフェイス
10. VACL が設定されていない、マルチキャストによる承認済みのハイ プライオリティ インターフェイス
11. VACL が設定されている、マルチキャストによる承認済みのハイ プライオリティ インターフェイス
12. ハイ プライオリティ インターフェイス (マルチキャストによって承認されていない)

例 次に、プライオリティを設定する例を示します。

```
Router(config-if)# tcam priority low
Router(config-if)#
```

■ tcam priority

関連コマンド

コマンド	説明
show tcam interface	インターフェイスベースの TCAM に関する情報を表示します。

test cable-diagnostics

10 ギガビットイーサネットリンク、または 48 ポート 10/100/1000 BASE-T モジュール上の銅ケーブルの状態をテストするには、**test cable-diagnostics** コマンドを使用します。

test cable-diagnostics tdr interface {*interface interface-number*}

シンタックスの説明	tdr	48 ポート 10/100/1000 BASE-T モジュール上の銅ケーブルの TDR テストをアクティブ化します。
	interface interface	インターフェイスタイプを指定します。有効値については、「使用上のガイドライン」を参照してください。
	<i>interface-number</i>	モジュールおよびポート番号

コマンドのデフォルト このコマンドにはデフォルト設定がありません。

コマンドモード 特権 EXEC (#)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン ケーブル診断を実行すれば、使用中のケーブルに接続上の問題があるかどうかを検出できます。TDR テストの注意事項は次のとおりです。

- TDR は、最大 115 m の長さのケーブルをテストできます。
- TDR をサポートするモジュールの一覧については、『Release Notes for Cisco IOS Release 12.2 ZY』を参照してください。
- **interface interface** の有効値は **fastethernet** および **gigabitethernet** です。
- テストはケーブルの両端で同時に開始しないでください。テストをケーブルの両端で同時に開始すると、誤ったテスト結果が得られることがあります。
- ケーブル診断テスト中は、ポートの設定を変更しないでください。変更すると、誤ったテスト結果が得られることがあります。
- インターフェイスは、TDR テスト実行前にアップになっている必要があります。ポートがダウンの場合、**test cable-diagnostics tdr** コマンドは拒否され、次のメッセージが表示されます。

```
Router# test cable-diagnostics tdr interface gigabitethernet2/12
% Interface Gi2/12 is administratively down
% Use 'no shutdown' to enable interface before TDR test start.
```

- ポート速度が 1000 でリンクがアップの場合、自動 MDIX 機能をディセーブルにしないでください。
- 固定 10/100 ポートでは、TDR テスト実行前に、自動 MDIX をケーブルの両端でディセーブルにしてください。そうしないと、誤った結果が得られることがあります。

- 他のすべての条件では、自動 MDIX 機能はケーブルの両端でディセーブルにする必要があります (**no mdix auto** コマンドを使用します)。自動 MDIX をディセーブルにしない場合、TDR テストが妨害され、誤った結果が得られます。
- リンクの相手側で自動 MDIX がイネーブルの場合は、この処理は TDR ケーブル診断テストを妨害し、テスト結果に誤りが生じます。ワークアラウンドはリンクの相手側で自動 MDIX をディセーブルにします。
- ポート速度を 1000 から 10/100 に変更した場合、**no mdix auto** コマンドを入力してから TDR テストを実行してください。**speed 1000** コマンドを入力すると、**no mdix auto** コマンドを実行済みかどうかに関係なく、自動 MDIX がイネーブルとなります。

例

次に、TDR ケーブル診断を実行する例を示します。

```
Router # test cable-diagnostics tdr interface gigabitethernet2/1
TDR test started on interface Gi2/1
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
Router #
```

関連コマンド

コマンド	説明
clear cable-diagnostics tdr	TDR をサポートする特定のインターフェイスまたはすべてのインターフェイスをクリアします。
show cable-diagnostics tdr	TDR ケーブル診断のテスト結果を表示します。

time-range

時間範囲コンフィギュレーション モードをイネーブルにし、機能（拡張アクセス リストなど）に対する時間範囲を定義するには、**time-range** コマンドを使用します。時間制限を削除するには、このコマンドの **no** 形式を使用します。

time-range *time-range-name*

no time-range *time-range-name*

シンタックスの説明

time-range-name 時間範囲の名前

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

time-range エントリは名前で識別され、1 つまたは複数のその他のコンフィギュレーション コマンドによって参照されます。1 つのアクセス リスト、または他の機能で複数の時間範囲が発生します。

time-range-name には、スペースまたは引用符を含めることができず、アルファベットの文字で開始する必要があります。



(注) IP および IPX 拡張アクセス リストは、時間範囲を使用できる唯一のタイプのアクセス リストです。

time-range コマンドを使用したあとに、**periodic** 時間範囲コンフィギュレーション コマンド、**absolute** 時間範囲コンフィギュレーション コマンド、またはこれらのコマンドの一部の組み合わせを使用して、機能が作用する時間を定義します。時間範囲には、複数の **periodic** コマンドを使用できますが、**absolute** コマンドに関しては 1 つだけ使用できます。



ヒント

混乱しないように、時間範囲および名前付きアクセス リストにそれぞれ別の名前を使用してください。

例

次に、月曜日から金曜日の午前 8 時から午後 6 時の間に HTTP トラフィックを拒否し、土曜日と日曜日の正午から午前 0 時の間だけ UDP トラフィックを許可する例を示します。

```
Router(config)# time-range no-http
Router(config)# periodic weekdays 8:00 to 18:00
!
Router(config)# time-range udp-yes
Router(config)# periodic weekend 12:00 to 24:00
!
```

time-range

```

Router(config)# ip access-list extended strict
Router(config)# deny tcp any any eq http time-range no-http
Router(config)# permit udp any any time-range udp-yes
!
Router(config)# interface ethernet 0
Router(config)# ip access-group strict in

```

関連コマンド

コマンド	説明
absolute	時間範囲が有効なときの絶対時間を指定します。
ip access-list	名前別に IP アクセス リストを定義します。
periodic	時間範囲機能をサポートする機能に繰り返し（週単位）の時間範囲を指定します。
permit (IP)	名前付き IP アクセス リストの条件を設定します。

traceroute mac

指定した送信元から指定した宛先までにパケットが通過するレイヤ 2 パスを表示するには、**traceroute mac** コマンドを使用します。

```
traceroute mac source-mac-address {destination-mac-address | {interface type
interface-number destination-mac-address}} [vlan vlan-id] [detail]
```

```
traceroute mac interface type interface-number source-mac-address
{destination-mac-address | {interface type interface-number
destination-mac-address}} [vlan vlan-id] [detail]
```

```
traceroute mac ip {source-ip-address | source-hostname} {destination-ip-address |
destination-hostname} [detail]
```

シンタックスの説明

<i>source-mac-address</i>	送信元スイッチの MAC アドレス (16 進形式)
<i>destination-mac-address</i>	宛先スイッチの MAC アドレス (16 進形式)
interface type	MAC アドレスが常駐するインターフェイスを指定します。有効値は、 FastEthernet 、 GigabitEthernet 、および Port-channel です。
<i>interface-number</i>	モジュールとポート番号またはポート チャネル番号。ポート チャネルの有効値は 1 ~ 282 です。
vlan vlan-id	(任意) 送信元スイッチから宛先スイッチまでにパケットが通過するレイヤ 2 パスをトレースする VLAN を指定します。有効値は 1 ~ 4094 です。
detail	(任意) レイヤ 2 トレースに関する詳細情報を表示します。
ip	MAC アドレスが常駐する IP アドレスを指定します。
<i>source ip-address</i>	送信元スイッチの IP アドレス (32 ビットのドット付き 10 進形式)
<i>source-hostname</i>	送信元スイッチの IP ホスト名
<i>destination-ip-address</i>	宛先スイッチの IP アドレス (32 ビットのドット付き 10 進形式)
<i>destination-hostname</i>	宛先スイッチの IP ホスト名

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

VLAN ID を入力するときに、先行ゼロを使用しないでください。

ネットワーク内のすべてのスイッチで、CDP をイネーブルにする必要があります。レイヤ 2 traceroute を適切に機能させるために、CDP をディセーブルにしないでください。

スイッチがレイヤ 2 パス内でレイヤ 2 traceroute をサポートしない装置を検出しても、スイッチはレイヤ 2 トレース クエリーの送信を続行し、タイムアウトになります。

パス内で識別される最大ホップ数は 10 です。

レイヤ 2 `tracertoute` は、ユニキャストトラフィックだけをサポートしています。マルチキャスト送信元または宛先 MAC アドレスを指定した場合、物理パスが識別されず、メッセージが表示されます。

指定された送信元アドレスと宛先アドレスが同じ VLAN に属しているときは、`tracertoute mac` コマンド出力にレイヤ 2 パスが表示されます。異なる VLAN に属する送信元アドレスと宛先アドレスを指定した場合、レイヤ 2 パスは識別されず、メッセージが表示されます。

送信元または宛先 MAC アドレスが複数の VLAN に属する場合は、送信元と宛先の両方の MAC アドレスが属する VLAN を指定する必要があります。その VLAN を指定しなかった場合は、パスが識別されず、メッセージが表示されます。

複数の装置がハブを通じて 1 つのポートに接続されているとき (1 つのポートで複数の CDP ネイバが検出された場合など)、レイヤ 2 `tracertoute` ユーティリティはそのホップで終了してエラーメッセージを表示します。

この機能は、トークンリング VLAN ではサポートされていません。

例

次に、レイヤ 2 パスに関する詳細情報を表示する例を示します。

```
Router# tracertoute mac 0001.0000.0204 0001.0000.0304 detail
Source 0001.0000.0204 found on VAYU[WS-C6509] (2.1.1.10)
1 VAYU / WS-C6509 / 2.1.1.10 :
Gi6/1 [full, 1000M] => Po100 [auto, auto]
2 PANI / WS-C6509 / 2.1.1.12 :
Po100 [auto, auto] => Po110 [auto, auto]
3 BUMI / WS-C6509 / 2.1.1.13 :
Po110 [auto, auto] => Po120 [auto, auto]
4 AGNI / WS-C6509 / 2.1.1.11 :
Po120 [auto, auto] => Gi8/12 [full, 1000M]
Destination 0001.0000.0304 found on AGNI[WS-C6509] (2.1.1.11)
Layer 2 trace completed.
Router#
```

次に、スイッチが送信元スイッチに接続されていないときの出力例を示します。

```
Router# tracertoute mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source .....
Source 0000.0201.0501 found on con5[WS-C6509] (2.2.5.5)
con5 / WS-C6509 / 2.2.5.5 :
Fa0/1 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C6509 / 2.2.1.1 :
Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C6509 / 2.2.2.2 :
Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C6509] (2.2.2.2)
Layer 2 trace completed.
Router#
```

次に、スイッチが送信元 MAC アドレスに対する宛先ポートを検出できないときの出力例を示します。

```
Router# tracertoute mac 0000.0011.1111 0000.0201.0201
Error:Source Mac address not found.
Layer2 trace aborted.
Router#
```

次に、送信元装置と宛先装置が異なる VLAN に存在するときの出力例を示します。

```
Router# tracertoute mac 0000.0201.0601 0000.0301.0201
Error:Source and destination macs are on different vlans.
Layer2 trace aborted.
Router#
```

次に、宛先 MAC アドレスがマルチキャスト アドレスのときの出力例を示します。

```
Router# traceroute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
Router#
```

次に、送信元スイッチと宛先スイッチが複数の VLAN に属するときの出力例を示します。

```
Router# traceroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
Router#
```

次に、送信元および宛先スイッチのインターフェイスを指定してレイヤ 2 パスを表示する例を示します。

```
Router# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3 0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C6509] (2.2.6.6)
con6 (2.2.6.6) :Fa0/1 =>Fa0/3
con5          (2.2.5.5      ) : Fa0/3 =>Gi0/1
con1          (2.2.1.1      ) : Gi0/1 =>Gi0/2
con2          (2.2.2.2      ) : Gi0/2 =>Fa0/1
Destination 0000.0201.0201 found on con2[WS-C6509] (2.2.2.2)
Layer 2 trace completed
Router#
```

次に、詳細な traceroute 情報を表示する例を示します。

```
Router# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac.....
2.2.66.66 =>0000.0201.0601
2.2.22.22 =>0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C6509] (2.2.6.6)
con6 / WS-C6509 / 2.2.6.6 :
      Fa0/1 [auto, auto] =>Fa0/3 [auto, auto]
con5 / WS-C6509 / 2.2.5.5 :
      Fa0/3 [auto, auto] =>Gi0/1 [auto, auto]
con1 / WS-C6509 / 2.2.1.1 :
      Gi0/1 [auto, auto] =>Gi0/2 [auto, auto]
con2 / WS-C6509 / 2.2.2.2 :
      Gi0/2 [auto, auto] =>Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C6509] (2.2.2.2)
Layer 2 trace completed.
Router#
```

次に、送信元および宛先ホスト名を指定してレイヤ 2 パスを表示する例を示します。

```
Router# traceroute mac ip con6 con2
Translating IP to mac .....
2.2.66.66 =>0000.0201.0601
2.2.22.22 =>0000.0201.0201

Source 0000.0201.0601 found on con6
con6 (2.2.6.6) :Fa0/1 =>Fa0/3
con5          (2.2.5.5      ) : Fa0/3 =>Gi0/1
con1          (2.2.1.1      ) : Gi0/1 =>Gi0/2
con2          (2.2.2.2      ) : Gi0/2 =>Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
Router#
```

次に、ARP が送信元 IP アドレスを対応する MAC アドレスに関連付けることができないときの出力例を示します。

■ traceroute mac

```
Router# traceroute mac ip 2.2.66.66 2.2.77.77  
Arp failed for destination 2.2.77.77.  
Layer2 trace aborted.  
Router#
```

track interface

インターフェイスをトラッキングするように設定し、トラッキング コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **track interface** コマンドを使用します。トラッキングを解除するには、このコマンドの **no** 形式を使用します。

track object-number interface type number {line-protocol | ip routing}

no track object-number interface type number {line-protocol | ip routing}

シンタックスの説明	object-number	トラッキングするインターフェイスを表すオブジェクト番号。有効値は、1 ~ 500 です。
	type number	トラッキングするインターフェイス タイプおよび番号
	line-protocol	インターフェイス回線プロトコルの状態をトラッキングします。
	ip routing	IP ルーティングがイネーブルであるか、インターフェイスに IP アドレスが設定されているか、インターフェイスがアップの状態であることをトラッキング クライアントに報告する前にインターフェイスの状態がアップであるかどうかをトラッキングします。

コマンドのデフォルト インターフェイスはトラッキングされません。

コマンドモード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン このコマンドは、状態値をクライアントに報告します。次のいずれかの状態に一致する場合、トラッキングされた IP ルーティング オブジェクトがアップの状態であると見なされます。

- インターフェイス上で IP ルーティングがイネーブルにされ、アクティブの状態である場合
- インターフェイス回線プロトコルがアップ状態である場合
- インターフェイスの IP アドレスが既知の場合。IP アドレスが Dynamic Host Configuration Protocol (DHCP) または IP Control Protocol (IPCP; IP コントロール プロトコル) ネゴシエーションで設定または受信されています。

次のいずれかの状態に一致する場合、インターフェイス IP ルーティングがダウンします。

- IP ルーティングがグローバルにディセーブルにされている場合
- インターフェイス回線プロトコルがダウン状態である場合
- インターフェイスの IP アドレスが不明の場合。IP アドレスが DHCP または IPCP ネゴシエーションで設定または受信されていません。

type number 値の間には、スペースは不要です。

IP アドレスがネゴシエーションされるインターフェイスでは特に、**track interface line-protocol** コマンドを使用して回線プロトコルの状態だけをトラッキングするより、**track interface ip routing** コマンドを使用してインターフェイスの IP ルーティング状態をトラッキングする方が状況によっては実用的である場合があります。たとえば、ポイントツーポイント プロトコル (PPP) を使用するシリアル インターフェイスでは、回線プロトコルがアップ状態であっても (Link Control Protocol (LCP; リンク コントロール プロトコル) が正常にネゴシエーションされている)、IP がダウン状態である場合があります (IPCP ネゴシエーションが失敗している)。

track interface ip routing コマンドは、次のいずれかの方法で取得された IP アドレスを使用するインターフェイスのトラッキングをサポートします。

- 従来の IP アドレスの設定
- PPP/IPCP
- DHCP
- 番号なしのインターフェイス

例

次に、シリアル インターフェイス 1/0 の IP ルーティング機能をトラッキングするトラッキング プロセスを設定する例を示します。

```
Router(config)# track 1 interface serial1/0 ip routing
Router(config)#
```

関連コマンド

コマンド	説明
show track	HSRP トラッキング情報を表示します。

transceiver type all monitoring

すべてのトランシーバのモニタリングをイネーブルにするには、**transceiver type all monitoring** コマンドを使用します。モニタリングをディセーブルにするには、このコマンドの **no** 形式を使用します。

transceiver type all monitoring

no transceiver type all monitoring

シンタックスの説明 このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト ディセーブル

コマンド モード グローバル コンフィギュレーション (config)

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン **transceiver type all monitoring** コマンドを使用して、すべてのトランシーバタイプのモニタリングをイネーブルにできます (たとえば、DOM 情報の収集およびしきい値違反の評価)。



(注) **no transceiver type all monitoring** コマンドは、**snmp-server enable traps transceiver type all** コマンドを上書きし、SNMP) トラップの生成を許可しません。

例 次に、すべてのトランシーバタイプのモニタリングをイネーブルにする例を示します。

```
Router(config)# transceiver type all monitoring
Router(config)#
```

次に、すべてのトランシーバタイプのモニタリングをディセーブルにする例を示します。

```
Router(config)# no transceiver type all monitoring
Router(config)#
```

コマンド	説明
snmp-server enable traps transceiver type all	すべてのトランシーバタイプでサポートされているすべての SNMP トランシーバタイプをイネーブルにします。

tunnel udlr address-resolution

UDL を通じて ARP および NHRP の転送をイネーブルにするには、**tunnel udlr address-resolution** コマンドを使用します。転送をディセーブルにするには、このコマンドの **no** 形式を使用します。

tunnel udlr address-resolution

no tunnel udlr address-resolution

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、次のモジュールだけでサポートされています。

- WS-X6704-10GE 4 ポート 10 ギガビット イーサネット
- WS-X6816-GBIC 16 ポート ギガビット イーサネット
- WS-X6516A-GBIC 16 ポート ギガビット イーサネット
- WS-X6516-GBIC 16 ポート ギガビット イーサネット

UDLR バック チャネル トンネルは IPv6 をサポートしません。

このコマンドは、ダウンストリーム ルータの送信専用トンネル インターフェイスだけでサポートされます。

非物理インターフェイスにはソフトウェアベースの UDE を設定できません。

UDL (イーサネット インターフェイス 0) 上のアップストリーム ルータから受信された ARP アドレス 解決要求には、レシーバーの送信専用トンネルから応答が返されます。ARP 要求は、送信専用トンネルを通じてダウンストリーム ルータによって送信され、応答は UDL を通じて受信されます。

例

次に、送信専用トンネルで ARP および NHRP 転送をイネーブルにする例を示します。

```
Router(config-if)# tunnel udlr address-resolution
Router(config-if)#
```

関連コマンド

コマンド	説明
show ip igmp udlr	UDL ヘルパー アドレスが設定されたインターフェイス上で、接続済みのマルチキャスト グループに関する UDLR 情報を表示します。
tunnel udlr receive-only	単一方向リンク ルーティングに設定されたインターフェイスからメッセージを受信するバック チャンネルとして動作する単一方向 GRE トンネルを設定します。

tunnel udlr receive-only

単一方向リンク ルーティングに設定されたインターフェイスからメッセージを受信するバック チャネルとして動作する単一方向 GRE トンネルを設定するには、**tunnel udlr receive-only** コマンドを使用します。トンネルを削除するには、このコマンドの **no** 形式を使用します。

tunnel udlr receive-only interface-type interface-number

no tunnel udlr receive-only interface-type interface-number

シンタックスの説明

<i>interface-type</i>	インターフェイス タイプおよびインターフェイス番号
<i>interface-number</i>	

コマンドのデフォルト

UDLR トンネルは設定されていません。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、次のモジュールだけでサポートされています。

- WS-X6704-10GE 4 ポート 10 ギガビット イーサネット
- WS-X6816-GBIC 16 ポート ギガビット イーサネット
- WS-X6516A-GBIC 16 ポート ギガビット イーサネット
- WS-X6516-GBIC 16 ポート ギガビット イーサネット

UDLR バック チャネル トンネルは IPv6 をサポートしません。

送信専用機能を備えた単一方向インターフェイスを持つルータを設定するには、このコマンドを使用します。たとえば、衛星を経由して送信されるトラフィックがある場合にこのコマンドを使用できます。

interface-type および *interface-number* 引数は、**interface** コマンドで指定される送信専用インターフェイス タイプおよびインターフェイス番号と一致している必要があります。

interface-type および *interface-number* 引数は、**interface** コマンドで指定される単一方向送信専用インターフェイス タイプおよびインターフェイス番号と一致している必要があります。トンネルでパケットが受信されると、上位レイヤ プロトコルは、単一方向送信専用インターフェイスで受信されたかのようにパケットを処理します。

トンネルの反対側で **tunnel udlr send-only** コマンドを設定する必要があります。

ip igmp unidirectional-link コマンドの詳細については、『Cisco IOS Release 12.2 Command Reference』を参照してください。

例 次に、単一方向リンク ルーティングに設定されたインターフェイスからメッセージを受信するバックチャンネルとして動作する単一方向 GRE トンネルを設定する例を示します。

```
Router(config-if)# tunnel udlr receive-only serial 0
Router(config-if)#
```

関連コマンド

コマンド	説明
interface	設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ip igmp unidirectional-link	インターフェイスを単一方向に設定し、IGMP UDLR に対してイネーブルにします。
show ip igmp udlr	UDL ヘルパー アドレスが設定されたインターフェイス上で、接続済みのマルチキャスト グループに関する UDLR 情報を表示します。
tunnel udlr send-only	単一方向リンク ルーティングに設定されたインターフェイスからメッセージを送信するバック チャンネルとして動作する単一方向 GRE トンネルを設定します。

tunnel udlr send-only

単一方向リンク ルーティングに設定されたインターフェイスからメッセージを送信するバック チャネルとして動作する単一方向 GRE トンネルを設定するには、**tunnel udlr send-only** コマンドを使用します。トンネルを削除するには、このコマンドの **no** 形式を使用します。

tunnel udlr send-only *interface-type interface-number*

no tunnel udlr send-only *interface-type interface-number*

シンタックスの説明

<i>interface-type</i>	インターフェイス タイプおよびインターフェイス番号
<i>interface-number</i>	

コマンドのデフォルト

UDLR トンネルは設定されていません。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、次のモジュールだけでサポートされています。

- WS-X6704-10GE 4 ポート 10 ギガビット イーサネット
- WS-X6816-GBIC 16 ポート ギガビット イーサネット
- WS-X6516A-GBIC 16 ポート ギガビット イーサネット
- WS-X6516-GBIC 16 ポート ギガビット イーサネット

UDLR バック チャネル トンネルは IPv6 をサポートしません。

受信専用機能を備えた単一方向インターフェイスを持つルータを設定するには、このコマンドを使用します。UDLR トンネルは、バック トンネルとして動作します。たとえば、衛星を経由して送信されるトラフィックがある場合にこのコマンドを使用できます。

interface-type および *interface-number* 引数は、**interface** コマンドで指定された単一方向受信専用インターフェイス タイプおよびインターフェイス番号と一致する必要があります。パケットがインターフェイスを通じて上位レイヤ プロトコルによって送信される場合、この GRE トンネルを通じてリダイレクトおよび送信されます。

interface-type および *interface-number* 引数は、**interface** コマンドで指定される受信専用インターフェイス タイプおよびインターフェイス番号と一致する必要があります。

トンネルの反対側で **tunnel udlr receive-only** コマンドを設定する必要があります。

例 次に、単一方向リンク ルーティングに設定されたインターフェイスからメッセージを送信するバックチャンネルとして動作する単一方向 GRE トンネルを設定する例を示します。

```
Router(config-if)# tunnel udlr send-only serial 1
Router(config-if)#
```

関連コマンド

コマンド	説明
interface	設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
show ip igmp udlr	UDL ヘルパー アドレスが設定されたインターフェイス上で、接続済みのマルチキャスト グループに関する UDLR 情報を表示します。
tunnel udlr address-resolution	UDL を通じて ARP および NHRP の転送をイネーブルにします。
tunnel udlr receive-only	単一方向リンク ルーティングに設定されたインターフェイスからメッセージを受信するバック チャンネルとして動作する単一方向 GRE トンネルを設定します。

udld

アグレッシブ モード UDLD または標準モード UDLD をイネーブルにしたり、設定可能なメッセージの時間を設定したりするには、**udld** コマンドを使用します。アグレッシブ モード UDLD または標準モード UDLD をディセーブルにするには、このコマンドの **no** 形式を使用します。

udld {enable | aggressive}

no udld {enable | aggressive}

udld message time message-timer-time

no udld message time

シンタックスの説明

udld enable	すべての光ファイバ インターフェイス上で、標準モード UDLD をデフォルトでイネーブルにします。
udld aggressive	すべての光ファイバ インターフェイス上で、アグレッシブ モード UDLD をデフォルトでイネーブルにします。
message time message-timer-time	アドバタイズ モードであり、現在双方向であると判別されているポートに、UDLD プロブ メッセージの間隔を設定します。有効値は 7 ~ 90 秒です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- UDLD はすべての光ファイバ インターフェイスでディセーブルです。
- message-timer-time* は 15 秒です。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドの **no** 形式は、次の場合に使用します。

- すべての光ファイバ ポート上で、標準モード UDLD をデフォルトでディセーブルにする。
- すべての光ファイバ ポート上で、アグレッシブ モード UDLD をデフォルトでディセーブルにする。
- メッセージ タイマーをディセーブルにする。

アグレッシブ モードがイネーブルである場合、ポートのすべてのネイバがアドバタイズ フェーズまたは検出フェーズ中に期限切れになると、UDLD はリンクアップシーケンスを再開して、同期化されない可能性のあるネイバと再同期化し、リンクからのメッセージ リリースが未定の場合は、ポートをシャットダウンします。

このコマンドは、光ファイバ インターフェイスにだけ作用します。他のインターフェイス タイプで UDLD をイネーブルにする場合は、**udld port** コマンドをインターフェイス コンフィギュレーション モードで使用します。

例

次に、すべての光インターフェイスで UDLD をイネーブルにする例を示します。

```
Router (config)# udld enable  
Router (config)#
```

関連コマンド

コマンド	説明
show udld	管理および動作上の UDLD ステータスを表示します。
udld port	インターフェイス上で UDLD をイネーブルにしたり、インターフェイス上でアグレッシブ モード UDLD をイネーブルにしたりします。

udld port

インターフェイス上で UDLD をイネーブルにしたり、インターフェイス上でアグレッシブ モード UDLD をイネーブルにしたりするには、**udld port** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

udld port [aggressive]

no udld port [aggressive]

シンタックスの説明

aggressive (任意) 現在のインターフェイス上でアグレッシブ モード UDLD をイネーブルにします。詳細については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- 光ファイバ インターフェイスは、グローバルな **udld** (**enable** または **aggressive**) コマンド状態にあります。
- 光ファイバ インターフェイス以外では、UDLD はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

CLI でこのコマンドを表示するには、イネーブルにしようとしているポートに GBIC を装着する必要があります。

グローバルな **udld** (**enable** または **aggressive**) コマンドの設定を上書きするには、光ファイバ ポート上で **udld port** および **udld port aggressive** コマンドを使用する必要があります。この設定を削除して、UDLD のイネーブル化に関する制御をグローバルな コマンドに戻したり、光ファイバ以外のポートの場合に UDLD をディセーブルにするには、光ファイバ ポート上で **udld** コマンドの **no** 形式を使用します。

アグレッシブ モードがイネーブルである場合、ポートのすべてのネイバがアドバタイズ フェーズまたは検出フェーズ中に期限切れになると、UDLD はリンクアップ シーケンスを再開して、同期化されない可能性のあるネイバと再同期化し、リンクからのメッセージ リリースが未定の場合は、ポートをシャットダウンします。

ポートが光ファイバ ポートから光ファイバ以外のポートに、またはその逆に変更された場合でも、プラットフォーム ソフトウェアによってモジュールまたは GBIC の変更が検出されるため、すべての設定が維持されます。

例

次に、現在のグローバルな **udld** 設定に関係なく、すべてのポート インターフェイスで UDLD をイネーブルにする例を示します。

```
Router (config-if)# udld port  
Router (config-if)#
```

次に、現在のグローバルな **udld** (**enable** または **aggressive**) 設定に関係なく、すべてのポート インターフェイス上でアグレッシブ モード UDLD をイネーブルにする例を示します。

```
Router (config-if)# udld port aggressive  
Router (config-if)#
```

次に、現在のグローバルな **udld** 設定に関係なく、光ファイバ ポート インターフェイスで UDLD をディセーブルにする例を示します。

```
Router (config-if)# no udld port  
Router (config-if)#
```

関連コマンド

コマンド	説明
show udld	管理および動作上の UDLD ステータスを表示します。
udld	アグレッシブ モード UDLD または標準モード UDLD をイネーブルにしたり、設定可能なメッセージ時間を設定したりします。

udld reset

UDLD によってシャットダウンされたすべてのポートをリセットしたり、これらのポートでのトラフィックの送受信を再開したりするには（ただしスパンニングツリー、PAgP、DTP などの他の機能がイネーブルの場合、通常に動作）、**udld reset** コマンドを使用します。

udld reset

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

EXEC モード

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

UDLD のインターフェイス コンフィギュレーションがまだイネーブルの場合、これらのポートは UDLD の再実行を開始します。シャットダウンの原因が修正されていない場合は、何らかの理由によりポートがシャットダウンすることがあります。

例

次に、UDLD によってシャットダウンされたすべてのポートをリセットする例を示します。

```
Router# udld reset
Router#
```

関連コマンド

コマンド	説明
show udld	管理および動作上の UDLD ステータスを表示します。

udp-port

テスト センダーがテスト パケットを送信する先、またはテスト レシーバーがステータス レポートを送信する先の UDP ポート番号を変更するには、**udp-port** コマンドを使用します。ポート番号を削除するには、このコマンドの **no** 形式を使用します。

udp-port [**test-packet** *port-number*] [**status-report** *port-number*]

no udp-port [**test-packet** *port-number*] [**status-report** *port-number*]

シンタックスの説明

test-packet <i>port-number</i>	(任意) テスト センダーがテスト パケットを送信する先の UDP ポート番号を指定します。
status-report <i>port-number</i>	(任意) テスト レシーバーがステータス レポートを送信する先の UDP ポート番号を指定します。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- **test-packet** *port-number* : 16384、音声ポートの最小値
- **status-report** *port-number* : 65535、ビデオ ポートの最大値

コマンド モード

マネージャ コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドは、次のモジュールだけでサポートされています。

- WS-X6704-10GE 4 ポート 10 ギガビット イーサネット
- WS-X6816-GBIC 16 ポート ギガビット イーサネット
- WS-X6516A-GBIC 16 ポート ギガビット イーサネット
- WS-X6516-GBIC 16 ポート ギガビット イーサネット

パケットが RTP カプセル化された場合、**test-packet** *port-number* は偶数である必要があります。

パケットが RTP カプセル化された場合、**status-report** *port-number* は奇数である必要があります。

例

次に、テストパケットの送信先の UDP ポート番号を 20000 に変更する例を示します。

```
Router(config-mrm-manager)# udp-port test-packet 20000
Router(config-mrm-manager)#
```

関連コマンド

コマンド	説明
ip mrm	MRM に対して、テスト センダーまたはテスト レシーバー、あるいはその両方として動作するように、インターフェイスを設定します。

undelete

フラッシュ ファイル システム上で [deleted] とマークされているファイルを復元するには、**undelete** コマンドを使用します。

undelete index [filesystem:]

シンタックスの説明

<i>Index</i>	dir コマンド出力内のファイルのインデックス番号を指定します。有効値は 1 ~ 1024 です。
<i>filesystem:</i>	(任意) 復元するファイルが格納されたファイル システムを指定します。直後にコロンを入力します。有効値は bootflash: 、 disk0: 、 disk1: 、 flash: 、 slot0: 、または sup-bootflash: です。

コマンドのデフォルト

デフォルト ファイル システムは **cd** コマンドを入力するときに指定されます。

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

クラス A のフラッシュ ファイル システム上では、ファイルを削除しても、Cisco IOS ソフトウェアがファイルを **deleted** とマークするだけで、ファイルは消去されません。このコマンドを使用すると、指定されたフラッシュ メモリ装置上で、削除されたファイルを復元できます。同じ名前を持つ複数のファイルが削除されている可能性があるため、インデックスを使用してファイルを復元する必要があります。たとえば、[deleted] リストに **router-config** という名前を持つ複数のコンフィギュレーション ファイルが含まれる場合があります。リスト内の複数の **router-config** ファイルのどれを復元するかを指定するインデックスを使用して、ファイルを復元します。復元するファイルのインデックス番号を取得するには、**dir** コマンドを使用します。

bootflash:、**flash:**、**disk0:**、**disk1:**、および **sup-bootflash:** は、クラス A のファイル システムです。同名の有効 (未削除) ファイルがすでに存在している場合、ファイルの復元はできません。既存のファイルを削除してから目的のファイルを復元する必要があります。たとえば、削除されていない **router-config** ファイルが存在しているときに、以前の削除済みのファイルを使用する場合は、インデックスを使用して以前のファイルを復元することはできません。まず、既存の **router-config** ファイルを削除してから、インデックスを使用して以前の **router-config** ファイルを復元する必要があります。1 ファイルにつき、15 回まで削除と復元を繰り返すことができます。

クラス A フラッシュ ファイル システム上では、**CONFIG_FILE** 環境変数によってポイントされたコンフィギュレーション ファイルを復元しようとする、ファイルを復元するかどうかを確認するプロンプトが表示されます。このプロンプトは、**CONFIG_FILE** 環境変数が復元対象ファイルを示していることをユーザに知らせます。フラッシュ メモリ装置上で [deleted] とマークされたすべてのファイルを永続的に削除するには、**squeeze** コマンドを EXEC モードで使用します。

例 次に、インデックス番号が 1 の削除済みファイルを、disk 0: に搭載されたフラッシュ PC カードに復元する例を示します。

```
Router# undelete 1 disk0:  
Router#
```

関連コマンド

コマンド	説明
delete	フラッシュ メモリ デバイスまたは NVRAM からファイルを削除します。
dir	ファイル システムのファイル リストを表示します。
squeeze	フラッシュ ファイル システムをスクイーズしてフラッシュ ファイルを永続的に削除します。

unidirectional

ソフトウェア ベースの UDE を設定するには、**unidirectional** コマンドを使用します。ソフトウェア ベースの UDE 設定を削除するには、このコマンドの **no** 形式を使用します。

unidirectional {send-only | receive-only}

no unidirectional

シンタックスの説明

send-only	単一方向トランシーバはトラフィックの送信専用であることを指定します。
receive-only	単一方向トランシーバはトラフィックの受信専用であることを指定します。

コマンドのデフォルト

UDE はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

UDE は、次のスイッチング モジュールのインターフェイスでサポートされます。

- WS-X6704-10GE 4 ポート 10 ギガビット イーサネット
- WS-X6816-GBIC 16 ポート ギガビット イーサネット
- WS-X6516A-GBIC 16 ポート ギガビット イーサネット
- WS-X6516-GBIC 16 ポート ギガビット イーサネット

ハードウェア ベースの UDE を実装しているポートでは、ソフトウェア ベースの UDE を設定する必要はありません。

インターフェイスが単一方向イーサネットを設定されている場合や、インターフェイスに受信専用トランシーバがある場合、UDLD は操作上、ディセーブルです。このインターフェイスの設定状態と動作状態を表示するには、**show udld** コマンドを使用します。

UDE 設定をインターフェイスに適用すると、次の警告メッセージが表示されます。

Warning!

```
Enable port unidirectional mode will automatically disable port udld. You must manually ensure that the unidirectional link does not create a spanning tree loop in the network.
```

```
Enable 13 port unidirectional mode will automatically disable ip routing on the port. You must manually configure static ip route and arp entry in order to route ip traffic.
```

例

次に、10 ギガビット イーサネット ポート 1/1 を UDE 送信専用ポートとして設定する例を示します。

```
Router(config-if)# unidirectional send-only
```

Warning!

