Catalyst 3750 スイッチ コマンド リファレンス

Catalyst 3750 Switch Command Reference

Cisco IOS Release 12.2(55)SE
2010 年 8 月

Text Part Number: OL-8552-09-J

【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を一切負わないものとします。

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S.and other countries.A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks.Third party trademarks mentioned 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.(1005R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Catalyst 3750 スイッチ コマンド リファレンス
© 2004–2010 Cisco Systems, Inc.
All rights reserved.

Copyright © 2004–2011, シスコシステムズ合同会社 .
All rights reserved.

CONTENTS

はじめに xxi

対象読者 xxi

目的 xxi

表記法 xxii

関連資料 xxiii

マニュアルの入手方法およびテクニカル サポート xxiv

CHAPTER 1

Command-Line Interface の使用 1-1

スイッチへのアクセス 1-1

CLI コマンド モード 1-2

ユーザ EXEC モード 1-3

特権 EXEC モード 1-3

グローバル コンフィギュレーション モード 1-4

インターフェイス コンフィギュレーション モード 1-4

VLAN コンフィギュレーション モード 1-5

ライン コンフィギュレーション モード 1-5

CHAPTER 2

Catalyst 3750 スイッチ Cisco IOS コマンド 2-1

aaa accounting dot1x 2-1

aaa authentication dot1x 2-3

aaa authorization network 2-5

action 2-6

archive copy-sw 2-8

archive download-sw 2-11

archive tar 2-15

archive upload-sw 2-18

arp access-list 2-20

authentication command bounce-port ignore 2-22

authentication command disable-port ignore 2-23

authentication control-direction 2-24

authentication event 2-26

authentication fallback 2-30

authentication host-mode 2-32
authentication mac-move permit 2-34
authentication open 2-36
authentication order 2-38
authentication periodic 2-40
authentication port-control 2-42
authentication priority 2-44
authentication timer 2-46
authentication violation 2-48
auto qos classify 2-50
auto qos trust 2-53
auto qos voip 2-56
boot auto-copy-sw 2-62
boot auto-download-sw 2-63
boot buffersize 2-65
boot config-file 2-66
boot enable-break 2-67
boot helper 2-68
boot helper-config-file 2-69
boot manual 2-70
boot private-config-file 2-71
boot system 2-72
cdp forward 2-74
channel-group 2-75
channel-protocol 2-79
cisp enable 2-80
class 2-81
class-map 2-84
clear dot1x 2-86
clear eap sessions 2-87
clear errdisable interface 2-88
clear arp inspection log 2-89
clear ip arp inspection statistics 2-90
clear ip dhcp snooping 2-91
clear ipc 2-93

clear ipv6 dhcp conflict 2-94
clear l2protocol-tunnel counters 2-95
clear lacp 2-96
clear mac address-table 2-97
clear mac address-table move update 2-99
clear nmsp statistics 2-100
clear pagp 2-101
clear port-security 2-102
clear spanning-tree counters 2-104
clear spanning-tree detected-protocols 2-105
clear vmps statistics 2-106
clear vtp counters 2-107
cluster commander-address 2-108
cluster discovery hop-count 2-110
cluster enable 2-111
cluster holdtime 2-112
cluster member 2-113
cluster outside-interface 2-115
cluster run 2-116
cluster standby-group 2-117
cluster timer 2-119
define interface-range 2-120
delete 2-122
deny（ARP アクセスリスト コンフィギュレーション） 2-124
deny（IPv6 アクセスリスト コンフィギュレーション） 2-126
deny（MAC アクセスリスト コンフィギュレーション） 2-132
diagnostic monitor 2-135
diagnostic schedule 2-138
diagnostic start 2-140
dot1x 2-142
dot1x auth-fail max-attempts 2-144
dot1x auth-fail vlan 2-146
dot1x control-direction 2-148
dot1x credentials（グローバル コンフィギュレーション） 2-150
dot1x critical（グローバル コンフィギュレーション） 2-151

dot1x critical（インターフェイス コンフィギュレーション） 2-153
dot1x default 2-155
dot1x fallback 2-156
dot1x guest-vlan 2-157
dot1x host-mode 2-160
dot1x initialize 2-162
dot1x mac-auth-bypass 2-163
dot1x max-reauth-req 2-165
dot1x max-req 2-167
dot1x multiple-hosts 2-168
dot1x pae 2-169
dot1x port-control 2-170
dot1x re-authenticate 2-172
dot1x re-authentication 2-173
dot1x reauthentication 2-174
dot1x supplicant force-multicast 2-175
dot1x test eapol-capable 2-176
dot1x test timeout 2-177
dot1x timeout 2-178
dot1x violation-mode 2-181
duplex 2-182
epm access-control open 2-184
errdisable detect cause 2-185
errdisable detect cause small-frame 2-188
errdisable recovery cause small-frame 2-190
errdisable recovery 2-191
exception crashinfo 2-194
fallback profile 2-195
flowcontrol 2-197
interface port-channel 2-199
interface range 2-201
interface vlan 2-203
ip access-group 2-205
ip address 2-208
ip admission 2-210

ip admission name proxy http 2-211
ip arp inspection filter vlan 2-213
ip arp inspection limit 2-215
ip arp inspection log-buffer 2-217
ip arp inspection trust 2-219
ip arp inspection validate 2-220
ip arp inspection vlan 2-222
ip arp inspection vlan logging 2-223
ip device tracking probe 2-225
ip device tracking 2-227
ip dhcp snooping 2-228
ip dhcp snooping binding 2-229
ip dhcp snooping database 2-231
ip dhcp snooping information option 2-233
ip dhcp snooping information option allow-untrusted 2-235
ip dhcp snooping information option format remote-id 2-237
ip dhcp snooping limit rate 2-238
ip dhcp snooping trust 2-239
ip dhcp snooping verify 2-240
ip dhcp snooping vlan 2-241
ip dhcp snooping vlan information option format-type circuit-id string 2-242
ip igmp filter 2-244
ip igmp max-groups 2-245
ip igmp profile 2-247
ip igmp snooping 2-249
ip igmp snooping last-member-query-interval 2-251
ip igmp snooping querier 2-253
ip igmp snooping report-suppression 2-255
ip igmp snooping tcn 2-257
ip igmp snooping tcn flood 2-259
ip igmp snooping vlan immediate-leave 2-260
ip igmp snooping vlan mrouter 2-261
ip igmp snooping vlan static 2-263
ip snap forwarding 2-265
ip source binding 2-266

ip ssh 2-268
ip sticky-arp（グローバル コンフィギュレーション） 2-269
ip sticky-arp（インターフェイス コンフィギュレーション） 2-271
ip verify source 2-273
ipv6 access-list 2-275
ipv6 address dhcp 2-278
ipv6 dhcp client request vendor 2-279
ipv6 dhcp ping packets 2-280
ipv6 dhcp pool 2-281
ipv6 dhcp server 2-283
ipv6 mld snooping 2-285
ipv6 mld snooping last-listener-query-count 2-287
ipv6 mld snooping last-listener-query-interval 2-289
ipv6 mld snooping listener-message-suppression 2-291
ipv6 mld snooping robustness-variable 2-292
ipv6 mld snooping tcn 2-294
ipv6 mld snooping vlan 2-296
ipv6 traffic-filter 2-298
l2protocol-tunnel 2-300
l2protocol-tunnel cos 2-304
lacp port-priority 2-305
lacp system-priority 2-307
link state group 2-309
link state track 2-311
location（グローバル コンフィギュレーション） 2-312
location（インターフェイス コンフィギュレーション） 2-314
logging event 2-316
logging event power-inline-status 2-317
logging file 2-318
mab request format attribute 32 2-320
mac access-group 2-322
mac access-list extended 2-324
mac address-table aging-time 2-326
mac address-table learning vlan 2-327
mac address-table move update 2-329

mac address-table notification 2-331
mac address-table static 2-333
mac address-table static drop 2-334
match（アクセス マップ コンフィギュレーション） 2-336
match（クラスマップ コンフィギュレーション） 2-338
mdix auto 2-340
mls qos 2-341
mls qos aggregate-policer 2-343
mls qos cos 2-345
mls qos dscp-mutation 2-347
mls qos map 2-349
mls qos queue-set output buffers 2-353
mls qos queue-set output threshold 2-355
mls qos rewrite ip dscp 2-357
mls qos srr-queue input bandwidth 2-359
mls qos srr-queue input buffers 2-361
mls qos srr-queue input cos-map 2-363
mls qos srr-queue input dscp-map 2-365
mls qos srr-queue input priority-queue 2-367
mls qos srr-queue input threshold 2-369
mls qos srr-queue output cos-map 2-371
mls qos srr-queue output dscp-map 2-373
mls qos trust 2-375
mls qos vlan-based 2-378
monitor session 2-379
mvr（グローバル コンフィギュレーション） 2-384
mvr（インターフェイス コンフィギュレーション） 2-387
network-policy 2-390
network-policy profile（グローバル コンフィギュレーション） 2-391
network-policy profile（ネットワークポリシー コンフィギュレーション） 2-393
nmsp 2-395
nmsp attachment suppress 2-397
no authentication logging verbose 2-398
no dot1x logging verbose 2-399
no mab logging verbose 2-400

nsf 2-401
pagp learn-method 2-403
pagp port-priority 2-405
permit（ARP アクセスリスト コンフィギュレーション） 2-407
permit（IPv6 アクセスリスト コンフィギュレーション） 2-409
permit（MAC アクセスリスト コンフィギュレーション） 2-415
police 2-418
police aggregate 2-420
policy-map 2-422
port-channel load-balance 2-425
power inline 2-426
power inline consumption 2-429
power rps 2-431
priority-queue 2-434
private-vlan 2-436
private-vlan mapping 2-439
queue-set 2-441
radius-server dead-criteria 2-442
radius-server host 2-444
rcommand 2-446
reload 2-448
remote command 2-450
remote-span 2-451
renew ip dhcp snooping database 2-453
reserved-only 2-455
rmon collection stats 2-456
sdm prefer 2-457
service password-recovery 2-462
service-policy 2-464
session 2-467
set 2-469
setup 2-471
setup express 2-474
show access-lists 2-476
show archive status 2-479

show arp access-list 2-480
show authentication 2-481
show auto qos 2-485
show boot 2-489
show cable-diagnostics tdr 2-491
show cdp forward 2-494
show cisp 2-495
show class-map 2-496
show cluster 2-497
show cluster candidates 2-499
show cluster members 2-501
show controllers cpu-interface 2-503
show controllers ethernet-controller 2-505
show controllers power inline 2-513
show controllers tcam 2-515
show controllers utilization 2-517
show diagnostic 2-519
show dot1q-tunnel 2-522
show dot1x 2-523
show dtp 2-527
show eap 2-529
show env 2-532
show errdisable detect 2-536
show errdisable flap-values 2-538
show errdisable recovery 2-540
show etherchannel 2-542
show fallback profile 2-545
show flowcontrol 2-547
show idprom 2-549
show interfaces 2-551
show interfaces counters 2-561
show inventory 2-564
show ip arp inspection 2-565
show ip dhcp snooping 2-569
show ip dhcp snooping binding 2-570

show ip dhcp snooping database 2-572
show ip dhcp snooping statistics 2-574
show ip igmp profile 2-577
show ip igmp snooping 2-578
show ip igmp snooping groups 2-581
show ip igmp snooping mrouter 2-583
show ip igmp snooping querier 2-585
show ip source binding 2-587
show ip verify source 2-588
show ipc 2-590
show ipv6 access-list 2-594
show ipv6 dhcp conflict 2-596
show ipv6 mld snooping 2-597
show ipv6 mld snooping address 2-599
show ipv6 mld snooping mrouter 2-601
show ipv6 mld snooping querier 2-603
show ipv6 route updated 2-605
show l2protocol-tunnel 2-607
show lacp 2-610
show lldp 2-614
show location 2-615
show link state group 2-618
show mac access-group 2-620
show mac address-table 2-621
show mac address-table address 2-623
show mac address-table aging-time 2-625
show mac address-table count 2-627
show mac address-table dynamic 2-629
show mac address-table interface 2-631
show mac address-table learning 2-633
show mac address-table move update 2-634
show mac address-table notification 2-636
show mac address-table static 2-638
show mac address-table vlan 2-640
show mls qos 2-642

show mls qos aggregate-policer 2-643
show mls qos input-queue 2-644
show mls qos interface 2-646
show mls qos maps 2-650
show mls qos queue-set 2-653
show mls qos vlan 2-655
show monitor 2-656
show mvr 2-658
show mvr interface 2-660
show mvr members 2-662
show network-policy profile 2-664
show nmsp 2-665
show pagp 2-668
show policy-map 2-670
show port-security 2-671
show power inline 2-674
show sdm prefer 2-677
show setup express 2-680
show spanning-tree 2-681
show storm-control 2-687
show switch 2-689
show system mtu 2-694
show udld 2-695
show version 2-698
show vlan 2-700
show vlan access-map 2-705
show vlan filter 2-706
show vmps 2-707
show vtp 2-709
shutdown 2-714
shutdown vlan 2-715
small-frame violation rate 2-716
snmp-server enable traps 2-718
snmp-server host 2-723
snmp trap mac-notification change 2-727

spanning-tree backbonefast 2-729
spanning-tree bpdufilter 2-730
spanning-tree bpduguard 2-732
spanning-tree cost 2-734
spanning-tree etherchannel guard misconfig 2-736
spanning-tree extend system-id 2-738
spanning-tree guard 2-740
spanning-tree link-type 2-742
spanning-tree loopguard default 2-744
spanning-tree mode 2-746
spanning-tree mst configuration 2-748
spanning-tree mst cost 2-750
spanning-tree mst forward-time 2-752
spanning-tree mst hello-time 2-753
spanning-tree mst max-age 2-755
spanning-tree mst max-hops 2-757
spanning-tree mst port-priority 2-759
spanning-tree mst pre-standard 2-761
spanning-tree mst priority 2-762
spanning-tree mst root 2-763
spanning-tree port-priority 2-765
spanning-tree portfast（グローバル コンフィギュレーション） 2-767
spanning-tree portfast（インターフェイス コンフィギュレーション） 2-770
spanning-tree transmit hold-count 2-773
spanning-tree uplinkfast 2-774
spanning-tree vlan 2-776
speed 2-779
srr-queue bandwidth limit 2-781
srr-queue bandwidth shape 2-783
srr-queue bandwidth share 2-785
stack-mac persistent timer 2-787
storm-control 2-790
switch 2-793
switch priority 2-795
switch provision 2-796

switch renumber 2-798
switchport 2-800
switchport access 2-802
switchport autostate exclude 2-804
switchport backup interface 2-806
switchport block 2-810
switchport host 2-812
switchport mode 2-813
switchport mode private-vlan 2-816
switchport nonegotiate 2-818
switchport port-security 2-820
switchport port-security aging 2-825
switchport priority extend 2-827
switchport private-vlan 2-829
switchport protected 2-831
switchport trunk 2-833
switchport voice detect 2-837
switchport voice vlan 2-838
system env temperature threshold yellow 2-840
system mtu 2-842
test cable-diagnostics tdr 2-844
traceroute mac 2-845
traceroute mac ip 2-848
trust 2-850
udld 2-852
udld port 2-854
udld reset 2-856
aaa authentication dot1x 2-857
vlan（VLAN コンフィギュレーション） 2-859
vlan access-map 2-860
vlan database 2-862
vlan dot1q tag native 2-863
vlan filter 2-865
vmps reconfirm（特権 EXEC） 2-867
vmps reconfirm（グローバル コンフィギュレーション） 2-868

vmps retry 2-869
vmps server 2-870
vtp（グローバル コンフィギュレーション） 2-872
vtp（インターフェイス コンフィギュレーション） 2-877
vtp（VLAN コンフィギュレーション） 2-878
vtp primary 2-879