Enable port unidirectional mode will automatically disable port udld. You must manually ensure that the unidirectional link does not create a spanning tree loop in the network.

Enable 13 port unidirectional mode will automatically disable ip routing on the port. You must manually configure static ip route and arp entry in order to route ip traffic.
Router(config-if)#

次に、10 ギガビットイーサネットポート 1/2 を UDE 受信専用ポートとして設定する例を示します。

Router(config-if)# **unidirectional receive-only**

Warning!

Enable port unidirectional mode will automatically disable port udld. You must manually ensure that the unidirectional link does not create a spanning tree loop in the network.

Enable 13 port unidirectional mode will automatically disable ip routing on the port. You must manually configure static ip route and arp entry in order to route ip traffic.
Router(config-if)#

関連コマンド

コマンド	説明
show interfaces status	インターフェイスステータスを表示したり、LANポートでerrdisableステートにあるインターフェイスだけのリストを表示したりします。
show interfaces unidirectional	受信専用トランシーバがあるインターフェイスの動作状態を表示します。

upgrade rom-monitor

ROMMON に関して実行優先順位を設定するには、**upgrade rom-monitor** コマンドを使用します。

```
upgrade rom-monitor {slot num} {sp | rp} {file filename}
```

```
upgrade rom-monitor {slot num} {sp | rp} {{invalidate | preference} {region1 | region2}}
```

シンタックスの説明

slot num	アップグレードする ROMMON のスロット番号を指定します。
sp	スイッチ プロセッサの ROMMON をアップグレードします。
rp	ルート プロセッサの ROMMON をアップグレードします。
file filename	SREC ファイル名を指定します。有効値については、「使用上のガイドライン」を参照してください。
invalidate	選択されたリージョンの ROMMON を無効にします。
preference	選択されたリージョンの ROMMON に関して実行優先順位を設定します。
region1	リージョン 1 内の ROMMON を選択します。
region2	リージョン 2 内の ROMMON を選択します。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



注意

パラメータを指定しないで **upgrade rom-monitor** コマンドを入力すると、処理が中断されることがあります。



注意

upgrade rom-monitor コマンドを、コンソール接続ではなく Telnet セッションから入力した場合、サービスが中断されることがあります。

このコマンドを正常に機能させるには、**slot num** は必須です。

sp または **rp** キーワードを指定する必要があるのは、指定されたスロットにスーパーバイザ エンジンが搭載されている場合です。

file filename の有効値は、次のとおりです。

- **bootflash:**
- **disk0:**
- **disk1:**

例

次に、新しい ROMMON イメージをフラッシュ装置にアップグレードする例を示します。

```
Router# upgrade rom-monitor slot 1 sp file tftp://dirt/tftpboot-users/A2_71059.srec
ROMMON image upgrade in progress
  Erasing flash
  Programming flash
  Verifying new image
  ROMMON image upgrade complete
  The card must be reset for this to take effect
Router#
```

関連コマンド

コマンド	説明
show rom-monitor	ROMMON ステータスを表示します。

username secret

ユーザ名に基づく認証システムを確立するには、**username secret** コマンドを使用します。

username name secret {0 | 5} password

シンタックスの説明

<i>name</i>	ユーザ ID
secret 0 5	シークレットを指定します。有効値は 0 (直後のテキストは暗号化されない) および 5 (直後のテキストは MD5 タイプ暗号化方式を使用して暗号化される) です。
<i>password</i>	パスワード

コマンドのデフォルト

ユーザ名に基づく認証システムは確立されていません。

コマンドモード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

このコマンドを使用すると、指定された取得不可能なユーザ名に対して拡張パスワードセキュリティがイネーブルになります。また、パスワードの MD5 暗号化がイネーブルになります。MD5 暗号化は強力な暗号化方式です。CHAP などのクリアテキスト パスワードを必要とするプロトコルと MD5 との併用はできません。

このコマンドは、特殊な取り扱いが必要なユーザ名を定義する場合に便利です。たとえば、このコマンドを使用すると、パスワードが不要で、ユーザを汎用の情報サービスに接続する [info] ユーザ名を定義できます。

username secret コマンドは、ログイン専用のユーザ名認証またはシークレット認証を提供します。*name* 引数に指定できるのは、1 ワードだけです。スペースや引用符は使用できません。単一ユーザのオプションを指定する場合は、複数の **username secret** コマンドを使用します。

例

次に、ユーザ名 **xena** を設定し、ユーザ名のパスワードとして保存されている MD5 暗号化テキスト ストリングを入力する例を示します。

```
Router(config)# username xena secret 5 $1$feb0$a104Qd9UZ./Ak00KTggPD0
Router(config)#
```

関連コマンド

コマンド	説明
enable password	各種のイネーブル レベルに対するアクセスを制御するローカル パスワードを設定します。
enable secret	enable password コマンドを使用して、追加のセキュリティ レイヤを指定します。

verify

フラッシュ メモリ ファイル システム上のファイルのチェックサムを確認したり、ファイルの MD5 シグニチャを計算したりするには、**verify** コマンドを使用します。

```
verify {{{/md5 flash-filesystem} [expected-md5-signature]} | {ios flash-filesystem} |
flash-filesystem}
```

シンタックスの説明

<code>/md5 flash-filesystem</code>	ファイルの MD5 シグニチャを計算します。有効値は bootflash: 、 disk0: 、 disk1: 、 flash: 、または sup-bootflash: です。
<code>expected-md5-signature</code>	(任意) MD5 シグニチャ
<code>/ios flash-filesystem</code>	圧縮した Cisco IOS イメージのチェックサムを確認します。有効値は bootflash: 、 disk0: 、 disk1: 、 flash: 、または sup-bootflash: です。
<code>flash-filesystem</code>	フラッシュ メモリが搭載された装置。有効値は bootflash: 、 disk0: 、 disk1: 、 flash: 、または sup-bootflash: です。

コマンドのデフォルト

デフォルトの装置は、現在動作中の装置です。

コマンド モード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

ディスクに配信された各ソフトウェア イメージでは、イメージ全体のチェックサムが 1 つ使用されます。このチェックサムは、イメージがフラッシュ メモリにコピーされるときにだけ表示されます。

ディスクのイメージに含まれている **Readme** ファイルには、イメージ名、ファイル サイズ、およびチェックサムが格納されています。**Readme** ファイルの内容を確認してから、新しいイメージのロードや複製を行ってください。そうすると、**Readme** ファイルをフラッシュ メモリまたはサーバにコピーするときに、チェックサムを確認できます。

ファイルの MD5 シグニチャを使用する前に、このシグニチャを確認するには、**verify /md5** コマンドを使用します。このコマンドは、事前に計算された MD5 シグニチャと、このコマンドによって計算されたシグニチャを比較して、コピーされたファイルの一貫性を検証します。2 つの MD5 シグニチャが一致する場合、コピーされたファイルは元のファイルと同じです。

Cisco.com ページでは、イメージとともに、公開された MD5 シグニチャを取得できます。

verify /md5 コマンドは、次のいずれかの方法で使用できます。

- **verify /md5 filename** コマンドを入力して、MD5 シグニチャを手動で確認します。
表示されたシグニチャを、Cisco.com ページに公開された MD5 シグニチャと比較します。
- **verify /md5 {flash-filesystem:filename} {expected-md5-signature}** コマンドを入力して、システムが MD5 シグニチャを比較できるようにします。
比較が終了すると、確認済みメッセージが表示されます。エラーが検出された場合は、次のような出力が表示されます。

verify

```

Router# verify /md5 disk0:c6msfc2-jsv-mz 0f
.....
.....
.....
.....Done!
%Error verifying disk0:c6msfc2-jsv-mz
Computed signature = 0f369ed9e98756f179d4f29d6e7755d3
Submitted signature = 0f

```

フラッシュ メモリの内容を表示するには、**show flash** コマンドを入力します。フラッシュ メモリの内容リストには、各ファイルのチェックサムは含まれません。イメージをフラッシュ メモリにコピーしたあとで、イメージのチェックサムを再計算したり、確認したりする場合は、**verify** コマンドを入力します。

装置を指定したあとに、コロン (:) を入力する必要があります。

例

次に、**verify** コマンドを使用する例を示します。

```

Router# verify cat6k_r47_1.cbi
.....
File cat6k_r47_1.cbi verified OK.
Router#

```

次に、MD5 シグニチャを手動でチェックする例を示します。

```

Router# verify /md5 c6msfc2-jsv-mz
.....
.....
.....Done!
verify /md5 (disk0:c6msfc2-jsv-mz) = 0f369ed9e98756f179d4f29d6e7755d3
Router#

```

次に、システムが MD5 シグニチャを比較できるようにする例を示します。

```

Router# verify /md5 disk0:c6msfc2-jsv-mz 0f369ed9e98756f179d4f29d6e7755d3
.....
.....
.....Done!
verified /md5 (disk0:c6sup12-jsv-mz) = 0f369ed9e98756f179d4f29d6e7755d3
Router#

```

次に、圧縮された Cisco IOS イメージのチェックサムを確認する例を示します。

```

Router# verify /ios disk0:c6k222-jsv-mz
Verified compressed IOS image checksum for disk0:c6k222-jsv-mz
Router#

```

関連コマンド

コマンド	説明
copy /noverify	現在のコピー操作の自動イメージ確認をディセーブルにします。
file verify auto	圧縮された Cisco IOS イメージのチェックサムを確認します。

コマンド	説明
show file systems (フラッシュ ファイル システム)	使用可能なファイル システムを表示します。
show flash	フラッシュ メモリのレイアウトと内容を表示します。

vlan (config-VLAN submode)

特定の VLAN を設定するには、config-VLAN サブモードで **vlan** コマンドを使用します。VLAN を削除するには、このコマンドの **no** 形式を使用します。

vlan *vlan-id*

no vlan *vlan*

シンタックスの説明

<i>vlan-id</i>	VLAN の番号。有効値は 1 ~ 4094 です。
----------------	----------------------------

コマンドのデフォルト

デフォルト設定は次のとおりです。

- *vlan-name* : [VLANxxxx]。[xxxx] は、VLAN ID 番号に等しい 4 桁の数値（先行ゼロを含む）を表します。
- **media type** : ethernet
- **state** : active
- *said-value* : 100000 に VLAN ID 番号を加えた値
- *mtu-size* : デフォルト値は、VLAN タイプによって異なります。
 - **ethernet** : 1500
 - **fddi** : 1500
 - **trcrf** : 1500 (V2 がイネーブルでない場合) または 4472 (V2 がイネーブルの場合)
 - **fd-net** : 1500
 - **trbrf** : 1500 (V2 がイネーブルでない場合) または 4472 (V2 がイネーブルの場合)
- *ring-number* : リング番号は指定されません。
- *bridge-number* : ブリッジ番号は指定されません。
- *parent-vlan-id* : 親 VLAN は指定されません。
- *type* : STP タイプは指定されません。
- *tb-vlan1* および *tb-vlan2* : 0 (トランスレーショナル ブリッジ VLAN が指定されないことを意味します)

コマンド モード

config-VLAN サブモード

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

VLAN 1 パラメータは出荷時に設定されていて、変更できません。VLAN 1 は削除できません。
config-VLAN サブモードを開始すると、次の構文が使用可能になります。

```
{are hops} {backupcrf mode} {bridge type | bridge-num} {exit} {media type} {mtu
mtu-size} {name vlan-name} {parent parent-vlan-id} {private-vlan} {remote-span}
{ring ring-number} {said said-value} {shutdown} {state {suspend | active}} {stp
type type} {ste hops} {tb-vlan1 tb-vlan1-id} {tb-vlan2 tb-vlan2-id}

no {are | backupcrf} {bridge type} | exit | media | mtu | name | parent | private-vlan |
remote-span | ring | said | shutdown | state | {stp type type} | {ste hops}}
```

are hops	この VLAN の All Route Explorer ホップの最大数を指定します。有効値は 0 ~ 13 です。値を指定しなければ 0 と見なされます。
backupcrf mode	VLAN のバックアップ CRF (コンセントレータ リレー機能) モードをイネーブルまたはディセーブルにします。有効値は enable または disable です。
bridge type bridge-num	VLAN のブリッジ特性またはブリッジの ID 番号を指定します。type の有効値は srb または srt です。bridge-num の有効値は 0 ~ 15 です。
exit	変更を適用し、リビジョン番号を増分して、config-VLAN サブモードを終了します。
media type	VLAN のメディア タイプを指定します。有効値は ethernet 、 fd-net 、 fddi 、 trcrf 、および trbrf です。
mtu mtu-size	VLAN が使用できる最大伝送ユニット (バイトで表したパケット サイズ) を指定します。有効値は 1500 ~ 18,190 です。
name vlan-name	VLAN 名として使用される文字列を定義します (1 ~ 32 文字)。
parent parent-vlan-id	FDDI の親 VLAN またはトークンリングタイプ VLAN の ID 番号を指定します。有効値は 1 ~ 1005 です。
private-vlan	(任意) VLAN を PVLAN として設定します。private-vlan コマンドを参照してください。
remote-span	VLAN を RSPAN VLAN として設定します。
ring ring-number	FDDI またはトークンリングタイプ VLAN のリング番号を指定します。有効値は 0 ~ 65,535 です。
said said-value	Security Association Identifier (SAID) を指定します。有効値は 1 ~ 4,294,967,294 です。
shutdown	VLAN スイッチングをシャットダウンします。
state {suspend active}	VLAN の状態がアクティブであるか一時停止であるかを指定します。
stp type type	STP タイプを指定します。有効値は ieee 、 ibm 、および auto です。
ste hops	Spanning-Tree Explorer フレームの最大ホップ数を指定します。有効値は 0 ~ 13 です。
tb-vlan1 tb-vlan1-id	この VLAN の第 1 のトランスレーショナル VLAN の ID 番号を指定します。有効値は 1 ~ 1005 です。値を指定しなければ 0 と見なされます。
tb-vlan2 tb-vlan2-id	この VLAN の第 2 のトランスレーショナル VLAN の ID 番号を指定します。有効値は 1 ~ 1005 です。値を指定しなければ 0 と見なされます。

**注意**

PVLAN (プライマリまたはセカンダリ) 上の `config-vlan` モードで `shutdown` コマンドを入力して、次に `no shutdown` コマンドを入力すると、PVLAN タイプおよびアソシエーション情報が削除されず、VLAN が PVLAN になるよう再設定する必要があります。

一時停止状態の VLAN は、パケットを送受信しません。

`config-VLAN` サブモードを終了するまで、作成または変更された VLAN は実行されません。

グローバル コンフィギュレーション モードで `vlan-range` を定義した場合は、`config-VLAN` サブモードで `vlan-name` を設定できません。

レイヤ 2 VLAN 名の最大長は 32 文字です。

**(注)**

新しい VLAN を追加しようとしたときに、VLAN がすでに存在する場合は、処理が行われません。

拡張範囲 VLAN (1006 ~ 4094) の場合に設定できる VLAN パラメータは、`private-vlan`、`rspan`、および `mtu` だけです。拡張範囲 VLAN では、残りの VLAN パラメータはデフォルトに設定されます。

`vlan-name` を定義する場合は、管理ドメイン内で一意な名前を付ける必要があります。

SAID は 802.10 に記載されています。`no` 形式を使用すると、VLAN の SAID はデフォルトに戻ります。`said-value` を定義する場合は、管理ドメイン内で一意な名前を付ける必要があります。

`bridge bridge-number` 引数は、トークンリングネットおよび FDDI ネット VLAN の場合だけ使用します。他のタイプの VLAN では、無視されます。`no` 形式を使用すると、VLAN のソースルーティングブリッジ番号はデフォルトに戻ります。

親 VLAN が削除されるか、または `media` キーワードによって VLAN タイプまたは親 VLAN の VLAN タイプが変更された場合、親 VLAN はデフォルトにリセットされます。

`tb-vlan1` および `tb-vlan2` は、特定の VLAN タイプのトランスレーショナルブリッジ VLAN を設定する場合に使用します。他のタイプの VLAN では、使用できません。トランスレーショナルブリッジ VLAN には、関係する VLAN と異なる VLAN タイプを指定する必要があります。2 つの VLAN を指定する場合は、それぞれ異なる VLAN タイプを指定する必要があります。

トランスレーショナルブリッジ VLAN が削除されるか、または `media` キーワードを入力して VLAN タイプまたは対応するトランスレーショナルブリッジ VLAN の VLAN タイプが変更された場合、トランスレーショナルブリッジ VLAN はデフォルトにリセットされます。

`shutdown` キーワードは、拡張範囲 VLAN をサポートしません。

VLAN が内部的にシャットダウンされているかどうかを判別するには、`show vlan` コマンド出力の `Status` フィールドを確認します。VLAN が内部的にシャットダウンされている場合、次の値が `Status` フィールドに表示されます。

- `act/ishut` : VLAN ステータスはアクティブですが、内部的にシャットダウンされています。
- `sus/ishut` : VLAN ステータスは一時停止ですが、内部的にシャットダウンされています。

例

次に、新しい VLAN データベースに、すべてのパラメータがデフォルトである新しい VLAN を追加する例を示します。

```
Router(config-vlan)# vlan 2
Router(config-vlan)#
```

次に、新しい VLAN を追加し、メディア タイプおよび親 VLAN ID 番号 3 を指定し、他のパラメータがすべてデフォルトとなるように装置を設定する例を示します。

```
Router(config-vlan)# media ethernet parent 3
VLAN 2 modified:
  Media type ETHERNET
  Parent VLAN 3
Router(config-vlan)#
```

次に、VLAN 2 を削除する例を示します。

```
Router(config-vlan)# no vlan 2
Router(config-vlan)#
```

次に、該当タイプの MTU およびトランスレーショナルブリッジ VLAN をデフォルト設定に戻す例を示します。

```
Router(config-vlan)# no mtu tb-vlan1 tb-vlan2
Router(config-vlan)#
```

関連コマンド

コマンド	説明
show vlan	VLAN 情報を表示します。

vlan (global configuration mode)

VLAN を追加して、config-VLAN サブモードを開始するには、**vlan** コマンドを使用します。VLAN を削除するには、このコマンドの **no** 形式を使用します。

```
vlan {vlan-id | vlan-range}
```

```
no vlan {vlan-id | vlan-range}
```

シンタックスの説明

<i>vlan-id</i>	VLAN の番号。有効値は 1 ～ 4094 です。
<i>vlan-range</i>	設定された VLAN の範囲。有効値の一覧については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドモード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

VLAN 1 パラメータは出荷時に設定されていて、変更できません。

config-VLAN サブモードを終了すると、指定された VLAN が VLAN データベースに対して追加または変更されます。

vlan *vlan-id* コマンドを入力すると、一時バッファ内のすべてのデフォルト パラメータを使用して新規 VLAN が作成され、CLI は config-VLAN サブモードを開始します。入力した *vlan-id* が既存の VLAN と一致する場合は、config-VLAN サブモードを開始する以外の処理は行われません。

vlan-range を定義した場合は、config-VLAN サブモードで *vlan-name* を設定できません。

vlan-range を入力するには、カンマ (,)、ダッシュ (-)、および数値を使用します。

config-VLAN サブモードで使用できるコマンドの詳細については、[vlan \(config-VLAN submode\)](#) コマンドを参照してください。

例

次に、新規 VLAN を追加して、config-VLAN サブモードを開始する例を示します。

```
Router (config)# vlan 2
Router (config-vlan)#
```

次に、新規 VLAN 範囲を追加して、config-VLAN サブモードを開始する例を示します。

```
Router (config)# vlan 2,5,10-12,20,25,4000
Router (config-vlan)#
```

次に、VLAN を削除する例を示します。

```
Router (config)# no vlan 2  
Router (config)#
```

関連コマンド

コマンド	説明
vlan (config-VLAN submode)	特定の VLAN を設定します。

vlan access-log

ログ テーブル サイズ、リダイレクト パケット レート、ロギングしきい値などの VACL ロギング プロパティを設定するには、**vlan access-log** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
vlan access-log { {maxflow max-number} | {ratelimit pps} | {threshold pkt-count} }
```

```
no vlan access-log { maxflow | ratelimit | threshold }
```

シンタックスの説明

maxflow <i>max-number</i>	最大ログ テーブル サイズを指定します。有効値は 0 ~ 2048 です。0 を指定すると、ログ テーブルの内容は削除されます。
ratelimit <i>pps</i>	リダイレクト VACL ロギング パケット レートの最大値を指定します。有効値は 0 ~ 5000 です。
threshold <i>pkt-count</i>	ロギング アップデートのしきい値を指定します。有効値は 0 ~ 2147483647 です。0 は、しきい値が設定されていないことを意味します。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- *max-number* は **500** です。
- *pps* は **2000 pps** です。
- *pkt-count* は設定されていません。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

リダイレクトされたパケットにはレート制限機能が適用されるため、VACL ログ カウンタが不正確になることがあります。

拒否された IP パケットだけが記録されます。

ログ テーブル サイズが限界に達した場合、新しいフローのロギング パケットはソフトウェアによって廃棄されます。

リダイレクト VACL ロギング パケット レートの最大値制限を超えるパケットは、ハードウェアによって廃棄されます。

5 分経過する前にフローのしきい値に達すると、ロギング メッセージが表示されます。

最大ログ テーブル サイズ、最大パケット レート、またはしきい値が設定されていない場合、またはこのコマンドの **no** 形式を入力した場合は、デフォルト値が使用されます。

例

次に、最大ログ テーブル サイズを設定する例を示します。

```
Router(config)# vlan access-log maxflow 500  
Router(config)#
```

次に、パケット廃棄基準となるリダイレクト VACL ログイング パケット レートの最大値を設定する例を示します。

```
Router(config)# vlan access-log ratelimit 200  
Router(config)#
```

次に、ログイング アップデートのしきい値を設定する例を示します。

```
Router(config)# vlan access-log threshold 3500  
Router(config)#
```

関連コマンド

コマンド	説明
show vlan access-log	設定されたログイング プロパティなどの VACL ログイングに関する情報を表示します。

vlan access-map

VLAN アクセス マップを作成したり、VLAN アクセス マップ コマンド モードを開始したりするには、**vlan access-map** コマンドを使用します。マッピング シーケンスまたはマップ全体を削除するには、このコマンドの **no** 形式を使用します。

```
vlan access-map name [seq#]
```

```
no vlan access-map name [seq#]
```

シンタックスの説明

<i>name</i>	VLAN アクセスマップのタグ
<i>seq#</i>	(任意) マップ シーケンス番号。有効値は 0 ~ 65,535 です。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンドのデフォルト

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

既存のマップ シーケンスのシーケンス番号を入力すると、VLAN アクセスマップ モードを開始します。シーケンス番号を指定しないと、番号が自動的に割り当てられます。各マップ シーケンスには、**match** 句および **action** 句をそれぞれ 1 つずつ指定できます。

シーケンス番号を指定しないで **no vlan access-map name [seq#]** コマンドを入力すると、マップ全体が削除されます。

VLAN アクセスマップ モードを開始すると、次のコマンドが使用可能になります。

- **action** : パケットの **action** 句を指定します。**action** コマンドを参照してください。
- **default** : コマンドをデフォルトに設定します。
- **end** : コンフィギュレーション モードを終了します。
- **exit** : VLAN アクセス マップ コンフィギュレーション モードを終了します。
- **match** : **match** 句を指定します。**match** コマンドを参照してください。
- **no** : コマンドを否定するか、またはデフォルトを設定します。

例 次に、VLAN アクセスマップ モードを開始する例を示します。

```
Router(config)# vlan access-map Bob
Router(config-access-map)#
```

関連コマンド

コマンド	説明
action	パケットの action 句を設定します。
match	VLAN アクセス マップ シーケンスの ACL を 1 つまたは複数選択して、match 句を指定します。
show vlan access-map	VLAN アクセス マップの内容を表示します。

vlan database

VLAN コンフィギュレーション サブモードを開始するには、**vlan database** コマンドを使用します。

vlan database

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC (#)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

VLAN コンフィギュレーション サブモードでは、次のような VLAN データベース編集バッファの **manipulation** コマンドにアクセスできます。

- **abort** : 変更を適用しないで、モードを終了します。
- **apply** : 現在の変更を適用して、リビジョン番号を増分します。
- **exit** : 変更を適用し、リビジョン番号を増分して、モードを終了します。
- **no** : コマンドを否定するか、またはデフォルトを設定します。有効なキーワードは **vlan** および **vtp** です。
- **reset** : 現在の変更を放棄して、現在のデータベースを再度読み込みます。
- **show** : データベース情報を表示します。
- **vlan** : 単一 VLAN に関連付けられた値を追加、削除、または変更するためのサブコマンドにアクセスします。**vlan** サブコマンドの詳細については、**vlan (config-VLAN submode)** コマンドを参照してください。
- **vtp** : VTP 管理機能を実行するためのサブコマンドにアクセスします。**vtp** サブコマンドの詳細については、**vtp** コマンドを参照してください。

例

次に、VLAN コンフィギュレーション モードを開始する例を示します。

```
Router# vlan database
Router(vlan)#
```

次に、VLAN コンフィギュレーション モードの場合に、変更を適用しないで VLAN コンフィギュレーション モードを終了する例を示します。

```
Router(vlan)# abort
Aborting....
Router#
```

次に、VLAN コンフィギュレーション モードの場合、VLAN を削除する例を示します。

```
Router(vlan)# no vlan 100
Deleting VLAN 100...
Router(vlan)#
```

次に、VLAN コンフィギュレーション モードの場合に、プルーンングをオフにする例を示します。

```
Router(vlan)# no vtp pruning
Pruning switched OFF
Router(vlan)#
```

関連コマンド

コマンド	説明
show vlan	VLAN 情報を表示します。

vlan dot1q tag native

Tdot1q タギングをトランク内のすべての VLAN についてイネーブルにするには、**vlan dot1q tag native** コマンドを使用します。設定を消去するには、このコマンドの **no** 形式を使用します。

vlan dot1q tag native

no vlan dot1q tag native

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

vlan dot1q tag native コマンドは、ネイティブ VLAN トラフィックにタグを付けて、802.1Q トランク上で 802.1Q タグ付きフレームだけを許可するようにスイッチを設定します。ネイティブ VLAN 内のタグなしトラフィックを含めて、タグなしトラフィックはすべて廃棄されます。

レイヤ 2 プロトコル トンネリングを設定する場合は、次に示す設定時の注意事項に従ってください。

- すべてのサービス プロバイダー エッジ スイッチの 802.1Q トンネル ポート上で、スパニングツリー BPDU フィルタリングをイネーブルにするには、**spanning-tree bpdupfilter enable** コマンドを入力する必要があります。
- ネイティブ VLAN タギングに対して、少なくとも 1 つの VLAN が使用可能であることを確認します。使用可能なすべての VLAN が使用されている場合に、**vlan dot1q tag native** コマンドを入力しても、ネイティブ VLAN タギングはイネーブルになりません。
- すべてのサービス プロバイダー コア スイッチ上で、ネイティブ VLAN 出力トラフィックにタグを付けて、タグなしネイティブ VLAN 入力トラフィックを廃棄するには、**vlan dot1q tag native** コマンドを入力します。
- すべてのカスタマー スイッチ上で、スイッチごとにネイティブ VLAN タギングをイネーブルまたはディセーブルにします。



(注) dot1q タギングがイネーブルになっているスイッチとディセーブルになっているスイッチが混在している場合は、すべてのトラフィックが廃棄されます。したがって、各スイッチ上で dot1q タギングの設定を同じにする必要があります。

例

次に、トランク内のすべての VLAN の dot1q タギングをイネーブルにする例を示します。

```
Router(config)# vlan dot1q tag native  
Router(config)#
```

関連コマンド

コマンド	説明
show vlan dot1q tag native	ネイティブ VLAN のタギング情報を表示します。

vlan filter

VLAN アクセス マップを適用するには、**vlan filter** コマンドを使用します。VLAN またはインターフェイスから VLAN アクセス マップをクリアするには、このコマンドの **no** 形式を使用します。

```
vlan filter map-name {vlan-list vlan-list | interface interface number}
```

```
no vlan filter map-name {vlan-list [vlan-list] | interface [interface interface-number]}
```

シンタックスの説明

<i>map-name</i>	VLAN アクセスマップのタグ
<i>vlan-list</i>	VLAN リスト。有効値は 1 ~ 4094 です。
interface <i>interface</i>	インターフェイス タイプを指定します。有効値は pos 、 atm 、または serial です。詳細については、「使用上のガイドライン」を参照してください。
<i>interface-number</i>	インターフェイス番号。詳細については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

VLAN アクセス マップに **action** 句を設定する場合は、次の点に注意してください。

- VLAN アクセス マップは、1 つまたは複数の VLAN または WAN インターフェイスに適用できます。
- *vlan-list* 引数には単一の VLAN ID、VLAN ID リスト、または VLAN ID 範囲 (*vlan-id-vlan-id*) を指定できます。複数のエントリはハイフン (-) またはカンマ (,) で区切ります。
- VACL が適用された WAN インターフェイスを削除すると、インターフェイス上の VACL 設定も削除されます。
- 各 VLAN または各 WAN インターフェイスには、VLAN アクセス マップを 1 つだけ適用できます。
- VLAN に適用した VACL がアクティブになるのは、レイヤ 3 VLAN インターフェイスが設定されている VLAN に適用された場合だけです。レイヤ 3 VLAN インターフェイスを備えていない VLAN に適用された VACL は、非アクティブです。レイヤ 3 VLAN インターフェイスを備えていない VLAN に VLAN アクセス マップを適用すると、VLAN アクセス マップをサポートするレイヤ 3 VLAN インターフェイスが、管理上のダウン状態で作成されます。レイヤ 3 VLAN インターフェイスの作成に失敗すると、VACL は非アクティブになります。

このコマンドの **no** 形式を入力する場合、*vlan-list* 引数はオプションです (ただし、キーワード **vlan-list** は必須です)。*vlan-list* 引数を入力しないと、*map-name* 引数が適用されるすべての VLAN から VACL が削除されます。

WAN インターフェイスにこのコマンドの **no** 形式を入力する場合、*interface* 引数はオプションです (ただし、**interface** キーワードは必須です)。*interface* 引数を入力しないと、*map-name* が適用されるインターフェイスから VACL が削除されます。

vlan filter map-name interface コマンドに対応しているのは、ATM、POS、またはシリアル インターフェイス タイプだけです。Catalyst 6500 シリーズスイッチにこれらのインターフェイス タイプが装備されていない場合は、**interface interface interface-number** キーワードおよび引数を使用できません。

interface-number の形式は、*mod/port* または *slot/port-adapter/port* です。サブインターフェイスまたはチャンネル グループ記述子を含めることができます。

例

次に、VLAN 7～9 に VLAN アクセス マップを適用する例を示します。

```
Router(config)# vlan filter ganymede vlan-list 7-9
Router(config)#
```

関連コマンド

コマンド	説明
action	パケットの action 句を設定します。
match	VLAN アクセス マップ シーケンスの ACL を 1 つまたは複数選択して、 match 句を指定します。
show vlan filter	VLAN フィルタに関する情報を表示します。

vlan internal allocation policy

内部 VLAN 割り当て方向を設定するには、**vlan internal allocation policy** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

vlan internal allocation policy {ascending | descending}

no vlan internal allocation policy

シンタックスの説明

ascending 1006 ~ 4094 の内部 VLAN を割り当てます。

descending 4094 ~ 1006 の内部 VLAN を割り当てます。

コマンドのデフォルト

ascending

コマンドモード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース

変更内容

12.2(18)ZY

このコマンドのサポートが追加されました。

使用上のガイドライン

内部 VLAN 割り当ては 1006 から昇順、あるいは 4094 から降順となるように設定できます。

内部 VLAN およびユーザ定義 VLAN は、1006 ~ 4094 の VLAN スペースを共有します。これらのスペースの割り当てには、先入れ先出し (FIFO) ポリシーが使用されます。

vlan internal allocation policy コマンドによる変更を有効にするには、システムを再起動する必要があります。システム起動中に、**startup-config** ファイルに記述された機能に必要な内部 VLAN が最初に割り当てられます。次に、**startup-config** ファイル内のユーザ定義 VLAN が設定されます。既存の内部 VLAN と競合する VLAN を設定すると、内部 VLAN が解放されて使用可能になるまで、設定された VLAN は動作不能状態になります。

write memory コマンドを入力して、リロードを行うと、ポート マネージャでは再設定された割り当てが使用されます。

例

次に、内部 VLAN 割り当てポリシーとして、VLAN を降順に設定する例を示します。

```
Router(config)# vlan internal allocation policy descending
Router(config)#
```

関連コマンド

コマンド

説明

[show vlan internal usage](#)

内部 VLAN 割り当てに関する情報を表示します。

vlan mapping dot1q

802.1Q VLAN と ISL VLAN をマッピングするには、**vlan mapping dot1q** コマンドを使用します。指定されたマッピング、または 802.1Q VLAN と ISL VLAN のすべてのマッピングを削除するには、このコマンドの **no** 形式を使用します。

```
vlan mapping {dot1q dot1q-vlan-id} {isl isl-vlan-id}
```

```
no vlan mapping {dot1q dot1q-vlan-id | all}
```

シンタックスの説明	
dot1q dot1q-vlan-id	発信されたトラフィックがローカル装置上の 802.1Q トランクに着信するときのマッピング元となる 802.1Q VLAN の VLAN ID を指定します。有効値は 1 ~ 4094 です。
isl isl-vlan-id	発信されたトラフィックがローカル装置上の 802.1Q トランクに着信するときのマッピング先となる ISL VLAN の VLAN ID を指定して、ローカル装置に着信したときにトラフィックを廃棄する 802.1Q VLAN の VLAN ID を指定します。有効値は 1 ~ 4094 です。
all	802.1Q VLAN と ISL VLAN のすべてのマッピングを削除します。

コマンドのデフォルト 802.1Q VLAN ID のデフォルトの ID マッピングは、1 ~ 4094 です。

コマンド モード グローバル コンフィギュレーション (config)

コマンドの履歴	リリース	変更内容
	12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン VLAN 1 パラメータは出荷時に設定されていて、変更できません。

最大 8 つの VLAN をマッピングできます。1 つの ISL VLAN にマッピングできる 802.1Q VLAN は 1 つだけです。たとえば、802.1Q VLAN 800 が ISL VLAN 800 に自動的にマッピングされている場合は、他の 802.1Q VLAN を ISL VLAN 800 に手動でマッピングしないでください。

既存の 802.1Q VLAN マッピングを上書きすることはできません。802.1Q VLAN 番号がすでに存在する場合、コマンドは中断されます。最初に、既存のマッピングを消去する必要があります。

テーブルがいっぱいである場合は、コマンドが中断され、テーブルがいっぱいであることを示すエラーメッセージが表示されます。

例 次に、VLAN 1001 の 802.1Q トランクに着信したトラフィックをローカル装置上の ISL VLAN 888 にマッピングし、VLAN 888 の 802.1Q トランクに着信したトラフィックを廃棄し、ローカル装置の ISL VLAN 888 から発信されたトラフィックを発信時に 802.1Q VLAN 1001 にマッピングする例を示します。

```
Router(config)# vlan mapping dot1q 1001 isl 888
Router(config)#
```

■ vlan mapping dot1q

次に、802.1Q VLAN 1001 と ISL VLAN 888 のマッピングを消去する例を示します。その結果、802.1Q VLAN 1001 トラフィックはローカル装置に着信するときに廃棄され、802.1Q VLAN 888 トラフィックは ISL VLAN 888 にマッピングされます（両方ともデフォルト状態）。

```
Router(config)# no vlan mapping dot1q 1001
No mapping for 1022
Router(config)#
```

関連コマンド

コマンド	説明
show vlan	VLAN 情報を表示します。
vlan (config-VLAN submode)	特定の VLAN を設定します。
vlan database	VLAN コンフィギュレーション サブモードを開始します。

vtp

グローバル VTP ステートを設定するには、**vtp** コマンドを使用します。デフォルト値に戻すには、次のようにします。

```

vtp {domain domain-name}
vtp {file filename}
vtp {interface interface-name} [only]
vtp {mode {client | server | transparent}}
vtp {password password-value}
vtp pruning
vtp {version {1 | 2}}

```

シンタックスの説明

domain <i>domain-name</i>	VTP 管理ドメイン名を設定します。
file <i>filename</i>	VTP コンフィギュレーションを保存する IFS ファイル システム ファイルの ASCII 名を設定します。
interface <i>interface-name</i>	この装置の VTP アップデータ ID の推奨送信元の名前を設定します。
only	(任意)VTP IP アップデータ アドレスとして現在のインターフェイスの IP アドレスだけを使用するように指定します。
mode client	VTP 装置のモードタイプをクライアント モードに設定します。
mode server	VTP 装置のモードタイプをサーバ モードに設定します。
mode transparent	VTP 装置のモードタイプをトランスペアレント モードに設定します。
password <i>password-value</i>	管理ドメイン パスワードを指定します。
pruning	管理ドメインによるプルーニングの許可をイネーブルにします。
version 1 2	管理ドメイン VTP バージョン番号を指定します。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- **vtp domain** および **vtp interface** コマンドには、デフォルト設定がありません。
- *filename* は **const-nvram:vlan.dat** です。
- VTP モードは **mode server** です。
- パスワードは設定されていません。
- プルーニングはディセーブルです。
- **version 1** です。

コマンド モード

グローバル コンフィギュレーション (config)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



(注)

vtp pruning、**vtp password**、および **vtp version** コマンドは、特権 EXEC モードでも使用できます。これらのコマンドはグローバル コンフィギュレーション モードだけで使用し、特権 EXEC モードでは使用しないでください。

拡張範囲 VLAN は、VTP ではサポートされません。

domain-name を定義する場合は、大文字と小文字を区別する 1 ~ 32 文字のドメイン名を指定してください。

filename および *interface-name* は、1 ~ 255 文字の ASCII 文字列です。

スイッチがセキュア モードの場合、管理ドメイン内の各ネットワーク装置にパスワードを設定する必要があります。



注意

VTP をセキュア モードで設定した場合、ドメイン内の各ネットワーク装置に管理ドメイン パスワードを割り当てないと、管理ドメインは正常に動作しません。

VTP バージョン 2 対応のネットワーク装置上で VTP バージョン 2 をディセーブルに設定している場合、その VTP バージョン 2 対応ネットワーク装置は、同じ VTP ドメイン内で、VTP バージョン 1 が実行されているネットワーク装置として動作できます (VTP バージョン 2 は、デフォルトでディセーブルに設定されています)。

同じ VTP ドメイン内のすべてのネットワーク装置がバージョン 2 に対応する場合以外は、ネットワーク装置上で VTP バージョン 2 をイネーブルにしないでください。いずれかのネットワーク装置上で VTP バージョン 2 をイネーブルにすると、ドメイン内のすべてのバージョン 2 対応ネットワーク装置上で VTP バージョン 2 がイネーブルになります。

トークンリング環境で、VLAN スイッチング機能を正常に動作させるには、VTP バージョン 2 をイネーブルにする必要があります。

VTP サーバ上で VTP プルーニングをイネーブルまたはディセーブルにすると、管理ドメイン全体で VTP プルーニングがイネーブルまたはディセーブルになります。

Catalyst 6500 シリーズ スイッチ上で VLAN をプルーニング適格または不適格として設定した場合に、影響を受けるのは、そのスイッチ上の VLAN のプルーニング適性だけです。VTP ドメイン内のすべてのネットワーク装置のプルーニング適性に影響するわけではありません。

vtp password、**vtp pruning**、および **vtp version** コマンドは、NVRAM に格納されず、VTP トランスペアレントモード スタートアップ コンフィギュレーション ファイルに格納されます。

拡張範囲 VLAN は、VTP ではサポートされません。

pruning は VTP サーバ モードで設定できます。**version** は、VTP サーバ モードまたはトランスペアレント モードで設定できます。

password-value は、装置の管理ドメインを識別する 8 ~ 64 文字の ASCII 文字列です。

VTP プルーニングが設定されていると、プルーニング適格 VLAN に属するステーションがない場合、この VLAN に関する情報が VTP アップデートから削除されます。

VTP ドメイン内のすべての Catalyst 6500 シリーズスイッチで、同じ VTP バージョンを実行する必要があります。同一 VTP ドメイン内の Catalyst 6500 シリーズスイッチで、VTP バージョン 1 とバージョン 2 を同時に実行することはできません。

ドメイン内のすべての Catalyst 6500 シリーズスイッチが VTP バージョン 2 対応である場合は、1 つの Catalyst 6500 シリーズスイッチ上で VTP バージョン 2 をイネーブルにすると、バージョン番号が VTP ドメイン内の他のバージョン 2 対応 Catalyst 6500 シリーズスイッチに伝播します。

バージョン 2 モードを切り替えると、特定のデフォルト VLAN のパラメータが変更されます。詳細については、『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*』を参照してください。

例

次に、装置の管理ドメインを設定する例を示します。

```
Router(config)# vtp domain DomainChandon
Router(config)#
```

次に、VTP コンフィギュレーションを保存する IFS ファイル システム内のファイルを指定する例を示します。

```
Router(config)# vtp file vtpconfig
Setting device to store VLAN database at filename vtpconfig.
Router(config)#
```

次に、VTP モードをクライアント モードに設定する例を示します。

```
Router(config)# vtp mode client
Setting device to VTP CLIENT mode.
Router(config)#
```

関連コマンド

コマンド	説明
show vtp	VTP 統計情報とドメイン情報を表示します。

wrr-queue

標準送信 Shaped Round Robin (SRR; シェイプド ラウンド ロビン)、DWRR、または WRR キュー間の帯域幅を割り当てるには、**wrr-queue** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
wrr-queue [bandwidth | shape] {percent low-priority-queue-percentage
[intermediate-priority-queue-percentages] high-priority-queue-percentage}
```

```
wrr-queue [bandwidth | shape] {percent low-priority-queue-weight
[intermediate-priority-queue-weight] high-priority-queue-weight}
```

```
no wrr-queue [bandwidth | shape]
```

シンタックスの説明

bandwidth	(任意) bandwidth キーワードを入力して、DWRR または WRR を設定します。
shape	(任意) shape キーワードを入力して、SRR を設定します。
percent low-priority-queue-percentage	(任意) 最小の割合を指定します。有効値は、1 ~ 100 です。
<i>intermediate-priority-queue-percentage</i>	(任意) 中間の割合。有効値は、1 ~ 100 です。
<i>high-priority-queue-percentage</i>	最大の割合。有効値は、1 ~ 100 です。
<i>low-priority-queue-weight</i>	最小の重み。有効値は、1 ~ 255 です。
<i>intermediate-priority-queue-weight</i>	(任意) 中間の重み。有効値は、1 ~ 255 です。
<i>high-priority-queue-weight</i>	最大の重み。有効値は、1 ~ 255 です。

コマンドのデフォルト

表 2-96 に、デフォルト設定を示します。

表 2-96 帯域幅のデフォルト値

ポート タイプ	デフォルト値
2q8t	90:10
8q4t	90:0:0:0:0:0:10
8q8t	90:0:0:0:0:0:10
1p7q8t	22:33:45:0:0:0:0
1p2q1t	100:255
2q2t、1p2q2t、および 1p2q1t	5:255
1p3q1t	100:150:255

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

SRR を使用する場合、キューは割り当てられた帯域幅だけを使用します。SRR は、Supervisor Engine 32 SFP 1p3q8t ポートおよび 1p7q4t ポート上のオプションとしてサポートされます。SRR を使用すると、完全優先キューの使用が妨げられます。SRR を設定するには、完全優先キューにマッピングされた CoS または DSCP 値を標準キューに再度マッピングする必要があります。

DWRR は、送信の際にハイ プライオリティ キューのトラフィックによって生じるロー プライオリティ キューをすべて追跡し、次のラウンドで補正します。DWRR は、1p3q1t、1p2q1t、1p3q8t、1p7q4t、および 1p7q8t ポート上でサポートされるデキューイング アルゴリズムです。

WRR では、他のキューが帯域幅を使用しない場合、キューは割り当てられた帯域幅を超えてポートの最大帯域幅を使用できます。WRR はすべてのポートでサポートされているデキューイング アルゴリズムです。

割り当てられた割合または重みが大きいキューほど、多くの送信帯域幅が割り当てられます。重みを入力する場合、重みの比率によってキューの合計帯域幅が分割されます。たとえば、ギガビットイーサネット ポート上の 3 つのキューの場合、重みは 25:25:50 になり、次のように割り当てられます。

- キュー 1 : 250 Mbps
- キュー 2 : 250 Mbps
- キュー 3 : 500 Mbps

WRR を使用すると、出力ポートで帯域幅を共有できます。このコマンドは、スケジューリング重みによって、出力 WRR の帯域幅を定義します。

WRR 重みは、すべてのキューが空でない場合に、キュー間で帯域幅を分割するために使用されます。たとえば、重み 1 : 3 を入力すると、1 つのキューに帯域幅の 25%、もう一方のキューに 75% が割り当てられます。

重み 1 : 3 を入力した場合と重み 10 : 30 を入力した場合で、必ずしも同じ結果が得られるとは限りません。重みが 10 : 30 の場合は、各キューで処理されるデータ量が増え、もう一方のキューで処理されるパケットの遅延が大きくなります。ロー プライオリティ キューで少なくとも 1 つのパケット（最大サイズ）を一度に処理できるように、重みを設定する必要があります。プライオリティが高いほうのキューには、一度に複数のパケットが処理されるように重みを設定します。

追加できる割合の最大値は 100 です。ポート上のすべての標準送信キューに対して割合を入力する必要があります。

重量範囲の有効値は、1 ~ 255 です。ポート上のすべての標準送信キューに対して重みを入力する必要があります。

例

次に、3 対 1 の帯域幅比率を割り当てる例を示します。

```
Router(config-if)# wrr-queue bandwidth 3 1
Router(config-if)#
```

関連コマンド

コマンド	説明
show queueing interface	キューイング情報を表示します。
wrr-queue queue-limit	インターフェイス上の送信キュー サイズ比を設定します。

■ `wrr-queue`

wrr-queue cos-map

CoS 値をキューの廃棄しきい値にマッピングするには、**wrr-queue cos-map** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
wrr-queue cos-map queue-id threshold-id cos-1 ... cos-n
```

```
no wrr-queue cos-map
```

シンタックスの説明

<i>queue-id</i>	キュー番号。有効値は 1 です。
<i>threshold-id</i>	しきい値 ID。有効値は 1 ~ 4 です。
<i>cos-1 ... cos-n</i>	CoS 値。有効値は 0 ~ 7 です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- 受信キュー 1/廃棄しきい値 1 および送信キュー 1/廃棄しきい値 1 : CoS 0 および 1。
- 受信キュー 1/廃棄しきい値 2 および送信キュー 1/廃棄しきい値 2 : CoS 2 および 3。
- 受信キュー 2/廃棄しきい値 3 および送信キュー 2/廃棄しきい値 1 : CoS 4 および 6。
- 受信キュー 2/廃棄しきい値 4 および送信キュー 2/廃棄しきい値 2 : CoS 7。
- 1p1q4t、1p2q2t、および 1p3q1t インターフェイスでは、CoS 5 が完全優先キューにマッピングされます。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

しきい値にマッピングする CoS 値を、最大 8 つ入力します。

1p3q1t のしきい値は常に 1 です。

例

次に、標準送信キュー 1/しきい値 1 に CoS 値 0 および 1 をマッピングする例を示します。

```
Router(config-if)# wrr-queue cos-map 1 1 0 1
Router(config-if)#
```

関連コマンド

[show queuing interface](#) キューイング情報を表示します。

wrr-queue dscp-map

ハードウェア DSCP 値をキューの廃棄しきい値にマッピングするには、**wrr-queue dscp-map** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

wrr-queue dscp-map queue-id threshold-id dscp-1 ... dscp-n

no wrr-queue dscp-map queue-id

シンタックスの説明

<i>queue-id</i>	キュー番号。有効値は 1 ~ 8 です。
<i>threshold-id</i>	しきい値 ID。有効値は 1 ~ 4 です。
<i>dscp-1 ... dscp-n</i>	DSCP 値。有効値は、0 ~ 7 です。

コマンドのデフォルト

CoS モード

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン



(注)

wrr-queue dscp-map コマンドを入力するには、インターフェイスが DSCP キューイング モードである必要があります。**mls qos queue-mode mode-dscp** コマンドを使用して、モードを DSCP に設定します。

このコマンドは、10 ギガビット イーサネット ポートだけでサポートされます。

DSCP 値をマッピングする場合、次の注意事項に従ってください。

- キューとしきい値にマッピングする DSCP 値を、最大 8 つ入力できます。
- コマンドを複数入力して、キューとしきい値にマッピングする DSCP 値を追加できます。
- 各キューとしきい値に対して、別個のコマンドを入力する必要があります。

例

次に、ハードウェア DSCP 値をキューの廃棄しきい値にマッピングする例を示します。

```
Router(config-if)# wrr-queue dscp-map 8 1 0 1 2 3
Router(config-if)#
```

関連コマンド

show queueing interface キューイング情報を表示します。

wrr-queue queue-limit

インターフェイス上の送信キューのサイズ比を設定するには、**wrr-queue queue-limit** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
wrr-queue queue-limit {queue1-weight [queue2-weight] queue3-weight}
```

```
no wrr-queue queue-limit
```

```
wrr-queue queue-limit {queue1-weight [queue2-weight] queue3-weight}
```

```
no wrr-queue queue-limit
```

シンタックスの説明

<i>queue1-weight</i>	ロー プライオリティ キューの重み比を指定します。有効値は 1 ~ 100% です。
<i>queue2-weight</i>	(任意) ミディウム プライオリティ キューの重み比を指定します。有効値は 1 ~ 100% です。
<i>queue3-weight</i>	ハイ プライオリティ キューの重み比を指定します。有効値については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- ロー プライオリティでは 90%
- ハイ プライオリティでは 10%

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

有効なハイ プライオリティ 重み値は 1 ~ 100% です。ただし、1p2q1t 出力 LAN ポートでは例外的に、ハイ プライオリティ キューの有効値は 5 ~ 100% です。

出力完全優先キューを持つ LAN ポートの場合、PFC QoS は出力完全優先キュー サイズをハイ プライオリティ キュー サイズと同じに設定します。

ネットワークにおけるロー プライオリティ トラフィックとハイ プライオリティ トラフィックの配分を算出してください (たとえば、ロー プライオリティ トラフィックの場合は 80%、ハイ プライオリティ トラフィックの場合は 20% に算出します)。算出した割合を、各キューの重みとして使用します。

ハードウェアのプログラミング精度により、ハードウェアに設定される値は、指定された値の近似値となります。たとえば、0% を指定した場合、実際にプログラムされる値は必ずしも 0 ではありません。

■ wrr-queue queue-limit

例

次に、送信キュー サイズ比を設定する例を示します。

```
Router (config-if)# wrr-queue queue-limit 75 25
Router (config-if)#
```

関連コマンド

コマンド	説明
show queueing interface	キューイング情報を表示します。
wrr-queue	標準送信キュー間の帯域幅を割り当てます。

wrr-queue random-detect

1p2q1t および 1p3q1t インターフェイスの指定キューに対して、WRED をイネーブルにしたり、最小および最大 WRED しきい値を指定したりするには、**wrr-queue random-detect** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

wrr-queue random-detect *queue-id*

wrr-queue random-detect {**max-threshold** | **min-threshold**} *queue-id* *threshold-percent-1* ... *threshold-percent-n*

no wrr-queue random-detect *queue-id*

no wrr-queue random-detect {**max-threshold** | **min-threshold**} *queue-id*

シンタックスの説明

<i>queue-id</i>	キュー番号。有効値は 1、2、または 3 です。
max-threshold	最大 WRED 廃棄しきい値を指定します。
min-threshold	最小 WRED 廃棄しきい値を指定します。
<i>threshold-percent-1</i> <i>threshold-percent-n</i>	しきい値の重み。有効値は 1 ~ 100% です。

コマンドのデフォルト

デフォルトでは、WRED はディセーブルです。WRED をイネーブルにした場合、デフォルトは次のとおりです。

- 最大しきい値は 40% (低) および 100% (高) です。
- 最小しきい値は、両方ともゼロに設定されます。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

1p2q1t および 1p3q1t インターフェイスの場合、標準送信キューに WRED 廃棄しきい値があります。1p3q1t 送信キューは、WRED 廃棄しきい値またはテール廃棄しきい値を使用するように設定できます。

1p2q1t インターフェイスの WRED 廃棄しきい値をイネーブルにするには、**wrr-queue random-detect** *queue-id* コマンドを使用します。WRED をディセーブルにするには、このコマンドの **no** 形式を使用します。

1p3q1t インターフェイスの WRED 廃棄しきい値をイネーブルにするには、**wrr-queue random-detect** *queue-id* コマンドを使用します。テール廃棄しきい値に戻すには、**no wrr-queue random-detect** *queue-id* コマンドを使用します。

queue-id は、標準ロー プライオリティ キューの場合は 1、標準ハイ プライオリティ キューの場合は 2、完全優先キューの場合は 3 です。

完全優先キューのしきい値は、設定できません。

■ **wrr-queue random-detect**

1p2q2t インターフェイスの各キューには 2 つのしきい値、1p3q1t インターフェイスには 1 つのしきい値があります。

しきい値には、それぞれロー WRED 値およびハイ WRED 値があります。

WRED 値はキュー容量のパーセントです。

WRED しきい値の設定方法については、『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*』の「QoS」の章を参照してください。

例

次に、ロー プライオリティ送信キューのハイ WRED 廃棄しきい値を設定する例を示します。

```
Router (config-if)# wrr-queue random-detect max-threshold 1 60 100  
Router (config-if)#
```

関連コマンド

コマンド	説明
show queueing interface	キューイング情報を表示します。
wrr-queue queue-limit	インターフェイス上の送信キュー サイズ比を設定します。

wrr-queue shape

SRR 最大キューの帯域幅を割合または重みで設定するには、**wrr-queue shape** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
wrr-queue shape {percent low-priority-queue-percentage
[intermediate-priority-queue-percentage] high-priority-queue-percentage}
```

```
wrr-queue shape {low-priority-queue-weight [intermediate-priority-queue-weight]
high-priority-queue-weight}
```

```
no wrr-queue shape
```

シンタックスの説明

<i>percent low-priority-queue-percentage</i>	SRR の最小の割合を指定します。有効値は、1 ~ 100 です。
<i>intermediate-priority-queue-percentage</i>	(任意) SRR の中間の割合。有効値は、1 ~ 100 です。
<i>high-priority-queue-percentage</i>	SRR の最大の割合。有効値は、1 ~ 100 です。
<i>low-priority-queue-weight</i>	SRR の最小の重み。有効値は、1 ~ 255 です。
<i>intermediate-priority-queue-weight</i>	(任意) SRR の中間の重み。有効値は、1 ~ 255 です。
<i>high-priority-queue-weight</i>	SRR の最大の重み。有効値は、1 ~ 255 です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- 1p3q8t - 22:33:45
- 1p7q4t - 100:150:200:0:0:0:0

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

SRR を使用する場合、キューは割り当てられた帯域幅だけを使用します。

このコマンドは、SFP 1q3q8t ポートおよび 1p7q4t ポートだけでサポートされます。

設定できるキューの重みは最大で 7 つです。

shape キーワードを入力して、SRR を設定します。SRR を使用する場合、完全優先キューを使用できません。SRR を設定するには、完全優先キューにマッピングされた CoS または DSCP 値を標準キューに再度マッピングする必要があります。

割り当てられた割合または重みが大きいキューほど、多くの送信帯域幅が割り当てられます。重みを入力する場合、重みの比率によってキューの合計帯域幅が分割されます。たとえば、ギガビットイーサネット ポート上の 3 つのキューの場合、重みは 25:25:50 になり、次のように割り当てられます。

- キュー 1 : 250 Mbps
- キュー 2 : 250 Mbps

wrr-queue shape

- キュー 3 : 500 Mbps

追加できる割合の最大値は 100 です。ポート上のすべての標準送信キューに対して割合を入力する必要があります。

重量範囲の有効値は、1 ~ 255 です。ポート上のすべての標準送信キューに対して重みを入力する必要があります。

例

次に、3 対 1 の帯域幅比率を割り当てる例を示します。

```
Router(config-if)# wrr-queue shape 3 1
Router(config-if)#
```

関連コマンド

コマンド	説明
show queuing interface	キューイング情報を表示します。
wrr-queue	DWRR または WRR 標準送信キュー間の帯域幅を割り当てます。

wrr-queue threshold

1q4t および 2q2t インターフェイスの標準受信キューおよび標準送信キューの廃棄しきい値パーセントを設定するには、**wrr-queue threshold** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

wrr-queue threshold *queue-id* *threshold-percent-1* ... *threshold-percent-n*

no wrr-queue threshold *queue-id*

シンタックスの説明

<i>queue-id</i>	キュー番号。有効値は 1 ~ 2 です。
<i>threshold-percent-1</i>	キュー 1 および 2 の重み値。有効値は 1 ~ 100% です。
<i>threshold-percent-n</i>	

コマンドのデフォルト

QoS をイネーブルにした場合、デフォルト値は次のとおりです。

- **100%** : しきい値 1
- **60%** : しきい値 2

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

使用上のガイドライン

送信キュー番号およびしきい値の番号を使用してください。

queue-id は、標準ロー プライオリティ キューの場合は 1、標準ハイ プライオリティ キューの場合は 2 です。

しきい値 2 は常に 100% に設定してください。

受信キューの廃棄しきい値は、trust CoS に設定されたギガビット イーサネット インターフェイスに限りサポートされます。

例

受信キュー 1/しきい値 1 および送信キュー 1/しきい値 1 を設定する例を示します。