APPENDIX A
Catalyst 3750 スイッチ ブート ローダー コマンド A-1
boot A-2
cat A-4
copy A-5
delete A-6
dir A-7
flash_init A-9
format A-10
fsck A-11
help A-12
memory A-13
mkdir A-15
more A-16
rename A-17
reset A-18
rmdir A-19
set A-20
type A-23
unset A-24
version A-26

APPENDIX B
Catalyst 3750 スイッチ デバッグ コマンド B-1
debug authentication B-2
debug auto qos B-4
debug backup B-6
debug cisp B-7
debug cluster B-8
debug dot1x B-10
debug dtp B-12

debug eap B-13
debug etherchannel B-14
debug ilpower B-15
debug interface B-16
debug ip dhcp snooping B-17
debug ip verify source packet B-18
debug ip igmp filter B-19
debug ip igmp max-groups B-20
debug ip igmp snooping B-21
debug lacp B-22
debug lldp packets B-23
debug mac-notification B-24
debug matm B-25
debug matm move update B-26
debug monitor B-27
debug mvrdbg B-29
debug nmsp B-30
debug nvram B-31
debug pagp B-32
debug platform acl B-33
debug platform backup interface B-34
debug platform cisp B-35
debug platform cli-redirection main B-36
debug platform configuration B-37
debug platform cpu-queues B-38
debug platform device-manager B-40
debug platform dot1x B-41
debug platform etherchannel B-42
debug platform fallback-bridging B-43
debug platform forw-tcam B-44
debug platform frontend-controller B-45
debug platform ip arp inspection B-46
debug platform ip dhcp B-47
debug platform ip igmp snooping B-48
debug platform ip multicast B-50

debug platform ip source-guard B-52
debug platform ip unicast B-53
debug platform ip wccp B-55
debug platform ipc B-56
debug platform led B-57
debug platform matm B-58
debug platform messaging application B-59
debug platform phy B-60
debug platform pm B-62
debug platform port-asic B-64
debug platform port-security B-65
debug platform qos-acl-tcam B-66
debug platform remote-commands B-67
debug platform resource-manager B-68
debug platform snmp B-69
debug platform span B-70
debug platform stack-manager B-71
debug platform supervisor-asic B-72
debug platform sw-bridge B-73
debug platform tcam B-74
debug platform udld B-77
debug platform vlan B-78
debug pm B-79
debug port-security B-81
debug qos-manager B-82
debug spanning-tree B-83
debug spanning-tree backbonefast B-85
debug spanning-tree bpdu B-86
debug spanning-tree bpdu-opt B-87
debug spanning-tree mstp B-88
debug spanning-tree switch B-90
debug spanning-tree uplinkfast B-92
debug sw-vlan B-93
debug sw-vlan ifs B-95
debug sw-vlan notification B-97

debug sw-vlan vtp B-99
debug udld B-101
debug vqpc B-103
debug platform wireless-controller B-104

APPENDIX C Catalyst 3750 スイッチ Show Platform コマンド C-1
show platform acl C-2
show platform backup interface C-3
show platform configuration C-4
show platform etherchannel C-5
show platform forward C-6
show platform frontend-controller C-8
show platform ip igmp snooping C-9
show platform ip multicast C-11
show platform ip unicast C-12
show platform ip unicast vrf compaction C-14
show platform ip unicast vrf tcam-label C-15
show platform ip wccp C-16
show platform ipc trace C-17
show platform ipv6 unicast C-18
show platform layer4op C-20
show platform mac-address-table C-21
show platform messaging C-22
show platform monitor C-23
show platform mvr table C-24
show platform pm C-25
show platform port-asic C-26
show platform port-security C-30
show platform qos C-31
show platform resource-manager C-32
show platform snmp counters C-34
show platform spanning-tree C-35
show platform stp-instance C-36
show platform stack manager C-37
show platform stack ports C-39
show platform tb C-41

show platform tcam C-43
show platform vlan C-46
show platform wireless-controller C-47

APPENDIX D オープン ソース ソフトウェアについて D-1

INDEX

はじめに

対象読者

このマニュアルは、Cisco IOS Command-Line Interface（CLI; コマンドライン インターフェイス）を使用して Catalyst 3750 スイッチ（以降、*スイッチ*）を管理するネットワーキング専門家を対象としています。このマニュアルは、すでに Cisco IOS コマンドおよびスイッチ ソフトウェア機能使用経験があることを前提にしています。また、イーサネットと LAN のコンセプトおよび用語に関してすでに習得済みであることも前提としています。

目的

Catalyst 3750 スイッチは、IP ベース イメージまたは IP サービス イメージのいずれか一方でサポートされます。IP ベース イメージは、Access Control List（ACL; アクセス コントロール リスト）、Quality of Service（QoS）、スタティック ルーティング、Routing Information Protocol（RIP）などのレイヤ 2+ 機能を備えています。IP サービス イメージは、さらに高度なエンタープライズ クラスの機能を備えています。これには、レイヤ 2+ 機能およびフル レイヤ 3 ルーティング（IP ユニキャスト ルーティング、IP マルチキャスト ルーティング、およびフォールバック ブリッジング）が含まれています。また、それをレイヤ 2+ スタティック ルーティングや RIP と区別するために、IP サービス イメージでは、Enhanced IGRP（EIGRP）や Open Shortest Path First（OSPF）といったプロトコルを搭載しています。

このマニュアルでは、Catalyst 3750 スイッチでの使用のために作成または変更されているレイヤ 2 およびレイヤ 3 のコマンドに関する情報を掲載しています。標準 Cisco IOS Release 12.2 コマンドについては、Cisco.com のホームページ（[Technical Support & Documentation] > [Cisco IOS Software]）にアクセスし、Cisco IOS のマニュアル セットを参照してください。

このマニュアルでは、お客様のスイッチを設定する手順については説明していません。設定手順については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

このマニュアルでは、表示されるシステム メッセージについては説明していません。詳細については、このリリースに対応するシステム メッセージ ガイドを参照してください。

資料の更新については、このリリースに対応するリリース ノートを参照してください。

表記法

このマニュアルでは、次の表記法を使用して説明および情報を表示しています。

コマンドの説明では、次の表記法を使用しています。

- コマンドおよびキーワードは、**太字**で示しています。
- 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。
- 必ずどれか 1 つを選択しなければならない要素は、波カッコ（{ }）で囲み、縦棒（|）で区切って示しています。
- 任意で選択する要素の中で、必ずどれか 1 つを選択しなければならない要素は、角カッコと波カッコで囲み、縦棒で区切って（[{ | }]）示しています。

対話形式の例では、次の表記法を使用しています。

- 端末セッションおよびシステムの表示は、`screen` フォントで示しています。
- ユーザが入力する情報は、太字の **`screen`** フォントで示しています。
- パスワードやタブのように、出力されない文字は、山カッコ（< >）で囲んで示しています。

（注）、注意、および警告には、次の表記法および記号を使用しています。

（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 「*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。

関連資料

次に挙げる、スイッチに関する詳細情報が記載されているマニュアルは、次の Cisco.com サイトから入手できます。
http://www.cisco.com/en/US/products/hw/switches/ps5023/tsd_products_support_series_home.html

（注） スイッチの取り付け、設定、アップグレードを行う前に、次のマニュアルを参照してください。

- 初期設定情報については、入門ガイドの「Using Express Setup」またはハードウェア インストレーション ガイドの付録「Configuring the Switch with the CLI-Based Setup Program」を参照してください。
- デバイス マネージャの要件については、リリース ノート（発注できませんが、Cisco.com で入手可能）の「System Requirements」を参照してください。
- Network Assistant の要件については、『*Getting Started with Cisco Network Assistant*』（発注できませんが、Cisco.com で入手可能）を参照してください。
- クラスタの要件については、『*Release Notes for Cisco Network Assistant*』（発注できませんが、Cisco.com で入手可能）を参照してください。
- アップグレード情報については、リリース ノートの「Downloading Software」を参照してください。

スイッチに関するその他の情報については、次のマニュアルを参照してください。

- 『*Release Notes for the Catalyst 3750, 3560, 2975, and 2960 Switches*』
- 『*Catalyst 3750 Switch Software Configuration Guide*』
- 『*Catalyst 3750 スイッチ コマンド リファレンス*』
- デバイス マネージャのオンライン ヘルプ（スイッチで利用可能）
- 『*Catalyst 3750 Switch Hardware Installation Guide*』
- 『*Catalyst 3750 Switch Getting Started Guide*』
- 『*Catalyst 3750 Integrated Wireless LAN Controller Switch Getting Started Guide*』
- 『*Regulatory Compliance and Safety Information for the Catalyst 3750 Switch*』
- 『*Catalyst 3750, 3560, 3550, 2975, 2975, 2970, 2960, and 2960-S Switch System Message Guide*』
- 『*Release Notes for Cisco Network Assistant*』
- 『*Getting Started with Cisco Network Assistant*』
- 『*Cisco RPS 300 Redundant Power System Hardware Installation Guide*』
- 『*Cisco RPS 675 Redundant Power System Hardware Installation Guide*』
- 『*Cisco Redundant Power System 2300 Hardware Installation Guide*』
- Network Admission Control（NAC）機能の詳細については、『*Network Admission Control Software Configuration Guide*』を参照してください。
- Cisco SFP、SFP+、および GBIC モジュールに関する情報は、Cisco.com の次のページで入手可能です。
  http://www.cisco.com/en/US/products/hw/modules/ps5455/prod_installation_guides_list.html

  これらの SFP 互換性マトリクス ドキュメントは、Cisco.com の次のページで入手可能です。
  http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

次のマニュアルには、Catalyst 3750G Integrated Wireless LAN Controller Switch および Integrated Wireless LAN Controller に関する詳細情報が記載されています。Cisco.com から入手できます。

- 『*Catalyst 3750 Integrated Wireless LAN Controller Switch Getting Started Guide*』(Customer Order Number DOC-7817540=)
- 『*Release Notes for Cisco Wireless LAN Controller and Lightweight Access Point, Release 4.0.x.0*』
- 『*Cisco Wireless LAN Controller Configuration Guide, Release 4.0*』
- 『*Cisco Wireless LAN Controller Command Reference, Release 4.0*』

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

Command-Line Interface の使用

Catalyst 3750 スイッチは Cisco IOS ソフトウェアによってサポートされています。ここでは、ソフトウェア機能を設定するためのスイッチ Command-Line Interface（CLI; コマンドライン インターフェイス）の使用方法について説明します。

- これらの機能をサポートするコマンドの詳細な説明については、第 2 章「Catalyst 3750 スイッチ Cisco IOS コマンド」を参照してください。
- ブート ローダー コマンドの詳細については、付録 A「Catalyst 3750 スイッチ ブート ローダー コマンド」を参照してください。
- **debug** コマンドの詳細については、付録 B「Catalyst 3750 スイッチ デバッグ コマンド」を参照してください。
- **show platform** コマンドの詳細については、付録 C「Catalyst 3750 スイッチ Show Platform コマンド」を参照してください。
- Cisco IOS Release 12.2 のさらに詳しい情報については、『*Cisco IOS Release 12.2 Command Summary*』を参照してください。
- タスク指向の設定手順については、このリリースのソフトウェア コンフィギュレーション ガイドを参照してください。

このマニュアルでは、明示的に IP バージョン 6（IPv6）を指す場合を除き、IP とは IP バージョン 4（IPv4）のことを指します。

スイッチへのアクセス

スイッチ スタックおよびスタック メンバ インターフェイスは、スタック マスターを経由して管理します。スイッチごとにスタック メンバを管理することはできません。スタック マスターには、1 台以上のスタック メンバのコンソール ポートを経由して接続できます。複数の CLI セッションをスタック マスターに使用する場合は注意が必要です。1 つのセッションで入力したコマンドは、別のセッションには表示されません。したがって、コマンドを入力したセッションを追跡できない場合があります。

（注） スイッチ スタックを管理する場合は、1 つの CLI セッションを使用することを推奨します。

特定のスタック メンバ ポートを設定する場合は、CLI コマンド インターフェイス表記にスタック メンバ番号を含めてください。インターフェイス表記の詳細情報については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring Interfaces」の章を参照してください。

特定のスタック メンバをデバッグする場合は、**session** *stack-member-number* 特権 EXEC コマンドでスタック マスターからアクセスできます。スタック メンバ番号は、システム プロンプトに追加されます。たとえば、Switch-2# はスタック メンバ 2 の特権 EXEC モードのプロンプトであり、スタック マスターのシステム プロンプトは Switch です。特定のスタック メンバへの CLI セッションで使用できるのは、**show** コマンドと **debug** コマンドに限ります。

CLI コマンド モード

ここでは、CLI コマンド モード構造について説明します。コマンド モードは、特定の Cisco IOS コマンドをサポートします。たとえば、**interface** *interface-id* コマンドは、グローバル コンフィギュレーション モードで入力されたときだけ機能します。

以下は、スイッチの主なコマンド モードです。

- ユーザ EXEC
- 特権 EXEC
- グローバル 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
- VLAN コンフィギュレーション
- ライン コンフィギュレーション

表 1-1 に、主なコマンド モード、各モードへのアクセス方法、各モードで表示されるプロンプト、およびモードの終了方法を示します。表示されているプロンプトは、デフォルト名 *Switch* を使用しています。

表 1-1　コマンド モードの概要

コマンド モード	アクセス方法	プロンプト	終了または次のモードのアクセス
ユーザ EXEC	これが最初のアクセス レベルです。 （スイッチについては）ターミナル設定を変更し、基本タスクを実行し、システム情報を一覧表示します。	`Switch>`	**logout** コマンドを入力します。 特権 EXEC モードを開始するには、**enable** コマンドを入力します。
特権 EXEC	ユーザ EXEC モードから、**enable** コマンドを入力します。	`Switch#`	ユーザ EXEC モードに戻る場合は、**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** 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 モードから、**configure** コマンドを入力します。	`Switch(config)#`	特権 EXEC モードに戻る場合は、**exit** または **end** コマンドを入力するか、**Ctrl+Z** 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。

表 1-1　コマンド モードの概要 （続き）

コマンド モード	アクセス方法	プロンプト	終了または次のモードのアクセス
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 モードから、**interface** コマンドを入力し、次にインターフェイス ID を入力することにより、インターフェイスを指定します。	`Switch(config-if)#`	特権 EXEC モードに戻る場合は、**end** コマンドを入力するか、**Ctrl+Z** を押します。 グローバル コンフィギュレーション モードに戻る場合は、**exit** コマンドを入力します。
VLAN 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 **vlan** *vlan-id* コマンドを入力します。	`Switch(config-vlan)#`	グローバル コンフィギュレーション モードに戻る場合は、**exit** コマンドを入力します。 特権 EXEC モードに戻る場合は、**end** コマンドを入力するか、**Ctrl+Z** を押します。
ライン 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 モードから、**line** コマンドを入力することにより、ラインを指定します。	`Switch(config-line)#`	グローバル コンフィギュレーション モードに戻る場合は、**exit** コマンドを入力します。 特権 EXEC モードに戻る場合は、**end** コマンドを入力するか、**Ctrl+Z** を押します。

ユーザ EXEC モード

装置にアクセスすると、自動的にユーザ EXEC コマンド モードに入ります。ユーザ レベルで使用可能な EXEC コマンドは、特権レベルで使用可能な EXEC コマンドのサブセットです。一般に、ユーザ EXEC コマンドは、端末設定の一時的変更、基本テストの実行、システム情報の一覧表示などに使用します。

サポートされているコマンドは、ご使用のソフトウェアのバージョンによって異なります。コマンドの包括的なリストを表示するには、プロンプトで疑問符（**?**）を入力します。

```
Switch> ?
```

特権 EXEC モード

特権コマンドの多くは動作パラメータの設定に関係しています。無許可の使用を防止するには、特権コマンドへのアクセスをパスワードで保護する必要があります。特権コマンド セットには、ユーザ EXEC モードのコマンドと、それ以外のコマンド モードにアクセスするための **configure** 特権 EXEC コマンドが含まれます。

システム管理者がパスワードを設定した場合、特権 EXEC モードへのアクセスが許可される前に、パスワードの入力を要求するプロンプトが表示されます。パスワードは画面には表示されません。また、大文字と小文字が区別されます。

特権 EXEC モードのプロンプトは、装置名の後にポンド記号（#）が付きます。

```
Switch#
```

特権 EXEC モードにアクセスするには、**enable** コマンドを入力します。

```
Switch> enable
Switch#
```

サポートされているコマンドは、ご使用のソフトウェアのバージョンによって異なります。コマンドの包括的なリストを表示するには、プロンプトで疑問符（**?**）を入力します。

```
Switch# ?
```

ユーザ EXEC モードに戻る場合は、**disable** 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 モード

グローバル コンフィギュレーション コマンドは、装置全体に影響を与える機能に適用されます。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** 特権 EXEC コマンドを使用します。デフォルトでは、管理コンソールからコマンドを入力します。

configure コマンドを入力すると、コンフィギュレーション コマンドの送信元の入力を要求するメッセージが表示されます。

```
Switch# configure
Configuring from terminal, memory, or network [terminal]?
```

コンフィギュレーション コマンドの送信元として、端末または NVRAM（不揮発性 RAM）のいずれかを指定することができます。

次の例では、グローバル コンフィギュレーション モードにアクセスする方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

サポートされているコマンドは、ご使用のソフトウェアのバージョンによって異なります。コマンドの包括的なリストを表示するには、プロンプトで疑問符（**?**）を入力します。

```
Switch(config)# ?
```

グローバル コンフィギュレーション コマンド モードを終了して特権 EXEC モードに戻る場合は、**end** コマンドまたは **exit** コマンドを入力するか、**Ctrl+Z** 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

インターフェイス コンフィギュレーション コマンドは、インターフェイスの動作を変更します。インターフェイス コンフィギュレーション コマンドは常に、インターフェイス タイプを定義するグローバル コンフィギュレーション コマンドの後に続きます。

インターフェイス コンフィギュレーション モードにアクセスするには、**interface** *interface-id* コマンドを使用します。次の新しいプロンプトはインターフェイス コンフィギュレーション モードを示しています。

```
Switch(config-if)#
```

サポートされているコマンドは、ご使用のソフトウェアのバージョンによって異なります。コマンドの包括的なリストを表示するには、プロンプトで疑問符（**?**）を入力します。

```
Switch(config-if)# ?
```

インターフェイス コンフィギュレーション モードを終了してグローバル コンフィギュレーション モードに戻る場合は、**exit** 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 モードを終了して特権 EXEC モードに戻る場合は、**end** コマンドを入力するか、**Ctrl+Z** を押します。

VLAN コンフィギュレーション モード

標準範囲 VLAN（VLAN ID 1 ～ 1005）を設定したり、VTP モードがトランスペアレントであるときに拡張範囲 VLAN（VLAN ID 1006 ～ 4094）を設定したりする場合は、このモードを使用します。VTP モードがトランスペアレントである場合は、VLAN および VTP 設定は実行コンフィギュレーション ファイルに保存されるため、**copy running-config startup-config** 特権 EXEC コマンドを実行して、この設定をスイッチのスタートアップ コンフィギュレーション ファイルに保存できます。VTP がトランスペアレント モードまたはサーバ モードの場合、VLAN ID が 1 ～ 1005 の VLAN 設定は、VLAN データベースに保存されます。拡張範囲 VLAN 設定は、VLAN データベースには保存されません。

config-vlan モードを開始するには、**vlan** *vlan-id* 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。

```
Switch(config)# vlan 2000
Switch(config-vlan)#
```

サポートされるキーワードはさまざまですが、VLAN コンフィギュレーション モードで利用できるコマンドと似ています。コマンドの包括的なリストを表示するには、プロンプトで疑問符（**?**）を入力します。

```
Switch(config-vlan)# ?
```

拡張範囲 VLAN については、MTU サイズ以外のすべての特性はデフォルト設定のままにしておいてください。

グローバル コンフィギュレーション モードに戻る場合は、**exit** を入力します。特権 EXEC モードに戻る場合は、**end** を入力します。**shutdown** 以外のすべてのコマンドは、config-vlan モードを終了したときに有効になります。

ライン コンフィギュレーション モード

ライン コンフィギュレーション コマンドは、端末ラインの動作を変更します。ライン コンフィギュレーション コマンドは、常にライン番号を定義するライン コマンドの後に来ます。端末パラメータ設定をラインごと、あるいはある範囲のライン全体で変更するには、このコマンドを使用します。

ライン コンフィギュレーション モードを開始するには、**line vty** *line_number* [*ending_line_number*] コマンドを使用します。次の新しいプロンプトはライン コンフィギュレーション モードを示しています。次の例では、仮想端末ライン 7 でライン コンフィギュレーション モードを開始する方法を示します。

```
Switch(config)# line vty 0 7
```

サポートされているコマンドは、ご使用のソフトウェアのバージョンによって異なります。コマンドの包括的なリストを表示するには、プロンプトで疑問符（**?**）を入力します。

```
Switch(config-line)# ?
```

ライン コンフィギュレーション モードを終了してグローバル コンフィギュレーション モードに戻る場合は、**exit** コマンドを使用します。ライン コンフィギュレーション モードを終了して特権 EXEC モードに戻る場合は、**end** コマンドを入力するか、**Ctrl+Z** を押します。

CHAPTER 2

Catalyst 3750 スイッチ Cisco IOS コマンド

aaa accounting dot1x

Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）アカウンティングをイネーブルにして、IEEE 802.1x セッションの特定のアカウンティング方式を、回線単位またはインターフェイス単位で定義する方式リストを作成するには **aaa accounting dot1x** グローバル コンフィギュレーション コマンドを使用します。IEEE 802.1x 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。

aaa accounting dot1x {*name* | **default**} **start-stop** {**broadcast group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**}...] | **group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**}...]}

no aaa accounting dot1x {*name* | **default**}

構文の説明

name	サーバ グループ名。これは、**broadcast group** および **group** キーワードの後に入力する場合に使用するオプションです。
default	デフォルト リストにあるアカウンティング方式を、アカウンティング サービス用に使用します。
start-stop	プロセスの開始時に start アカウンティング通知を送信し、プロセスの終了時に stop アカウンティング通知を送信します。start アカウンティング レコードはバックグラウンドで送信されます。アカウンティング サーバが start アカウンティング通知を受け取ったかどうかには関係なく、要求されたユーザ プロセスが開始されます。
broadcast	複数の AAA サーバに送信されるアカウンティング レコードをイネーブルにして、アカウンティング レコードを各グループの最初のサーバに送信します。最初のサーバが利用できない場合、スイッチはバックアップ サーバのリストを使用して最初のサーバを識別します。
group	アカウンティング サービスに使用するサーバ グループを指定します。有効なサーバ グループ名は次のとおりです。 • *name*：サーバ グループ名 • **radius**：全 RADIUS ホストのリスト • **tacacs+**：全 TACACS+ ホストのリスト **broadcast group** および **group** キーワードの後に入力する場合、**group** キーワードはオプションです。オプションの **group** キーワードより多くのキーワードを入力できます。

radius	（任意）RADIUS 認証をイネーブルにします。
tacacs+	（任意）TACACS+ アカウンティングをイネーブルにします。

デフォルト

AAA アカウンティング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

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、RADIUS サーバへのアクセスが必要です。

インターフェイスに IEEE 802.1x RADIUS アカウンティングを設定する前に、**dot1x reauthentication** インターフェイス コンフィギュレーション コマンドを入力することを推奨します。

例

次の例では、IEEE 802.1x アカウンティングを設定する方法を示します。

```
Switch(config)# aaa new-model
Switch(config)# aaa accounting dot1x default start-stop group radius
```

（注）RADIUS 認証サーバは、AAA クライアントから更新パケットやウォッチドッグ パケットを受け入れて記録するよう、適切に設定する必要があります。

関連コマンド

コマンド	説明
aaa authentication dot1x	IEEE 802.1x が動作しているインターフェイスで使用する 1 つ以上の AAA メソッドを指定します。
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
dot1x reauthentication	定期的な再認証をイネーブルまたはディセーブルにします。
dot1x timeout reauth-period	再認証の試行の間隔（秒）を設定します。

aaa authentication dot1x

IEEE 802.1x 認証に準拠するポートで Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）メソッドを使用するように指定するには **aaa accounting dot1x** グローバル コンフィギュレーション コマンドを使用します。認証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。

aaa authentication dot1x {**default**} *method1*

no aaa authentication dot1x {**default**}

構文の説明

default	この引数の後に続く、リストされた認証方式をログイン時のデフォルトの方式として使用します。
method1	認証用にすべての RADIUS サーバのリストを使用するには、**group radius** キーワードを入力します。

（注）　他のキーワードがコマンドラインのヘルプ ストリングに表示されますが、サポートされているのは **default** および **group radius** キーワードだけです。

デフォルト

認証は実行されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

method 引数には、認証アルゴリズムがクライアントからのパスワードを確認するために一定の順序で試みる方式を指定します。実際に IEEE 802.1x に準拠している唯一の方式は、クライアント データが RADIUS 認証サーバに対して確認される **group radius** 方式です。

group radius を指定した場合、**radius-server host** 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 RADIUS サーバを設定する必要があります。

設定された認証方式のリストを表示するには、**show running-config** 特権 EXEC コマンドを使用します。

例

次の例では AAA をイネーブルにして IEEE 802.1x 準拠の認証リストを作成する方法を示します。この認証は、最初に RADIUS サーバとの交信を試みます。この動作でエラーが返信された場合、ユーザはネットワークへのアクセスが許可されません。

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
show running-config	現在の動作設定を表示します。

aaa authorization network

aaa ユーザ Access Control List（ACL; アクセス コントロール リスト）や IEEE 802.1x VLAN 割り当てといったすべてのネットワーク関連サービス要求に対してユーザ RADIUS 認証を使用するようにスイッチを設定するには、**aaa authorization network** グローバル コンフィギュレーション コマンドを使用します。RADIUS ユーザ認証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。

aaa authorization network default group radius

no aaa authorization network default

構文の説明

default group radius	デフォルトの認証リストとして、サーバ グループ内のすべての RADIUS ホストのリストを使用します。

デフォルト

認証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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

スイッチが、デフォルトの認証リスト内にある RADIUS サーバから IEEE 802.1x 認証パラメータをダウンロードできるようにするには、**aaa authorization network default group radius** グローバル コンフィギュレーション コマンドを使用します。認証パラメータは、ユーザごとの ACL または VLAN 割り当てなど、RADIUS サーバからパラメータを取得する機能で使用されます。

設定された認証方式リストを表示するには、**show running-config** 特権 EXEC コマンドを使用します。

例

この例では、すべてのネットワーク関連サービス要求に対してユーザ RADIUS 認証を行うようスイッチを設定する方法を示します。

```
Switch(config)# aaa authorization network default group radius
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	現在の動作設定を表示します。

action

VLAN アクセス マップ エントリに対してアクションを設定するには、**action** アクセス マップ コンフィギュレーション 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。

action {drop | forward}

no action

構文の説明

drop	指定された条件に一致する場合に、パケットをドロップします。
forward	指定された条件に一致する場合に、パケットを転送します。

デフォルト

デフォルトのアクションは、パケットの転送です。

コマンド モード

アクセス マップ コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

vlan access-map 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、アクセス マップ コンフィギュレーション モードを開始します。

アクションが **drop** の場合は、一致条件に Access Control List（ACL; アクセス コントロール リスト）名を設定後、そのマップを VLAN に適用してアクセス マップを定義する必要があります。定義しない場合、すべてのパケットがドロップされることがあります。

アクセス マップ コンフィギュレーション モードでは、**match** アクセス マップ コンフィギュレーション コマンドを使用して、VLAN マップの一致条件を定義できます。**action** コマンドを使用すると、パケットが条件に一致したときに実行するアクションを設定できます。

drop パラメータおよび forward パラメータは、このコマンドの **no** 形式では使用されません。

例

次の例では、VLAN アクセス マップ *vmap4* を指定し VLAN 5 と VLAN 6 に適用する方法を示します。このアクセス マップは、パケットがアクセス リスト *al2* に定義された条件に一致する場合に、VLAN がその IP パケットを転送するように指定します。