```
Router(config-if)# wrr-queue threshold 1 60 100
Router(config-if)#
```

関連コマンド

コマンド	説明
show queueing interface	キューイング情報を表示します。
wrr-queue queue-limit	インターフェイス上の送信キュー サイズ比を設定します。

■ wrr-queue threshold



APPENDIX A

略語

表 A-1 に、このマニュアルで使用されている略語の定義を示します。

表 A-1 略語リスト

略語	説明
AAL	ATM Adaptation Layer : ATM アダプテーション レイヤ
ACE	Access Control Entry : アクセス制御エントリ
ACL	Access Control List : アクセス制御リスト
ACNS	Application and Content Networking System
AFI	Authority and Format Identifier
Agport	Aggregation port
ALPS	Airline Protocol Support
AMP	Active Monitor Present
APaRT	Automated Packet Recognition and Translation : 自動パケット認識および変換
ARP	Address Resolution Protocol : アドレス解決プロトコル
ATA	Analog Telephone Adaptor または Advanced Technology Attachment
ATM	Asynchronous Transfer Mode : 非同期転送モード
AV	Attribute Value : アトリビュート値
BDD	Binary Decision Diagram
BECN	Backward Explicit Congestion Notification : 逆方向明示的輻輳通知
BGP	Border Gateway Protocol : ボーダーゲートウェイ プロトコル
Bidir-PIM	Bidirectional PIM : 双方向 PIM
BMA	Broadcast Multiaccess : ブロードキャスト マルチアクセス
BPDU	Bridge Protocol Data Unit : ブリッジ プロトコル データ ユニット
BRF	Bridge Relay Function : ブリッジ リレー機能
BSC	Bisync : バイナリ同期
BSR	Bootstrap Router : ブートストラップ ルータ
BSTUN	Block Serial Tunnel : ブロック シリアル トンネル
BUS	Broadcast and Unknown Server
BVI	Bridge-group Virtual Interface : ブリッジグループ仮想インターフェイス

表 A-1 略語リスト (続き)

略語	説明
CAM	Content-Addressable Memory : 連想メモリ
CAR	Committed Access Rate : 専用アクセス レート
CASA	Cisco Appliance Services Architecture
CBAC	Context-Based Access Control : コンテキスト ベースのアクセス制御
CCA	Circuit Card Assembly
CDP	Cisco Discovery Protocol
CE	Customer Edge : カスタマー エッジ
CEF	Cisco Express Forwarding
CHAP	Challenge Handshake Authentication Protocol
CIR	Committed Information Rate : 認定情報レート
CIST	Common and Internal Spanning-Tree
CLI	Command-Line Interface : コマンドライン インターフェイス
CLNS	Connection-Less Network Service
CMM	Communication Media Module : 通信メディア モジュール
CMNS	Connection-Mode Network Service : コネクション モード ネットワーク サービス
CNS	Cisco Networking Services
CoPP	Control Plane Policing : コントロール プレーン ポリシング
COPS	Common Open Policy Server
COPS-DS	Common Open Policy Server Differentiated Services
CoS	Class of Service : サービス クラス
CPLD	Complex Programmable Logic Device
CRC	Cyclic Redundancy Check : 巡回冗長検査
CRF	Concentrator Relay Function : コンセントレータ リレー機能
CSM	Content Switching Module
CST	Common Spanning-Tree
CUDD	University of Colorado Decision Diagram
CBWFQ	Class-Based Weighted Fair Queuing : クラス ベース均等化キューイング
DAI	Dynamic ARP Inspection
DCC	Data Country Code
dCEF	distributed Cisco Express Forwarding
DDR	Dial-on-Demand Routing : ダイアル オンデマンドルーティング
DE	Discard Eligibility : 廃棄適性
DEC	Digital Equipment Corporation
DF	Designated Forwarder
DFC	Distributed Forwarding Card
DFI	Domain-Specific Part Format Identifier
DFP	Dynamic Feedback Protocol

表 A-1 略語リスト (続き)

略語	説明
DHCP	Dynamic Host Configuration Protocol
DISL	Dynamic Inter-Switch Link
DLC	Data Link Control : データ リンク制御
DLCI	Data-Link Connection Identifier : データ リンク接続識別子
DLSw	Data Link Switching : データ リンク スイッチング
DMP	Data Movement Processor
DNS	Domain Name System : ドメイン ネーム システム
DoD	Department of Defense : 米国国防総省
DOM	Digital Optical Monitoring : デジタル オプティカル モニタリング
DoS	Denial of Service
dot1q	802.1Q
dot1x	802.1X
DRAM	Dynamic RAM : ダイナミック RAM
DRiP	Dual Ring Protocol
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DSPU	Downstream SNA Physical Units
DSS	Digital Signature Standard
DTP	Dynamic Trunking Protocol : ダイナミック トランキング プロトコル
DTR	Data Terminal Ready : データ ターミナル レディ
DVMRP	Distance Vector Multicast Routing Protocol : 距離ベクトル マルチキャスト ルーティング プロトコル
DWRR	Deficit Weighted Round Robin
DXI	Data Exchange Interface : データ交換インターフェイス
EAP	Extensible Authentication Protocol
EAPoUDP	Extensible Authentication Protocol over User Datagram Protocol
EARL	Enhanced Address Recognition Logic
EEPROM	Electrically Erasable Programmable Read-Only Memory : 電氣的に消去可能でプログラミング可能な ROM
EHSA	Enhanced High System Availability : 拡張高システム可用性
EIA	Electronic Industries Association : 米国電子工業会
ELAN	Emulated Local Area Network : エミュレート LAN
EOBC	Ethernet Out-of-Band Channel
EOF	End of File
EoMPLS	Ethernet over Multiprotocol Label Switching
ERM	Exception Recovery Manager
ESI	End-System Identifier
FAT	File Allocation Table
FIB	Forwarding Information Base : 転送情報ベース

表 A-1 略語リスト (続き)

略語	説明
FIE	Feature Interaction Engine
FECN	Forward Explicit Congestion Notification : 前方明示的輻輳通知
FM	Feature Manager
FPD	Field Programmable Devices
FRU	Field-Replaceable Unit : 現場交換可能ユニット
fsck	file system consistency check
FSM	Feasible Successor Metrics
FSU	Fast Software Upgrade
FTP	File Transfer Protocol : ファイル転送プロトコル
FWSM	Firewall Services Module
GARP	General Attribute Registration Protocol
GBIC	Gigabit Interface Converter : ギガビット インターフェイス コンバータ
GBTE	Guaranteed Bandwidth Traffic Engineering : 保証帯域幅トラフィック エンジニアリング
GE-WAN	ギガビット イーサネット WAN
GMRP	GARP Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol
HSRP	Hot Standby Routing Protocol
ICC	Inter-card Communication または Interface Controller Card
ICD	International Code Designator
ICMP	Internet Control Message Protocol
IDB	Interface Descriptor Block
IDP	Initial Domain Part または Internet Datagram Protocol
IDS	Intrusion Detection System Module
IFS	IOS File System
IGMP	Internet Group Management Protocol
IGMPv2	IGMP version 2 : IGMP バージョン 2
IGMPv3	IGMP version 3 : IGMP バージョン 3
IGP	Interior Gateway Protocol : 内部ゲートウェイ プロトコル
IGRP	Interior Gateway Routing Protocol
ILMI	Integrated Local Management Interface
IP	Internet Protocol
IPC	Interprocessor Communication : プロセッサ間通信
IPG	Inter Packet Gap
IPX	Internetwork Packet Exchange
IS-IS	Intermediate System/Intermediate System Intradomain Routing Protocol
ISL	Inter-Switch Link : スイッチ間リンク
ISL VLAN	Inter-Switch Link VLAN

表 A-1 略語リスト (続き)

略語	説明
ISO	International Organization for Standardization : 国際標準化機構
ISR	Integrated SONET Router
LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol Data Unit
LAN	Local Area Network
LANE	LAN Emulation : LAN エミュレーション
LAPB	Link Access Procedure, Balanced : 平衡型リンク アクセス手順
LCP	Link Control Protocol : リンク コントロール プロトコル
LDA	Local Director Acceleration
LEC	LAN Emulation Client : LANE クライアント
LECS	LAN Emulation Configuration Server : LANE コンフィギュレーションサーバ
LEM	Link Error Monitor : リンク エラー モニタ
LER	Link Error Rate : リンク エラー レート
LES	LAN Emulation Server : LANE サーバ
LLC	Logical Link Control : 論理リンク制御
LOU	Logical Operation Units : 論理演算ユニット
LTL	Local Target Logic
MAC	Media Access Control : メディア アクセス制御
MD5	Message Digest 5
MDIX	Media-Dependent Interface crossover : メディア依存型インターフェイスクロスオーバー
MDS	Multicast Distributed Switching : マルチキャスト配信スイッチング
MDSS	Multicast Distributed Shortcut Switching
MDT	Multicast Distribution Tree : マルチキャスト配信ツリー
MFD	Multicast Fast Drop
MFIB	Multicast Forwarding Information Base : マルチキャスト転送情報ベース
mGRE	multipoint Generic Routing Encapsulation : マルチポイント総称ルーティングカプセル化
MIB	Management Information Base : 管理情報ベース
MII	Media-Independent Interface : メディア独立型インターフェイス
MLDv2	Multicast Listener Discovery version 2 : マルチキャスト リスナー ディスカバリ バージョン 2
MLS	Multilayer Switching : マルチレイヤ スwitching
MLSE	Maintenance Loop Signaling Entity
MLSM	MultiLayer Switching for Multicast
MN	Mobil Node
MOP	Maintenance Operation Protocol
MOTD	Message-of-The-Day : ログイン バナー

表 A-1 略語リスト (続き)

略語	説明
MPLS	Multiprotocol Label Switching : マルチプロトコル ラベル スイッチング
MQC	Modular QoS CLI : モジュラ QoS CLI
mrinfo	multicast router information : マルチキャスト ルータ情報
MRM	Multicast Routing Monitor
mroute	multicast route : マルチキャスト ルート
mrouter	multicast router : マルチキャスト ルータ
MSDP	Multicast Source Discovery Protocol
MSM	Multilayer Switch Module
MSS	Maximum Segment Size : 最大セグメント サイズ
MST	Multiple Spanning-Tree (802.1s)
MSTCI	MST Configuration Identifier
MTU	Maximum Transmission Unit : 最大伝送ユニット
MVAP	Multiple VLAN Access Port
NAM	Network Analysis Module : ネットワーク解析モジュール
NAT	Network Address Translation : ネットワーク アドレス変換
NBMA	Nonbroadcast Multiaccess : 非ブロードキャスト マルチアクセス
NBP	Name Binding Protocol : ネーム バインディング プロトコル
NCIA	Native Client Interface Architecture : ネイティブ クライアント インターフェイス アーキテクチャ
NDE	NetFlow Data Export : NetFlow データ エクスポート
NDR	No Drop Rate
NET	Network Entity Title
NetBIOS	Network Basic Input/Output System
NFFC	NetFlow Feature Card : NetFlow フィーチャ カード
NHRP	Next Hop Resolution Protocol
NMP	Network Management Processor : ネットワーク管理プロセッサ
NSAP	Network Service Access Point : ネットワーク サービス アクセス ポイント
NSF	Non-STOP Forwarding
NTP	Network Time Protocol
NVGEN	Nonvolatile Generation
NVRAM	Nonvolatile RAM : 不揮発性 RAM
OAL	Optimized ACL Logging
OAM	Operation, Administration, and Maintenance : 運用管理および保守
ODM	Order Dependent Merge
OIF	Outgoing interface of a multicast {*,G} or {source, group} flow : マルチキャスト {*,G} または {S,G} フローの Outgoing Interface
OSI	Open Systems Interconnection : 開放型システム間相互接続
OSPF	Open Shortest Path First

表 A-1 略語リスト (続き)

略語	説明
PAE	Port Access Entity
PAgP	Port Aggregation Protocol : ポート集約プロトコル
PBD	Packet Buffer Daughterboard
P bit	Prioritization bit : 優先順位ビット
PBR	Policy-Based Routing : ポリシー ベース ルーティング
PC	Personal Computer : パーソナル コンピュータ (従来の PCMCIA)
PCM	Pulse Code Modulation : パルス符号変調
PCR	Peak Cell Rate : ピーク セル レート
PDP	Policy Decision Point : ポリシー デシジョン ポイント
PDU	Protocol Data Unit : プロトコル データ ユニット
PE	Provider Edge : プロバイダー エッジ
PEP	Policy Enforcement Point
PE router	Provider Edge router : PE ルータ
PFC	Policy Feature Card : ポリシー フィーチャ カード
PGM	Pragmatic General Multicast
PHY	Physical Sublayer : 物理サブレイヤ
PIB	Policy Information Base
PIR	Peak Information Rate : 最大情報レート
PIM	Protocol Independent Multicast : プロトコル独立マルチキャスト
PIM-SM	Protocol Independent Multicast Sparse Mode : プロトコル独立マルチキャスト疎モード
PISA	Programmable Intelligent Services Accelerator
PoS	Packet over Sonet
PPP	Point-to-Point Protocol : ポイントツーポイント プロトコル
ppsec	packets per second
PRID	Policy Rule Identifiers
psecure	ポート セキュリティ
PVL	Per VLAN Learning : VLAN 単位学習
PVLAN	Private VLAN
PVST+	Per VLAN Spanning-Tree Plus
QDM	QoS Device Manager
QM	QoS Manager
QM-SP	SP QoS Manager
QoS	Quality of Service : サービス品質
QinQ	IEEE 802.1Q in 802.1Q
RACL	Router Interface Access Control List
RADIUS	Remote Access Dial-In User Service
RAM	Random-Access Memory : ランダムアクセス メモリ

表 A-1 略語リスト (続き)

略語	説明
RCP	Remote Copy Protocol : リモート コピー プロトコル
RF	Redundancy Facility
RGMP	Router-Ports Group Management Protocol
RIB	Routing Information Base
RIF	Routing Information Field : ルーティング情報フィールド
RM	Routed MAC : ルーテッド MAC
RMON	Remote Network Monitor : リモート ネットワーク モニタ
ROM	Read-Only Memory : 読み出し専用メモリ
ROMMON	ROM モニタ
RP	Route Processor : ルート プロセッサ、または Rendezvous Point : ランデブー ポイント
RPC	Remote Procedure Call : リモート プロシージャ コール
RPF	Reverse Path Forwarding
RPR	Route Processor Redundancy
RSPAN	Remote SPAN
RST	reset
RSTP	Rapid Spanning-Tree Protocol
RSTP+	Rapid Spanning-Tree Protocol Plus
RSVP	Resource Reservation Protocol
RTP	Real-Time Transport Protocol
SA	Source Active : 送信元アクティブ
SAID	Security Association Identifier
SAP	Service Access Point : サービス アクセス ポイント
SCM	Service Connection Manager
SCP	Switch-Module Configuration Protocol または Serial Control Protocol
SDLC	Synchronous Data Link Control
SFP	Small Form-factor Pluggable : 着脱可能小型フォーム ファクタ
SGBP	Stack Group Bidding Protocol
SIMM	Single In-Line Memory Module : シングル インライン メモリ モジュール
SLB	Server Load Balancing
SLCP	Supervisor Line-Card Processor
SLIP	Serial Line Internet Protocol : シリアル ライン インターネット プロトコル
SMDS	Software Management and Delivery Systems
SMF	Software MAC Filter : ソフトウェア MAC フィルタ
SMP	Standby Monitor Present
SMRP	Simple Multicast Routing Protocol : シンプル マルチキャスト ルーティング プロトコル
SMT	Station Management : ステーション管理
SNAP	Subnetwork Access Protocol

表 A-1 略語リスト (続き)

略語	説明
SNMP	Simple Network Management Protocol : 簡易ネットワーク管理プロトコル
SPAN	Switched Port Analyzer : スイッチドポートアナライザ
SREC	S-Record 形式 (Motorola により定義された ROM 内容の形式)
SRR	Shaped Round Robin : シェイプドラウンドロビン
SSL	Secure Sockets Layer
SSM	Source Specific Multicast
SSO	Stateful Switch Over
SSTP	Shared Spanning Tree Protocol
STP	Spanning-Tree Protocol : スパニングツリープロトコル
SVC	Switched Virtual Circuit : 相手先選択接続
SVI	Switched Virtual Interface
TACACS+	Terminal Access Controller Access Control System Plus
TARP	Target Identifier Address Resolution Protocol
TCAM	Ternary CAM
TCL	Table Contention Level
TCP/IP	Transmission Control Protocol/Internet Protocol
TDR	Time Domain Reflectometry
TFTP	Trivial File Transfer Protocol : 簡易ファイル転送プロトコル
TIA	Telecommunications Industry Association : 米国電気通信工業会
TopN	ユーザがレポートを使用してポートトラフィックを分析するためのユーティリティ
ToS	Type of Service : サービスタイプ
TLV	Type-Length-Value
TTL	Time To Live : 存続可能時間
TVX	valid transmission
UDE	Unidirectional Ethernet
UDL	Unidirectional Link : 単一方向リンク
UDLD	UniDirectional Link Detection : 単一方向リンク検出
UDLR	UniDirectional Link Routing : 単一方向リンクルーティング
UDP	User Datagram Protocol
UNI	User-Network Interface
uRPF	unicast Reverse Path Forwarding
UTC	Coordinated Universal Time : 協定世界時
VACL	VLAN Access Control List : VLAN アクセス制御リスト
VCC	Virtual Channel Circuit : 仮想チャネル回線
VCI	Virtual Circuit Identifier : 仮想回線識別子
VCR	Virtual Configuration Register : 仮想コンフィギュレーションレジスタ
VFI	Virtual Forwarding Instance

表 A-1 略語リスト (続き)

略語	説明
VINES	Virtual Network System
VLAN	Virtual LAN : 仮想 LAN
VMPS	VLAN Membership Policy Server : VLAN メンバーシップ ポリシーサーバ
VMR	Value Mask Result
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network : 仮想私設網
VPF	VPN Routing/Forwarding : VPN ルーティング/転送
VTP	VLAN Trunking Protocol : VLAN トランキング プロトコル
VVID	Voice VLAN ID
WAN	Wide Area Network
WCCP	Web Cache Coprocessor Protocol
WFQ	Weighted Fair Queueing : 重み付け均等化キューイング
WLSM	Wireless LAN Services Module
WRED	Weighted Random Early Detection : 重み付けランダム早期検出
WRR	Weighted Round-Robin : 重み付けラウンドロビン
XCM	External Column Memory
XNS	Xerox Network System



APPENDIX **B**

オープンソースソフトウェアについて

The Cisco IOS software on the Catalyst 6500 series switches software pipe command uses Henry Spencer's regular expression library (regex).

Henry Spencer's regular expression library (regex). Copyright 1992, 1993, 1994, 1997 Henry Spencer. All rights reserved. This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it.
2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.
3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.
4. This notice may not be removed or altered.

The Cisco IOS software on the Catalyst 6500 series switches software pipe command uses Softfloat.

Softfloat was written by John R. Hauser. This work was made possible in part by the International Computer Science Institute, located at Suite 600, 1947 Center Street, Berkeley, California 94704. Funding was partially provided by the National Science Foundation under grant MIP-9311980. The original version of this code was written as part of a project to build a fixed-point vector processor in collaboration with the University of California at Berkeley, overseen by Profs. Nelson Morgan and John Wawrzynek. More information is available through the Web page <http://www.cs.berkeley.edu/~jhauser/arithmetic/SoftFloat.html>.

THIS SOFTWARE IS DISTRIBUTED AS IS, FOR FREE. Although reasonable effort has been made to avoid it, THIS SOFTWARE MAY CONTAIN FAULTS THAT WILL AT TIMES RESULT IN INCORRECT BEHAVIOR. USE OF THIS SOFTWARE IS RESTRICTED TO PERSONS AND ORGANIZATIONS WHO CAN AND WILL TAKE FULL RESPONSIBILITY FOR ALL LOSSES, COSTS, OR OTHER PROBLEMS THEY INCUR DUE TO THE SOFTWARE, AND WHO FURTHERMORE EFFECTIVELY INDEMNIFY JOHN HAUSER AND THE INTERNATIONAL COMPUTER SCIENCE INSTITUTE (possibly via similar legal warning) AGAINST ALL LOSSES, COSTS, OR OTHER PROBLEMS INCURRED BY THEIR CUSTOMERS AND CLIENTS DUE TO THE SOFTWARE.

Derivative works of Softfloat are acceptable, even for commercial purposes, so long as (1) the source code for the derivative work includes prominent notice that the work is derivative, and (2) the source code includes prominent notice with these four paragraphs for those parts of this code that are retained.



INDEX

記号

# 記号 (特権 EXEC モード プロンプト)	1-6
\$ 文字	1-8, 1-10
* (アスタリスク)	1-8
+ (プラス記号)	1-8
. (ピリオド)	1-8
? 1-2	
^ (キャレット)	1-8, 1-10
_ (アンダースコア)	1-8, 1-10
(パイプまたは縦棒)	
選択パターンの指定	1-10

数字

802.1Q	
ISL VLAN マッピング	2-1289
イネーブル化	
トンネリング	2-344
カプセル化	
イネーブル化	2-134
ディセーブル化	2-134
指定	
EtherType 値	2-1207
設定	
CoS 値	2-346
インターフェイス上での廃棄しきい値	2-347
グローバルな廃棄しきい値	2-349
最大処理プロトコル パケット数	2-350
ポート インターフェイス タイプ	2-1209
モード	2-1209
ディセーブル化	
トンネリング	2-344

トランクのカプセル化特性の設定	2-1224
表示	
対応ポート	2-708
トンネリング プロトコル	2-887
802.1Q タギング	
VLAN 上でのイネーブル化	2-1284
VLAN 上でのディセーブル化	2-1284
情報の表示	2-1116
802.1s	
「MST」を参照	
802.1w	
「RSTP+」を参照	
802.1X	
イネーブル化	
クライアントの定期的な再認証	2-127
グローバル	2-128
設定	
再認証カウント	2-123
認証タイマー	2-129
ポート制御値	2-125
ディセーブル化	
クライアントの定期的な再認証	2-127
グローバル	2-128
デフォルト設定	2-122
デフォルトへのリセット	2-122
表示	
すべてのインターフェイスの情報	2-709
複数のホストの許可	2-124
複数のホストの不許可	2-124
802.3ad	
「LACP」を参照	
802.3af	
管理モードの設定	2-618

A

ACL

TCAM

更新中のデフォルト動作の設定 **2-405**

イネーブル化

時間ベース ACL **2-1241**

クリア

カウンタ **2-66**

削除

時間制限 **2-1241**

選択

BDD ベース マージ関数 **2-403**ODM ベース マージ関数 **2-403**

定義

時間範囲 **2-1241**統計情報の削除 **2-42**

統合

現行方式の表示 **2-747**

ポート アクセス マップ

削除 **2-609**作成 **2-609**

ACL カウンタ

ハードウェアでスイッチングされたパケットの表示 **2-1097**

ARP

テーブルの表示 **2-678**

ARP ACL

句の追加 **2-6**サブモードの開始 **2-6**

定義

アクセス リスト **2-6**リストからの削除 **2-6**

ASIC

表示

タイプ **2-679**バージョン **2-679**

ATA フラッシュ

制限 **2-1185, 2-1262****B**

BDD

ACL マージ関数を選択 **2-403**

BGP

イネーブル化

決定性処理時間の正規表現エンジン **2-12**正規表現エンジン **2-12**最大パラレル ルート数の設定 **2-395**

Binary Decision Diagram

「BDD」を参照

boot **2-16**boot system コマンド **2-16**

BOOT 環境変数

指定 **2-16**情報の表示 **2-682**

BPDU

プロトコル トンネリング リンクによる変換 **2-19**

BPDU ガード

イネーブル化

インターフェイス上 **2-1150**デフォルトで **2-1175**

ディセーブル化

インターフェイス上 **2-1150**デフォルトで **2-1175**

BPDU フィルタリング

イネーブル化

インターフェイス上 **2-1148**デフォルトで **2-1173**

ディセーブル化

インターフェイス上 **2-1148**デフォルトで **2-1173****C**

CAM テーブル使用状況モニタリング

イネーブル化 **2-382**ディセーブル化 **2-382**

CASA

設定

フォワーディング エージェントとして機能 **2-191**

ディセーブル化

フォワーディング エージェントとして機能 **2-191**

CDP

表示

ネイバ情報 **2-689**

CEF

一貫性チェッカーのタイプ

イネーブル化 **2-193**

ディセーブル化 **2-193**

一貫性チェッカーのパラメータ

イネーブル化 **2-193**

ディセーブル化 **2-193**

イネーブル化

MLS プレフィクス単位のアカウンティング **2-420**

トンネル フラグメンテーション **2-412**

不明のプレフィクスの検出 **2-193**

レート制限 **2-423**

エポック

新しいエポックを開始 **2-46**

情報の表示 **2-805**

増分 **2-46**

クリア

プレフィクス単位の IPv6 アカウンティング統計 **2-69**

プレフィクス単位の IP アカウンティング統計 **2-68**

指定

各スキャンでチェックする最大プレフィクス数 **2-193**

パッシブ スキャン チェック **2-193**

設定

経過時間 **2-193**

スキャン間隔 **2-193**

チェッカー タイプ **2-193**

プロトコル単位のルート制限 **2-410**

レート制限 **2-423**

ロードバランス **2-421**

選択

ロードバランス アルゴリズム **2-192**

ディセーブル化

MLS プレフィクス単位のアカウンティング **2-420**

トンネル フラグメンテーション **2-412**

レート制限 **2-423**

表示

IPv4 ユニキャスト アドレス **2-926, 2-940**

VLAN インターフェイス ステータス **2-810**

VLAN 設定情報 **2-810**

最大ルート システム コンフィギュレーション **2-941**

ネクストホップ情報 **2-810**

不一致

クリア **2-48**

表示 **2-807**

CIR

レートの設定 **2-469**

Cisco Appliance Services Architecture

「CASA」を参照

Cisco Express Forwarding

「CEF」を参照

Cisco IOS VLAN サブインターフェイス

情報の表示 **2-1125**

class (ポリシーマップ) コマンド **2-31**

CLI

アクセス

モジュール固有の CLI **2-648**

リモート ログイン **2-648**

ストリング検索

位置指定 **1-10**

繰り返し指定 **1-9**

出力の検索 **1-7**

使用 **1-7**

選択 **1-10**

単一文字パターン **1-8**