```
Switch(config)# vlan access-map vmap4
Switch(config-access-map)# match ip address al2
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan filter vmap4 vlan-list 5-6
```

設定を確認するには、**show vlan access-map** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
access-list {deny | permit}	番号付き標準 ACL を設定します。
ip access-list	名前付きアクセス リストを作成します。
mac access-list extended	名前付き MAC アドレス アクセス リストを作成します。
match（クラスマップ コンフィギュレーション）	VLAN マップの一致条件を定義します。
show vlan access-map	スイッチで作成された VLAN アクセス マップを表示します。
vlan access-map	VLAN アクセス マップを作成します。

archive copy-sw

特定のスタック メンバ上のフラッシュ メモリから実行イメージを、1 つ以上の別のスタック メンバ上にあるフラッシュ メモリにコピーするには、スタック マスター上で **archive copy-sw** 特権 EXEC コマンドを使用します。

archive copy-sw [**/destination-system** *destination-stack-member-number*] [**/force-reload**] [**leave-old-sw**] [**/no-set-boot**] [**/overwrite**] [**/reload**] [**/safe**] *source-stack-member-number*

構文の説明

/destination-system *destination-stack-member-number*	（任意）実行イメージのコピー先のメンバ番号。指定できる範囲は 1 ～ 9 です。
/force-reload	（任意）ソフトウェア イメージのダウンロードが成功した後、無条件にシステムのリロードを強制します。
/leave-old-sw	（任意）ダウンロードが成功した後、古いソフトウェア バージョンを保存します。
/no-set-boot	（任意）新しいソフトウェア イメージのダウンロードが成功した後、BOOT 環境変数の設定は新しいソフトウェア イメージを示すように変更されません。
/overwrite	（任意）ダウンロードされたソフトウェア イメージで、フラッシュ メモリのソフトウェア イメージを上書きします。
/reload	（任意）変更された設定が保存されていない場合を除き、イメージをダウンロードした後でシステムをリロードします。
/safe	（任意）現在のソフトウェア イメージを保存します。新しいイメージがダウンロードされるまでは、新しいソフトウェア イメージ用の領域を作る目的で現在のソフトウェア イメージを削除しません。ダウンロード終了後に現在のイメージが削除されます。
source-stack-member-number	実行イメージのコピー元のメンバ番号。指定できる範囲は 1 ～ 9 です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

現行のソフトウェア イメージは、コピーされたイメージで上書きされません。

ソフトウェア イメージと HTML ファイルの両方がコピーされます。

新しいイメージは flash: ファイル システムにコピーされます。

BOOT 環境変数は、flash: ファイル システムの新しいソフトウェア イメージを示すよう変更されます。

イメージ名では大文字と小文字が区別されます。イメージ ファイルは tar フォーマットで提供されます。

（注）　**archive copy-sw** 特権 EXEC コマンドを正しく使用するには、追加されるスタック メンバ スイッチおよびマスターの両方のイメージを Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバからダウンロードしておく必要があります。ダウンロードを実行するには、**archive download-sw** 特権 EXEC コマンドを使用します。

互換性のないソフトウェアが搭載されたスイッチにコピーされるイメージは、少なくとも 1 つのメンバで実行している必要があります。

アップグレードする各メンバのコマンドで **/destination-system** *destination-stack-member-number* のオプションを繰り返すことで、複数の具体的なメンバにイメージをコピーできます。*destination-stack-member-number* を指定しなかった場合は、デフォルト設定で、実行中のイメージ ファイルがすべてのメンバにコピーされます。

/safe または **/leave-old-sw** オプションを使用した場合に、十分なフラッシュ メモリがないと、新しいイメージのコピーに失敗する場合があります。ソフトウェアを残すことによってフラッシュ メモリの空き容量が不足し、新しいイメージが入りきらなかった場合にエラーが発生します。

/leave-old-sw オプションを使用したために、新しいイメージをコピーしても古いイメージが上書きされなかった場合、**delete** 特権 EXEC コマンドを使用して古いイメージを削除できます。詳細については、「delete」（P.2-122）を参照してください。

フラッシュ デバイスのイメージを、コピーされたイメージで上書きする場合は、**/overwrite** オプションを使用します。

/overwrite オプション*なし*でこのコマンドを指定した場合は、新しいイメージが、スイッチ フラッシュ デバイス上のイメージと同じでないことや、いずれのメンバでも実行中ではないことが、アルゴリズムによって確認されます。イメージが同じである場合には、コピーは行われません。イメージが異なっている場合、古いイメージは削除され、新しいイメージがコピーされます。

新しいイメージをコピーした後で、**reload** 特権 EXEC コマンドを入力して新しいイメージの使用を開始するか、または **archive copy-sw** コマンドで **/reload** か **/force-reload** オプションを指定してください。

source-stack-member-number オプションを使用する場合、次のオプションを 1 つ以上入力できます。

- **/destination-system** *destination-stack-member-number*
- **/force-reload**
- **/leave-old-sw**
- **/no-set-boot**
- **/overwrite**
- **/reload**
- **/safe**

これよりも前にあるいずれかのオプションの前に *source-stack-member-number* オプションを入力する場合は、**archive copy-sw** *source-stack-member-number* コマンドだけを入力できます。

次の例では、**archive copy-sw** コマンドを入力する方法を示します。

- 実行イメージをメンバから別のメンバにコピーして、2 つめのメンバのフラッシュ メモリのソフトウェア イメージ（すでに存在する場合）をコピーしたイメージで上書きするには、**archive copy-sw/destination** *destination-stack-member-number* **/overwrite** *source-stack-member-number* コマンドを入力します。
- 実行イメージをメンバから別のメンバにコピーして、現在のソフトウェア イメージを保持しながらイメージのコピー後にシステムをリロードするには、**archive copy-sw/destination** *destination-stack-member-number***/safe/reload** *source-stack-member-number* コマンドを入力します。

例

次の例では、スタック メンバ 6 から実行イメージをメンバ 8 にコピーする方法を示します。

```
Switch# archive copy-sw /destination-system 8 6
```

次の例では、メンバ 6 から実行イメージを他のすべてのメンバにコピーする方法を示します。

```
Switch# archive copy-sw 6
```

次の例では、メンバ 5 から実行イメージをメンバ 7 にコピーする方法を示します。2 つめのメンバのフラッシュ メモリにイメージがすでに存在する場合は、コピーされたイメージで上書きされます。イメージがコピーされた後、システムはリロードされます。

```
Switch# archive copy-sw /destination-system 7 /overwrite /force-reload 5
```

関連コマンド

コマンド	説明
archive download-sw	TFTP サーバからスイッチに新しいイメージをダウンロードします。
archive tar	tar ファイルを作成し、tar ファイルのファイルを一覧表示し、tar ファイルからファイルを抽出します。
archive upload-sw	スイッチの既存のイメージをサーバにアップロードします。
delete	フラッシュ メモリ デバイスのファイルまたはディレクトリを削除します。

archive download-sw

新しいイメージを TFTP サーバからスイッチまたはスイッチ スタックにダウンロードして、既存のイメージを上書きまたは保持するには、**archive download-sw** 特権 EXEC コマンドを使用します。

archive download-sw {**/allow-feature-upgrade** | **/directory** | **/force-reload** | **/imageonly** | **/leave-old-sw** | **/no-set-boot** | **/no-version-check** | **/destination-system** *stack-member-number* | **/only-system-type** *system-type* | **/overwrite** | **/reload** | **/safe**} *source-url*

構文の説明

/allow-feature-upgrade	異なるフィーチャ セットを持つイメージをインストールできます（たとえば、IP ベース イメージから IP サービス イメージへのアップグレード）。
/directory	イメージのディレクトリを指定します。
/force-reload	ソフトウェア イメージのダウンロードが成功した後で無条件にシステムのリロードを強制します。
/imageonly	ソフトウェア イメージだけをダウンロードし、組み込みデバイス マネージャに関連する HTML ファイルはダウンロードしません。既存のバージョンの HTML ファイルは、既存のバージョンが上書きまたは削除されている場合にだけ削除されます。
/leave-old-sw	ダウンロードに成功した後で古いソフトウェア バージョンを保存します。
/no-set-boot	新しいソフトウェア イメージのダウンロードに成功した後に、BOOT 環境変数の設定が新しいソフトウェア イメージを指定するように変更されません。
/no-version-check	そのバージョンのスイッチ上で動作中のイメージとの互換性を確認せずに、ソフトウェア イメージをダウンロードします。スイッチ スタックでは、イメージ上およびスタック上のスタック プロトコル バージョンの互換性を確認せずに、ソフトウェア イメージをダウンロードします。
/destination-system *stack-member-number*	アップグレードする特定のメンバを指定します。指定できる範囲は 1 ～ 9 です。
/only-system-type *system-type*	アップグレードする特定のシステム タイプを指定します。指定できる範囲は 0 ～ FFFFFFFF です。
/overwrite	ダウンロードされたイメージで、フラッシュ メモリのソフトウェア イメージを上書きします。
/reload	変更された設定が保存されていない場合を除き、イメージのダウンロードに成功した後でシステムをリロードします。
/safe	現在のソフトウェア イメージを保存します。新しいイメージがダウンロードされるまでは、新しいソフトウェア イメージ用の領域を作る目的で現在のソフトウェア イメージを削除しません。ダウンロード終了後に現在のイメージが削除されます。

source-url	ローカルまたはネットワーク ファイル システム用の送信元 URL エイリアス。次のオプションがサポートされています。 • セカンダリ ブート ローダー（BS1）の構文： **bs1:** • スタンドアロン スイッチまたはマスター上のローカル フラッシュ ファイル システムの構文： **flash:** メンバ上のローカル フラッシュ ファイル システムの構文： **flash** *member number***:** • FTP の構文： **ftp:**[[//*username*[**:***password*]**@***location*]/*directory*]/*image-name***.tar** • HTTP サーバの構文： **http:**//[[*username***:***password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name***.tar** • セキュア HTTP サーバの構文： **https:**//[[*username***:***password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name***.tar** • Remote Copy Protocol（RCP）の構文： **rcp:**[[//*username***@***location*]/*directory*]/*image-name***.tar** • TFTP の構文： **tftp:**[[//*location*]/*directory*]/*image-name***.tar** *image-name***.tar** は、スイッチにダウンロードし、インストールするソフトウェア イメージです。

デフォルト

現行のソフトウェア イメージは、ダウンロードされたイメージで上書きされません。

ソフトウェア イメージと HTML ファイルの両方がダウンロードされます。

新しいイメージは flash: ファイル システムにダウンロードされます。

BOOT 環境変数は、flash: ファイル システムの新しいソフトウェア イメージを示すよう変更されます。

イメージ名では大文字と小文字が区別されます。イメージ ファイルは tar フォーマットで提供されます。

ダウンロードするイメージのスタック プロトコル バージョンの互換性は、スタックのバージョンと検査されます。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(20)SE	**http** および **https** キーワードが追加されました。
12.2(35)SE	**allow-feature-upgrade** および **directory** キーワードが追加されました。

使用上のガイドライン

/allow-feature-upgrade オプションを使用すると、異なるフィーチャ セットを持つイメージをインストールできます（たとえば、IP ベース イメージから IP サービス イメージへのアップグレード）。

archive download-sw /directory コマンドを使用すると、ディレクトリを一度指定します。その後に、ダウンロードする tar ファイルや tar ファイル リストを指定するため、tar ファイルごとに完全なパスを指定することはしません。たとえば、**archive download-sw /directory tftp://10.1.1.10/ c3750-ipservices-tar.122-35.SE.tar c3750-ipbase-tar.122-35.SE.tar** と入力します。

/imageonly オプションは、既存のイメージが削除または置き換えられている場合に、既存のイメージの HTML ファイルを削除します。（HTML ファイルのない）Cisco IOS イメージだけがダウンロードされます。

/safe または **/leave-old-sw** オプションを指定すると、十分なフラッシュ メモリがない場合には新しいイメージのダウンロードが行われないようにすることができます。ソフトウェアを残すことによってフラッシュ メモリの空き容量が不足し、新しいイメージが入りきらなかった場合に、エラーが発生します。

/leave-old-sw オプションを使用し、新しいイメージをダウンロードしたときに古いイメージが上書きされなかった場合、**delete** 特権 EXEC コマンドを使用して古いイメージを削除することができます。詳細については、「delete」（P.2-122）を参照してください。

スタックに存在しているバージョンとは異なるスタック プロトコルのバージョンのイメージをダウンロードする場合は、**/no-version-check** オプションを使用します。このオプションを使用する場合は **/destination-system** オプションを使用し、イメージでアップグレードする具体的なメンバを指定してください。

（注）**/no-version-check** オプションの使用には注意が必要です。同一のスタックにするためには、マスターを含め、すべてのメンバで、スタック プロトコルのバージョンが同一である必要があります。このオプションを指定すると、最初にスタック プロトコルのバージョンと、スタックのバージョンの互換性を確認することなく、イメージをダウンロードできます。

アップグレードするスタック メンバごとのコマンドで **/destination-system** オプションを繰り返すことで、複数のスタック メンバを指定し、アップグレードできます。

フラッシュ デバイスのイメージをダウンロードされたイメージで上書きする場合は、**/overwrite** オプションを使用します。

/overwrite オプション**なし**でこのコマンドを指定する場合、ダウンロード アルゴリズムは、新しいイメージが、スイッチ フラッシュ デバイスのイメージ、またはスタック メンバで実行中のものと同じではないことを確認します。イメージが同じである場合は、ダウンロードは行われません。イメージが異なっている場合、古いイメージは削除され、新しいイメージがダウンロードされます。

新しいイメージをダウンロードした後で、**reload** 特権 EXEC コマンドを入力して新しいイメージの使用を開始するか、または **archive download-sw** コマンドの **/reload** オプションか **/force-reload** オプションを指定してください。

/directory オプションを使用して、イメージのディレクトリを指定します。

例

次の例では、172.20.129.10 の TFTP サーバから新しいイメージをダウンロードし、スイッチでイメージを上書きする方法を示します。

```
Switch# archive download-sw /overwrite tftp://172.20.129.10/test-image.tar
```

次の例では、172.20.129.10 の TFTP サーバからソフトウェア イメージだけをスイッチにダウンロードする方法を示します。

```
Switch# archive download-sw /imageonly tftp://172.20.129.10/test-image.tar
```

次の例では、ダウンロードに成功した後で古いソフトウェア バージョンを保存する方法を示します。

```
Switch# archive download-sw /leave-old-sw tftp://172.20.129.10/test-image.tar
```

次の例では、毎回パスを指定しないで 2 つの tar イメージの場所を指定します。

```
Switch# archive download-sw /directory tftp://10.1.1.10/
c3750-ipservices-tar.122-35.SE.tar c3750-ipbase-tar.122-35.SE.tar.
```

次の例では、スタック メンバ 6 および 8 をアップグレードする方法を示します。

```
Switch# archive download-sw /imageonly /destination-system 6 /destination-system 8
tftp://172.20.129.10/test-image.tar
```

関連コマンド

コマンド	説明
archive copy-sw	あるスタック メンバのフラッシュ メモリから実行イメージを、別の 1 つ以上のスタック メンバ上のフラッシュ メモリにコピーします。
archive tar	tar ファイルを作成し、tar ファイルのファイルを一覧表示し、tar ファイルからファイルを抽出します。
archive upload-sw	スイッチの既存のイメージをサーバにアップロードします。
delete	フラッシュ メモリ デバイスのファイルまたはディレクトリを削除します。

archive tar

archive tar 特権 EXEC コマンドを使用して、tar ファイルの作成、tar ファイル内のファイルの一覧表示、または tar ファイルからのファイルの抽出を行います。

archive tar {/**create** *destination-url* **flash:**/*file-url*} | {/**table** *source-url*} | {/**xtract** *source-url* **flash:**/*file-url* [*dir/file...*]}

構文の説明

/**create** *destination-url* **flash:**/*file-url*	ローカルまたはネットワーク ファイル システムに新しい tar ファイルを作成します。 *destination-url* には、ローカルまたはネットワーク ファイル システムの宛先 URL エイリアスおよび作成する tar ファイルの名前を指定します。次のオプションがサポートされています。 • ローカル フラッシュ ファイル システムの構文： **flash:** • FTP の構文： **ftp:**[[//*username*[**:***password*]**@***location*]/*directory*]/*tar-filename***.tar** • HTTP サーバの構文： **http://**[[*username***:***password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name***.tar** • セキュア HTTP サーバの構文： **https://**[[*username***:***password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name***.tar** • Remote Copy Protocol（RCP）の構文： **rcp:**[[//*username***@***location*]/*directory*]/*tar-filename***.tar** • TFTP の構文： **tftp:**[[//*location*]/*directory*]/*tar-filename***.tar** *tar-filename***.tar** は、作成する tar ファイルです。 **flash:**/*file-url* には、新しい tar ファイルが作成されるローカル フラッシュ ファイル システムの場所を指定します。 送信元ディレクトリ内のファイルまたはディレクトリのオプションのリストを指定して、新しい tar ファイルに書き込むことができます。何も指定しないと、このレベルのすべてのファイルおよびディレクトリが、新しく作成された tar ファイルに書き込まれます。

/table *source-url*	既存の tar ファイルの内容を画面に表示します。 *source-url* には、ローカル ファイル システムまたはネットワーク ファイル システムの送信元 URL エイリアスを指定します。次のオプションがサポートされています。 • ローカル フラッシュ ファイル システムの構文： **flash:** • FTP の構文： **ftp:**[[//*username*[**:***password*]**@***location*]/*directory*]/*tar-filename***.tar** • HTTP サーバの構文： **http://**[[*username***:***password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name***.tar** • セキュア HTTP サーバの構文： **https://**[[*username***:***password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name***.tar** • RCP の構文： **rcp:**[[//*username***@***location*]/*directory*]/*tar-filename***.tar** • TFTP の構文： **tftp:**[[//*location*]/*directory*]/*tar-filename***.tar** *tar-filename***.tar** は、表示する tar ファイルです。
/xtract *source-url* **flash:**/*file-url* [*dir/file...*]	tar ファイルからローカル ファイル システムにファイルを抽出します。 *source-url* には、ローカル ファイル システムの*送信元* URL エイリアスを指定します。次のオプションがサポートされています。 • ローカル フラッシュ ファイル システムの構文： **flash:** • FTP の構文： **ftp:**[[//*username*[**:***password*]**@***location*]/*directory*]/*tar-filename***.tar** • HTTP サーバの構文： **http://**[[*username***:***password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name***.tar** • セキュア HTTP サーバの構文： **https://**[[*username***:***password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name***.tar** • RCP の構文： **rcp:**[[//*username***@***location*]/*directory*]/*tar-filename***.tar** • TFTP の構文： **tftp:**[[//*location*]/*directory*]/*tar-filename***.tar** *tar-filename***.tar** は、抽出される tar ファイルです。 **flash:**/*file-url* [*dir/file...*] には、tar ファイルが抽出されるローカル フラッシュ ファイル システムの場所を指定します。tar ファイルから抽出されるファイルまたはディレクトリのオプション リストを指定するには、*dir/file...* オプションを使用します。何も指定されないと、すべてのファイルとディレクトリが抽出されます。

デフォルト

デフォルト設定はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

イメージ名では、大文字と小文字が区別されます。

例

次の例では、tar ファイルを作成する方法を示します。このコマンドはローカル フラッシュ デバイスの *new-configs* ディレクトリの内容を、172.20.10.30 の TFTP サーバの *saved.tar* という名前のファイルに書き込みます。

```
Switch# archive tar /create tftp:172.20.10.30/saved.tar flash:/new_configs
```

次の例では、フラッシュ メモリに含まれるファイルの内容を表示する方法を示します。tar ファイルの内容が画面に表示されます。

```
Switch# archive tar /table flash:c3750-ipservices-12-25.SEB.tar
info (219 bytes)

c3750-ipservices-mz.12-25.SEB/ (directory)
c3750-ipservices-mz.12-25.SEB (610856 bytes)
c3750-ipservices-mz.12-25.SEB/info (219 bytes)
info.ver (219 bytes)
```

次の例では、*/html* ディレクトリおよびその内容だけを表示する方法を示します。

```
flash:c3750-ipservices-12-25.SEB.tar c3750-ipservices-12-25/html
c3750-ipservices-mz.12-25.SEB/html/ (directory)
c3750-ipservices-mz.12-25.SEB/html/const.htm (556 bytes)
c3750-ipservices-mz.12-25.SEB/html/xhome.htm (9373 bytes)
c3750-ipservices-mz.12-25.SEB/html/menu.css (1654 bytes)
<output truncated>
```

次の例では、172.20.10.30 のサーバにある tar ファイルの内容を抽出する方法を示します。ここでは、ローカル フラッシュ ファイル システムのルート ディレクトリに単に *new-configs* ディレクトリを抽出しています。*saved.tar* ファイルの残りのファイルは無視されます。

```
Switch# archive tar /xtract tftp://172.20.10.30/saved.tar flash:/new-configs
```

関連コマンド

コマンド	説明
archive copy-sw	あるスタック メンバのフラッシュ メモリから実行イメージを、別の 1 つ以上のスタック メンバ上のフラッシュ メモリにコピーします。
archive download-sw	TFTP サーバからスイッチに新しいイメージをダウンロードします。
archive upload-sw	スイッチの既存のイメージをサーバにアップロードします。

archive upload-sw

archive upload-sw 特権 EXEC コマンドを使用して、既存のスイッチ イメージをサーバにアップロードします。

archive upload-sw [**/source-system-num** *stack member number* | **/version** *version_string*] **destination-url**

構文の説明

/source-system-num *stack member number*	アップロードするイメージを持った特定のスタック メンバを指定します。
/version *version_string*	（任意）アップロードするイメージの特定バージョン文字列を指定します。
destination-url	ローカルまたはネットワーク ファイル システムの宛先 URL エイリアスです。次のオプションがサポートされています。 • スタンドアロン スイッチまたはスタック マスター上のローカル フラッシュ ファイル システムの構文： **flash:** スタック メンバ上のローカル フラッシュ ファイル システムの構文： **flash** *member number***:** • FTP の構文： **ftp:**[[//*username*[**:***password*]**@***location*]/*directory*]/*image-name***.tar** • HTTP サーバの構文： **http://**[[*username***:***password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name***.tar** • セキュア HTTP サーバの構文： **https://**[[*username***:***password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name***.tar** • Secure Copy Protocol（SCP）の構文： **scp:**[[//*username***@***location*]/*directory*]/*image-name***.tar** • Remote Copy Protocol（RCP）の構文： **rcp:**[[//*username***@***location*]/*directory*]/*image-name***.tar** • TFTP の構文： **tftp:**[[//*location*]/*directory*]/*image-name***.tar** *image-name***.tar** は、サーバに保存するソフトウェア イメージの名前です。

デフォルト

フラッシュ ファイル システムから現在稼動中のイメージをアップロードします。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

/version オプションを使用するためには、**/source-system-num** オプションを指定する必要があります。これらのオプションを同時に使用することで、指定のスタック メンバの特定のイメージ（実行イメージではない）をアップロードできます。

組み込みデバイス マネージャに関連付けられている HTML ファイルが既存のイメージとともにインストールされている場合にだけ、アップロード機能を使用します。

ファイルは、Cisco IOS イメージ、HTML ファイル、info の順序でアップロードされます。これらのファイルがアップロードされると、ソフトウェアは tar ファイルを作成します。

イメージ名では、大文字と小文字が区別されます。

例

次の例では、スタック メンバ 6 で現在実行中のイメージを、172.20.140.2 の TFTP サーバへアップロードする方法を示します。

```
Switch# archive upload-sw/source-system-num 6 tftp://172.20.140.2/test-image.tar
```

関連コマンド

コマンド	説明
archive copy-sw	あるスタック メンバのフラッシュ メモリから実行イメージを、別の 1 つ以上のスタック メンバ上のフラッシュ メモリにコピーします。
archive download-sw	新しいイメージをスイッチにダウンロードします。
archive tar	tar ファイルを作成し、tar ファイルのファイルを一覧表示し、tar ファイルからファイルを抽出します。

arp access-list

Address Resolution Protocol（ARP; アドレス解決プロトコル）Access Control List（ACL; アクセス コントロール リスト）を定義する場合、または以前定義したリストの最後にコマンドを追加する場合は、**arp access-list** グローバル コンフィギュレーション コマンドを使用します。指定された ARP 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。

arp access-list *acl-name*

no arp access-list *acl-name*

構文の説明

acl-name	ACL の名前

デフォルト

ARP アクセス リスト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

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

arp access-list コマンドを入力すると、ARP アクセス リスト コンフィギュレーション モードに入り、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設定に戻します。
- **deny**：パケットを拒否するように指定します。詳細については、「deny（ARP アクセスリスト コンフィギュレーション）」（P.2-124）を参照してください。
- **exit**：ARP アクセス リスト コンフィギュレーション モードを終了します。
- **no**：コマンドを無効にするか、デフォルト設定に戻します。
- **permit**：パケットを転送するように指定します。詳細については、「permit（ARP アクセスリスト コンフィギュレーション）」（P.2-407）を参照してください。

指定された一致条件に基づいて ARP パケットを転送またはドロップするには、**permit** または **deny** アクセス リスト コンフィギュレーション コマンドを使用します。

ARP ACL が定義されると、**ip arp inspection filter vlan** 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 VLAN（仮想 LAN）に ARP ACL を適用できます。IP/MAC アドレス 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。それ以外のすべてのパケット タイプは、検証されずに、入力 VLAN 内でブリッジングされます。ACL がパケットを許可すると、スイッチがパケットを転送します。明示的拒否ステートメントによって ACL がパケットを拒否すると、スイッチがパケットをドロップします。暗黙拒否ステートメントによって ACL がパケットを拒否すると、スイッチはパケットを DHCP バインディングのリストと比較します。ただし、ACL がスタティック（パケットがバインディングと比較されない）である場合を除きます。

例

次の例では、ARP アクセス リストを定義し、IP アドレスが 1.1.1.1 で MAC アドレスが 0000.0000.abcd のホストからの ARP 要求と ARP 応答の両方を許可する方法を示します。

```
Switch(config)# arp access-list static-hosts
Switch(config-arp-nacl)# permit ip host 1.1.1.1 mac host 00001.0000.abcd
Switch(config-arp-nacl)# end
```

設定を確認するには、**show arp access-list** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
deny（ARP アクセス リスト コンフィギュレーション）	DHCP バインディングとの比較による一致に基づいて ARP パケットを拒否します。
ip arp inspection filter vlan	スタティック IP アドレスで設定されたホストからの ARP 要求および応答を許可します。
permit（ARP アクセスリスト コンフィギュレーション）	DHCP バインディングとの比較による一致に基づいて ARP パケットを許可します。
show arp access-list	ARP アクセス リストに関する詳細を表示します。

authentication command bounce-port ignore

スイッチがポートを一時的にディセーブルにするコマンドを無視できるようにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **authentication command bounce-port ignore** グローバル コンフィギュレーション コマンドを使用します。デフォルトの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。

authentication command bounce-port ignore

no authentication command bounce-port ignore

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このスイッチは、RADIUS Change of Authorization（CoA; 権限変更）**bounce port** コマンドを受け入れます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(52)SE	このコマンドが追加されました。

使用上のガイドライン

CoA **bounce port** コマンドによってリンク フラップが発生し、ホストからの DHCP 再ネゴシエーションが作動します。これは VLAN 変更が発生した場合に有益であり、エンドポイントは、変更を検出するサプリカントを持たないプリンタなどのデバイスです。スイッチが **bounce port** コマンドを無視するように設定するには、このコマンドを使用します。

例

次の例では、スイッチが CoA **bounce port** コマンドを無視するように設定する方法を示します。

```
Switch(config)# authentication command bounce-port ignore
```

関連コマンド

コマンド	説明
authentication command disable-port ignore	スイッチが CoA **disable port** コマンドを無視するように設定します。

authentication command disable-port ignore

スイッチがポートをディセーブルにするコマンドを無視できるようにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **authentication command disable-port ignore** グローバル コンフィギュレーション コマンドを使用します。デフォルトの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。

authentication command disable-port ignore

no authentication command disable-port ignore

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このスイッチは、RADIUS Change of Authorization（CoA; 権限変更）**disable port** コマンドを受け入れます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(52)SE	このコマンドが追加されました。

使用上のガイドライン

CoA **disable port** コマンドはセッションをホスティングするポートを管理上シャットダウンし、セッションを終了させます。スイッチがこのコマンドを無視するように設定するには、このコマンドを使用します。

例

次の例では、スイッチが CoA **disable port** コマンドを無視するように設定する方法を示します。

```
Switch(config)# authentication command disable-port ignore
```

関連コマンド

コマンド	説明
authentication command bounce-port ignore	スイッチが CoA **bounce port** コマンドを無視するように設定します。

authentication control-direction

authentication control-direction インターフェイス コンフィギュレーション コマンドを使用して、ポート モードを単一方向または双方向に設定します。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。

authentication control-direction {both | in}

no authentication control-direction

構文の説明

both	ポートの双方向制御をイネーブルにします。ポートは、ホストにパケットを送受信できません。
in	ポートの単一方向制御をイネーブルにします。ポートは、ホストにパケットを送信できますが、受信はできません。

デフォルト

ポートは双方向モード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

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

デフォルト設定の双方向モードに戻すには、このコマンドの **both** キーワードまたは **no** 形式を使用します。

例

次の例では、双方向モードをイネーブルにする方法を示します。

```
Switch(config-if)# authentication control-direction both
```

次の例では、単一方向モードをイネーブルにする方法を示します。