表現 [1-7](#)
 フィルタリング [1-7](#)
 複数文字パターン [1-9](#)
 リコール機能用カッコ [1-11](#)

CNS

Cisco Networking Services

「オンライン診断」を参照

Content Switching Module

「CSM」を参照

CoPP

コンフィギュレーションモードの開始 [2-97](#)

削除

 コントロールプレーンからサービス ポリシー [2-663](#)

設定

 トラフィック ポリシング [2-604](#)

表示

 ポリシー マップ クラス情報 [2-1053](#)

付加

 コントロールプレーンへのポリシー マップ [2-663](#)

CoS

内部 CoS から外部 CoS への変換

 実行バージョン情報表示 [2-986](#)

 設定情報の表示 [2-986](#)

 マッピング [2-479](#)

CoS/CoS

削除

 インターフェイスからの CoS 変換マップ [2-474](#)

付加

 インターフェイスへの CoS 変換マップ [2-474](#)

CoS/CoS マッピング

設定 [2-479](#)

CoS 値

完全優先キューへのマッピング [2-621](#)

デフォルト値の定義 [2-473](#)

デフォルト マッピングへのリセット [2-621](#)

CoS 変換マップ

インターフェイスからの削除 [2-474](#)

 インターフェイスへの付加 [2-474](#)

CPU 時間

 処理時間の保証 [2-660](#)

CSM

 シャットダウン [2-162](#)

D
DAI

ARP ACL サブモードの開始 [2-6](#)

DoS からの保護 [2-178](#)

VLAN への ARP ACL の適用 [2-176](#)

イネーブル化

 IP ARP インスペクション確認 [2-183](#)

 グローバル [2-185](#)

クリア

 統計情報 [2-44](#)

 ログ バッファのステータス [2-43](#)

削除

 ARP ACL [2-6](#)

設定

 IP ARP ログ バッファ [2-180](#)

 ポート単位で設定可能な信頼状態 [2-182](#)

追加

 ARP ACL に対する句 [2-6](#)

定義

 ARP ACL [2-6](#)

ディセーブル化

 IP ARP インスペクション確認 [2-183](#)

 グローバル [2-185](#)

表示

 VLAN のステータス [2-788](#)

 ログ バッファのステータス [2-791](#)

default 形式、コマンドの、使用 [1-7](#)

Denial of Service

「DoS」を参照

Designated Forwarder

「DF」を参照

DF

- インターフェイス情報の表示 [2-861](#)
- DFC
 - リモート ログイン
 - remote login コマンド [2-648](#)
- DHCP
 - イネーブル化
 - インターフェイスを信頼できる送信元として [2-196](#)
 - すべてのインターフェイスを信頼できる送信元として [2-195](#)
 - クリア
 - スヌーピング データベース エントリ [2-49](#)
 - スヌーピング統計エントリ [2-49](#)
 - スヌーピング バインディング エントリ [2-49](#)
 - 指定
 - 接続ルート [2-197](#)
 - スヌーピング データベース
 - テーブル エントリのクリア [2-49](#)
 - スヌーピング統計
 - テーブル エントリのクリア [2-49](#)
 - スヌーピング バインディング
 - テーブル エントリのクリア [2-49](#)
 - ディセーブル化
 - インターフェイスを信頼できる送信元として [2-196](#)
 - すべてのインターフェイスを信頼できる送信元として [2-195](#)
 - 表示
 - 設定済みの信頼されたインターフェイス [2-811](#)
- DHCP スヌーピング
 - option 82 のイネーブル化 [2-203](#)
 - イネーブル化
 - MAC アドレス比較 [2-208](#)
 - VLAN [2-210](#)
 - VLAN のグループ [2-210](#)
 - グローバル [2-198](#)
 - トンネル インターフェイス [2-206](#)
 - 指定
 - エントリ格納用 URL [2-201](#)
 - 設定
 - 書き込み遅延時間 [2-201](#)
 - 受信される DHCP メッセージ数 [2-205](#)
 - 中断タイムアウト インターバル [2-201](#)
 - データベース [2-201](#)
 - ディセーブル化
 - MAC アドレス比較 [2-208](#)
 - VLAN [2-210](#)
 - VLAN のグループ [2-210](#)
 - グローバル [2-198](#)
 - トンネル インターフェイス [2-206](#)
 - バインディング設定の確立 [2-199](#)
 - 表示
 - DHCP データベース ステータス [2-817](#)
 - 設定情報 [2-812](#)
 - 統計情報 [2-812](#)
 - バインディング テーブル エントリ [2-814](#)
- DHCP バインディング
 - バインディングの設定 [2-199](#)
- Distributed Forwarding Card
 - 「DFC」を参照
- DOM
 - イネーブル化
 - トランシーバ トラップ [2-1140](#)
 - ディセーブル化
 - トランシーバ トラップ [2-1140](#)
 - 表示
 - トランシーバしきい値違反 [2-779](#)
 - トランシーバ動作情報 [2-779](#)
- DoS
 - CoPP
 - コントロールプレーンからのサービス ポリシーの削除 [2-663](#)
 - コントロールプレーンへのポリシー マップの付加 [2-663](#)
 - コンフィギュレーションモードの開始 [2-97](#)
 - ポリシー マップ クラス情報の表示 [2-1053](#)
 - イネーブル化
 - レート制限 [2-423](#)
 - 開始

- CoPP コンフィギュレーションモード **2-97**
- 設定
 - トラフィック ポリシング **2-604**
 - レート制限 **2-423**
- ディセーブル化
 - レート制限 **2-423**
- DoS からの保護
 - ARP ブロードキャスト **2-496**
 - DAI の設定 **2-178**
 - VACL ログ ケースのレート リミッタ
 - VACL ログ ケースのディセーブル化 **2-535**
 - 情報の表示 **2-993**
 - 設定
 - IPv4 マルチキャスト レート リミッタ **2-522**
 - IPv6 マルチキャスト レート リミッタ **2-524**
 - ディセーブル化
 - IPv4 マルチキャスト レート リミッタ **2-522**
 - IPv6 マルチキャスト レート リミッタ **2-524**
 - レート リミッタ
 - ACL ブリッジド レート リミッタのイネーブル化 **2-527**
 - ACL ブリッジド レート リミッタの設定 **2-527**
 - ACL ブリッジド レート リミッタのディセーブル化 **2-527**
 - CEF レート リミッタのイネーブル化 **2-529**
 - CEF レート リミッタの設定 **2-529**
 - CEF レート リミッタのディセーブル化 **2-529**
 - VACL ログ ケースのイネーブル化 **2-535**
 - VACL ログ ケースの設定 **2-535**
 - イネーブル化 **2-519**
 - ディセーブル化 **2-519**
 - ユニキャスト パケットに対するイネーブル化 **2-531**
 - ユニキャスト パケットに対するディセーブル化 **2-531**
 - ユニキャスト パケットへの設定 **2-531**
 - レイヤ 3 セキュリティ レート リミッタのイネーブル化 **2-534**
 - レイヤ 3 セキュリティ レート リミッタの設定 **2-534**
 - レイヤ 3 セキュリティ レート リミッタのディセーブル化 **2-534**
 - dot1q
 - 「802.1Q」も参照
 - dot1x
 - 「802.1x」を参照
 - DSCP
 - 削除
 - インターフェイスからの DSCP 変換マップ **2-475**
 - 定義
 - 変換マップ **2-483**
 - 表示
 - 変換マップ **2-981**
 - 付加
 - インターフェイスへの DSCP 変換マップ **2-475**
 - DSCP 変換マップ
 - インターフェイスからの削除 **2-475**
 - インターフェイスへの付加 **2-475**
 - DSS
 - 範囲無効化プロファイルの表示 **2-712**
 - duplex コマンドと speed コマンドの関係 **2-1183**
 - DWRR キュー
 - 設定
 - 帯域幅 **2-1294**
 - Dynamic ARP Inspection
 - 「DAI」を参照
 - Dynamic Host Configuration Protocol
 - 「DHCP」を参照

E

 - EIGRP
 - 設定
 - イベント ログ サイズ **2-133**
 - Enhanced Address Recognition Logic
 - 「EARL」を参照
 - EOBC インターフェイス
 - 情報の表示 **2-722**

EoMPLS

イネーブル化

VLAN ベースの転送 **2-576**ルーティング **2-576**

ディセーブル化

VLAN ベースの転送 **2-576**ルーティング **2-576**

errdisable

回復

回復原因の指定 **2-140**情報の表示 **2-728**タイマーの設定 **2-140**

検出

回復原因の指定 **2-138**タイマーの設定 **2-138**パケット バッファ エラー **2-138**

状態

情報の表示 **2-772**

errdisable の検出

情報の表示 **2-726, 2-727**

ERSPAN

宛先セッション コンフィギュレーション モードの開始 **2-566**インターフェイスまたは VLAN の削除 **2-571**インターフェイスまたは VLAN の追加 **2-571**新規セッションの開始 **2-571**セッションの開始 **2-566**セッションの削除 **2-571**セッションの終了 **2-566**送信元セッション コンフィギュレーション モードの開始 **2-566**

テーブル

宛先セッション コンフィギュレーション モードの構文 **2-572**送信元セッション コンフィギュレーション モードの構文 **2-573**

表示

セッション情報 **2-1013**

EtherChannel

EtherChannel グループへのインターフェイスの割り当て **2-22**インターフェイスを EtherChannel グループから削除 **2-22**

ガードの設定ミス検出

イネーブル化 **2-1152**エラー メッセージ **2-1152**検出 **2-1152**ディセーブル化 **2-1152**

最小のリンク

設定 **2-615**

表示

情報 **2-729**

Ethernet over Multiprotocol Label Switching

「EoMPLS」を参照

EtherType

値の指定 **2-1207**

Exception Recovery Manager

「ERM」を参照

EXEC レベルのコマンド

他のモードでの使用 **2-121**

EXP MAP

削除

インターフェイスからの EXP 変換マップ **2-476**

付加

インターフェイスへの EXP 変換マップ **2-476**

EXP 変換マップ

インターフェイスからの削除 **2-476**インターフェイスへの付加 **2-476**

External Column Memory

「XCM」を参照

F

Fast Software Upgrade

「FSU」を参照

Feature Interaction Engine

「FIE」を参照

FIB TCAM 例外

IPv4、IPv6、および MPLS プロトコルのステータス表示 [2-725](#)

FIB 使用表示 [2-946](#)

Field [A-4](#)

Field Programmable Devices
「FPD」を参照

file system consistency check
「fsck ユーティリティ」を参照

Firewall Services Module
「FWSM」を参照

Flexlink
イネーブル化 [2-1200](#)
ディセーブル化 [2-1200](#)
表示
Flexlink ペア [2-777](#)

FM
「機能マネージャ」を参照

FRU
IDPROM 情報の表示 [2-752](#)
統計情報の表示 [2-717](#)

fsck ユーティリティ
イネーブル化 [2-150](#)
自動モードの設定 [2-150](#)

FSU
redundancy force-switchover コマンド [2-644](#)

G

GBIC
タイプの表示 [2-761](#)

GBTE
トンネル情報の表示 [2-1020](#)

Guaranteed Bandwidth TE
「GBTE」を参照

H

HSRP

設定
初期化の遅延 [2-1187](#)
トラッキング [2-1189](#)
ハードウェア レイヤ 3 スイッチング [2-1191](#)
ディセーブル化
遅延期間 [2-1187](#)
表示
遅延期間情報 [2-1090](#)

I

ICC
カウンタおよびステータス情報の表示 [2-750](#)

ICMPv6 neighbor-discovery ACL
イネーブル化
TCAM サポートの最適化 [2-598](#)
ディセーブル化
TCAM サポートの最適化 [2-598](#)

IDPROM
情報の表示 [2-752](#)

ifIndex 永続性
インターフェイス コンフィギュレーション モードでの設定済みの SNMP ifIndex コマンドの削除 [2-1134](#)
インターフェイス上でのイネーブル化 [2-1136](#)
インターフェイス上でのディセーブル化 [2-1136](#)
グローバルにイネーブル化 [2-1141](#)
グローバルにディセーブル化 [2-1141](#)

IGMP
IGMP グループ キャッシュ エントリの削除 [2-51](#)
スヌーピング
イネーブル化 [2-231](#)
クエリア機能のイネーブル化 [2-243](#)
高速脱退の設定 [2-234](#)
最終メンバー クエリー インターバル [2-238](#)
サブネット内のマルチキャスト サポートのイネーブル化 [2-243](#)
情報の表示 [2-827](#)
着信メッセージのレート制限の設定 [2-245, 2-328](#)

- ディセーブル化 [2-231](#)
- 統計情報の削除 [2-53](#)
- 統計情報の表示 [2-829](#)
- マルチキャスト パケットの定期的フラッディング [2-247](#)
- マルチキャスト ルータ ポートとしてレイヤ 2 ポートを設定 [2-241](#)
- 明示的なトラッキング データベース サイズの制限 [2-240](#)
- レイヤ 2 エントリの最大数 [2-237](#)
- レート制限情報の表示 [2-828](#)
- 設定
 - TCN クエリー [2-250](#)
 - 最終メンバー クエリー インターバル [2-230](#)
- ディセーブル化
 - プロキシ レポート [2-232](#)
- 表示
 - VLAN インターフェイスのスヌーピング情報 [2-824](#)
 - VLAN のステータスおよび設定情報 [2-824](#)
 - インターフェイス ステータス情報 [2-824](#)
 - インターフェイス設定情報 [2-824](#)
 - ステータスおよび設定情報 [2-824](#)
 - マルチキャスト グループ [2-821](#)
 - 明示的なトラッキング情報 [2-1001](#)
 - 明示的なトラッキング ステータス [2-824](#)
- 明示的なホスト トラッキング
 - イネーブル化 [2-232](#)
 - ディセーブル化 [2-232](#)
- レート制限
 - 設定 [2-245, 2-328](#)
- IGMP スヌーピング
 - イネーブル化 [2-231](#)
 - 高速脱退処理 [2-234](#)
 - サブネット内のマルチキャスト サポート [2-243](#)
 - 明示的なホスト トラッキング [2-232](#)
- 設定
 - 最終メンバー クエリー インターバル [2-238](#)
 - レイヤ 2 エントリの最大数 [2-237](#)
- ディセーブル化 [2-231](#)
- 高速脱退処理 [2-234](#)
- サブネット内のマルチキャスト サポート [2-243](#)
- 明示的なホスト トラッキング [2-232](#)
- マルチキャスト ルータ
 - 学習方式、設定 [2-241](#)
 - ネクスト ホップ インターフェイス、指定 [2-241](#)
- Intelligent Traffic Redirect [2-593, 2-1046](#)
- Inter-Card Communication
 - 「ICC」を参照
- Intermediate System/Intermediate System
 - 「IS-IS」を参照
- Internet Group Management Protocol
 - 「IGMP」を参照
- Internetwork Packet Exchange
 - 「IPX」を参照
- Inter Packet Gap
 - 「IPG」を参照
- Inter-Switch Link VLAN
 - 「ISL VLAN」を参照
- IP
 - IPv4 ユニキャスト アドレスの表示 [2-926, 2-940](#)
 - NetFlow
 - スイッチングのイネーブル化 [2-315](#)
 - インターフェイスのユーザビリティ ステータスの表示 [2-833](#)
 - クリア
 - アクセス リスト統計情報 [2-42](#)
- ip [2-210](#)
- IP ARP
 - VLAN への ARP ACL の適用 [2-176](#)
 - イネーブル化
 - インスペクション確認 [2-183](#)
 - ダイナミック インスペクション [2-185](#)
 - クリア
 - DAI 統計情報 [2-44](#)
 - ログ バッファのステータス [2-43](#)
- 信頼状態

- 設定 [2-182](#)
- 設定
 - ポート単位で設定可能な信頼状態 [2-182](#)
 - ログ バッファ [2-180](#)
- 着信要求のレート制限 [2-178](#)
- ディセーブル化
 - DAI [2-185](#)
 - インスペクション確認 [2-183](#)
- パケット ロギングの制御 [2-186](#)
- 表示
 - DAI ステータス [2-788](#)
 - ログ バッファのステータス [2-791](#)
- ログ バッファ
 - ステータスのクリア [2-43](#)
 - ステータスの表示 [2-791](#)
- IPC
 - キャッシュ フロー エントリの表示 [2-796](#)
- IPG
 - デフォルト モードに戻す [2-174](#)
 - モードの設定 [2-174](#)
- IP IGMP
 - 「IGMP」を参照
- ip pim snooping sgr-prune コマンド [2-309](#)
- IPv4
 - クリア
 - ソフトウェアがインストールされたエントリ [2-74](#)
 - 設定
 - マルチキャスト レート リミッタ [2-522](#)
 - ディセーブル化
 - マルチキャスト レート リミッタ [2-522](#)
 - 表示
 - FIB TCAM 例外 [2-725](#)
 - 情報 [2-951](#)
- IPv6
 - ACL
 - 圧縮モードのイネーブル化 [2-450](#)
 - 再帰 ACL の NetFlow エントリの表示 [2-968](#)
 - ハードウェア NetFlow IPv6 設定の表示 [2-978](#)
- MLDv2 スヌーピング
 - 統計情報の表示 [2-885](#)
 - マルチキャスト ルータ インターフェイスの表示 [2-885](#)
 - 明示的トラッキング情報の表示 [2-885](#)
 - レポート抑制ステータスの表示 [2-885](#)
- イネーブル化
 - CEF ベースのマルチキャスト転送 [2-322](#)
 - 圧縮モード [2-450](#)
 - 送信元マルチキャスト アドレスからのパケットの拒否 [2-452](#)
 - 送信元ループバック アドレスからのパケットの拒否 [2-452](#)
 - ハードウェア アシスト [2-322](#)
- クリア
 - ソフトウェアがインストールされたエントリ [2-74](#)
 - プレフィクス単位のアカウンティング統計 [2-69](#)
- 設定
 - NDE フロー マスク [2-417](#)
 - マルチキャスト レート リミッタ [2-524](#)
- ディセーブル化
 - CEF ベースのマルチキャスト転送 [2-322](#)
 - 圧縮モード [2-450](#)
 - 送信元マルチキャスト アドレスからのパケットの拒否 [2-452](#)
 - 送信元ループバック アドレスからのパケットの拒否 [2-452](#)
 - ハードウェア アシスト [2-322](#)
 - マルチキャスト レート リミッタ [2-524](#)
- ハードウェア アシスト
 - イネーブル化 [2-322](#)
- 表示
 - ACL エントリ [2-1097](#)
 - DSS IPv6 範囲無効化プロファイル [2-712](#)
 - DSS IP 範囲無効化プロファイル [2-712](#)
 - FIB TCAM 例外 [2-725](#)
 - MFIB 情報 [2-879](#)
 - MLS IP 情報 [2-951](#)
 - MLS QoS 情報 [2-981](#)

- NetFlow エントリ [2-968](#)
- NetFlow ハードウェアの設定 [2-968](#)
- スイッチング テーブル エントリ情報 [2-936](#)
- 送信元 / 宛先ペアの厳密なルート [2-936](#)
- ハードウェア NetFlow IPv6 設定 [2-978](#)
- プラットフォーム ソフトウェア マルチキャスト
情報 [2-1043](#)
- プレフィクス単位のアカウンティング統
計 [2-936](#)
- マイクロフロー ポリシング情報 [2-978](#)
- マルチキャスト エントリ [2-936](#)
- マルチキャスト共有隣接関係 [2-1043](#)
- マルチキャスト サブネット / 接続済みハードウ
ェア エントリ [2-1043](#)
- マルチキャスト ハードウェア ショートカット
数 [2-1043](#)
- プレフィクス単位のアカウンティング
統計情報の表示 [2-936](#)
- 防止
 - ACL エントリのインストレーション [2-323](#)
 - マルチキャスト接続されたエントリのインス
トレーション [2-323](#)
- IPv6 スヌーピング
 - 「MLDv2 スヌーピング」を参照
- IPv6 ハードウェア設定情報 [2-978](#)
- IPX (Internetwork Packet Exchange)
 - アクセス リスト、時間範囲 [2-1241](#)
- IPX MLS
 - エントリをクリア [2-74](#)
- IPX ショートカット、MSFC への
 - イネーブル化 [2-539](#)
 - ディセーブル化 [2-539](#)
- IP 高速スイッチング、内容の表示 [2-836](#)
- IP 出力キュー
 - サイズの制限 [2-153](#)
 - デフォルト サイズに戻す [2-153](#)
- IP ショートカット、MSFC への
 - イネーブル化 [2-537](#)
 - ディセーブル化 [2-537](#)
- IP 処理
 - イネーブル化 [2-320](#)
 - ディセーブル化 [2-320](#)
- IP マルチキャスト [2-287](#)
 - Bidir
 - エントリをクリア [2-70](#)
 - イネーブル化
 - 複数のパス間の負荷分割 [2-284](#)
 - 許可
 - ブロードキャスト専用インターネットワーク間の
ルーティング [2-281](#)
 - 削除
 - 管理用スコープの境界 [2-277](#)
 - グループ [2-71](#)
 - 循環バッファ [2-279](#)
 - 自動 RP メッセージのフィルタリング [2-277](#)
 - 循環バッファ ストレージの割り当て [2-279](#)
 - 設定
 - 管理用スコープの境界 [2-277](#)
 - ディセーブル化
 - 複数のパス間の負荷分割 [2-284](#)
 - ルーティング [2-287](#)
 - テーブルに追加されるルート数の制限 [2-286](#)
 - 統計カウンタ
 - リセット [2-72](#)
 - フィルタリング
 - mrinfo 要求パケット [2-283](#)
 - ルーティング
 - スヌーピング情報の表示 [2-827](#)
 - ルーティング テーブルの表示 [2-842, 2-847](#)
- IP マルチキャスト ルーティング
 - MRM
 - UDP ポート番号 [2-1261](#)
 - mroute、設定 [2-252](#)
 - 「mroute」も参照
 - PIM
 - 最短パス ツリー、使用の遅延 [2-310](#)
 - ネイバ、表示 [2-867](#)
 - RP
 - Auto-RP、対象となるグループ [2-302, 2-303](#)

Auto-RP、マッピング エージェント **2-305**
 PIM バージョン 2 候補、アドバタイズ **2-301**
 RP アナウンスメントのフィルタリング
 アドレス、設定 **2-292**
 パケット ヘッダー、格納 **2-279, 2-841**

IP ルーティング プロトコル
 最大パラレル ルート数の設定 **2-395**

IS-IS
 Network Entity Title の設定 **2-585**

ISL
 カプセル化
 イネーブル化 **2-135**
 ディセーブル化 **2-135**

ISL VLAN
 802.1Q VLAN へのマッピング **2-1289**

L

LACP
 インターフェイスの設定 **2-22**
 設定
 システム プライオリティ **2-356**
 チャネル プロトコル **2-25**
 入力パケット レート **2-355**
 ポート チャネルのバンドルごとの最大ポー
 ト **2-353**
 ポート プライオリティ **2-354**
 チャネル プロトコルの選択を解除 **2-25**
 表示
 システム ID **2-891**
 統計情報 **2-891**
 内部情報 **2-891**
 ネイバ情報 **2-891**
 プロトコル設定 **2-729**

Link Aggregation Control Protocol
 「LACP」を参照

link-status イベント メッセージ
 イネーブル化
 インターフェイス上 **2-365**

グローバル **2-363**
 サブインターフェイス上 **2-366**
 システム初期化 **2-363**

ディセーブル化
 インターフェイス上 **2-365**
 グローバル **2-363**
 サブインターフェイス上 **2-366**
 システム初期化 **2-363**

logging **2-368**

M

MAC ACL QoS フィルタリング
 削除
 ARP ACL **2-6**
 設定
 ARP ACL **2-6**
 レイヤ 2 パケットとしてのレイヤ 3 パケットの分
 類 **2-388**

MAC ACL フィルタリング
 VLAN フィールドのイネーブル化 **2-390**
 VLAN フィールドのディセーブル化 **2-390**

MAC アドレス
 イネーブル化
 VLAN 単位の MAC 制限 **2-379**
 インターフェイス単位の MAC 制限 **2-379**
 グローバルな MAC 制限 **2-379**
 スティック MAC **2-1215**
 ポート単位の MAC 制限 **2-379**

カウンタ
 マルチキャスト アドレスの表示 **2-896**

削除
 スティック MAC **2-1215**

MAC アドレス テーブル
 イネーブル化
 CAM テーブル使用状況モニタリング通
 知 **2-382**
 MAC アドレス ラーニング **2-377**
 MAC 移動通知 **2-381**

- スタティック エントリの削除 [2-64, 2-384](#)
- スタティック エントリの追加 [2-384](#)
- セキュアまたは特定のアドレスの削除 [2-87](#)
- 設定
 - MAC 帯域外同期 [2-387](#)
 - RM パージング タイム [2-375](#)
 - エージング タイム [2-375](#)
- ダイナミック エントリの削除 [2-64](#)
- ディセーブル化
 - CAM テーブル使用状況モニタリング通知 [2-382](#)
 - MAC アドレス ラーニング [2-377](#)
 - MAC 移動通知 [2-381](#)
 - スタティック MAC アドレスの IGMP スヌーピング [2-384](#)
- 表示
 - DFC 固有の情報 [2-896](#)
 - MAC アドレス ラーニング ステート [2-902](#)
 - MAC 移動通知 [2-896](#)
 - VLAN 固有の情報 [2-896](#)
 - インターフェイス固有の情報 [2-896](#)
 - エージング タイム [2-896](#)
 - エントリ数 [2-896](#)
 - 手動で設定されたエントリ数 [2-896](#)
 - 情報 [2-896](#)
 - スタティック テーブル エントリ [2-896](#)
 - ダイナミック テーブル エントリ [2-896](#)
 - マルチキャスト テーブル エントリ [2-896](#)
- MAC アドレスのフィルタリング
 - イネーブル化 [2-384](#)
 - 設定 [2-384](#)
 - ディセーブル化 [2-384](#)
- MAC アドレス ラーニング
 - イネーブル化 [2-377](#)
 - 状態の表示 [2-902](#)
 - ディセーブル化 [2-377](#)
- MAC 移動通知
 - イネーブル化 [2-381](#)
 - ディセーブル化 [2-381](#)
- MAC 制限
 - イネーブル化 [2-379](#)
 - ディセーブル化 [2-379](#)
- MAC 帯域外同期
 - 設定 [2-387](#)
- Maintenance Loop Signaling Entity
 - 「MLSE」を参照
- Maintenance Operation Protocol
 - 「MOP」を参照
- match サブコマンド
 - アクセス [2-26](#)
- MD5 シグニチャ
 - コンピューティング [2-1269](#)
- MDIX
 - イネーブル化 [2-396](#)
 - ディセーブル化 [2-396](#)
- MDS
 - イネーブル化
 - IP マルチキャスト ルーティング [2-287](#)
 - ディセーブル化
 - IP マルチキャスト ルーティング [2-287](#)
 - 表示
 - インターフェイス情報 [2-838](#)
- MDSS
 - Multicast Distributed Shortcut Switching
- MDT
 - イネーブル化
 - データ MDT の再利用の記録 [2-400](#)
 - 設定
 - グループのアドレス範囲 [2-398](#)
 - デフォルト グループ [2-399](#)
 - ディセーブル化
 - データ MDT の再利用の記録 [2-400](#)
 - 表示
 - 受信したアドバタイズ [2-864](#)
 - 詳細な BGP アドバタイズ情報 [2-862](#)
 - 送信されたアドバタイズ [2-866](#)
 - データ再利用情報 [2-863](#)
 - デフォルト グループ情報 [2-862](#)

- ハードウェア アクセラレーション情報 **2-955**
- Message Digest 5
「MD5」を参照
- MFIB
エントリとインターフェイスの表示 **2-879**
- mGRE
指定
NBMA から BMA への変換 **2-551**
ネットワーク ID **2-551**
設定
モビリティ **2-551**
ワイヤレス mGRE トンネル **2-551**
- MIB
SNMP インターフェイス インデックス識別番号の表示 **2-1078**
- MLDv2
ディセーブル化
プロキシ レポート **2-325**
表示
MAC アドレス テーブル情報 **2-896**
統計情報 **2-885**
マルチキャスト ルータ インターフェイス **2-885**
明示的トラッキング情報 **2-885**
レポート抑制ステータス **2-885**
- MLDv2 スヌーピング
イネーブル化
グローバル **2-324**
スヌーピング クエリア **2-331**
明示的なトラッキング **2-325**
レポート抑制 **2-333**
最終メンバー クエリー インターバル **2-327**
設定
マルチキャスト ルータ ポートとしてレイヤ 2 ポートを設定 **2-330**
ディセーブル化
グローバル **2-324**
スヌーピング クエリア **2-331**
明示的なトラッキング **2-325**
レポート抑制 **2-333**
- 表示
明示的トラッキング データベース **2-885**
明示的なトラッキング データベース サイズの制限 **2-328**
- MLS
ACL マージ関数を選択 **2-403**
CEF
CEF テーブル情報の表示 **2-948**
特定の VRF に対する情報の表示 **2-948**
NDE
アドレスの削除 **2-542**
アドレスの指定 **2-542**
エクスポート機能のイネーブル化 **2-460**
カウンタをクリア **2-73**
ステータスおよび設定情報の表示 **2-991**
追加フィールドの入力のイネーブル化 **2-459**
追加フィールドの入力のディセーブル化 **2-459**
フィルタ オプションの削除 **2-457**
フィルタ オプションの指定 **2-457**
- QoS
ToS から DSCP への書き換え **2-500**
ToS から DSCP への書き換えのイネーブル化 **2-500**
ToS から DSCP への書き換えのディセーブル化 **2-500**
QoS 統計データのエクスポート
宛先アドレス **2-511**
インターバル **2-513**
クラス マップ **2-507**
グローバルにイネーブル化 **2-502**
グローバルにディセーブル化 **2-502**
集約ポリサー **2-505**
デリミタ **2-510**
ポート単位のイネーブル化 **2-503**
ポート単位のディセーブル化 **2-503**
- TCL
情報の表示 **2-999**
- VLAN
統計情報の表示 **2-1009**
- VTP ドメイン

- 削除 [2-544](#)
- リンク [2-544](#)
- イネーブル化
 - NetFlow インターフェイスベースのエントリ機能 [2-461](#)
 - NetFlow プロトコルベース エントリ機能 [2-461](#)
 - PDU レートリミッタ [2-520](#)
 - 転送ブロードキャスト [2-429](#)
 - レートリミッタ [2-520](#)
- インターフェイス
 - VLAN ID の削除 [2-543](#)
 - VLAN ID の割り当て [2-543](#)
 - 管理インターフェイスの削除 [2-541](#)
 - 管理インターフェイスの指定 [2-541](#)
- クリア
 - 統計情報 [2-79](#)
 - 統計情報 (廃止予定) [2-80](#)
- 除外するプロトコル ポートの削除 [2-415](#)
- 除外するプロトコル ポートの指定 [2-415](#)
- 設定
 - fast エージング タイム [2-407](#)
 - long エージング タイム [2-408](#)
 - normal エージング タイム [2-409](#)
 - ポートセキュリティ レートリミッタ [2-520](#)
 - レートリミッタ [2-520](#)
- 定義
 - 例外プライオリティ [2-413](#)
- ディセーブル化
 - レイヤ 2 プロトコル トンネリング レートリミッタ [2-520](#)
 - レートリミッタ [2-520](#)
- 転送ブロードキャスト
 - 情報の表示 [2-914](#)
- 転送ブロードキャストのディセーブル化 [2-429](#)
- トラフィックの許可 [2-431](#)
- 表示
 - ACL 統合方式 [2-747](#)
 - ASIC バージョン [2-908](#)
 - すべてのミス フローの集約カウント [2-999](#)
 - 対応するレジスタの最新の値 [2-999](#)
 - 統計情報 [2-997](#)
 - 統計データ エクスポート情報 [2-991](#)
 - パケット エラー情報 [2-997](#)
 - 例外プライオリティ [2-920](#)
 - フロー マスクの指定 [2-417](#)
 - フロー マスクの復元 [2-417](#)
 - 例外プライオリティ
 - 情報の表示 [2-920](#)
 - 定義 [2-413](#)
 - レートリミッタ
 - ACL ブリッジド レートリミッタのイネーブル化 [2-527](#)
 - ACL ブリッジド レートリミッタの設定 [2-527](#)
 - CEF レートリミッタのイネーブル化 [2-529](#)
 - CEF レートリミッタの設定 [2-529](#)
 - VACL ログ ケースのイネーブル化 [2-535](#)
 - VACL ログ ケースの設定 [2-535](#)
 - イネーブル化 [2-531](#)
 - 情報の表示 [2-993](#)
 - 設定 [2-519](#)
 - ユニキャストおよびマルチキャスト パケットに対するイネーブル化 [2-519](#)
 - ユニキャスト パケットへの設定 [2-531](#)
 - レイヤ 3 セキュリティ レートリミッタのイネーブル化 [2-534](#)
 - レイヤ 3 セキュリティ レートリミッタの設定 [2-534](#)
- MLS CEF
 - 表示
 - 一貫性チェッカー情報 [2-924](#)
- MLS IP
 - MSFC への IP ショートカット
 - イネーブル化 [2-537](#)
 - ディセーブル化 [2-537](#)
 - イネーブル化
 - TCAM 内のショートカット [2-449](#)
 - インターフェイス上の OAL [2-370](#)
 - グローバルな OAL [2-368](#)
 - 出力レプリケーション モード [2-442](#)

- 入力レプリケーション モード [2-442](#)
- レイヤ 4 ポート上での ACL の論理動作の拡張 [2-419](#)
- インターフェイス
 - 外部スイッチのイネーブル化 [2-538](#)
 - 外部スイッチのディセーブル化 [2-538](#)
 - ショートカットのイネーブル化 [2-435](#)
 - ショートカットのディセーブル化 [2-435](#)
 - 内部ルータのイネーブル化 [2-418](#)
 - 内部ルータのディセーブル化 [2-418](#)
 - 非 RPF マルチキャスト高速廃棄のイネーブル化 [2-444](#)
- 組み込み
 - ACL しきい値 [2-432](#)
- クリア
 - エントリ [2-74](#)
 - ソフトウェアがインストールされたエントリ [2-74](#)
- グローバル
 - 一貫性チェッカーのイネーブル化 [2-439](#)
 - 一貫性チェッカーのディセーブル化 [2-439](#)
 - イネーブル化 [2-433](#)
 - サブネット ダウンロードのイネーブル化 [2-437](#)
 - サブネット ダウンロードのディセーブル化 [2-437](#)
 - しきい値の設定 [2-446](#)
 - 双方向 RP RPF のスキャン インターバルの設定 [2-436](#)
 - ディセーブル化 [2-433](#)
 - ポリシー ルーティング パケット サポートのイネーブル化 [2-448](#)
 - ポリシー ルーティング パケット サポートのディセーブル化 [2-448](#)
- 再帰 NDR
 - TCAM 内のショートカットのイネーブル化 [2-449](#)
 - TCAM 内のショートカットのディセーブル化 [2-449](#)
- 削除
 - ACL しきい値 [2-428](#)
- 設定
 - インターフェイス上の OAL [2-370](#)