```
Switch(config-if)# authentication control-direction in
```

show authentication 特権 EXEC コマンドを入力することにより、設定を確認できます。

関連コマンド

コマンド	説明
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。

コマンド	説明
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートの再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータと再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートにすでに最大数のデバイスが接続しているときに、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

authentication event

authentication event インターフェイス コンフィギュレーション コマンドを使用して、ポートの特定の認証イベントに関するアクションを設定します。

authentication event {**fail [action [authorize vlan** *vlan-id* | **next-method]** {| **retry {***retry count*}]} { **no-response action authorize vlan** *vlan-id*} {**server {alive action reinitialize**} | {**dead action** [**authorize** | **reinitialize vlan** *vlan-id*]}}

no authentication event {**fail [action [authorize vlan** *vlan-id* | **next-method]** {| **retry** {*retry count*}]} {**no-response action authorize vlan** *vlan-id*} {**server** {**alive action reinitialize**} | {**dead action** [**authorize** | **reinitialize vlan** *vlan-id*]}}

構文の説明

action	認証イベントの必須アクションを設定します。
alive	Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバ稼動アクションを設定します。
authorize	ポートを認証します。
dead	AAA サーバ停止アクションを設定します。
fail	失敗認証のパラメータを設定します。
next-method	次の認証方式に移動します。
no-response	非応答ホスト アクションを設定します。
reinitialize	認証済みクライアントすべてを再初期化します。
retry	失敗認証後の再試行の試行をイネーブルにします。
retry count	0 ～ 5 の再試行の回数です。
server	AAA サーバ イベントのアクションを設定します。
vlan	1 ～ 4094 で認証失敗 VLAN を指定します。
vlan-id	1 ～ 4094 の VLAN ID 番号です。

デフォルト

イベント応答はポートに設定されません。

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

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。
12.2(52)SE	**reinitialize** キーワードが追加されました。

使用上のガイドライン

このコマンドに **fail**、**no-response**、または **event** キーワードを付けて使用して、特定のアクションのスイッチ応答を設定します。

server-dead イベントの場合：

- スイッチが critical-authentication ステートに移ると、認証を試行している新しいホストが critical-authentication VLAN（または*クリティカル VLAN*）に移動されます。ポートがシングルホスト モード、マルチホスト モード、マルチ認証モード、または MDA モードの場合、これが適用されます。認証済みホストは認証済み VLAN に残り、再認証タイマーはディセーブルになります。
- クライアントで Windows XP を稼動し、クライアントが接続されているクリティカル ポートが critical-authentication ステートである場合、Windows XP はインターフェイスが認証されていないことを報告します。

  Windows XP クライアントに DHCP が設定されており、DHCP サーバからの IP アドレスが設定されている場合に、クリティカル ポートで EAP 認証成功メッセージを受信しても、DHCP 設定プロセスは再初期化できません。

no-response イベントの場合：

- IEEE 802.1x ポートでゲスト VLAN をイネーブルにした場合、認証サーバが Extensible Authentication Protocol over LAN（EAPOL）Request/Identity フレームに対する応答を受信しないか、EAPOL パケットがクライアントから送信されないと、スイッチではクライアントをゲスト VLAN に割り当てます。
- スイッチは EAPOL パケット履歴を保持します。リンクの存続時間内に別の EAPOL パケットがポート上で検出された場合、ゲスト VLAN 機能はディセーブルになります。ポートがすでにゲスト VLAN ステートにある場合、ポートは無許可ステートに戻り、認証が再開されます。EAPOL 履歴はクリアされます。
- スイッチ ポートがゲスト VLAN（マルチホスト モード）に移動されると、IEEE 802.1x 対応でないクライアントに、アクセスが許可されます。IEEE 802.1x 対応クライアントが、ゲスト VLAN を設定しているポートと同じポートに加わると、ポートは RADIUS 設定 VLAN またはユーザ設定アクセス VLAN の無許可ステートに移行し、認証が再開されます。

  Remote Switched Port Analyzer（RSPAN; リモート スイッチド ポート アナライザ）VLAN、プライマリ プライベート VLAN、または音声 VLAN 以外のアクティブなすべての VLAN は、IEEE 802.1x のゲスト VLAN として設定できます。ゲスト VLAN 機能は、アクセス ポートでだけサポートされます。内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされません。
- MAC 認証バイパスが IEEE 802.1x ポートでイネーブルの場合に、EAPOL メッセージ交換を待機している間に IEEE802.1x 認証が期限切れになると、スイッチでは、クライアントの MAC アドレスに基づいてクライアントを許可できます。スイッチは、IEEE 802.1x ポート上のクライアントを検出した後で、クライアントからのイーサネット パケットを待機します。スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。
  - 認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。
  - 認証に失敗すると、スイッチはポートにゲスト VLAN を割り当てます（指定されていない場合）。

  詳細については、ソフトウェア コンフィギュレーション ガイドの「Configuring IEEE802.1x Port-Based Authentication」の章の「Using IEEE 802.1x Authentication with MAC Authentication Bypass」の項を参照してください。

authentication-fail イベントの場合：

- サプリカントが認証に失敗すると、ポートは制限 VLAN に移動され、EAP 成功メッセージがサプリカントに送信されます。これは、サプリカントには実際の認証の失敗が通知されないためです。
  - EAP の成功メッセージが送信されない場合、サプリカントは 60 秒ごと（デフォルト）に EAP 開始メッセージを送信して認証を行おうとします。
  - 一部のホスト（たとえば、Windows XP を実行中のデバイス）は、EAP の成功メッセージを受け取るまで Dynamic Host Configuration Protocol（DHCP）を実装できません。

  制限 VLAN は、シングルホスト モード（デフォルトのポート モード）でだけサポートされます。ポートが制限 VLAN に配置されると、サプリカントの MAC アドレスが MAC アドレス テーブルに追加されます。ポート上の他の MAC アドレスはすべてセキュリティ違反として扱われます。
- レイヤ 3 ポートの内部 VLAN を制限 VLAN として設定することはできません。同じ VLAN を制限 VLAN としておよび音声 VLAN として指定することはできません。

  制限 VLAN による再認証をイネーブルにしてください。再認証がディセーブルにされていると、制限 VLAN に含まれているポートでは、ディセーブルにされている場合に再認証要求を受け取りません。

  再認証プロセスを開始するには、制限 VLAN がポートからリンクダウン イベントまたは Extensible Authentication Protocol（EAP）ログオフ イベントを受け取る必要があります。ホストがハブ経由で接続されている場合：
  - ホストが切断された場合にポートではリンクダウン イベントを受け取らないことがあります。
  - ポートでは、次の再認証試行が行われるまで、新しいホストを検出しないことがあります。

  制限 VLAN を異なるタイプの VLAN として再設定すると、制限 VLAN のポートも移行され、それらは現在認証されたステートのままになります。

例

次の例では、**authentication event fail** コマンドの設定方法を示します。

```
Switch(config-if)# authentication event fail action authorize vlan 20
```

次の例では、応答なしアクションの設定方法を示します。

```
Switch(config-if)# authentication event no-response action authorize vlan 10
```

次の例では、サーバ応答アクションの設定方法を示します。

```
Switch(config-if)# authentication event server alive action reinitialize
```

次の例では、RADIUS サーバが使用できない場合に、新規および既存のホストをクリティカル VLAN に送信するようポートを設定する方法を示します。マルチ認証（multiauth）モードのポートの場合、またはポートの音声ドメインが MDA モードである場合、このコマンドを使用します。

```
Switch(config-if)# authentication event server dead action authorize vlan 10
```

次の例では、RADIUS サーバが使用できない場合に、新規および既存のホストをクリティカル VLAN に送信するようポートを設定する方法を示します。マルチホスト モードまたはマルチ認証モードのポートの場合、このコマンドを使用します。

```
Switch(config-if)# authentication event server dead action reinitialize vlan 10
```

show authentication 特権 EXEC コマンドを入力することにより、設定を確認できます。

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートの再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータと再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

authentication fallback

authentication fallback インターフェイス コンフィギュレーション コマンドを使用して、IEEE 802.1x 認証をサポートしないクライアントに対し、Web 認証をフォールバック方式として使用するようにポートを設定します。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。

authentication fallback *name*

no authentication fallback *name*

構文の説明

name	Web 認証のフォールバック プロファイルを指定します。

デフォルト

フォールバックはイネーブルではありません。

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

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

フォールバック方式を設定する前に **authentication port-control auto** インターフェイス コンフィギュレーション コマンドを入力する必要があります。

Web 認証をフォールバック方式として設定できるのは、802.1x または MAB に対してだけです。したがってフォールバックできるようにするには、この認証方式の 1 つまたは両方を設定する必要があります。

例

次の例では、ポートのフォールバック プロファイルを指定する方法を示します。

```
Switch(config-if)# authentication fallback profile1
```

show authentication 特権 EXEC コマンドを入力することにより、設定を確認できます。

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルにします。

コマンド	説明
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータおよび再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

authentication host-mode

authentication host-mode インターフェイス コンフィギュレーション コマンドを使用して、ポートで認証マネージャ モードを設定します。

authentication host-mode [**multi-auth** | **multi-domain** | **multi-host** | **single-host**]

no authentication host-mode [**multi-auth** | **multi-domain** | **multi-host** | **single-host**]

構文の説明

multi-auth	ポートのマルチ認証モード（multiauth モード）をイネーブルにします。
multi-domain	ポートのマルチドメイン モードをイネーブルにします。
multi-host	ポートのマルチホスト モードをイネーブルにします。
single-host	ポートのシングルホスト モードをイネーブルにします。

デフォルト

シングルホスト モードがイネーブルにされています。

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

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

接続されているデータ ホストが 1 つだけの場合は、シングルホスト モードを設定する必要があります。シングルホスト ポートでの認証のために音声デバイスを接続しないでください。ポートで音声 VLAN が設定されていないと、音声デバイスの許可が失敗します。

データ ホストが IP Phone 経由でポートに接続されている場合は、マルチドメイン モードを設定する必要があります。音声デバイスを認証する必要がある場合は、マルチドメイン モードを設定する必要があります。

ハブ越しの 8 台までのデバイスに、個別の認証を通じて保護されたポート アクセスの取得を許可するには、マルチ認証モードを設定する必要があります。音声 VLAN が設定されている場合は、このモードで認証できる音声デバイスは 1 つだけです。

マルチホスト モードでも、ハブ越しの複数ホストのためのポート アクセスが提供されますが、マルチホスト モードでは、最初のユーザが認証された後でデバイスに対して無制限のポート アクセスが与えられます。

例

次の例では、ポートの**マルチ認証** モードをイネーブルにする方法を示します。

```
Switch(config-if)# authentication host-mode multi-auth
```

次の例では、ポートの**マルチドメイン** モードをイネーブルにする方法を示します。

```
Switch(config-if)# authentication host-mode multi-domain
```

次の例では、ポートの**マルチホスト** モードをイネーブルにする方法を示します。

```
Switch(config)# authentication host-mode multi-host
```

次の例では、ポートの**シングルホスト** モードをイネーブルにする方法を示します。

```
Switch(config-if)# authentication host-mode single-host
```

show authentication 特権 EXEC コマンドを入力することにより、設定を確認できます。

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータと再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

authentication mac-move permit

スイッチ上で MAC 移動をイネーブルにするには、**authentication mac-move permit** グローバル コンフィギュレーション 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。

authentication mac-move permit

no authentication mac-move permit

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

MAC 移動はイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(52)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、スイッチの 802.1x 対応ポート間で認証ホストを移動できます。たとえば、認証されたホストとポートの間にデバイスがあり、そのホストが別のポートに移動した場合、認証セッションは最初のポートから削除され、ホストは新しいポート上で再認証されます。

MAC 移動がディセーブルで、認証されたホストが別のポートに移動した場合、そのホストは再認証されず、違反エラーが発生します。

MAC 移動は、ポート セキュリティ対応の 802.1x ポートではサポートされません。MAC 移動がスイッチ上でグローバルに設定され、ポート セキュリティ対応ホストが 802.1x 対応ポートに移動した場合、違反エラーが発生します。

例

次の例では、スイッチ上で MAC 移動をイネーブルにする方法を示します。

```
Switch(config)# authentication mac-move permit
```

関連コマンド

コマンド	説明
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。
authentication order	ポートで使用する認証方式の順序を設定します。

コマンド	説明
authentication periodic	ポートの再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータと再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートにすでに最大数のデバイスが接続しているときに、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

authentication open

authentication open インターフェイス コンフィギュレーション コマンドを使用して、ポートでオープン アクセスをイネーブルまたはディセーブルにします。オープン アクセス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。

authentication open

no authentication open

デフォルト

オープン アクセスはディセーブルにされています。

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

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

認証の前にネットワーク アクセスを必要とするデバイスでは、オープン認証がイネーブルにされている必要があります。

オープン認証をイネーブルにしてあるときは、ポート ACL を使用してホスト アクセスを制限する必要があります。

例

次の例では、ポートのオープン アクセスをイネーブルにする方法を示します。

```
Switch(config-if)# authentication open
```

次の例では、ポートのオープン アクセスをディセーブルにするようポートを設定する方法を示します。

```
Switch(config-if)# no authentication open
```

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。

コマンド	説明
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータおよび再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

authentication order

authentication order インターフェイス コンフィギュレーション コマンドを使用して、ポートで使用する認証方式の順序を設定します。

authentication order [**dot1x** | **mab**] {**webauth**}

no authentication order

構文の説明

dot1x	認証方式の順序に 802.1x を追加します。
mab	認証方式の順序に MAC 認証バイパス（MAB）を追加します。
webauth	認証方式の順序に Web 認証を追加します。

コマンド デフォルト

デフォルトの認証順序は **dot1x**、**mab**、および **webauth** の順です。

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

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

順序付けでは、スイッチがポートに接続された新しいデバイスを認証しようとするときに試行する方式の順序を設定します。リスト内の方式の 1 つで成功しないと、次の方式が試行されます。

各方式は一度だけ試行できます。弾力的順序付けは、802.1x と MAB の間でだけ可能です。

Web 認証は、スタンドアロン方式として設定するか、順序において 802.1x または MAB のいずれかの後で最後の方式として設定することができます。Web 認証は **dot1x** または **mab** に対するフォールバックとしてだけ設定する必要があります。

例

次の例では、最初の認証方式として 802.1x を、2 番目の方式として MAB を、3 番目の方式として Web 認証を追加する方法を示します。

```
Switch(config-if)# authentication order dotx mab webauth
```

次の例では、最初の認証方式として MAC 認証バイパス（MAB）を、2 番目の認証方式として Web 認証を追加する方法を示します。

```
Switch(config-if)# authentication order mab webauth
```

show authentication 特権 EXEC コマンドを入力することにより、設定を確認できます。

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータおよび再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
mab	ポートの MAC 認証バイパスをイネーブルにします。
mab eap	Extensible Authentication Protocol（EAP）を使用するようポートを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

authentication periodic

authentication periodic インターフェイス コンフィギュレーション コマンドを使用して、ポートで再認証をイネーブルまたはディセーブルにします。再認証をディセーブルにする場合は、このコマンドの **no** 形式を入力します。

authentication periodic

no authentication periodic

コマンド デフォルト

再認証はディセーブルにされています。

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

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

authentication timer reauthentication インターフェイス コンフィギュレーション コマンドを使用して、定期的に再認証を行う間隔の時間量を設定します。

例

次の例では、ポートの定期的再認証をイネーブルにする方法を示します。

```
Switch(config-if)# authentication periodic
```

次の例では、ポートの定期的再認証をディセーブルにする方法を示します。

```
Switch(config-if)# no authentication periodic
```

show authentication 特権 EXEC コマンドを入力することにより、設定を確認できます。

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。

コマンド	説明
authentication timer	802.1x 対応ポートのタイムアウト パラメータおよび再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

authentication port-control

authentication port-control インターフェイス コンフィギュレーション コマンドを使用して、ポート許可ステートの手動制御をイネーブルにします。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。

authentication port-control {**auto** | **force-authorized** | **force-un authorized**}

no authentication port-control {**auto** | **force-authorized** | **force-un authorized**}

構文の説明

auto	ポートの IEEE 802.1x 認証をイネーブルにします。ポートは、IEEE 802.1x 認証情報のスイッチとクライアントの間での交換に基づいて、許可ステートまたは無許可ステートに変わります。
force-authorized	ポートの IEEE 802.1x 認証をディセーブルにします。ポートは、認証情報を交換することなく、許可ステートに変わります。ポートはクライアントとの IEEE 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。
force-un authorized	ポートへのアクセスをすべて拒否します。ポートは、クライアントによる認証の試行をすべて無視して、無許可ステートに変わります。スイッチはポートを介してクライアントに認証サービスを提供できません。

デフォルト

デフォルトの設定は force-authorized 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

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

auto キーワードは、次のいずれかのポート タイプでだけ使用してください。

- トランク ポート：トランク ポートで IEEE 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートのモードをトランクに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。
- ダイナミック ポート：ダイナミック ポートは、ネイバーとネゴシエートして、トランク ポートになることができます。ダイナミック ポートで IEEE 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x 認証はイネーブルになりません。IEEE 802.1x 対応ポートのモードをダイナミックに変更しようとすると、エラー メッセージが表示され、ポート モードは変更されません。
- ダイナミック アクセス ポート：ダイナミック アクセス（VLAN Query Protocol（VQP））ポートで IEEE 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x 認証はイネーブルになりません。IEEE 802.1x 対応ポートをダイナミック VLAN に変更しようとすると、エラー メッセージが表示され、VLAN 設定は変更されません。

- EtherChannel ポート：アクティブまたはアクティブでない EtherChannel メンバであるポートを IEEE 802.1x ポートとして設定しないでください。EtherChannel ポートで IEEE 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x 認証はイネーブルになりません。
- Switched Port Analyzer（SPAN）および Remote SPAN（RSPAN）宛先ポート：SPAN または RSPAN 宛先ポートであるポートの IEEE 802.1x 認証をイネーブルにすることができます。ただし、そのポートが SPAN または RSPAN 宛先として削除されるまで、IEEE 802.1x 認証はディセーブルのままです。SPAN または RSPAN 送信元ポートでは IEEE 802.1x 認証をイネーブルにすることができます。

スイッチで IEEE 802.1x 認証をグローバルにディセーブルにするには、**no dot1x system-auth-control** グローバル コンフィギュレーション コマンドを使用します。特定のポートで IEEE 802.1x 認証をディセーブルにするか、デフォルト設定に戻すには、**no authentication port-control** 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。

例

次の例では、ポート ステートを自動に設定する方法を示します。

```
Switch(config-if)# authentication port-control auto
```

次の例では、ポート ステートを force- authorized ステートに設定する方法を示します。