 - グローバルな OAL [2-368](#)
- ディセーブル化
 - TCAM 内のショートカット [2-449](#)
 - インターフェイス上の OAL [2-370](#)
 - グローバルな OAL [2-368](#)
 - 出力レプリケーション モード [2-442](#)
 - 入力レプリケーション モード [2-442](#)
 - レイヤ 4 ポート上での ACL の論理動作の拡張 [2-419](#)
- 表示
 - NetFlow エントリの統計情報 [2-966](#)
 - NetFlow ルーティング エントリ [2-963](#)
 - OAL キャッシュ エントリ [2-894](#)
 - OAL 設定情報 [2-894](#)
 - PIM グループとアクティブ ランデブー ポイントのマッピング [2-959](#)
 - 情報 [2-951](#)
 - ソフトウェアに組み込まれたスタティック エントリ情報 [2-965](#)
 - ソフトウェアに組み込まれた非スタティック エントリ情報 [2-962](#)
 - マルチキャスト レプリケーション機能 [2-955](#)
 - モード情報 [2-955](#)
- マルチキャスト
 - 出力機能のイネーブル化 [2-433](#)
- レプリケーション モード
 - 出力モードのイネーブル化 [2-442](#)
 - 出力モードのディセーブル化 [2-442](#)
 - 入力モードのイネーブル化 [2-442](#)
 - 入力モードのディセーブル化 [2-442](#)
- MLS IPX
 - MSFC への IPX ショートカット
 - イネーブル化 [2-539](#)
 - ディセーブル化 [2-539](#)
 - インターフェイス
 - 外部スイッチのイネーブル化 [2-540](#)
 - 外部スイッチのディセーブル化 [2-540](#)
- MLS QoS
 - DSCP 変換マッピング

- 削除 [2-483](#)
- 定義 [2-483](#)
- EXP 変換マップ
 - 削除 [2-485](#)
 - 定義 [2-485](#)
- MPLS
 - インターフェイス サマリーの表示 [2-988](#)
- VLAN スイッチ ポート
 - イネーブル化 [2-518](#)
 - ディセーブル化 [2-518](#)
- イネーブル化
 - ACL リダイレクト パケットのポリシング [2-494](#)
 - EtherChannel バンドリングに関するポート属性チェック [2-472](#)
 - ポートキューイング モード [2-498](#)
 - ポート信頼の無視 [2-491](#)
 - ポリサーのトラフィック クラス ID [2-492](#)
- インターフェイス
 - イネーブル化 [2-468](#)
 - 信頼されたポート状態の設定 [2-493, 2-514](#)
 - 信頼できないポート状態への変更 [2-493, 2-514](#)
 - ディセーブル化 [2-468](#)
- インターフェイスからのポリシー マップの削除 [2-662](#)
- インターフェイスへのポリシー マップの対応付け [2-662](#)
- 拡張された信頼
 - 信頼モードの設定 [2-516](#)
 - 信頼モードの表示 [2-1067](#)
- グローバル
 - PFC QoS のディセーブル化およびポート キューイングのイネーブル化 [2-466](#)
 - イネーブル化 [2-466](#)
 - ディセーブル化 [2-466](#)
- 削除
 - インターフェイスからの CoS 変換マップ [2-474](#)
 - インターフェイスからの DSCP 変換マップ [2-475](#)
 - インターフェイスからの EXP 変換マップ [2-476](#)
- 集約ポリサー
 - 削除 [2-469](#)
 - 定義 [2-469](#)
- 統計情報のクリアおよび高レートおよび低レートのポリサー バケットのトークン数 [2-77](#)
- 出力 DSCP/CoS マップ
 - 削除 [2-481](#)
 - 定義 [2-481](#)
- 出力 DSCP/EXP マップ
 - 削除 [2-482](#)
 - 定義 [2-482](#)
- 定義
 - 入力 EXP/DSCP マップ [2-484](#)
- ディセーブル化
 - ACL リダイレクト パケットのポリシング [2-494](#)
 - EtherChannel バンドリングに関するポート属性チェック [2-472](#)
 - ポートキューイング モード [2-498](#)
 - ポート信頼の無視 [2-491](#)
 - ポリサーのトラフィック クラス ID [2-492](#)
- デフォルト CoS 値
 - 削除 [2-473](#)
 - 定義 [2-473](#)
- 統計情報のクリアおよび高レートおよび低レートのポリサー バケットのトークン数 [2-77](#)
- 入力 CoS/DSCP マップ
 - 削除 [2-478](#)
 - 定義 [2-478](#)
- 入力 EXP/DSCP マップ
 - 削除 [2-484](#)
 - 定義 [2-484](#)
- 入力 IP precedence/DSCP マップ
 - 削除 [2-487](#)
 - 定義 [2-487](#)
- 表示
 - IPv6 情報 [2-981](#)
 - MPLS インターフェイス サマリー [2-988](#)

- 実行バージョン情報 [2-986](#)
- 情報 [2-981](#)
- スイッチ プロセッサおよび DFC 上の空の集約 RAM インデックス数 [2-985](#)
- マップ設定情報 [2-986](#)
- 付加
 - インターフェイスへの CoS 変換マップ [2-474](#)
 - インターフェイスへの DSCP 変換マップ [2-475](#)
 - インターフェイスへの EXP 変換マップ [2-476](#)
- ブリッジド トラフィックのマイクロフロー ポリシング
 - イネーブル化 [2-471](#)
 - 削除 [2-471](#)
- ポリシー マップ コンフィギュレーション モード
 - アクセス [2-606](#)
 - 既存の [2-606](#)
- ポリシング
 - ACL リダイレクト パケット [2-494](#)
- ポリシング済み適合 DSCP マップ
 - 削除 [2-489](#)
 - 定義 [2-489](#)
- マッピング
 - CoS/CoS マップの定義 [2-479](#)
- MLS QoS ポリシー マップ
 - class オプションの説明、表 [2-601, 2-607](#)
 - 設定 [2-606](#)
- MLS プレフィクス単位のアカウンティング
 - イネーブル化 [2-420](#)
 - ディセーブル化 [2-420](#)
- MMLS
 - 表示
 - 情報 [2-1002](#)
 - 明示的トラッキング情報 [2-1001](#)
- mobility [2-551](#)
- MOP (Maintenance Operation Protocol)
 - サーバ
 - 自動的に起動 [2-16](#)
- more コマンド
 - 検索 [1-7](#)
- フィルタ [1-7](#)
- More-- プロンプト [1-7](#)
- 検索 [1-7](#)
- フィルタ [1-7](#)
- MPLS
 - GB-TE フローの DSCP マップの設定 [2-455](#)
 - イネーブル化
 - 再循環 [2-453](#)
 - 集約ラベル再循環 [2-455](#)
 - タグ間のロードバランス [2-578](#)
 - トンネル再循環 [2-455](#)
 - クリア
 - ソフトウェアがインストールされたエントリ [2-74](#)
 - 削除
 - DSCP/EXP マップ [2-482](#)
 - 指定
 - 最適化された MPLS タギングの使用 [2-579](#)
 - 標準 MPLS タギングの使用 [2-579](#)
 - 設定
 - GB-TE フローのバースト期間 [2-455](#)
 - グローバルなパラメータ [2-455](#)
 - 試験値 [2-672](#)
 - 冗長モード [2-553](#)
 - レイヤ 2 WAN インターフェイスの信頼状態 [2-673](#)
 - タギング
 - 最適化されたタギングの使用の指定 [2-579](#)
 - 標準タギングの指定 [2-579](#)
 - タグ スイッチング
 - テーブル情報の表示 [2-1023](#)
 - ロードバランスのイネーブル化 [2-578](#)
 - ロードバランスのディセーブル化 [2-578](#)
 - 定義
 - DSCP/EXP マップ [2-482](#)
 - ディセーブル化
 - 再循環 [2-453](#)
 - 集約ラベル再循環 [2-455](#)
 - タグ間のロードバランス [2-578](#)

- トンネル再循環 [2-455](#)
- 表示
 - EoMPLS 対応インターフェイス情報 [2-1020](#)
 - FIB TCAM 例外 [2-725](#)
 - LAN および WAN 間の共有コード [2-1020](#)
 - VPN/VLAN マッピング テーブル [2-1020](#)
 - インターフェイス サマリー [2-988](#)
 - 現在のルーテッド VC ステート [2-1017](#)
 - コントロール プレイン統計 [2-1020](#)
 - 情報 [2-951](#)
 - プラットフォーム固有の情報 [2-1020](#)
- 負荷分散方式
 - 設定 [2-613](#)
 - デフォルトへのリセット [2-613](#)
 - ルーティングのイネーブル化 [2-576](#)
 - ルーティングのディセーブル化 [2-576](#)
- MPLS EXP
 - MPLS の試験的フィールド
 - 「MPLS」を参照
- mroute
 - 設定
 - スタティック ルート [2-252](#)
- MSDP
 - イネーブル化
 - ピアの管理上シャット ダウン [2-275](#)
 - クリア
 - MSDP ピアへの TCP 接続 [2-56](#)
 - SA キャッシュ エントリ [2-57](#)
 - 統計カウンタ [2-58](#)
 - 削除
 - 送信フィルタ リスト [2-271](#)
 - 着信フィルタ リスト [2-269](#)
 - ピア [2-265](#)
 - 作成
 - SA ステート [2-256](#)
 - 制限
 - マルチキャスト データ パケット [2-276](#)
 - 設定
 - PIM sparse (疎) モード リージョン [2-254](#)
 - SA メッセージでアドバタイズされるエント
リ [2-267](#)
 - SA 要求メッセージを送信するルータ [2-273](#)
 - SA 要求を送信するルータ [2-260](#)
 - 送信フィルタ リスト [2-271](#)
 - 着信フィルタ リスト [2-269](#)
 - 発信者 ID [2-263](#)
 - ピア [2-265](#)
 - メッシュ グループへのピア [2-262](#)
- 追加
 - 設定への説明文 [2-259](#)
- 定義
 - デフォルト ピア [2-257](#)
- ピア ステータスの表示 [2-855](#)
- ピアの立ち上げ [2-275](#)
- 表示
 - MSDP ピアから学習した状態 [2-853](#)
 - 送信元とグループの数 [2-849](#)
 - ピア情報 [2-851](#)
 - メッシュ グループからのピアの削除 [2-262](#)
- MSFC
 - 実行優先順位の設定 [2-1266](#)
 - 表示
 - スタンバイ MSFC2 DRAM [2-682](#)
 - フラッシュへの新規 ROMMON のプログラミング [2-1266](#)
- MST
 - PVST モードへの切り替え [2-1158](#)
 - インスタンス
 - VLAN のマッピング [2-164](#)
 - コンフィギュレーション サブモード コマンド
 - show [2-674](#)
 - インスタンス [2-164](#)
 - 名前 [2-582](#)
 - リビジョン [2-653](#)
 - コンフィギュレーションサブモードの開始 [2-1160](#)
 - 設定
 - hello タイム [2-1163](#)
 - MST リージョン名 [2-582](#)

- インスタンスのパス コスト [2-1159](#)
- インスタンスのポートプライオリティ [2-1159](#)
- コンフィギュレーション リビジョン番号の設定 [2-653](#)
- 最大ホップ [2-1165](#)
- セカンダリとしてのルート [2-1168](#)
- 先行標準の BPDU を送信するポート [2-1166](#)
- 転送遅延 [2-1162](#)
- プライマリとしてのルート [2-1168](#)
- 有効期限 [2-1164](#)
- 表示
 - MST プロトコル情報 [2-1086](#)
 - MST リージョン コンフィギュレーション情報 [2-1086](#)
 - 現在の設定 [2-674](#)
 - 設定の保留 [2-674](#)
- プロトコル マイグレーションを再開 [2-89](#)
- マッピング
 - PVLAN とインスタンス間のマッピング [2-629](#)
 - VLAN [2-164](#)
- MTU
 - グローバル MTU 設定の表示 [2-1094](#)
 - システム MTU 設定の表示 [2-1094](#)
 - 設定
 - 最大サイズ [2-580](#)
 - 最大パケット サイズ [2-580](#)
 - レイヤ 2 の最大ペイロード サイズ [2-1235](#)
 - レイヤ 3 の最大ペイロード サイズ [2-1235](#)
 - デフォルト値 [2-580](#)
 - デフォルト値の復元 [2-580](#)
- Multiple Spanning Tree
 - 「MST」を参照
- mVPN
 - MSDP ピアの立ち上げ [2-275](#)
 - PIM 登録メッセージのフィルタリング [2-291](#)
 - イネーブル化
 - Bidir-PIM [2-294](#)
 - IP マルチキャスト ルーティング [2-287](#)
 - ピアの管理上シャット ダウン [2-275](#)
 - 複数のパス間の負荷分割 [2-284](#)
 - クリア
 - MSDP ピアへの TCP 接続 [2-56](#)
 - SA キャッシュ エントリ [2-57](#)
 - 統計カウンタ [2-58](#)
 - 削除
 - Auto-RP キャッシュ エントリ [2-59](#)
 - Auto-RP メッセージ フィルタ [2-300](#)
 - IGMP グループ キャッシュからのエントリ [2-51](#)
 - IP マルチキャストルーティング テーブルからのエントリ [2-54](#)
 - 循環バッファ [2-279](#)
 - 送信フィルタ リスト [2-271](#)
 - 着信フィルタ リスト [2-269](#)
 - ピア [2-265](#)
 - 作成
 - SA ステート [2-256](#)
 - 循環バッファ ストレージの割り当て [2-279](#)
 - 制限
 - マルチキャスト データ パケット [2-276](#)
 - 設定
 - Auto-RP の使用 [2-303](#)
 - BSR 候補 [2-296](#)
 - BSR にアドバタイズ [2-301](#)
 - MSDP の PIM sparse (疎) モード リージョン [2-254](#)
 - PIM メッセージの受け入れ [2-292](#)
 - SA メッセージでアドバタイズされるエントリ [2-267](#)
 - SA 要求メッセージを送信するルータ [2-273](#)
 - SA 要求を送信するルータ [2-260](#)
 - 最短パス ツリー、使用の遅延 [2-310](#)
 - 送信フィルタ リスト [2-271](#)
 - 着信フィルタ リスト [2-269](#)
 - デフォルト グループ [2-399](#)
 - 登録送信元 [2-299](#)
 - 登録メッセージ制限 [2-298](#)
 - 発信者 ID [2-263](#)
 - ピア [2-265](#)

メッシュ グループへのピア [2-262](#)
 ランデブー ポイント マッピング エージェント [2-305](#)

追加

MSDP 設定への説明文 [2-259](#)

定義

IP マルチキャストアドレスの SSM 範囲 [2-311](#)
 デフォルト ピア [2-257](#)

ディセーブル化

Bidir-PIM [2-294](#)

IP マルチキャストアドレスの SSM 範囲 [2-311](#)
 IP マルチキャスト ルーティング [2-287](#)
 複数のパス間の負荷分割 [2-284](#)

テーブルに追加されるルート数の制限 [2-286](#)

表示

BSR 情報 [2-859](#)
 IP 高速スイッチング キャッシュの内容 [2-836](#)
 MDS インターフェイス情報 [2-838](#)
 MSDP ピアから学習した状態 [2-853](#)
 MSDP ピア ステータス [2-855](#)
 キャッシュされたランデブー ポイント [2-871](#)
 グループのランデブー ポイント [2-869](#)
 指定フォワーダ インターフェイス情報 [2-861](#)
 受信した MDT アドバタイズ [2-864](#)
 循環キャッシュ ヘッダー バッファの内容 [2-840](#)
 詳細な BGP アドバタイズ情報 [2-862](#)
 送信された MDT アドバタイズ [2-866](#)
 送信元とグループの数 [2-849](#)
 データ MDT 再利用情報 [2-863](#)
 トリガーされた RPF チェック イベント [2-876](#)
 発見されたネイバ [2-867](#)
 ピア情報 [2-851](#)

フィルタリング

Auto-RP メッセージ [2-300](#)
 mrinformo 要求パケット [2-283](#)

メッシュ グループからのピアの削除 [2-262](#)

N

NDE

アドレスの削除 [2-542](#)
 アドレスの指定 [2-542](#)
 イネーブル化
 インターフェイスでのサンプリング済み NetFlow [2-463](#)
 エクスポート機能 [2-460](#)
 追加フィールドの入力 [2-459](#)

クリア

カウンタ [2-73](#)

サンプリング済み NetFlow

インターフェイス上でのイネーブル化 [2-463](#)
 インターフェイス上でのディセーブル化 [2-463](#)
 サンプリング方式の指定 [2-545](#)

ディセーブル化

インターフェイスでのサンプリング済み NetFlow [2-463](#)
 追加フィールドの入力 [2-459](#)

表示

エージング情報 [2-968](#)
 サンプリング済み NetFlow ステータス [2-996](#)
 ステータスおよび設定情報 [2-991](#)
 ステータス情報 [2-967](#)
 ハードウェア ステータス [2-968](#)

フィルタ オプション

削除 [2-457](#)
 指定 [2-457](#)

NDE インターフェイスのエクスポート

フィルタ オプションの指定 [2-457](#)
 フロー マスク [2-457](#)

NET

設定 [2-585](#)

NetFlow

IPv6

ハードウェア設定情報の表示 [2-978](#)
 イネーブル化
 インターフェイス ベースの NDE [2-220](#)

- インターフェイスベースのエントリの作成 **2-461**
- サンプリング済み NetFlow (グローバル) **2-545**
- スイッチング **2-315**
- ハードウェアでスイッチングされるフローの NDE **2-216**
- ブリッジドフローにグローバルに **2-226**
- ブリッジドフローの着信 NDE **2-225**
- プロトコルベース エントリの作成 **2-461**
- マルチキャスト入力アカウンティング **2-285**
- インターフェイス
 - 送信元インターフェイスの指定 **2-221**
- インターフェイスベースの NDE
 - イネーブル化 **2-220**
 - ディセーブル化 **2-220**
- カウンタをクリア **2-39**
- 指定
 - Supervisor Engine 720 上でのエクスポート フローバージョン **2-223**
 - ハードウェアでスイッチングされるフローの NDE バージョン **2-219**
- 集約
 - キャッシュ フロー エントリの表示 **2-796**
 - 特定の集約キャッシュの設定 **2-212**
- スイッチ プロセッサ上でのテーブルの使用
 - モニタリング **2-465**
- スイッチング
 - キャッシュ エントリのエクスポート **2-217**
 - キャッシュ サイズの設定 **2-214**
 - キャッシュ フロー エントリの表示 **2-796**
 - 送信元インターフェイスの指定 **2-221**
 - 統計情報のクリア **2-50**
- 設定
 - 最大フロー割り当て **2-462**
 - 集約キャッシュ - 特定 **2-212**
 - 複数のエクスポートの宛先 **2-217**
- ソフトウェア スwitchング
 - 情報の表示 **2-819**
- ディセーブル化
 - インターフェイスベースの NDE **2-220**
 - サンプリング済み NetFlow (グローバル) **2-545**
 - ハードウェアでスイッチングされるフローの NDE **2-216**
 - ブリッジドフローにグローバルに **2-226**
 - ブリッジドフローの着信 NDE **2-225**
 - マルチキャスト入力アカウンティング **2-285**
- ハードウェア スwitchング
 - CEF テーブル情報の表示 **2-809**
 - インターフェイスベース エントリの作成のイネーブル化 **2-461**
 - インターフェイスベース エントリの作成のディセーブル化 **2-461**
 - プロトコルベース エントリの作成のイネーブル化 **2-461**
 - プロトコルベース エントリの作成のディセーブル化 **2-461**
- 表示 **2-978**
 - IP 情報 **2-968**
 - IP フロー情報 **2-971**
 - IP フロー マスク **2-968**
 - エージング情報 **2-968**
 - キャッシュ フロー エントリ **2-796**
 - 詳細統計サマリー **2-800**
 - スイッチングされたパケット数 **2-997**
 - ソフトウェアに組み込まれた非スタティック エントリ情報 **2-976**
 - テーブル情報 **2-951**
 - 統計情報 **2-951**
 - ハードウェア ステータス **2-968**
 - フラグメント オフセット情報 **2-800**
 - マイクロフロー ポリシング統計情報 **2-971**
- ブリッジングされた VLAN 内トラフィックの取り込み **2-471**
- モニタリング
 - スイッチ プロセッサ上での NetFlow テーブルの使用 **2-465**
- NetFlow データ エクスポート
 - 「NDE」を参照
- Network Entity Title

「NET」を参照

Next Hop Resolution Protocol

「NHRP」を参照

NHRP

表示

 キャッシュ **2-856**

Non-STOP Forwarding

「NSF」を参照

no 形式、コマンドの、使用 **1-7**

NSF

OSPF 再開のキャンセル **2-587**

イネーブル化

 BGP ルーティング プロセス **2-659**

 EIGRP ルーティング プロセス **2-659**

 IS-IS ルーティング プロセス **2-659**

 OSPF ルーティング プロセス **2-659**

指定

 IETF IS-IS 方式 **2-587**

 IS-IS データベース同期化の待機時間 **2-587**

 シスコ独自の IS-IS 方式 **2-587**

 フェールオーバーのインターバル **2-587**

 ルート プロセッサ スタビライザのインターバル **2-587**

ディセーブル化 **2-587**

 BGP ルーティング プロセス **2-659**

 EIGRP ルーティング プロセス **2-659**

 IS-IS ルーティング プロセス **2-659**

 OSPF ルーティング プロセス **2-659**

O

OAL

 エントリをクリア **2-63**

 設定

 インターフェイス **2-370**

 グローバル **2-368**

 表示

 キャッシュ エントリ **2-894**

 設定情報 **2-894**

ODM

 ACL マージ関数を選択 **2-403**

ODM アルゴリズム

 「ODD」を参照

Optimized ACL Logging

 「OAL」を参照

OSPF

 指定

 CPU プロセス時間の最小の割合 **2-630**

P

PAgP

 インターフェイスの設定 **2-22**

 情報のクリア **2-81**

 設定

 チャンネル プロトコル **2-25**

 着信パケットの入力インターフェイス

 学習 **2-590**

 デフォルトに戻す **2-590**

 チャンネル プロトコルの選択を解除 **2-25**

 表示

 プロトコル情報 **2-729**

 ポート チャンネル

 情報の表示 **2-1024**

 ホットスタンバイ モード

 デフォルトに戻す **2-591**

 ポートの選択 **2-591**

PBR

 イネーブル化 **2-448**

 null0 ルート マップへのハードウェア サポート **2-448**

 ディセーブル化 **2-448**

Per VLAN Spanning-Tree

 「PVST+」を参照

PIM

 イネーブル化

 Bidir-PIM **2-294**

- PIM dense (密) モード ステート リフレッシュ制御メッセージの処理および転送 [2-312](#)
- SGR-prune の抑制 [2-309](#)
- インターフェイス上でのスヌーピング [2-307](#)
- グローバルにスヌーピング [2-306](#)
- 指定ルータへのパケットのフラッドイング [2-308](#)
- クリア
 - VLAN の統計情報 [2-61](#)
 - グローバルな統計情報 [2-60](#)
- 削除
 - Auto-RP キャッシュ エントリ [2-59](#)
 - Auto-RP メッセージ フィルタ [2-300](#)
- スヌーピング
 - VLAN の統計情報の削除 [2-61](#)
 - インターフェイス上でのイネーブル化 [2-307](#)
 - インターフェイス上でのディセーブル化 [2-307](#)
 - グローバルな統計情報の削除 [2-60](#)
 - グローバルにイネーブル化 [2-306](#)
 - グローバルにディセーブル化 [2-306](#)
- 設定
 - Auto-RP の使用 [2-303](#)
 - BSR 候補 [2-296](#)
 - BSR にアドバタイズ [2-301](#)
 - MSDP の PIM sparse (疎) モード リージョン [2-254](#)
 - 最短パス ツリー、使用の遅延 [2-310](#)
 - 待機インターバル [2-288](#)
 - チェック インターバル [2-290](#)
 - 登録送信元 [2-299](#)
 - 登録メッセージ制限 [2-298](#)
 - メッセージの受け入れ [2-292](#)
 - 誘発型チェック インターバル [2-288](#)
 - ランデブー ポイント マッピング エージェント [2-305](#)
- 定義
 - IP マルチキャストアドレスの SSM 範囲 [2-311](#)
- ディセーブル化
 - Bidir-PIM [2-294](#)
 - IP マルチキャストアドレスの SSM 範囲 [2-311](#)
- PIM dense (密) モード ステート リフレッシュ制御メッセージの処理および転送 [2-312](#)
- SGR-prune の抑制 [2-309](#)
- インターフェイス上でのスヌーピング [2-307](#)
- グローバルにスヌーピング [2-306](#)
- 指定ルータへのパケットのフラッドイング [2-308](#)
- 誘発型 RPF チェック [2-288](#)
- 登録メッセージのフィルタリング [2-291](#)
- 表示
 - BSR 情報 [2-859](#)
 - IP マルチキャスト ルーティング テーブル情報 [2-847](#)
 - PIM グループとアクティブ ランデブー ポイントのマッピング [2-959](#)
 - キャッシュされたランデブー ポイント [2-871](#)
 - グループのランデブー ポイント [2-869](#)
 - 指定フォワーダインターフェイス情報 [2-861](#)
 - 受信した MDT アドバタイズ [2-864](#)
 - 詳細な BGP アドバタイズ情報 [2-862](#)
 - スヌーピング情報 [2-873](#)
 - 送信された MDT アドバタイズ [2-866](#)
 - データ MDT 再利用情報 [2-863](#)
 - トリガーされた RPF チェック イベント [2-876](#)
 - 発見されたネイバ [2-867](#)
- フィルタリング
 - Auto-RP メッセージ [2-300](#)
- PIR
 - ピーク レートの設定 [2-469](#)
- PISA
 - 表示
 - カウンタ情報 [2-1036](#)
 - 分割された VLAN [2-1050](#)
- portName MIB オブジェクト
 - 設定 [2-1186](#)
- Private VLAN
 - 「PVLAN」を参照
- Programmable Intelligent Services Accelerator
 - 「PISA」を参照
- psecure

「ポートセキュリティ」を参照

PVL

イネーブル化 [2-377](#)

ディセーブル化 [2-377](#)

PVLAN [2-1122](#)

VLAN インターフェイス コンフィギュレーション
モード

プライマリおよびセカンダリ VLAN のマッピング [2-627](#)

マッピング [2-627](#)

マッピングの削除 [2-627](#)

VLAN サブモード

VLAN の削除 [2-624](#)

VLAN の指定 [2-624](#)

VLAN の追加 [2-624](#)

アソシエーションの設定 [2-624](#)

アソシエーションの削除 [2-1221](#)

アソシエーションの定義 [2-1221](#)

イネーブル化

インターフェイスごとのスティッキ
ARP [2-319](#)

グローバル スティッキ ARP [2-317](#)

設定

インターフェイス タイプ [2-1209](#)

混合モード [2-1209](#)

ホスト ポート [2-1209](#)

ディセーブル化

インターフェイスごとのスティッキ
ARP [2-319](#)

グローバル スティッキ ARP [2-317](#)

表示

現在設定されている情報 [2-1122, 2-1127](#)

設定情報 [2-775, 2-777](#)

マッピング情報 [2-771](#)

マッピング

インスタンスへのマッピング [2-629](#)

混合モード ポート用 [2-1222](#)

プライマリおよびセカンダリ VLAN [2-627](#)

「PVL」を参照

PVST

MST モードへの切り替え [2-1158](#)

PVST+ BPDU および 802.1d BPDU 変換、プロトコル ト
ンネリングリンクによる [2-19](#)

PVST および PVST+ のインターオペラビリティ

ignore-bpdu-pid キーワード [2-19](#)

L2PT トポロジー [2-20](#)

Q

QDM

セッションの切断 [2-120](#)

表示

クライアント ID [2-1063](#)

現在アクティブな QDM クライアントに関する情
報およびステータス [2-1063](#)

QinQ

IEEE 802.1Q in 802.1Q

「802.1Q トンネリング」を参照

イネーブル化

二重タグ付き VLAN 変換 [2-555](#)

削除

リンク バンドル (ポート チャネル) 仮想イン
ターフェイス [2-169](#)

作成

リンク バンドル (ポート チャネル) 仮想イン
ターフェイス [2-169](#)

設定

優先順位ビット [2-666](#)

ディセーブル化

二重タグ付き VLAN 変換 [2-555](#)

QM

スイッチ プロセッサ情報の表示 [2-1064](#)

QoS

FM NetFlow カウンタをクリア [2-39](#)

Intelligent Traffic Redirect [2-593](#)

rcv-queue レート制限

設定 [2-636](#)

アクセス

クラス マップ コンフィギュレーション モー
ド [2-26](#)

- イネーブル化
 - 時間ベース ACL [2-1241](#)
 - キューイング モード [2-499](#)
 - クラス マップ
 - 情報の表示 [2-693](#)
 - グローバル インターフェイス カウンタのクリア [2-37](#)
 - 削除
 - ACL 時間範囲の制限 [2-1241](#)
 - 設定
 - キューイング モード [2-499](#)
 - クラス マップ [2-26](#)
 - 時間ベース ACL [2-1241](#)
 - 送信キュー サイズ比
 - 設定 [2-1299](#)
 - 定義
 - マーキング [2-495](#)
 - 表示
 - プロトコル [2-990](#)
 - ポリシー マップ
 - 一致するトラフィックへの DSCP 値のマーキング [2-668](#)
 - 一致するトラフィックへの IP precedence 値のマーキング [2-670](#)
 - インターフェイス単位の情報の表示 [2-1055](#)
 - 情報の表示 [2-1051](#)
 - マーキング設定の消去 [2-668](#)
 - マネージャ
 - 情報の表示 [2-1064](#)
 - ルーティング プロトコル パケット ポリシングの回避 [2-495](#)
 - ルーティング プロトコル パケット ポリシングの制御 [2-495](#)
 - QoS Device Manager
 - 「QDM」を参照
 - QoS 統計データのエクスポート
 - 「MLS QoS 統計データのエクスポート」を参照
 - QoS フィルタリング
 - イネーブル化
 - DSCP ベースの出力 [2-596](#)
 - IP precedence ベースの [2-596](#)
 - question コマンド [1-2](#)
-
- ## R
- Rapid Spanning Tree Protocol+
 - 「RSTP+」を参照
 - Rapid Spanning-Tree Protocol
 - 「RSTP」を参照
 - rcv-queues
 - CoS 値のマッピング [2-634](#)
 - サイズ比制限の設定 [2-636](#)
 - 最大しきい値の指定 [2-637](#)
 - デフォルト値へのリセット [2-637](#)
 - 廃棄しきい値の設定 [2-639](#)
 - regex
 - 「Regular Expression Library」を参照
 - Regular Expression Library
 - オープン ソース ソフトウェアの許諾 [B-1](#)
 - Remote SPAN
 - 「RSPAN」を参照
 - Reverse Path Forwarding
 - 「RPF」を参照
 - RFC 1340 [2-796](#)
 - RFC 1757、RMON MIB [2-655](#)
 - RMON イベント テーブル
 - イベントの削除 [2-656](#)
 - イベントの追加 [2-656](#)
 - RFC 1757、RMON アラーム グループ
 - アラームの設定 [2-654](#)
 - RGMP
 - イネーブル化 [2-313](#)
 - ディセーブル化 [2-313](#)
 - RM
 - 設定
 - パーズング タイム [2-375](#)
 - パーズング インターバルの設定 [2-375](#)
 - パーズング タイムのディセーブル化 [2-375](#)
 - RMON

- MIB オブジェクト アラームのディセーブル化 [2-654](#)
 - MIB オブジェクトのアラームの設定 [2-654](#)
 - アラーム、イネーブル化 [2-654](#)
 - アラーム、ディセーブル化 [2-654](#)
 - イベントの削除 [2-656](#)
 - イベントの追加 [2-656](#)
 - ディセーブル化 [2-656](#)
 - 「RM」を参照
 - ROMMON
 - 現場アップグレード [2-1266](#)
 - 実行優先順位の設定 [2-1266](#)
 - ステータスの表示 [2-1072](#)
 - フラッシュへの新規 ROMMON のプログラミング [2-1266](#)
 - ROM、自動的に起動 [2-16](#)
 - ROM モニタ モード、概要 [1-6](#)
 - Route Processor Redundancy
 - 「RPR」を参照
 - RPC
 - 情報の表示 [2-1073](#)
 - RPF
 - イネーブル化
 - Exists-only チェック [2-336](#)
 - インターフェイス上 [2-334](#)
 - 設定
 - PIM 待機インターバル [2-288](#)
 - チェック インターバル [2-290](#)
 - 誘発型チェック インターバル [2-288](#)
 - ディセーブル化
 - Exists-only チェック [2-336](#)
 - インターフェイス上 [2-334](#)
 - 誘発型チェック [2-288](#)
 - 表示
 - トリガーされたチェック イベント [2-876](#)
 - ハードウェア情報 [2-944](#)
 - RSPAN
 - インターフェイスまたは VLAN の削除 [2-566](#)
 - インターフェイスまたは VLAN の追加 [2-566](#)
 - 新規セッションの開始 [2-566](#)
 - セッションの削除 [2-566](#)
 - 表示
 - セッション情報 [2-1013](#)
 - リストの表示 [2-1124](#)
 - RSTP+
 - リンク タイプの設定 [2-1156](#)
-
- ## S
- SCP
 - イネーブル化
 - 高速リトライ [2-599](#)
 - 情報の表示 [2-1077](#)
 - 設定
 - 高速リトライのインターバル [2-599](#)
 - ディセーブル化
 - 高速リトライ [2-599](#)
 - Secure Sockets Layer
 - 「SSL」を参照
 - Server Load Balancing
 - 「SLB」を参照
 - show [2-948](#)
 - show platform software pisa split-vlan コマンド [2-1050](#)
 - show コマンド
 - 検索 [1-7](#)
 - フィルタ [1-7](#)
 - SLB
 - 帯域内パケット数の表示 [2-736](#)
 - SNMP
 - ifIndex 永続性
 - インターフェイス コンフィギュレーション モードでの設定済みの SNMP ifIndex コマンドの削除 [2-1134](#)
 - インターフェイス上でのイネーブル化 [2-1136](#)
 - インターフェイス上でのディセーブル化 [2-1136](#)
 - グローバルにイネーブル化 [2-1141](#)
 - グローバルにディセーブル化 [2-1141](#)

- イネーブル化
 - スイッチ フェールオーバー時のリンクダウン **2-1146**
 - トランシーバ トラップ **2-1140**
 - 不明なコンテキスト エラー発生時の許可トラップ **2-1145**
- インフォーム
 - イネーブル化 **2-1138**
 - ディセーブル化 **2-1138**
- 指定
 - 送信元インターフェイス
 - SNMP 指定
 - インフォームの送信元指定 **2-1143**
 - トラップの送信元指定 **2-1143**
 - 送信元指定の削除 **2-1143**
- ディセーブル化
 - スイッチ フェールオーバー時のリンクダウン **2-1146**
 - トランシーバ トラップ **2-1140**
 - 不明なコンテキスト エラー発生時の許可トラップ **2-1145**
- トラップ
 - イネーブル化 **2-1138**
 - ディセーブル化 **2-1138**
- 表示
 - インターフェイス インデックス識別番号 **2-1078**
- Softfloat
 - オープン ソース ソフトウェアの許諾 **B-1**
- Source Specific Multicast