```
Switch(config-if)# authentication port-control force-authorized
```

次の例では、ポート ステートを force-unauthorized ステートに設定する方法を示します。

```
Switch(config-if)# authentication port-control force-unauthorized
```

show authentication 特権 EXEC コマンドを入力することにより、設定を確認できます。

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータと再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

authentication priority

authentication priority インターフェイス コンフィギュレーション コマンドを使用して、ポート プライオリティ リストに認証方式を追加します。

auth priority [**dot1x** | **mab**] {**webauth**}

no auth priority [**dot1x** | **mab**] {**webauth**}

構文の説明

dot1x	認証方式の順序に 802.1x を追加します。
mab	認証方式の順序に MAC 認証バイパス（MAB）を追加します。
webauth	認証方式の順序に Web 認証を追加します。

コマンド デフォルト

デフォルトのプライオリティは、802.1x 認証、MAC 認証バイパス、Web 認証の順です。

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

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

順序付けでは、スイッチがポートに接続された新しいデバイスを認証しようとするときに試行する方式の順序を設定します。

ポートにフォールバック方式を複数設定するときは、Web 認証（webauth）を最後に設定してください。

異なる認証方式にプライオリティを割り当てることにより、プライオリティの高い方式を、プライオリティの低い進行中の認証方式に割り込ませることができます。

（注）　クライアントがすでに認証されている場合に、プライオリティの高い方式の割り込みが発生すると、再認証されることがあります。

認証方式のデフォルトのプライオリティは、実行リストの順序におけるその位置と同じで、802.1x 認証、MAC 認証バイパス、Web 認証の順です。このデフォルトの順序を変更するには、キーワード **dot1x**、**mab**、および **webauth** を使用します。

例

次の例では、802.1x を最初の認証方式、Web 認証を 2 番目の認証方式として設定する方法を示します。

```
Switch(config-if)# authentication priority dotx webauth
```

次の例では、MAC 認証バイパス（MAB）を最初の認証方式、Web 認証を 2 番目の認証方式として設定する方法を示します。

```
Switch(config-if)# authentication priority mab webauth
```

show authentication 特権 EXEC コマンドを入力することにより、設定を確認できます。

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication timer	802.1x 対応ポートのタイムアウト パラメータと再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
mab	ポートの MAC 認証バイパスをイネーブルにします。
mab eap	Extensible Authentication Protocol（EAP）を使用するようポートを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

authentication timer

authentication timer インターフェイス コンフィギュレーション コマンドを使用して、802.1x 対応ポートのタイムアウトと再認証のパラメータを設定します。

authentication timer {{[**inactivity** | **reauthenticate**] [**server** | *am*]} {**restart** *value*}}

no authentication timer {{[**inactivity** | **reauthenticate**] [**server** | *am*]} {**restart** *value*}}

構文の説明

inactivity	この時間間隔を過ぎてもアクティビティがない場合に、クライアントが無許可にされる秒数です。
reauthenticate	自動再認証の試行が開始されるまで時間（秒）です。
server	無許可ポートの認証の試行が行われるまでの間隔（秒）です。
restart	無許可ポートの認証の試行が行われるまでの間隔（秒）です。
value	1 から 65535 までの値（秒）を入力します。

デフォルト

キーワード **inactivity**、**server**、および **restart** は、オフに設定されます。**reauthenticate** キーワードは 1 時間に設定されます。

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

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

タイムアウト値を設定しないと、802.1x セッションは、無期限で認証されたままになります。他のホストではそのポートを使用できず、接続されているホストは、同じスイッチの別のポートに移動できません。

例

次の例では、認証非アクティビティ タイマーを 60 秒に設定する方法を示します。

```
Switch(config-if)# authentication timer inactivity 60
```

次の例では、再認証タイマーを 120 秒に設定する方法を示します。

```
Switch(config-if)# authentication timer restart 120
```

show authentication 特権 EXEC コマンドを入力することにより、設定を確認できます。

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。

コマンド	説明
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

authentication violation

authentication violation インターフェイス コンフィギュレーション コマンドを使用して、新しいデバイスがポートに接続するとき、または最大数のデバイスがポートに接続されている状態で新しいデバイスがポートに接続するときに発生する違反モードを設定します。

authentication violation {**protect** | **replace** | **restrict** | **shutdown**}

no authentication violation {**protect** | **replace** | **restrict** | **shutdown**}

構文の説明

protect	予期しない着信 MAC アドレスはドロップされます。syslog エラーは生成されません。
replace	現在のセッションを削除し、新しいホストによる認証を開始します。
restrict	違反エラーの発生時に Syslog エラーを生成します。
shutdown	エラーによって、予期しない MAC アドレスが発生するポートまたは仮想ポートがディセーブルになります。

デフォルト

デフォルトでは、**authentication violation shutdown** モードはイネーブルです。

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

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。
12.2(55)SE	**replace** キーワードが追加されました。

例

次の例では、新しいデバイスがポートに接続する場合に、errdisable になり、シャットダウンするように IEEE 802.1x 対応ポートを設定する方法を示します。

```
Switch(config-if)# authentication violation shutdown
```

次の例では、新しいデバイスがポートに接続する場合に、システム エラー メッセージを生成して、ポートを制限モードに変更するように 802.1x 対応ポートを設定する方法を示します。

```
Switch(config-if)# authentication violation restrict
```

次の例では、新しいデバイスがポートに接続するときに、そのデバイスを無視するように 802.1x 対応ポートを設定する方法を示します。

```
Switch(config-if)# authentication violation protect
```

次の例では、新しいデバイスがポートに接続するときに、現在のセッションを削除し、新しいデバイスによる認証を開始するように 802.1x 対応ポートを設定する方法を示します。

```
Switch(config-if)# authentication violation replace
```

show authentication 特権 EXEC コマンドを入力することにより、設定を確認できます。

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータと再認証パラメータを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

auto qos classify

Quality of Service（QoS）ドメイン内で信頼できないデバイスの QoS 分類を自動設定するには、**auto qos classify** 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。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。

auto qos classify [**police**]

no auto qos classify [**police**]

構文の説明

police	（任意）信頼できないデバイスの QoS ポリシングを設定します。

デフォルト

auto-QoS 分類は、すべてのポートでディセーブルです。

auto-QoS がイネーブルの場合は、入力パケットのラベルを使用して、トラフィックの分類、パケットラベルの割り当て、および入力/出力キューの設定を行います。

表 2-1　入力キューに対する Auto-QoS の設定

入力キュー	キュー番号	CoS からキューへのマッピング	キューの重み（帯域幅）	キュー（バッファ）サイズ
SRR [1] 共有	1	0、1、2、3、6、7	70%	90%
プライオリティ	2	4、5	30%	10%

1. SRR = Shaped Round Robin。入力キューは共有モードだけをサポートします。

表 2-2 に、出力キューに対して生成される auto-QoS の設定を示します。

表 2-2　出力キューに対する auto-QoS の設定

出力キュー	キュー番号	CoS からキューへのマッピング	キューの重み（帯域幅）	ギガビット対応ポートのキュー（バッファ）サイズ	10/100 イーサネット ポートのキュー（バッファ）サイズ
プライオリティ（シェイプド）	1	4、5	最大 100%	25%	15%
SRR 共有	2	2、3、6、7	10%	25%	25%
SRR 共有	3	0	60%	25%	40%
SRR 共有	4	1	20%	25%	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

コマンド履歴

リリース	変更内容
12.2(55)SE	このコマンドが追加されました。

使用上のガイドライン

QoS ドメイン内の信頼インターフェイスに QoS を設定する場合は、このコマンドを使用します。QoS ドメインには、スイッチ、ネットワーク内部、QoS の着信トラフィックを分類することのできるエッジ装置などが含まれます。

Auto-QoS は、スイッチが信頼インターフェイスと接続するように設定します。着信パケットの QoS ラベルは信頼されます。非ルーテッド ポートの場合は、着信パケットの CoS 値が信頼されます。ルーテッド ポートでは、着信パケットの DSCP 値が信頼されます。

auto-QoS のデフォルトを利用するには、auto-QoS をイネーブルにしてから、その他の QoS コマンドを設定する必要があります。auto-QoS をイネーブルにした*後*で、auto-QoS を調整できます。

これは、**auto qos classify** コマンドが設定されている場合のポリシー マップです。

```
policy-map AUTOQOS-SRND4-CLASSIFY-POLICY
class AUTOQOS_MULTIENHANCED_CONF_CLASS
set dscp af41
class AUTOQOS_BULK_DATA_CLASS
set dscp af11
class AUTOQOS_TRANSACTION_CLASS
set dscp af21
class AUTOQOS_SCAVANGER_CLASS
set dscp cs1
class AUTOQOS_SIGNALING_CLASS
set dscp cs3
class AUTOQOS_DEFAULT_CLASS
set dscp default
```

これは、**auto qos classify police** コマンドが設定されている場合のポリシー マップです。

```
policy-map AUTOQOS-SRND4-CLASSIFY-POLICE-POLICY
class AUTOQOS_MULTIENHANCED_CONF_CLASS
set dscp af41
police 5000000 8000 exceed-action drop
class AUTOQOS_BULK_DATA_CLASS
set dscp af11
police 10000000 8000 exceed-action policed-dscp-transmit
class AUTOQOS_TRANSACTION_CLASS
set dscp af21
police 10000000 8000 exceed-action policed-dscp-transmit
class AUTOQOS_SCAVANGER_CLASS
set dscp cs1
police 10000000 8000 exceed-action drop
class AUTOQOS_SIGNALING_CLASS
set dscp cs3
police 32000 8000 exceed-action drop
class AUTOQOS_DEFAULT_CLASS
set dscp default
police 10000000 8000 exceed-action policed-dscp-transmit
```

（注） スイッチは、Command-Line Interface（CLI; コマンドライン インターフェイス）からコマンドが入力された場合と同じように、auto-QoS によって生成されたコマンドを適用します。既存のユーザ設定では、生成されたコマンドの適用に失敗することがあります。また、生成されたコマンドで既存の設定が上書きされることもあります。これらのアクションは、警告を表示せずに実行されます。生成されたコマンドがすべて正常に適用された場合、上書きされなかったユーザ入力の設定は実行コンフィギュレーション内に残ります。上書きされたユーザ入力の設定は、現在の設定をメモリに保存せずに、スイッチをリロードすると復元できます。生成されたコマンドの適用に失敗した場合は、前の実行コンフィギュレーションが復元されます。

auto-QoS をイネーブルにした後、名前に *AutoQoS* を含むポリシー マップや集約ポリサーを変更しないでください。ポリシー マップや集約ポリサーを変更する必要がある場合、そのコピーを作成し、コピーしたポリシー マップやポリサーを変更します。生成されたポリシー マップの代わりに新しいポリシー マップを使用するには、生成したポリシー マップをインターフェイスから削除して、新しいポリシー マップを適用します。

auto-QoS がイネーブルのときに自動的に生成される Quality of Service（QoS）の設定を表示するには、auto-QoS をイネーブルにする前にデバッグをイネーブルにします。**debug auto qos** 特権 EXEC コマンドを使用すると、auto-QoS のデバッギングがイネーブルになります。詳細については、**debug auto qos** コマンドを参照してください。

ポートの auto-QoS をディセーブルにするには、**no auto qos trust** 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。このポートに対して、auto-QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが削除されます。auto-QoS をイネーブルにした最後のポートで、**no auto qos trust** コマンドを入力すると、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドが残っている場合でも、auto-QoS はディセーブルと見なされます（グローバル コンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため）。**no mls qos** 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、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドをディセーブルにできます。QoS がディセーブルの場合は、パケットが変更されないため、信頼できるポートまたは信頼できないポートといった概念はありません。パケット内の CoS、DSCP、および IP precedence 値は変更されません。トラフィックは Pass-Through モードでスイッチングされます。パケットは書き換えられることなくスイッチングされ、ポリシングなしのベスト エフォートに分類されます。

例

次の例では、信頼できないデバイスの auto-QoS 分類をイネーブルにし、トラフィックをポリシングする方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos classify police
```

設定を確認するには、**show auto qos interface** *interface-id* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
debug auto qos	auto-QoS 機能のデバッグをイネーブルにします。
mls qos trust	ポートの信頼状態を設定します。
srr-queue bandwidth share	共有する重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅の共有をイネーブルにします。
queue-set	ポートをキューセットにマッピングします。
show auto qos	auto-QoS 情報を表示します。
show mls qos interface	ポート レベルで QoS 情報を表示します。

auto qos trust

Quality of Service（QoS）ドメイン内で信頼できるインターフェイスの QoS 分類を自動設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で、**auto qos trust** 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。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。

auto qos trust {cos | dscp}

no auto qos trust {cos | dscp}

構文の説明

cos	CoS パケット分類を信頼します。
dscp	DSCP パケット分類を信頼します。

デフォルト

auto-QoS 信頼は、すべてのポートでディセーブルです。

auto-QoS がイネーブルの場合は、入力パケットのラベルを使用して、トラフィックの分類、パケット ラベルの割り当て、および入力/出力キューの設定を行います。

表 2-3　トラフィック タイプ、パケット ラベル、およびキュー

	VoIP データ トラフィック	VoIP コントロール トラフィック	ルーティング プロトコル トラフィック	STP[1] BPDU[2] トラフィック	リアルタイム ビデオ トラフィック	その他すべてのトラフィック	
DSCP[3]	46	24、26	48	56	34	–	
CoS[4]	5	3	6	7	3	–	
CoS から入力キューへのマッピング	4、5（キュー 2）					0、1、2、3、6、7（キュー 1）	
CoS から出力キューへのマッピング	4、5（キュー 1）	2、3、6、7（キュー 2）			0（キュー 3）	2（キュー 3）	0、1（キュー 4）

1. STP = Spanning-Tree Protocol（スパニング ツリー プロトコル）
2. BPDU = Bridge Protocol Data Unit（ブリッジ プロトコル データ ユニット）
3. DSCP = Differentiated Service Code Point（Diffserv コード ポイント）
4. CoS = Class of Service（サービス クラス）

表 2-4　入力キューに対する Auto-QoS の設定

入力キュー	キュー番号	CoS からキューへのマッピング	キューの重み（帯域幅）	キュー（バッファ）サイズ
SRR [1] 共有	1	0、1、2、3、6、7	70%	90%
プライオリティ	2	4、5	30%	10%

1. SRR = Shaped Round Robin。入力キューは共有モードだけをサポートします。

表 2-5　出力キューに対する auto-QoS の設定

出力キュー	キュー番号	CoS からキューへのマッピング	キューの重み（帯域幅）	ギガビット対応ポートのキュー（バッファ）サイズ	10/100 イーサネット ポートのキュー（バッファ）サイズ
プライオリティ（シェイプド）	1	4、5	最大 100%	25%	15%
SRR 共有	2	2、3、6、7	10%	25%	25%
SRR 共有	3	0	60%	25%	40%
SRR 共有	4	1	20%	25%	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

コマンド履歴

リリース	変更内容
12.2(55)SE	このコマンドが追加されました。

使用上のガイドライン

QoS ドメイン内の信頼インターフェイスに QoS を設定する場合は、このコマンドを使用します。QoS ドメインには、スイッチ、ネットワーク内部、QoS の着信トラフィックを分類することのできるエッジ装置などが含まれます。