 - 「SSM」を参照
- SPAN
 - イネーブル化
 - サービス モジュール セッション **2-566**
 - サービス モジュール セッション
 - イネーブル化 **2-566**
 - ディセーブル化 **2-566**
 - ディセーブル化
 - サービス モジュール セッション **2-566**
- 表示
 - 宛先ポート許可リスト **2-1012**
 - セッション情報 **2-1013**
- SPAN 宛先ポート許可リスト
 - 設定 **2-564**
 - 表示 **2-1012**
- SPAN セッション
 - インターフェイスまたは VLAN の削除 **2-566**
 - インターフェイスまたは VLAN の追加 **2-566**
 - 新規セッションの開始 **2-566**
 - セッションの削除 **2-566**
- SP QoS Manager
 - 「QM-SP」を参照
- SRM、SSO 付き
 - 冗長モードの設定 **2-553**
 - 設定
 - ルート コンバージェンス遅延間隔 **2-658**
- SRR キュー
 - 設定
 - 帯域幅 **2-1303**
- SSL
 - シャットダウン **2-162**
- SSM マッピング **2-248**
 - イネーブル化 **2-248**
 - 設定
 - スタティック マッピング データベース **2-248**
 - ディセーブル化 **2-248**
- SSO
 - 冗長モードの設定 **2-553**
 - 設定
 - ルート コンバージェンス遅延間隔 **2-658**
- Stateful Switch Over
 - 「SSO」を参照
- sticky ポート
 - 削除 **2-87**
- sup-bootflash
 - ファイル システム情報の表示 **2-1091**
- Switch-Module Configuration Protocol
 - 「SCP」を参照

T

Table Contention Level

「TCL」を参照

Tab キー

コマンド補完機能 **1-1**

TAC

情報の表示 **2-1099**

TCAM

ACL

一致カウンタのクリア **2-66**更新中のデフォルト動作の設定 **2-405**

イネーブル化

IPv6 ACL の最適化 **2-598**グローバルなデフォルト ACL の共有 **2-406**ショートカット **2-449**インターフェイスのプライオリティの設定 **2-1237**

クリア

ACL 一致カウンタ **2-66**

更新

デフォルト動作の設定 **2-405**

設定

更新中のデフォルト動作 **2-405**

ディセーブル化

IPv6 ACL の最適化 **2-598**グローバルなデフォルト ACL の共有 **2-406**ショートカット **2-449**

表示

インターフェイス ベースの情報 **2-1097**統計情報 **2-1095**プロトコル ベースの情報 **2-1097**TCAM ACL 一致カウンタ、クリア **2-66**

TCL

MLS 情報の表示 **2-999**

TDR

クリア

すべてのインターフェイス **2-35**特定のインターフェイス **2-35**ケーブル診断テスト結果の表示 **2-685**ケーブル診断の実行 **2-1239**

Ternary CAM

「TCAM」を参照

Time Domain Reflectometer

「TDR」を参照

time-range コマンド **2-1241**

TopN

イネーブル化

プロセスおよびレポート **2-95**

設定

サンプリング インターバル **2-95**統計タイプによるソート **2-95**レポートのクリア **2-91**

traceroute MAC

表示

インターフェイスによる **2-1243**送信元 IP から宛先 IP **2-1243**送信元 MAC から宛先 MAC **2-1243**

U

UDE

ソフトウェア ベースの

設定 **2-1264**設定の削除 **2-1264**

表示

動作ステータス **2-785**

UDLD

UDLD によってシャットダウンされたすべてのポートのリセット **2-1260**

アグレッシブ モード

インターフェイス上でのイネーブル化 **2-1258**インターフェイス上でのディセーブル化 **2-1258**光ファイバインターフェイス上でのグローバルなイネーブル化 **2-1256**光ファイバインターフェイス上でのグローバルなディセーブル化 **2-1256**

インターフェイス コンフィギュレーション モード

インターフェイス上でのイネーブル化 **2-1258**

グローバル コンフィギュレーション モード

光ファイバインターフェイス上でのみイネーブル化 **2-1256**

ディセーブル化

インターフェイス **2-1258**

UDLR

UDP ポート番号の変更 **2-1261**

イネーブル化

ARP および NHRP の転送 **2-1250**

削除

GRE トンネル受信バック チャンネル **2-1252**

GRE トンネル送信バック チャンネル **2-1254**

設定

受信バック チャンネルとしての GRE トンネル **2-1252**

メッセージ送信バック チャンネルとしての GRE トンネル **2-1254**

表示

情報 **2-831**

UDP

設定

CASA キューの長さ **2-191**

ポート番号の変更 **2-1261**

UDP データグラム

スパニングツリー アルゴリズムを使用するフラッディング **2-227**

すべての送信パケット上の UDP チェックサム **2-227**

フラッディングのディセーブル化 **2-227**

uRPF

イネーブル化

Exists-only チェック **2-336**

RPF ACL がイネーブルのハードウェア **2-425**

ディセーブル化

Exists-only チェック **2-336**

RPF ACL がイネーブルのハードウェア **2-425**

UUFB

スイッチ ポート

パケット転送の禁止 **2-1202**

V

VACL

VLAN アクセス マップの適用 **2-1286**

開始

VLAN アクセスマップ モード **2-1280**

拡張 MAC アクセス リストの定義 **2-372**

キャプチャ機能のイネーブル化 **2-1203**

キャプチャ機能のディセーブル化 **2-1203**

作成

VLAN アクセス マップ **2-1280**

指定

match 句 **2-391**

アクセス マップ シーケンス **2-391**

パケット アクション

設定 **2-2**

転送 **2-2**

廃棄 **2-2**

リダイレクト **2-2**

VACL ロギング

しきい値 **2-1278**

設定

パラメータ **2-1278**

リダイレクト パケット レート **2-1278**

ロギングしきい値 **2-1278**

ロギング パラメータ **2-1278**

ログ テーブル サイズ **2-1278**

デフォルト値へのリセット **2-1278**

デフォルトのロギング値へのリセット **2-1278**

表示

設定情報 **2-1112**

フロー テーブルの内容 **2-1112**

ロギング プロパティ情報 **2-1112**

リダイレクト パケット レート **2-1278**

ログ テーブル サイズ **2-1278**

Value Mask Result

「VMR」を参照

VFI

作成 **2-352**

- 手動コンフィギュレーションモードの開始 [2-352](#)
- Virtual Forwarding Instance
 - 「VFI」を参照
- Virtual Private LAN Service
 - 「VPLS」を参照
- VLAN
 - ARP ACL の適用 [2-176](#)
 - config-VLAN サブモード
 - RSPAN の指定 [2-1272](#)
 - 開始 [2-1272](#)
 - 削除 [2-1272](#)
 - 設定 [2-1272](#)
 - DAI のイネーブル化 [2-185](#)
 - DAI のディセーブル化 [2-185](#)
 - ISL VLAN へのマッピング [2-1289](#)
 - ISL VLAN マッピングの削除 [2-1289](#)
 - MST インスタンスにマッピング [2-164](#)
 - VLAN データベース コンフィギュレーション ファイルを消去 [2-136](#)
 - イネーブル化
 - dot1q タギング [2-1284](#)
 - クリア
 - DAI 統計情報 [2-44](#)
 - カウンタ [2-92](#)
 - ハードウェア ロジック [2-41](#)
 - コンフィギュレーションサブモードの開始 [2-1282](#)
 - コンフィギュレーションモードの開始 [2-1276](#)
 - 削除
 - config-VLAN サブモード [2-1272](#)
 - グローバル コンフィギュレーション モード [2-1276](#)
 - 新規データベースの実装 [2-4](#)
 - 設定
 - ARE ホップ [2-1272](#)
 - config-VLAN サブモード [2-1272](#)
 - FDDI リング番号 [2-1272](#)
 - MTU サイズ [2-1272](#)
 - SAID ID [2-1272](#)
 - STP タイプ [2-1272](#)
 - VLAN 名 [2-1272](#)
 - 親 VLAN ID [2-1272](#)
 - 状態 [2-1272](#)
 - トークンリング番号 [2-1272](#)
 - トランスレーショナル ID [2-1272](#)
 - 内部割り当て方式 [2-1288](#)
 - バックアップ CRF モード [2-1272](#)
 - ブリッジング特性 [2-1272](#)
 - メディア タイプ [2-1272](#)
- 設定番号の増分 [2-4](#)
- 追加
 - グローバル コンフィギュレーション モード [2-1276](#)
- ディセーブル化
 - dot1q タギング [2-1284](#)
- データベースの実装 [2-4](#)
- 内部的にシャットダウン [2-1274](#)
- 表示
 - CEF 情報 [2-810](#)
 - CEF ネクストホップ情報 [2-810](#)
 - Cisco IOS VLAN サブインターフェイス情報 [2-1125](#)
 - DAI ステータス [2-788](#)
 - dot1q タギング情報 [2-1116](#)
 - RSPAN VLAN [2-1124](#)
 - インターフェイス VLAN の総数 [2-774](#)
 - 現在の動作情報 [2-1075](#)
 - 設定情報 [2-1112](#)
 - 双方向 [2-1122](#)
 - ソフトウェア キャッシュ カウンタ値 [2-1115](#)
 - 内部 VLAN ステータス [2-1108](#)
 - 内部 VLAN の割り当て情報 [2-1119](#)
 - 必要な論理仮想ポート数 [2-1127](#)
 - フィルタ情報 [2-1117](#)
 - フロー テーブルの内容 [2-1112](#)
 - ポート単位のマッピング [2-1121](#)
 - レイヤ 2 VLAN 情報 [2-1108](#)
 - ロギング プロパティ情報 [2-1112](#)
 - ワークアラウンド VLAN [2-1119](#)

- ローカル トラフィックの再起動 [2-1133](#)
- ローカル トラフィックのシャットダウン [2-1133](#)
- VLAN 1 の最小化
 - コマンド [2-1224](#)
 - 使用上のガイドライン [2-1225](#)
- VLAN アクセス制御リスト
 - 「VACL」を参照
- VLAN アクセスマップ コマンド モード
 - 開始 [2-1280](#)
- VLAN 単位の高速スパンニングツリー
 - 「高速 PVST」を参照
- VLAN データベース
 - 開始 [2-1282](#)
 - リセット [2-651](#)
- VLAN のマッピング、ポート単位の
 - イネーブル化 [2-1229](#)
 - クリア [2-1227](#)
 - 設定 [2-1227](#)
 - ディセーブル化 [2-1229](#)
 - 表示
 - 802.1Q VLAN と ISL VLAN のマッピング [2-1121](#)
 - マッピングのステータス [2-787](#)
- VLAN 変換
 - イネーブル化
 - ポート単位の VLAN のマッピング [2-1229](#)
 - サポート モジュール [2-1227](#)
 - 設定
 - ポート単位のマッピング [2-1227](#)
 - ディセーブル化
 - ポート単位の VLAN のマッピング [2-1229](#)
- VLAN リンクアップ計算
 - スイッチ ポートを加える [2-1198](#)
 - スイッチ ポートを除く [2-1198](#)
- VMR
 - Value Mask Result の略語
- VPLS
 - L2 VFI コンフィギュレーション モードの開始 [2-352](#)
- VPN ID の設定 [2-352](#)
- レイヤ 2 VFI の作成 [2-352](#)
- VRF
 - イネーブル化
 - データ MDT の再利用の記録 [2-400](#)
 - 設定
 - グループのアドレス範囲 [2-398](#)
 - デフォルト グループ [2-399](#)
 - ディセーブル化
 - データ MDT の再利用の記録 [2-400](#)
 - 表示
 - デフォルトではないエントリ [2-948](#)
- VTP
 - グローバル コンフィギュレーション モード
 - IFS ファイルの設定 [2-1291](#)
 - アップデート ID の推奨送信元の設定 [2-1291](#)
 - ドメイン名の設定 [2-1291](#)
 - モードの設定 [2-1291](#)
 - 指定
 - パスワード [2-1291](#)
 - 設定
 - IFS ファイル システム [2-1291](#)
 - アップデート ID の推奨送信元 [2-1291](#)
 - クライアント モード [2-1291](#)
 - サーバ モード [2-1291](#)
 - ドメイン名 [2-1291](#)
 - トランスペアレント モード [2-1291](#)
 - バージョン [2-1291](#)
 - 表示
 - 統計情報 [2-1129](#)
 - ドメイン情報 [2-1129](#)
 - プルーニング
 - イネーブル化 [2-1291](#)
 - ディセーブル化 [2-1291](#)
- VTP ドメイン
 - 削除 [2-544](#)
 - リンク [2-544](#)

-
- ## W
- ### WAN
- イネーブル化
 - 802.1Q 透過性 [2-600](#)
 - ディセーブル化
 - 802.1Q 透過性 [2-600](#)
- ### WCCP
- イネーブル化
 - IP マルチキャスト パケット受信 [2-338](#)
 - パケット リダイレクション [2-340](#)
 - マスク割り当てハードウェア アクセラレーション [2-342](#)
 - ディセーブル化
 - IP マルチキャスト パケット受信 [2-338](#)
 - パケット リダイレクション [2-340](#)
 - マスク割り当てハードウェア アクセラレーション [2-342](#)
 - 表示
 - グローバルな統計情報 [2-877](#)
 - 帯域内パケット数 [2-736](#)
- ### Web Cache Coprocessor Protocol
- 「WCCP」を参照
- ### Wireless LAN Services Module
- 「WLSM」を参照
- ### WLSM
- 指定
 - NBMA から BMA への変換 [2-551](#)
 - ネットワーク ID [2-551](#)
 - 情報の表示 [2-1007](#)
 - 設定
 - モビリティ [2-551](#)
 - ワイヤレス mGRE トンネル [2-551](#)
- ### WRED
- 最大しきい値の指定 [2-1301](#)
- ### write erase コマンド
- 「erase コマンド」を参照 [2-136](#)
- ### WRR
- キュー マッピング
 - CoS および廃棄しきい値間 [2-1297](#)
 - DSCP および廃棄しきい値間 [2-1298](#)
 - 送信キュー サイズ比の設定 [2-1299](#)
 - デフォルト キュー値へのリセット [2-1301](#)
- ### WRR キュー
- 最大しきい値の指定 [2-1301](#)
 - 設定
 - 帯域幅 [2-1294](#)
-
- ## X
- ### XL モード
- サポート モジュール [2-411](#)
 - 定義 [2-411](#)
-
- ## あ
- ### アクセス
- DFC を搭載したモジュール [2-648](#)
 - モジュール固有の CLI [2-665](#)
- ### アクセス制御リスト
- 「ACL」を参照
- ### アクセス マップ
- シーケンスの指定 [2-391](#)
 - 適用 [2-1286](#)
- ### アクセス リスト
- IPX、時間範囲 [2-1241](#)
- ### アグレッシブ UDLD
- 「UDLD、アグレッシブ モード」を参照
- ### 圧縮モード
- オフ [2-450](#)
 - オン [2-450](#)
- ### 宛先アドレス
- MLS QoS
 - 統計データ エクスポートの宛先アドレスの設定 [2-511](#)
 - アドレス解決プロトコル
 - 「ARP」を参照

い

一貫性チェッカー

イネーブル化 [2-439](#)設定 [2-439](#)ディセーブル化 [2-439](#)

表示

情報 [2-955](#)

イネーブル化

ルーティング [2-287](#)

イベント トレーシング

設定

グローバル コンフィギュレーション モード [2-561](#)特権 EXEC モード [2-558](#)

イメージ

イメージの確認 [2-144](#)現在のコピー操作の確認のディセーブル化 [2-99](#)チェックサムの自動確認のイネーブル化 [2-144](#)

インスタンスの番号付け

デフォルトに戻す [2-164](#)マッピング [2-164](#)

インターフェイス

インターフェイス コンフィギュレーション モードの開始 [2-166](#)

スイッチング ポート

Flexlink ペアの表示 [2-777](#)管理ステータスおよび動作ステータスの表示 [2-775](#)ステータスの表示 [2-775, 2-777](#)

設定

インターフェイス速度 [2-1182](#)デュプレックス モード [2-131](#)半二重モード [2-131](#)

表示

errdisable ステート [2-772](#)PVLAN のマッピング [2-771](#)アカウンティング情報 [2-759](#)インターフェイス VLAN の総数 [2-774](#)インターフェイス機能 [2-761](#)エラー カウンタ [2-763](#)管理ステータス [2-775, 2-777](#)合計抑制廃棄数 [2-763](#)ステータス [2-768](#)ステータス サマリー [2-774](#)説明 [2-768](#)動作ステータス [2-775, 2-777](#)トラフィック [2-756](#)トランク カウンタ [2-763](#)トランク情報 [2-782](#)フロー制御情報 [2-769](#)インターフェイス アカウンティング情報、表示 [2-759](#)

インターフェイス カウンタ

情報の表示 [2-694](#)

インターフェイス コンフィギュレーション モード

開始 [2-166](#)概要 [1-6](#)テーブル定義モード [1-6](#)

インターフェイス レンジ マクロ

作成 [2-103](#)インフォーム、イネーブル化 [2-1138](#)

インライン パワー

管理モードの設定 [2-618](#)

表示

ステータス情報 [2-1059](#)モジュールの消費電力 [2-1059](#)

う

ウォッチ リスト

IP アドレスの追加 [2-189](#)イネーブル化 [2-189](#)エントリをクリア [2-45](#)設定 [2-189](#)最大ログイン試行回数 [2-188](#)ディセーブル化 [2-189](#)表示 [2-793](#)

-
- え**
- エージング タイム
 - MAC アドレス テーブル **2-375**
 - エクスポート インターバル
 - MLS QoS
 - 設定 **2-513**
 - エポック
 - CEF テーブルの再構築 **2-46**
 - 情報の表示 **2-805**
 - 増分 **2-46**
 - エラー カウンタ
 - サマリーの表示 **2-1099**
 - エラー検出
 - 設定
 - パケット バッファ メモリ障害時のモジュール アクション **2-142**
-
- お**
- 重み付けラウンドロビン
 - 「WRR」を参照
 - 重み付けランダム早期検出
 - 「WRED」を参照
 - 音声 VLAN
 - 削除
 - スイッチ ポートから **2-1231**
 - スイッチ ポートでの設定 **2-1231**
 - オンデマンド診断
 - 設定 **2-113**
 - テストが失敗した場合のアクション **2-113**
 - 温度
 - 情報の表示 **2-720**
 - オンライン診断
 - イネーブル化
 - CNS イベント バスへの送信 **2-107**
 - CNS 診断イベントの受信 **2-107**
 - syslog メッセージ **2-110**
 - スケジュール **2-114**
 - グローバル コンフィギュレーション モード
 - スケジュールの設定 **2-105**
 - スケジュールをクリア **2-105**
 - テストごとの診断の設定 **2-114**
 - テストごとのテスト スケジュールの解除 **2-114**
 - ブートアップ診断レベルの設定 **2-105**
 - ヘルス モニタリング診断テスト スケジュールの設定 **2-110**
 - ヘルス モニタリング診断テスト スケジュールのディセーブル化 **2-110**
 - ヘルス モニタリング診断テストの設定 **2-110**
 - 削除
 - スケジュール **2-114**
 - 指定
 - ヘルス モニタリング診断テスト **2-110**
 - スケジューリングされたスイッチオーバー
 - イネーブル化 **2-114**
 - ディセーブル化 **2-114**
 - 設定
 - オンデマンド診断 **2-113**
 - 診断レベル **2-105**
 - テストが失敗した場合のアクション **2-113**
 - テスト間隔 **2-114**
 - ヘルス モニタリング診断テスト **2-110**
 - ディセーブル化
 - CNS イベント バスへの送信 **2-107**
 - CNS 診断イベントの受信 **2-107**
 - テストの開始 **2-117, 2-119**
 - デフォルト設定へのリセット **2-105**
 - 表示
 - CNS サブジェクト **2-702**
 - イベント ログ **2-697**
 - 現在のスケジューリング済みタスク **2-697**
 - 健全性チェックの結果 **2-703**
 - サポートされているテストスイート **2-697**
 - 設定されたブートアップ カバレッジ レベル **2-697**
 - テスト ID **2-697**
 - テスト結果 **2-697**

テスト統計情報 [2-697](#)
ブートアップ診断テストを省略 [2-105](#)

か

開始、VLAN コンフィギュレーション サブモード
の [2-1282](#)

カウンタ

NetFlow カウンタをクリア [2-39](#)
インターフェイス カウンタのクリア [2-37](#)
ハードウェアのインターフェイス カウンタのク
リア [2-37](#)
表示
 インターフェイス カウンタ情報 [2-694](#)

拡張 MAC アクセス リスト

定義 [2-372](#)

拡張システム ID の表示

イネーブル化 [2-1154](#)
ディセーブル化 [2-1154](#)

拡張パスワードのセキュリティ

確立 [2-1268](#)

拡張範囲 VLAN

config-VLAN モードの開始 [2-1276](#)

開始

新規 ERSPAN セッション [2-571](#)
新規 RSPAN セッション [2-566](#)
新規 SPAN セッション [2-566](#)

キャプチャ モードのイネーブル化 [2-1203](#)

キャプチャ モードのディセーブル化 [2-1203](#)

削除

ERSPAN セッション [2-571](#)
PVLAN アソシエーション [2-1221](#)
RSPAN セッション [2-566](#)
SPAN セッション [2-566](#)
ダイナミック SVI [2-173](#)

設定

STP [2-1180](#)
アクセス モード時 [2-1196](#)
キャプチャ モードの特性 [2-1205](#)

ダイナミック SVI の作成 [2-173](#)

定義

PVLAN アソシエーション [2-1221](#)

表示

現在の動作情報 [2-1075](#)

フィルタ情報 [2-1117](#)

複数のインターフェイスでコマンドを実行 [2-171](#)

カスタム EtherType

EtherType 値の指定 [2-1207](#)

カプセル化

802.1Q

イネーブル化 [2-134](#)

ディセーブル化 [2-134](#)

ISL

イネーブル化 [2-135](#)

ディセーブル化 [2-135](#)

空のスロットの電源切断 [2-617](#)

環境アラーム

情報の表示 [2-713](#)

環境変数

BOOT、指定 [2-16](#)

完全優先キュー

CoS 値のマッピング [2-621](#)

関連資料 [xxvi](#)

き

ギガビット イーサネット WAN

「GE-WAN」を参照

ギガビット イーサネット インターフェイス

ハードウェア ロジックのクリア [2-40](#)

ギガビット イーサネット インターフェイスのク
リア [2-40](#)

起動

フラッシュから [2-16](#)

機能マネージャ

表示

CBACが設定された ACLおよびポート [2-737,](#)
[2-745](#)

- VLAN 単位の情報 [2-748](#)
 - 一般情報 [2-734](#)
 - インターフェイス単位の情報 [2-738, 2-741](#)
 - サマリー [2-747](#)
 - 帯域内パケット数 [2-736](#)
 - ダイナミック再帰エントリ [2-746](#)
 - キューイング
 - 情報の表示 [2-1067](#)
 - 許諾、オープン ソース ソフトウェアの
 - Regular Expression Library [B-1](#)
 - Softfloat [B-1](#)
-
- く
- クライアント ID [2-1063](#)
 - クラス ポリシー
 - 設定 [2-31](#)
 - デフォルト クラス、設定 [2-31, 2-607](#)
 - クラス マップ
 - MLS QoS
 - イネーブル化 [2-507](#)
 - コンフィギュレーション モード
 - アクセス [2-26](#)
 - 削除
 - プロトコル単位の一致基準 [2-393](#)
 - 情報の表示 [2-693](#)
 - 設定
 - IPv6 パケットの一致基準 [2-393](#)
 - IP パケットの一致基準 [2-393](#)
 - プロトコル単位の一致基準 [2-393](#)
 - グループ キャッシュ エントリ
 - クリア [2-51](#)
 - グローバル コンフィギュレーション モード、概要 [1-6](#)
-
- け
- ケーブル診断
 - TDR
 - すべてのインターフェイスのクリア [2-35](#)
-
- こ
- 高速 PVST
 - イネーブル化 [2-1158](#)
 - ディセーブル化 [2-1158](#)
 - コピー、内部から外部 .1pbits への
 - エントリの削除 [2-479](#)
 - 設定 [2-479](#)
 - コマンド [1-2](#)
 - 複数のインターフェイスを同時に実行 [2-171](#)
 - モード タイプ [1-5](#)
 - コマンド モード
 - アクセス [1-5](#)
 - 概要 [1-5](#)
 - 既存の [1-5](#)
 - コマンドライン インターフェイス
 - 「CLI」を参照
 - 混合モード ポート
 - モードの設定 [2-1209](#)
 - コントロール プレーン ポリシング
 - 「CoPP」を参照
-
- か
- テスト結果の表示 [2-685](#)
 - テストの実行 [2-1239](#)
 - 特定のインターフェイスのクリア [2-35](#)
 - 決定性処理時間の正規表現エンジン
 - イネーブル化 [2-12](#)
 - ディセーブル化 [2-12](#)
 - 健全性チェックの結果、表示 [2-703](#)
 - 現場アップグレード可能 ROMMON
 - アップグレード
 - スイッチ プロセッサ [2-1266](#)
 - ルート プロセッサ [2-1266](#)
 - 現場交換可能ユニット
 - 「FRU」を参照
-
- さ
- サービス モジュール

- セッションのイネーブル化 [2-566](#)
 - セッションのディセーブル化 [2-566](#)
 - 再帰 NDR
 - TCAM 内のショートカットのイネーブル化 [2-449](#)
 - TCAM 内のショートカットのディセーブル化 [2-449](#)
 - 最終メンバー クエリー インターバル
 - IGMP スヌーピング用の設定 [2-238](#)
 - IGMP に対する設定 [2-230](#)
 - MLDv2 スヌーピング用の設定 [2-327](#)
 - 最小のリンク
 - 設定 [2-615](#)
 - 最大 NetFlow テーブル割り当て
 - 設定 [2-462](#)
 - 最大伝送ユニット
 - 「MTU」を参照
 - 最大ルート
 - コンフィギュレーションの表示 [2-941](#)
 - 最長プレフィクス一致機能 [2-926, 2-940](#)
 - 削除、インターフェイスをチャンネルグループから [2-22](#)
 - サブインターフェイス コンフィギュレーション モード、概要 [1-6](#)
 - サンプリング済み NetFlow
 - イネーブル化
 - インターフェイス上 [2-463](#)
 - グローバル [2-545](#)
 - 指定
 - サンプリング方式 [2-545](#)
 - ステータスの表示 [2-996](#)
 - ディセーブル化
 - インターフェイス上 [2-463](#)
 - グローバル [2-545](#)
-
- し
- シェイプド ラウンド ロビン
 - 「SRR」を参照
 - 時間ベース ACL
 - イネーブル化 [2-1241](#)
 - 削除
 - 時間制限 [2-1241](#)
 - 設定
 - 時間範囲 [2-1241](#)
 - システム
 - FIFO オーバーフロー エラー カウントの設定 [2-1234](#)
 - システム イメージ
 - デフォルト ファイル名 [2-16](#)
 - システム ソフトウェア
 - アクティブになってからのアップタイムの表示 [2-1106](#)
 - 起動 [2-16](#)
 - コンフィギュレーション ファイルの名前および送信元の表示 [2-1106](#)
 - バージョン表示 [2-1106](#)
 - システム プロンプト [1-6](#)
 - 実行コンフィギュレーション
 - 現在の動作情報の表示 [2-1075](#)
 - 実サーバ
 - アクティブ接続の制限 [2-394](#)
 - アクティブ接続の変更 [2-394](#)
 - 新規接続
 - SYN 数の定義 [2-641](#)
 - デフォルトの定義 [2-641](#)
 - 自動ネゴシエーション
 - 遅延タイマーの設定 [2-1233](#)
 - シャーシ
 - 表示
 - 現在およびピーク時のトラフィック メータの値 [2-687](#)
 - シャーシ MAC アドレス範囲 [2-687](#)
 - シリアル番号 [2-754](#)
 - スイッチングクロック障害回復モード [2-687](#)
 - 製品番号 [2-754](#)
 - バックプレーンの利用率 [2-687](#)
 - モデル タイプ [2-754](#)
 - シャーシ シリアル番号、表示 [2-752](#)
 - ジャンボ フレーム
 - 最大伝送ユニット サイズの設定 [2-580](#)

- 最大パケット サイズの設定 [2-580](#)
 - デフォルト値 [2-580](#)
 - デフォルト値の復元 [2-580](#)
 - 集約カウント
 - ミス フロー [2-999](#)
 - 集約ポリサー
 - MLS QoS
 - イネーブル化 [2-505](#)
 - 削除 [2-469](#)
 - 現在のクラスからの [2-601](#)
 - 指定
 - 現在のクラスの [2-601](#)
 - 定義 [2-469](#)
 - 統計情報のクリアおよび高レートおよび低レートのポリサー パケットのトークン数 [2-77](#)
 - 受信キュー
 - 「rcv-queues」を参照
 - 受信バック チャンネル
 - 削除 [2-1252](#)
 - 設定 [2-1252](#)
 - 出力
 - 削除
 - DSCP/CoS マップ [2-481](#)
 - DSCP/DSCP マップ [2-483](#)
 - DSCP/EXP マップ [2-482](#)
 - EXP/EXP マップ [2-485](#)
 - インターフェイスからの DSCP 変換マップ [2-475](#)
 - 入力 EXP/DSCP マップ [2-484](#)
 - 定義
 - DSCP/CoS マップ [2-481](#)
 - DSCP/DSCP マップ [2-483](#)
 - DSCP/EXP マップ [2-482](#)
 - DSCP 変換マッピング [2-483](#)
 - EXP/EXP マップ [2-485](#)
 - EXP 変換マップ [2-485](#)
 - 入力 EXP/DSCP マップ [2-484](#)
 - 表示
 - DSCP 変換マッピング [2-981](#)
 - キューイング情報 [2-1067](#)
 - モード情報 [2-955](#)
 - 付加
 - インターフェイスへの DSCP 変換マップ [2-475](#)
 - 出力レプリケーション機能 [2-433](#)
 - 循環キャッシュ ヘッダー バッファ、内容の表示 [2-840](#)
 - 障害のあるサーバによって試行される接続
 - 経過時間の定義 [2-652](#)
 - デフォルトへの変更 [2-652](#)
 - 冗長性
 - Fast Software Upgrade [2-644](#)
 - 自動同期化をオフにする [2-11](#)
 - スイッチ全体のリロード [2-645](#)
 - スーパーバイザ エンジンの同期化 [2-642](#)
 - 表示
 - RF クライアント リスト [2-1069](#)
 - RF ステート [2-1069](#)
 - RF 動作カウンタ [2-1069](#)
 - 情報 [2-1069](#)
 - モードの設定 [2-553](#)
 - ルート プロセッサ
 - BOOTVAR の同期 [2-11](#)
 - BOOTVAR の同期化およびコンフィギュレーション レジスタのデフォルト設定 [2-11](#)
 - コンフィギュレーション レジスタの同期 [2-11](#)
 - スタートアップ コンフィギュレーションの同期化 [2-11](#)
 - 省略、コマンドの
 - コンテキスト ヘルプ [1-1](#)
-
- ## す
- スイッチ コンソール、アクセス [2-648](#)
 - スイッチのリロード [2-645](#)
 - スイッチ ポート
 - 宛先 VLAN の指定 [2-1205](#)
 - イネーブル化
 - ポート単位の VLAN のマッピング [2-1229](#)
 - クリア

- ポート単位の VLAN のマッピング [2-1227](#)
- 削除
 - PVLAN のマッピング [2-1221](#)
 - 音声 VLAN [2-1231](#)
 - 混合モード ポートの PVLAN マッピング [2-1222](#)
- 設定
 - アクセス モード時の VLAN [2-1196](#)
 - 音声 VLAN [2-1231](#)
 - キャプチャ ポート [2-1203](#)
 - トランクの特性 [2-1224](#)
 - ポート単位の VLAN のマッピング [2-1227](#)
 - モード [2-1209](#)
- 定義
 - PVLAN アソシエーション [2-1221](#)
- ディセーブル化
 - ポート単位の VLAN のマッピング [2-1229](#)
- 特性の変更 [2-1194](#)
- パケット転送の禁止 [2-1202](#)
- ポート セキュリティ
 - イネーブル化 [2-1211](#)
 - 違反アクション [2-1219](#)
 - 違反アクションの設定 [2-1219](#)
 - エージング タイプの設定 [2-1213](#)
 - エージング タイムの設定 [2-1213](#)
 - セキュア アドレスの最大数の設定 [2-1217](#)
 - 設定情報の表示 [2-1057](#)
 - ディセーブル化 [2-1211](#)
 - リストからの MAC アドレスの削除 [2-1215](#)
- マッピング
 - 混合モード ポートの PVLAN [2-1222](#)
- スイッチング、NetFlow
 - キャッシュ サイズの設定 [2-214](#)
 - 統計情報のクリア [2-50](#)
- スイッチング インターフェイス
 - Flexlink ペアの表示 [2-777](#)
 - 管理ステータスおよび動作ステータスの表示 [2-775](#)
- スイッチングの特性
 - イネーブル化
 - Flexlink [2-1200](#)
 - キャプチャ機能 [2-1203](#)
 - インターフェイスに戻す場合
 - キャプチャ機能 [2-1194, 2-1198](#)
 - 修正 [2-1194, 2-1196, 2-1198](#)
 - キャプチャ機能 [2-1205](#)
 - ディセーブル化
 - Flexlink [2-1200](#)
 - キャプチャ モード [2-1203](#)
 - ホスト接続用ポート設定の最適化 [2-1194](#)
 - リンクアップ計算から除く [2-1198](#)
 - スケジューリングされたスイッチオーバー
 - イネーブル化 [2-114, 2-115](#)
 - ディセーブル化 [2-114, 2-115](#)
 - スタティック MAC アドレス エントリ
 - クリア [2-64](#)
 - スタブ
 - 非 RPF マルチキャスト高速廃棄のイネーブル化 [2-444](#)
 - スティッキ ARP
 - イネーブル化
 - インターフェイスごと [2-319](#)
 - グローバル [2-317](#)
 - ディセーブル化
 - インターフェイスごと [2-319](#)
 - グローバル [2-317](#)
 - スティッキ MAC
 - イネーブル化 [2-1215](#)
 - 削除 [2-1215](#)
 - ストーム制御
 - 抑制モードのイネーブル化 [2-1192](#)
 - 抑制モードのディセーブル化 [2-1192](#)
 - 抑制レベルの設定 [2-1192](#)
 - スパニングツリー
 - EtherChannel
 - ガードの設定ミス検出 [2-1152](#)
 - UplinkFast
 - イネーブル化 [2-1179](#)
 - ディセーブル化 [2-1179](#)

VLAN

設定 [2-1180](#)デフォルト値に戻す場合 [2-1180](#)

アクティブ ステート

表示 [2-1080](#)

イネーブル化

BackboneFast [2-1147](#)BPDU ガード [2-1150](#)BPDU フィルタリング [2-1148](#)PortFast BPDU ガード [2-1175](#)PortFast BPDU フィルタリング [2-1173](#)PortFast、デフォルト [2-1176](#)インターフェイス上の PortFast [2-1171](#)拡張システム ID の表示 [2-1154](#)すべてのアクセス ポートでの PortFast、デフォルト [2-1176](#)ルート ガード モード [2-1155](#)ループ ガード モード [2-1155](#)ループ ガードをデフォルトとして [2-1157](#)

インターフェイス

PortFast モード、イネーブル化 [2-1171](#)PortFast モード、ディセーブル化 [2-1171](#)

指定

送信ホールド カウント [2-1178](#)

ディセーブル化

BackboneFast [2-1147](#)BPDU ガード [2-1150](#)BPDU フィルタリング [2-1148](#)PortFast BPDU ガード [2-1175](#)PortFast BPDU フィルタリング [2-1173](#)PortFast、デフォルト [2-1176](#)インターフェイス上の PortFast [2-1171](#)拡張システム ID の表示 [2-1154](#)すべてのアクセス ポートでの PortFast、デフォルト [2-1176](#)ルート ガード モード [2-1155](#)ループ ガード モード [2-1155](#)ループ ガードをデフォルトとして [2-1157](#)デフォルトのパス コスト計算方式の設定 [2-1170](#)

パス コスト

設定 [2-1151](#)デフォルト値に戻す場合 [2-1151](#)

表示

BackboneFast ステータス [2-1080](#)UplinkFast ステータス [2-1080](#)VLAN 単位のステータス [2-1080](#)アクティブ ステート [2-1080](#)アクティブなインターフェイスのみ [2-1080](#)インターフェイス情報のサマリー [2-1080](#)ステータス情報 [2-1080](#)デフォルト パス コスト方式 [2-1080](#)ブリッジのステータスおよびコンフィギュレーション [2-1080](#)プロトコル マイグレーションを再開 [2-89](#)

ポート プライオリティ

設定 [2-1177](#)デフォルト値に戻す場合 [2-1177](#)リンク タイプの設定 [2-1156](#)

せ

設定

端末回線の指定 [2-357](#)ライン コンフィギュレーション コレクション モードの開始 [2-357](#)設定、信頼されたポート状態の [2-493, 2-514](#)設定、保存 [1-11](#)

そ

送信キュー

サイズ比の設定 [2-1299](#)

送信バック チャネル

削除 [2-1254](#)設定 [2-1254](#)

送信ホールド カウント

スパニングツリー

指定 [2-1178](#)

送信元専用タイマー

デフォルト設定へのリセット [2-247](#)

マルチキャスト パケットの定期的フラッディングの設定 [2-247](#)

双方向

設定

RP RPF のスキャン インターバル [2-436](#)

表示

DF インターフェイス情報 [2-861](#)

IP マルチキャスト テーブル情報 [2-842, 2-847](#)

IP マルチキャスト ルーティング テーブル情報 [2-847](#)

キャッシュされたランデブー ポイント情報 [2-958](#)

双方向 CDP

管理モードの設定 [2-618](#)

双方向 PIM

「[BIDIR](#)」を参照

双方向 VLAN

表示 [2-1122](#)

ソフトウェア リソース

分割された VLAN の表示 [2-1050](#)

ソフトリンク

イネーブル化 [2-163](#)

ディセーブル化 [2-163](#)

た

対象読者 [xxv](#)

ダイナミック MAC アドレス エントリ

クリア [2-64](#)

ダイナミック SVI

アクセス [2-173](#)

削除 [2-173](#)

作成 [2-173](#)

タグ間のロードバランス

イネーブル化 [2-578](#)

ディセーブル化 [2-578](#)

単位、VLAN 学習 [A-7](#)

単一方向トランシーバ

動作状態の表示 [2-785](#)

表示

タイプ [2-772](#)

単一方向リンク

「[UDLR](#)」を参照

単一方向リンク ルーティング

「[UDLR](#)」を参照

単一文字パターン

特殊文字、テーブル [1-8](#)

単方向イーサネット

「[UDE](#)」を参照

ち

チェックサム

確認

圧縮イメージ [2-144](#)

フラッシュ メモリ ファイル [2-1269](#)

コンピューティング

MD5 シグニチャ [2-1269](#)

て

ディセーブル化、DNS 検索の [2-248](#)

ディレクトリ

作成 [2-402](#)

デフォルト値の設定 [2-21](#)

テーブル

class の構文 [2-601, 2-607](#)

CoS/DSCP マッピング テーブル [2-478](#)

duplex コマンドと speed コマンドの関係 [2-132, 2-1184](#)

ERSPAN 宛先セッション コンフィギュレーション モードの構文 [2-572](#)

ERSPAN 送信元セッション コンフィギュレーション モードの構文 [2-573](#)

fsck ユーティリティのチェック内容およびアクション内容 [2-150](#)

group 構文説明 [2-29](#)

- mac access-list extended サブコマンド **2-373**
- match 構文説明 **2-27, 2-29**
- MFIB 転送エントリとインターフェイス フラグ **2-880**
- MFIB プラットフォーム フラグ **2-884**
- show cable-diagnostics tdr コマンドの出力フィールド **2-686**
- show cdp neighbors detail のフィールドの説明 **2-691**
- show cdp neighbors のフィールドの説明 **2-690**
- show environment status コマンドの出力フィールド **2-718**
- show environment temperature コマンドの出力フィールド **2-721**
- show interfaces accounting コマンド出力フィールド **2-760**
- show interfaces flowcontrol コマンドの出力フィールド **2-770**
- show ip cache flow コマンドの出力フィールド - NetFlow プロトコル別アクティビティ **2-798**
- show ip cache flow コマンドの出力フィールド - 現行フロー **2-799**
- show ip cache flow コマンドの出力フィールド - パケット サイズ分布 **2-797**
- show ip cache flow コマンドの出力フィールド - フロー スイッチング キャッシュ **2-798**
- show ip cache verbose flow の NetFlow Cache 出力のフィールドの説明 **2-801**
- show ip cache verbose flow のプロトコル別アクティビティ出力のフィールドの説明 **2-802**
- show ip cef inconsistency のフィールドの説明 **2-808**
- show ip dhcp snooping コマンド出力 **2-815**
- show ip igmp groups フィールドの説明 **2-822**
- show ip interface のフィールドの説明 **2-834, 2-903**
- show ip mcache のフィールドの説明 **2-836**
- show ip mds interface のフィールドの説明 **2-838**
- show ip mpacket のフィールドの説明 **2-841**
- show ip mroute のフィールドの説明 **2-830, 2-844**
- show ip msdp count のフィールドの説明 **2-850**
- show ip msdp peer のフィールドの説明 **2-851**
- show ip msdp sa-cache のフィールドの説明 **2-854**
- show ip msdp summary のフィールドの説明 **2-855**
- show ip pim bsr のフィールドの説明 **2-859**
- show ip pim mdt bgp のフィールドの説明 **2-862**
- show ip pim mdt history のフィールドの説明 **2-863**
- show ip pim mdt receive のフィールドの説明 **2-864**
- show ip pim mdt send のフィールドの説明 **2-866**
- show ip pim neighbor のフィールドの説明 **2-867**
- show ip pim rp-hash のフィールドの説明 **2-870**
- show ip pim rp mapping のフィールドの説明 **2-872**
- show ipv6 mfib active のフィールドの説明 **2-882**
- show ipv6 mfib count のフィールドの説明 **2-883**
- show ipv6 mfib verbose のフィールドの説明 **2-884**
- show ipv6 mfib のフィールドの説明 **2-881**
- show ip wccp web-cache detail コマンドの出力フィールド **2-878**
- show lacp コマンドの出力フィールド **2-892**
- show memory dead のフィールドの説明 **2-907**
- show mls cef summary コマンドの出力フィールド **2-946**
- show mls cef コマンドの出力フィールド **2-913, 2-928**
- show mpls l2transport vc コマンドのフィールドの説明 **2-1018**
- show policy-map control-plane のフィールドの説明 **2-1054**
- show spanning-tree vlan コマンドの出力フィールド **2-1084**
- show spanning-tree コマンドの出力フィールド **2-1081**
- show tcam counts コマンドの出力フィールド **2-1096**
- show version のフィールドの説明 **2-1107**
- show vlan private-vlan コマンドの出力フィールド **2-1123**
- show vlans コマンドの出力フィールド **2-1126**
- show vlan コマンドの出力フィールド **2-1111**
- show vtp コマンドの出力フィールド **2-1130**
- speed コマンドのオプション **2-1182**
- URL の共通キーワード エイリアス **2-99**
- サポートされている duplex コマンド オプション **2-131**
- サポートされている speed コマンド オプション **2-1183**

時間ベース サンプリングのインターバル **2-545**

帯域幅のデフォルト値 **2-1294**

デフォルトの DSCP/CoS マッピング テーブル **2-481**

デフォルトの DSCP/EXP マッピング テーブル **2-482**

デフォルトの EXP/DSCP マッピング テーブル **2-484**

デフォルトの EXP/EXP 変換マッピング テーブル **2-485**

デフォルトの IP precedence/DSCP マップ **2-487**

デフォルトの MTU 値 **2-580**

特殊文字

- 位置指定で使用 **1-10**
- 繰り返し指定、テーブル **1-9**

特別なファイル システムの URL プレフィクス エイリアス **2-100**

特別の意味を持つ文字 **1-8**

ネットワーク ファイル システムの URL プレフィクス エイリアス **2-100**

有効なインターフェイス タイプ **2-166**

有効なクラスタ番号 **2-152**

ローカルで書き込み可能なストレージ ファイル システムの URL プレフィクス エイリアス **2-100**

デジタル オプティカル モニタリング

「DOM」を参照

デッド プロセスの統計情報、表示 **2-906**

デバウンス タイマー

- イネーブル化 **2-359**
- 設定 **2-359**
- ディセーブル化 **2-359**
- デバウンス タイマー設定の表示 **2-766**

デュアルモード アップリンク

- コネクタ タイプの選択 **2-401**

デュプレックス モード

- 設定 **2-131**

デリミタ

- MLS QoS に対する設定 **2-510**

電源冗長モード

- 設定 **2-620**

電源装置

電源冗長モードの設定 **2-620**

表示

シリアル番号 **2-753**

製品番号 **2-753**

タイプ **2-753**

転送ブロードキャスト

イネーブル化 **2-429**

情報の表示 **2-914**

ディセーブル化 **2-429**

電力状況

表示 **2-1059**

と

同期化、スーパーバイザ エンジンの **2-642**

統計情報の検索

間隔の設定 **2-661**

統計データのエクスポート

「MLS QoS 統計データのエクスポート」を参照

特殊文字

位置指定、テーブル **1-10**

特権 EXEC モード、概要 **1-6**

トラッキング

インターフェイスの設定 **2-1247**

設定

指定ルータ **2-1189**

トラッキング コンフィギュレーション モードの開始 **2-1247**

トラッキングの解除 **2-1247**

トラップ、イネーブル化 **2-1138**

トラブルシューティング

情報の表示 **2-1099**

トランクの特性

VLAN の削除 **2-1224**

VLAN の追加 **2-1224**

情報の表示 **2-782**

設定 **2-1224**

デフォルトへのリセット **2-1224**

トランシーバ

イネーブル化

- トラップ [2-1140](#)
- モニタリング [2-1249](#)

ディセーブル化

- トラップ [2-1140](#)
- モニタリング [2-1249](#)

表示

- しきい値違反 [2-779](#)
- 動作情報 [2-779](#)

な

内部 CoS から外部 CoS への変換

- 定義 [2-479](#)
- 表示 [2-986](#)
- マッピング [2-986](#)

内部 VLAN

- ステータスの表示 [2-1108](#)

内部 VLAN の割り当て

- 設定 [2-1288](#)
- デフォルト設定 [2-1288](#)
- 表示
- 割り当て情報 [2-1119](#)

に

二重タグ付き Q-in-Q

「QinQ」を参照

入力

- IP precedence/DSCP マップの削除 [2-487](#)
- IP precedence/DSCP マップの定義 [2-487](#)

削除

- CoS/DSCP マッピング [2-478](#)
- インターフェイスからの CoS 変換マップ [2-474](#)
- インターフェイスからの EXP 変換マップ [2-476](#)

定義

- CoS/DSCP マッピング [2-478](#)

表示

- キューイング情報 [2-1067](#)

付加

- インターフェイスへの CoS 変換マップ [2-474](#)
- インターフェイスへの EXP 変換マップ [2-476](#)

認証

- ユーザ名の設定 [2-1268](#)

認証プロキシ

- ウォッチ リスト
- IP アドレスの追加 [2-189](#)
- イネーブル化 [2-189](#)
- エントリをクリア [2-45](#)
- 最大ログイン試行回数の設定 [2-188](#)
- 設定 [2-189](#)
- ディセーブル化 [2-189](#)
- 表示 [2-793](#)

認定情報レート

「CIR」を参照

ね

ネクストホップ

- CEF VLAN 情報の表示 [2-810](#)

ネットプロセッサ

- 表示
- カウンタ情報 [2-1036](#)

の

- ノードル NSF、設定 [2-658](#)

は

ハードウェア

- 表示
- FIB TCAM 例外ステータス [2-725](#)
- プログラミングされた値の確認 [2-1064](#)
- ハードウェア ACL カウンタ

- ハードウェアによりスイッチングされたパケット情報の表示 [2-1097](#)
 - ハードウェア スwitchング
 - イネーブル化
 - 一貫性チェッカー [2-439](#)
 - グローバル [2-547](#)
 - チェックサムのエラー チェック [2-549](#)
 - 入力レプリケーション モード [2-442](#)
 - ユニキャスト トラフィック [2-548](#)
 - レイヤ 3 のエラー チェック [2-549](#)
 - 設定
 - SP から RP へのフロー統計情報メッセージ [2-441](#)
 - 一貫性チェッカー [2-439](#)
 - ディセーブル化
 - 一貫性チェッカー [2-439](#)
 - グローバル [2-547](#)
 - チェックサムのエラー チェック [2-549](#)
 - 長さの一貫性チェック [2-549](#)
 - 入力レプリケーション モード [2-442](#)
 - ユニキャスト トラフィック [2-548](#)
 - レイヤ 3 のエラー チェック [2-549](#)
 - 表示
 - (* ,G/m) エントリに基づく情報 [2-929](#)
 - (* ,G) ショートカット [2-929](#)
 - Bidir (* ,G/m) ショートカットに基づく情報 [2-929](#)
 - Bidir 情報 [2-929](#)
 - CEF テーブル情報 [2-809](#)
 - IP サブネット プレフィクスに基づく情報 [2-929](#)
 - RPF VLAN ID に基づく情報 [2-929](#)
 - (S,G) ショートカットに基づく情報 [2-929](#)
 - VRF CEF テーブル情報 [2-948](#)
 - 一貫性チェッカー情報 [2-955](#)
 - グループ アドレスに基づく情報 [2-929](#)
 - コンパクト フォーマットの CEF テーブル情報 [2-929](#)
 - 送信元 IP に基づく情報 [2-929](#)
 - マルチキャスト レプリケーション機能 [2-955](#)
- ハードウェアのインターフェイス カウンタ
 - クリア [2-37](#)
 - ハードウェア リソース
 - 情報の表示 [2-1030](#)
 - ハードウェア レイヤ 3 スwitchング
 - HSRP [2-1191](#)
 - イネーブル化
 - トンネル フラグメンテーション [2-412](#)
 - 設定
 - プロトコル単位のルート制限 [2-410](#)
 - ディセーブル化
 - トンネル フラグメンテーション [2-412](#)
 - 表示
 - IP エントリ情報 [2-926](#)
 - RPF 譲歩 [2-944](#)
 - TCAM エントリ インデックス情報 [2-926, 2-940](#)
 - エントリ情報 [2-909](#)
 - 最大ルート システム コンフィギュレーション [2-941](#)
 - 統計情報 [2-945](#)
 - ハードウェア テーブル エントリ情報 [2-922](#)
 - ハードウェア レイヤ 3 スwitchング テーブル内のプレフィクス数 [2-946](#)
 - ハードウェア ロードシェアリング情報 [2-919](#)
 - パケット情報 [2-946](#)
 - プライオリティ情報 [2-920](#)
 - 隣接テーブル情報 [2-676](#)
 - 隣接ノード情報 [2-914](#)
 - 例外ステータス [2-920](#)
 - ハードウェア ロジック
 - VLAN でクリア [2-41](#)
 - バイト数、表示 [2-763](#)
 - パイブ記号
 - 選択パターンの指定 [1-10](#)
 - パケット エラー情報、表示 [2-997](#)
 - パケット数、表示 [2-763](#)
 - パケット バッファ エラー
 - エラー検出のイネーブル化 [2-138](#)
 - ステータスの表示 [2-726, 2-727](#)

- パス コスト
 STP のデフォルトのパス コスト計算方式の設定 **2-1170**
- パスワード
 拡張パスワードセキュリティの確立 **2-1268**
 ユーザ名の設定 **2-1268**
- パワー サイクリング、モジュールの **2-161**
- 半二重モード
 設定 **2-131**
-
- ひ**
- 非 RPF トラフィック廃棄
 イネーブル化 **2-444**
- 非 XL モード
 定義
 サポート モジュール **2-411**
- 非アクティブ ステート
 非アクティブ ステートの理由の表示 **2-772**
- 表現
 選択パターンの指定 **1-10**
 単一文字パターン **1-8**
 パターンの繰り返し **1-11**
 複数の表現の繰り返しに一致 **1-9**
 複数文字パターン **1-9**
-
- ふ**
- ファイル
 イメージの確認 **2-144**
 コピー **2-99**
 自動イメージ確認のディセーブル化 **2-99**
 チェックサムの自動確認のイネーブル化 **2-144**
- ファイル システム
 消去 **2-136**
- ファイルのコピー **2-99**
 イメージの確認 **2-144**
 チェックサムの自動確認のイネーブル化 **2-144**
- ファイルの復元 **2-1262**
- ファン トレイ
 バージョンの設定 **2-157**
 部品番号の表示 **2-717**
- ブート コンフィギュレーション ファイル
 装置およびファイル名の指定 **2-14**
 デフォルト位置へのリセット **2-14**
- ブートフラッシュ
 ファイル システム、情報の表示 **2-680**
- 負荷統計インターバル **2-361**
- 複数の NetFlow エクスポートの宛先、設定 **2-217**
- 複数パスのユニキャスト RPF チェック
 RPF モード
 interface-group **2-427**
 pass **2-427**
 punt **2-427**
- インターフェイス グループ
 削除 **2-426**
 作成 **2-426**
 定義 **2-426**
- 削除
 インターフェイス グループ **2-426**
- 作成
 インターフェイス グループ **2-426**
- 設定
 モード **2-427**
- 複数文字パターン **1-9**
- 不明なコンテキスト エラー発生時の許可トラップ
 イネーブル化 **2-1145**
 ディセーブル化 **2-1145**
- 不明なユニキャスト トラフィック、禁止 **2-1202**
- 不明なユニキャスト フラッドブロッキング
 「UUFb」を参照
- フラッシュ ファイル システム
 fsck ユーティリティのイネーブル化 **2-150**
 新規ディレクトリの作成 **2-402**
 損傷のチェック **2-150**
 チェックおよび修復 **2-150**
 チェックサムの確認 **2-1269**
 ディレクトリの復元 **2-1262**

- デフォルト値の設定 [2-21](#)
- ファイルの永続的な削除 [2-1185](#)
- ファイルの復元 [2-1262](#)
- フォーマット [2-147](#)
- フラッシュ メモリ
 - 自動的に起動 [2-16](#)
 - フォーマット [2-147](#)
- プラットフォーム
 - クリア
 - 割り込みスロットリング カウンタ [2-82](#)
 - 表示
 - CPU EEPROM 情報 [2-1026](#)
 - IP マルチキャスト関連情報 [2-1026](#)
 - MSFC 情報 [2-1026](#)
 - 障害データ [2-1026](#)
 - ネット割り込み情報 [2-1026](#)
 - ハードウェア リソース [2-1030](#)
 - バッファ割り当て情報 [2-1026](#)
 - プロセッサ TLB レジスタ情報 [2-1026](#)
 - 割り込みスロットリング情報 [2-1026](#)
- ブリッジド トラフィック
 - マイクロフロー ポリシング [2-471](#)
- ブリッジド トラフィックのマイクロフロー ポリシング
 - イネーブル化 [2-471](#)
 - 削除 [2-471](#)
- ブリッジド フロー
 - イネーブル化
 - NDE にグローバルに [2-226](#)
 - 着信 NDE [2-225](#)
 - ディセーブル化
 - NDE にグローバルに [2-226](#)
 - 着信 NDE [2-225](#)
- ブリッジ プロトコル データ ユニット
 - 「BPDU」を参照
- フレーム リレー
 - 指定
 - 平均負荷計算のインターバル [2-361](#)
 - トラフィックの表示 [2-756](#)
- フレーム リレー MIB 拡張
 - 指定
 - 平均負荷計算のインターバル [2-361](#)
 - プレフィクス単位のアカウンティング
 - イネーブル化 [2-420](#)
 - ディセーブル化 [2-420](#)
 - フロー制御
 - receive モードの設定 [2-145](#)
 - send モードの設定 [2-145](#)
 - 設定情報の表示 [2-769](#)
 - ポートの注意事項 [2-146](#)
 - フロー フラグメント
 - 設定の許可 [2-175](#)
 - フロー マスク
 - 指定 [2-417](#)
 - 復元 [2-417](#)
 - プロキシ レポート
 - イネーブル化
 - デフォルトでオン [2-232, 2-325](#)
 - ディセーブル化 [2-232, 2-325](#)
 - プロセッサ間通信
 - 「IPC」を参照
 - プロトコル独立マルチキャスト
 - 「PIM」を参照
 - プロトコル トンネリング
 - インターフェイスのイネーブル化 [2-344](#)
 - インターフェイスのディセーブル化 [2-344](#)
 - 最大処理プロトコル パケット数の指定 [2-350](#)
 - 設定
 - CoS 値 [2-346](#)
 - インターフェイス上での廃棄しきい値 [2-347](#)
 - グローバルな廃棄しきい値 [2-349](#)
 - プロトコルの表示 [2-887](#)
 - プロトコル トンネリング リンク
 - PVST+ および 802.1d BPDU の変換 [2-19](#)
 - プロンプト
 - システム [1-6](#)

-
- へ
- ページング プロンプト
「--More-- プロンプト」を参照
- ヘルス モニタリング診断テスト
設定 [2-110](#)
- ヘルパー アドレス、IP [2-834](#)
- 変更、信頼できないポート状態への [2-493, 2-514](#)
-
- ほ
- ポイントツーポイント リンク タイプ
設定 [2-1156](#)
- ボーダー ゲートウェイ プロトコル
「BGP」を参照
- ポート アクセス マップ
削除 [2-609](#)
作成 [2-609](#)
- ポート許可リスト
宛先リストの表示 [2-1012](#)
- ポートクロッキング モード
アクティブ モード [2-93](#)
イネーブル化 [2-93](#)
自動モード [2-93](#)
パッシブ モード [2-93](#)
- ポート信頼の無視
イネーブル化 [2-491](#)
ディセーブル化 [2-491](#)
- ポート セキュリティ
イネーブル化 [2-1211](#)
違反アクション [2-1219](#)
削除
リストの MAC アドレス [2-1215](#)
セキュアまたは特定のアドレスの削除 [2-87](#)
設定 [2-140](#)
違反アクション [2-1219](#)
エージング タイプ [2-1213](#)
エージング タイム [2-1213](#)
セキュア アドレスの最大数 [2-1217](#)
- 設定情報の表示 [2-1057](#)
ディセーブル化 [2-1211](#)
- ポート速度
設定 [2-1182](#)
デフォルト [2-1182](#)
- ポート チャンネル
アクセス [2-169](#)
作成 [2-169](#)
情報のクリア [2-81](#)
設定
MPLS パケットの負荷分散方式 [2-613](#)
最小のリンク [2-615](#)
- 表示
インターフェイス機能 [2-761](#)
カウンタ情報 [2-763](#)
チャンネル グループ情報 [2-1024](#)
- 負荷分散方式
デフォルトへのリセット [2-616](#)
特定のモジュールの設定 [2-611](#)
バンドルされたポートの設定 [2-611](#)
バンドルされたポートのデフォルトへのリセット [2-611](#)
モジュール単位の設定 [2-616](#)
- ポート範囲
実行 [2-171](#)
- ホスト接続
ポート設定の最適化 [2-1194](#)
- 保存、設定変更の [1-11](#)
- ホットスタンバイ ルータ プロトコル
「HSRP」を参照
- ポリサー
現在のクラスからの集約ポリサーの削除 [2-601](#)
削除
マイクロフロー ポリサー [2-601](#)
指定
現在のクラスを集約ポリサー [2-601](#)
「集約ポリサー」を参照
定義
フロー マスク タイプ [2-601](#)

- マイクロフロー ポリサー **2-601**
 - マイクロフロー
 - 削除 **2-601**
 - 定義 **2-601**
 - ポリシー ベース ルーティング
 - 「PBR」を参照
 - ポリシー マップ
 - 一致するトラフィックへの DSCP 値のマーキング **2-668**
 - 一致するトラフィックへの IP precedence 値のマーキング **2-670**
 - インターフェイス単位の情報の表示 **2-1055**
 - 集約ポリサーの定義 **2-469**
 - 情報の表示 **2-1051**
 - マーキング設定の消去 **2-668**
 - 出力 EXP/EXP マップ **2-485**
 - 入力 EXP/DSCP マップ **2-484**
 - 入力 IP precedence/DSCP マップ **2-487**
 - ポリシング済み DSCP 値とマーキング済み DSCP 値のマップ **2-489**
 - 設定
 - DSCP 変換マップ **2-483**
 - EXP 変換マップ **2-485**
 - QoS クラス マップ **2-26**
 - QoS ポリシー マップ **2-606**
 - 出力 DSCP/CoS マップ **2-481**
 - 出力 DSCP/DSCP マップ **2-483**
 - 出力 DSCP/EXP マップ **2-482**
 - 出力 EXP/EXP マップ **2-485**
 - 入力 EXP/DSCP マップ **2-484**
 - 入力 IP precedence/DSCP マップ **2-487**
 - ポリシング済み DSCP 値とマーキング済み DSCP 値のマップ **2-489**
 - 定義
 - CoS/CoS マップ **2-479**
 - 表示
 - クラス マップ情報 **2-693**
 - 情報 **2-771**
 - ポリシーマップインターフェイス情報 **2-1055**
 - ポリシー マップ情報 **2-1051**
 - マニュアル
 - 構成 **xxv**
 - マニュアルの構成 **xxvi**
 - マルチキャスト SSO
 - コンバージェンス タイマーの設定 **2-443**
 - 設定
 - リーク インターバル **2-443**
 - リーク パーセンテージ **2-443**
 - 表示
 - 情報 **2-960**
 - 統計情報 **2-960**
 - マルチキャスト スタティック ルート
 - 「mroute」を参照
 - マルチキャスト転送情報ベース
-
- ま**
- マイクロフロー ポリサー
 - 定義
 - フロー マスク タイプ **2-601**
 - マイクロフロー ポリシング統計情報、表示 **2-971**
 - マクロ
 - インターフェイス レンジ マクロの作成 **2-103**
 - マッピング
 - 802.1Q VLAN と ISL VLAN **2-1289**
 - VLAN アクセスマップ コマンド モードの開始 **2-1280**
 - VLAN アクセス マップの削除 **2-1280**
 - VLAN アクセス マップの作成 **2-1280**
 - アクセス
 - QoS ポリシー マップ コンフィギュレーション モード **2-606**
 - 削除
 - CoS/DSCP マッピング **2-478**
 - QoS クラス マップ **2-26**
 - QoS ポリシー マップ **2-606**
 - 出力 DSCP/CoS マップ **2-481**
 - 出力 DSCP/DSCP マップ **2-483**
 - 出力 DSCP/EXP マップ **2-482**

「MFIB」を参照
 マルチキャスト配信スイッチング
 「MDS」を参照
 マルチキャスト配信ツリー
 「MDT」を参照
 マルチキャスト ルータ
 スヌーピング情報の表示 **2-827**
 ルーティング テーブルの表示 **2-842, 2-847**
 マルチプロトコル ラベル スwitching
 「MPLS」を参照
 マルチポイント総称ルーティングカプセル化
 「mGRE」を参照
 マルチレイヤ スwitching
 「MLS」を参照

め

明示的なトラッキング
 IGMP スヌーピング
 データベース サイズの制限 **2-240**
 MLDv2 スヌーピング
 データベース サイズの制限 **2-328**
 MLDv2 スヌーピングのイネーブル化 **2-325**
 MLDv2 スヌーピングのディセーブル化 **2-325**
 情報の表示 **2-1001**
 表示
 データベース **2-885**
 明示的なホスト トラッキング
 イネーブル化 **2-232**
 ディセーブル化 **2-232**
 メディア アクセス制御
 「MAC アドレス テーブル」を参照
 メディア依存型インターフェイス、クロスオーバー検出を
 備えた
 「MDIX」を参照

も

モード

「コマンド モード」を参照
 モジュール
 NAM のシャットダウン **2-162**
 SSL のシャットダウン **2-162**
 イネーブル化
 オーバーサブスクリプション モード **2-159**
 指定
 ブート オプション **2-155**
 ディセーブル化
 オーバーサブスクリプション モード **2-159**
 電源切断 **2-617**
 電源投入 **2-617**
 パワー サイクリング **2-161**
 表示
 ステータス情報 **2-1009**
 バージョン情報 **2-1009**
 プロビジョニング情報 **2-1009**

ゆ

ユーザ EXEC モード、概要 **1-6**
 ユーザ名
 イネーブル レベルの設定 **2-1268**
 設定 **2-1268**
 パスワードの設定 **2-1268**
 ユニキャスト RPF
 「uRPF」を参照
 ユニキャスト エントリ
 fast エージング タイム
 設定 **2-407**
 デフォルトに戻す **2-407**
 long エージング タイム
 設定 **2-408**
 デフォルトに戻す **2-408**
 normal エージング タイム
 設定 **2-409**
 デフォルトに戻す **2-409**

り

リポート

 バインディングの復元 [2-199](#)

リモート アクセス

 スーパーバイザ エンジン [2-9](#)

リモート コマンド

 モジュールに対する直接実行 [2-647](#)

 ルート プロセッサに対する直接実行 [2-647](#)

リモート スイッチ コマンドの実行 [2-647](#)

リモート プロシージャ コール

 「RPC」を参照

リモート ログイン [2-648](#)

略語、リスト [A-1](#)

リンクアップ条件のシミュレーション [2-163](#)

リンク タイプ

 設定 [2-1156](#)

リンク デバウンス タイマー

 イネーブル化 [2-359](#)

 設定 [2-359](#)

 ディセーブル化 [2-359](#)

 デバウンス タイマー設定の表示 [2-766](#)

隣接

表示

 テーブル情報 [2-676](#)

 ノード情報 [2-914](#)

る

ルーティング プロトコル パケット

ポリシング

 制御 [2-495](#)

ルーティング プロトコル パケット ポリシング [2-495](#)

ルーテッド MAC [A-8](#)

ルート ガード

 イネーブル化 [2-1155](#)

 ディセーブル化 [2-1155](#)

表示

 ルート不一致ステート [2-1080](#)

ループ ガード

 イネーブル化 [2-1155](#)

 ディセーブル化 [2-1155](#)

れ

冷却

 情報の表示 [2-716](#)

レイヤ 2

 インターフェイス タイプ

 設定 [2-1209](#)

 リセット [2-1209](#)

 マルチキャスト ルータ ポートとしてポートを設定 [2-241](#)

レイヤ 2 分類、IP パケットの

 イネーブル化 [2-390](#)

 設定 [2-388](#)

 ディセーブル化 [2-390](#)

レイヤ 3

 マネージャ

 情報の表示 [2-889](#)

レート制限

 設定 [2-423](#)

 レート制限のイネーブル化 [2-423](#)

 レート制限のディセーブル化 [2-423](#)

レート リミッタ

 ACL ブリッジド レート リミッタのイネーブル化 [2-527](#)

 ACL ブリッジド レート リミッタの設定 [2-527](#)

 ACL ブリッジド レート リミッタのディセーブル化 [2-527](#)

 CEF レート リミッタの設定 [2-529](#)

MLS

 レイヤ 2 ポート セキュリティ情報 [2-993](#)

MLS ユニキャスト

 情報の表示 [2-993](#)

 VACL ログ ケースのイネーブル化 [2-535](#)

 VACL ログ ケースの設定 [2-535](#)

 VACL ログ ケースのディセーブル化 [2-535](#)

 イネーブル化

- PDU レート リミッタ [2-520](#)
- ポートセキュリティ レート リミッタ [2-520](#)
- ユニキャスト パケットのレイヤ 3 セキュリティ レート リミッタ [2-534](#)
- レイヤ 2 プロトコル トンネリング レート リミッタ [2-520](#)

設定

- IPv4 マルチキャスト レート リミッタ [2-522](#)
- IPv6 マルチキャスト レート リミッタ [2-524](#)
- PDU レート リミッタ [2-520](#)
- ポートセキュリティ レート リミッタ [2-520](#)
- ユニキャスト パケットのレイヤ 3 セキュリティ レート リミッタ [2-534](#)
- レイヤ 2 プロトコル トンネリング レート リミッタ [2-520](#)

ディセーブル化

- CEF レート リミッタ [2-529](#)
- IPv4 マルチキャスト レート リミッタ [2-522](#)
- IPv6 マルチキャスト レート リミッタ [2-524](#)
- PDU レート リミッタ [2-520](#)
- ポートセキュリティ レート リミッタ [2-520](#)
- ユニキャスト パケットのレイヤ 3 セキュリティ レート リミッタ [2-534](#)
- レイヤ 2 プロトコル トンネリング レート リミッタ [2-520](#)

マルチキャスト

- 情報の表示 [2-993](#)

ユニキャストおよびマルチキャスト パケットに対するイネーブル化 [2-519](#)

ユニキャストおよびマルチキャスト パケットに対するディセーブル化 [2-519](#)

ユニキャスト パケットに対するイネーブル化 [2-531](#)

ユニキャスト パケットに対するディセーブル化 [2-531](#)

ユニキャスト パケットへの設定 [2-519, 2-531](#)

レプリケーション モード

イネーブル化 [2-442](#)

ディセーブル化 [2-442](#)

ろ

ロードバランス

選択

Catalyst 6500 シリーズ スイッチのロードバランス アルゴリズム [2-421](#)

Cisco IOS のロードバランス アルゴリズム [2-421](#)

ロードバランス アルゴリズム

選択 [2-192](#)

ロギング

IP ARP パケットの制御 [2-186](#)

ログイン バナー

「MOTD」を参照

論理仮想ポート

必要な数の表示 [2-1127](#)

わ

ワークアラウンド VLAN [2-1119](#)

ワイヤレス ネットワーク

mGRE トンネルの設定 [2-551](#)

情報の表示 [2-1007](#)

割り当て、チャンネル グループへのインターフェイスの [2-22](#)

割り込みスロットリング

クリア

カウンタ [2-82](#)

表示

情報 [2-1026](#)