Auto-QoS は、スイッチが信頼インターフェイスと接続するように設定します。着信パケットの QoS ラベルは信頼されます。非ルーテッド ポートの場合は、着信パケットの CoS 値が信頼されます。ルーテッド ポートでは、着信パケットの DSCP 値が信頼されます。

auto-QoS のデフォルトを利用するには、auto-QoS をイネーブルにしてから、その他の QoS コマンドを設定する必要があります。auto-QoS をイネーブルにした*後*で、auto-QoS を調整できます。

ポートに auto-QoS 信頼が設定されると、ポートはポート上のすべてのパケットを信頼します。パケットに DSCP または CoS 値がマーキングされていない場合、デフォルトのマーキングが実行されます。

（注）スイッチは、Command-Line Interface（CLI; コマンドライン インターフェイス）からコマンドが入力された場合と同じように、auto-QoS によって生成されたコマンドを適用します。既存のユーザ設定では、生成されたコマンドの適用に失敗することがあります。また、生成されたコマンドで既存の設定が上書きされることもあります。これらのアクションは、警告を表示せずに実行されます。生成されたコマンドがすべて正常に適用された場合、上書きされなかったユーザ入力の設定は実行コンフィギュレーション内に残ります。上書きされたユーザ入力の設定は、現在の設定をメモリに保存せずに、スイッチをリロードすると復元できます。生成されたコマンドの適用に失敗した場合は、前の実行コンフィギュレーションが復元されます。

auto-QoS をイネーブルにした後、名前に *AutoQoS* を含むポリシー マップや集約ポリサーを変更しないでください。ポリシー マップや集約ポリサーを変更する必要がある場合、そのコピーを作成し、コピーしたポリシー マップやポリサーを変更します。生成されたポリシー マップの代わりに新しいポリシー マップを使用するには、生成したポリシー マップをインターフェイスから削除して、新しいポリシー マップを適用します。

auto-QoS がイネーブルのときに自動的に生成される Quality of Service（QoS）の設定を表示するには、auto-QoS をイネーブルにする前にデバッグをイネーブルにします。**debug auto qos** 特権 EXEC コマンドを使用すると、auto-QoS のデバッギングがイネーブルになります。詳細については、**debug auto qos** コマンドを参照してください。

ポートの auto-QoS をディセーブルにするには、**no auto qos trust** 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。このポートに対して、auto-QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが削除されます。auto-QoS をイネーブルにした最後のポートで、**no auto qos trust** コマンドを入力すると、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドが残っている場合でも、auto-QoS はディセーブルと見なされます（グローバル コンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため）。**no mls qos** 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、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドをディセーブルにできます。QoS がディセーブルの場合は、パケットが変更されない（パケット内の CoS、DSCP、および IP precedence 値は変更されない）ため、信頼できるポートまたは信頼できないポートといった概念はありません。トラフィックは Pass-Through モードでスイッチングされます（パケットは書き換えられることなくスイッチングされ、ポリシングなしのベスト エフォートに分類されます）。

例

次の例では、特定の cos 分類を持つ信頼できるインターフェイスの auto-QoS をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# auto qos trust cos
```

設定を確認するには、**show auto qos interface** *interface-id* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
debug auto qos	auto-QoS 機能のデバッグをイネーブルにします。
mls qos trust	ポートの信頼状態を設定します。
srr-queue bandwidth share	共有する重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅の共有をイネーブルにします。
queue-set	ポートをキューセットにマッピングします。
show auto qos	auto-QoS 情報を表示します。
show mls qos interface	ポート レベルで QoS 情報を表示します。

auto qos voip

auto qos voip インターフェイス コンフィギュレーション コマンドを使用して、Quality of Service（QoS）ドメイン内で Voice over IP（VoIP）の QoS を自動設定します。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。

auto qos voip {**cisco-phone** | **cisco-softphone** | **trust**}

no auto qos voip [**cisco-phone** | **cisco-softphone** | **trust**]

構文の説明

cisco-phone	このポートが Cisco IP Phone に接続されていると判断し、VoIP の QoS を自動設定します。着信パケットの QoS ラベルが信頼されるのは、IP Phone が検知される場合に限ります。このキーワードは、10 ギガビット イーサネット インターフェイスではサポートされません。
cisco-softphone	このポートが Cisco SoftPhone が動作している装置に接続されていると判断し、VoIP の QoS を自動設定します。このキーワードは、10 ギガビット イーサネット インターフェイスではサポートされません。
trust	このポートが信頼できるスイッチまたはルータに接続されていると判断し、自動的に VoIP の QoS を設定します。着信パケットの QoS ラベルは信頼されます。非ルーテッド ポートの場合は、着信パケットの CoS 値が信頼されます。ルーテッド ポートでは、着信パケットの DSCP 値が信頼されます。

デフォルト

auto-QoS がイネーブルの場合は、入力パケットのラベルを使用して、トラフィックの分類、パケット ラベルの割り当て、および入力 / 出力キューの設定を行います。

表 2-6　トラフィック タイプ、パケット ラベル、およびキュー

	VoIP データ トラフィック	VoIP コントロール トラフィック	ルーティング プロトコル トラフィック	STP[1] BPDU[2] トラフィック	リアルタイム ビデオ トラフィック	その他すべてのトラフィック	
DSCP[3]	46	24、26	48	56	34	–	
CoS[4]	5	3	6	7	3	–	
CoS から入力キューへのマッピング	4、5（キュー 2）					0、1、2、3、6、7（キュー 1）	
CoS から出力キューへのマッピング	4、5（キュー 1）	2、3、6、7（キュー 2）			0（キュー 3）	2（キュー 3）	0、1（キュー 4）

1. STP = Spanning-Tree Protocol（スパニング ツリー プロトコル）
2. BPDU = Bridge Protocol Data Unit（ブリッジ プロトコル データ ユニット）
3. DSCP = Differentiated Service Code Point（Diffserv コード ポイント）
4. CoS = Class of Service（サービス クラス）

表 2-7　入力キューに対する Auto-QoS の設定

入力キュー	キュー番号	CoS からキューへのマッピング	キューの重み（帯域幅）	キュー（バッファ）サイズ
SRR [1] 共有	1	0、1、2、3、6、7	70%	90%
プライオリティ	2	4、5	30%	10%

1. SRR = Shaped Round Robin。入力キューは共有モードだけをサポートします。

表 2-8　出力キューに対する auto-QoS の設定

出力キュー	キュー番号	CoS からキューへのマッピング	キューの重み（帯域幅）	ギガビット対応ポートのキュー（バッファ）サイズ	10/100 イーサネット ポートのキュー（バッファ）サイズ
プライオリティ（シェイプド）	1	4、5	最大 100%	25%	15%
SRR 共有	2	2、3、6、7	10%	25%	25%
SRR 共有	3	0	60%	25%	40%
SRR 共有	4	1	20%	25%	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

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。
12.2(20)SE	**cisco-softphone** キーワードが追加され、生成される auto-QoS の設定が変更されました。
12.2(40)SE	コマンド出力の情報が変更されました。
12.2(55)SE	拡張 auto-QoS のサポートが追加されました。

使用上のガイドライン

QoS ドメイン内の VoIP トラフィックに適切な QoS を設定する場合は、このコマンドを使用します。QoS ドメインには、スイッチ、ネットワーク内部、QoS の着信トラフィックを分類することのできるエッジ装置などが含まれます。

Auto-QoS は、スイッチとルーテッド ポート上の Cisco IP Phone を使用した VoIP と、Cisco SoftPhone アプリケーションが稼動する装置を使用した VoIP に対してスイッチを設定します。これらのリリースは Cisco IP SoftPhone バージョン 1.3(3) 以降だけをサポートします。接続される装置は Cisco Call Manager バージョン 4 以降を使用する必要があります。

show auto qos コマンド出力は Cisco IP Phone のサービス ポリシー情報を表示します。

auto-QoS のデフォルトを利用するには、auto-QoS をイネーブルにしてから、その他の QoS コマンドを設定する必要があります。auto-QoS をイネーブルにした*後*で、auto-QoS を調整できます。

（注）スイッチは、Command-Line Interface（CLI; コマンドライン インターフェイス）からコマンドが入力された場合と同じように、auto-QoS によって生成されたコマンドを適用します。既存のユーザ設定では、生成されたコマンドの適用に失敗することがあります。また、生成されたコマンドで既存の設定が上書きされることもあります。これらのアクションは、警告を表示せずに実行されます。生成されたコマンドがすべて正常に適用された場合、上書きされなかったユーザ入力の設定は実行コンフィギュレーション内に残ります。上書きされたユーザ入力の設定は、現在の設定をメモリに保存せずに、スイッチをリロードすると復元できます。生成されたコマンドの適用に失敗した場合は、前の実行コンフィギュレーションが復元されます。

これが auto-QoS をイネーブルにする最初のポートの場合は、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドに続いてインターフェイス コンフィギュレーション コマンドが実行されます。別のポートで auto-QoS をイネーブルにすると、そのポートに対して auto-QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが実行されます。

最初のポートで auto-QoS 機能をイネーブルにすると、次の自動アクションが実行されます。

- QoS はグローバルにイネーブル化され（**mls qos** グローバル コンフィギュレーション コマンド）、その他のグローバル コンフィギュレーション コマンドが追加されます。
- Cisco IP Phone に接続されたネットワーク エッジのポートで **auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドを入力すると、スイッチにより信頼境界の機能がイネーブルになります。スイッチは、Cisco Discovery Protocol（CDP）を使用して、Cisco IP Phone が存在するかしないかを検出します。Cisco IP Phone が検出されると、ポートの入力分類は、パケットで受け取った QoS ラベルを信頼するように設定されます。また、スイッチはポリシングを使用してパケットがプロファイル内か、プロファイル外かを判断し、パケットに対するアクションを指定します。パケットに 24、26、または 46 という DSCP 値がない場合、またはパケットがプロファイル外にある場合、スイッチは DSCP 値を 0 に変更します。Cisco IP Phone がない場合、入力分類は、パケットの QoS ラベルを信頼しないように設定されます。スイッチは、ポートの入力キューと出力キューを、表 2-7 および表 2-8 の設定値に従って設定します。ポリシングがポリシーマップ分類と一致したトラフィックに適用された後で、スイッチが信頼境界の機能をイネーブルにします。

  スイッチ ポートが Cisco IOS Release 12.2(37)SE かそれよりも前のリリースで **auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドを使用して設定された場合、auto-QoS によって Cisco IOS Release 12.2(40)SE に新しく生成されたコマンドは、ポートに適用されません。このようなコマンドを自動的に適用するには、設定を削除してからポートに再度適用する必要があります。
- Cisco SoftPhone が動作する装置に接続されたネットワーク エッジにあるポートに **auto qos voip cisco-softphone** インターフェイス コンフィギュレーション コマンドを入力した場合、スイッチはポリシングを使用してパケットがプロファイル内かプロファイル外かを判断し、パケットに対するアクションを指定します。パケットに 24、26、または 46 という DSCP 値がない場合、またはパケットがプロファイル外にある場合、スイッチは DSCP 値を 0 に変更します。スイッチは、ポートの入力キューと出力キューを、表 2-7 および表 2-8 の設定値に従って設定します。
- ネットワーク内部に接続されたポート上で、**auto qos voip trust** インターフェイス コンフィギュレーション コマンドを入力した場合、スイッチは、入力パケットでルーティングされないポートの CoS 値、またはルーテッド ポートの DSCP 値を信頼します（トラフィックが他のエッジ装置ですでに分類されていることが前提条件になります）。スイッチは、ポートの入力キューと出力キューを、表 2-7 および表 2-8 の設定値に従って設定します。

スタティック ポート、ダイナミック アクセス ポート、音声 VLAN アクセス ポート、およびトランク ポートで auto-QoS をイネーブルにすることができます。ルーテッド ポートにある Cisco IP Phone で auto-QoS をイネーブルにする場合、スタティック IP アドレスを IP Phone に割り当てる必要があります。

（注）Cisco SoftPhone が稼動する装置がスイッチまたはルーテッド ポートに接続されている場合、スイッチはポートごとに 1 つの Cisco SoftPhone アプリケーションだけをサポートします。

auto-QoS をイネーブルにした後、名前に *AutoQoS* を含むポリシー マップや集約ポリサーを変更しないでください。ポリシー マップや集約ポリサーを変更する必要がある場合、そのコピーを作成し、コピーしたポリシー マップやポリサーを変更します。生成されたポリシー マップの代わりに新しいポリシー マップを使用するには、生成したポリシー マップをインターフェイスから削除して、新しいポリシー マップを適用します。

auto-QoS がイネーブルのときに自動的に生成される QoS の設定を表示するには、auto-QoS をイネーブルにする前にデバッグをイネーブルにします。**debug auto qos** 特権 EXEC コマンドを使用すると、auto-QoS のデバッギングがイネーブルになります。

ポートの auto-QoS をディセーブルにするには、**no auto qos voip** 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。このポートに対して、auto-QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが削除されます。auto-QoS をイネーブルにした最後のポートで、**no auto qos voip** コマンドを入力すると、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドが残っている場合でも、auto-QoS はディセーブルと見なされます（グローバル コンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため）。**no mls qos** 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、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドをディセーブルにできます。QoS がディセーブルの場合は、パケットが変更されない（パケット内の CoS、DSCP、および IP precedence 値は変更されない）ため、信頼できるポートまたは信頼できないポートといった概念はありません。トラフィックは Pass-Through モードでスイッチングされます（パケットは書き換えられることなくスイッチングされ、ポリシングなしのベスト エフォートに分類されます）。

auto qos voip コマンドがイネーブルであるポートでは、生成される queue-set ID はインターフェイスによって異なります。

- ファスト イーサネット インターフェイスでは、auto-QoS は queue-set 1（デフォルト）を生成します。
- ギガビット イーサネット インターフェイスでは、auto-QoS は queue-set 2 を生成します。

これは、**auto qos voip cisco-phone** コマンドの拡張コンフィギュレーションです。

```
Switch(config)# mls qos map policed-dscp  0 10 18 to 8
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
Switch(config)# class-map match-all AUTOQOS_VOIP_DATA_CLASS
Switch(config-cmap)# match ip dscp ef
Switch(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Switch(config)# class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-cmap)# match ip dscp cs3
Switch(config)# policy-map AUTOQOS-SRND4-CISCOPHONE-POLICY
Switch(config-pmap)# class AUTOQOS_VOIP_DATA_CLASS
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap-c)# police 128000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Switch(config-pmap-c)# set dscp default
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Switch(config-if)# service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
```

これは、**auto qos voip cisco-softphone** コマンドの拡張コンフィギュレーションです。

```
Switch(config)# mls qos map policed-dscp  0 10 18 to 8
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
```

```
Switch(config)# class-map match-all AUTOQOS_MULTIENHANCED_CONF_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-MULTIENHANCED-CONF
Switch(config)# class-map match-all AUTOQOS_VOIP_DATA_CLASS
Switch(config-cmap)# match ip dscp ef
Switch(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Switch(config)# class-map match-all AUTOQOS_TRANSACTION_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-TRANSACTIONAL-DATA
Switch(config)# class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-cmap)# match ip dscp cs3
Switch(config)# class-map match-all AUTOQOS_SIGNALING_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SIGNALING
Switch(config)# class-map match-all AUTOQOS_BULK_DATA_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-BULK-DATA
Switch(config)# class-map match-all AUTOQOS_SCAVANGER_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SCAVANGER

Switch(config)# policy-map AUTOQOS-SRND4-SOFTPHONE-POLICY
Switch(config-pmap)# class AUTOQOS_VOIP_DATA_CLASS
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap-c)# police 128000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_MULTIENHANCED_CONF_CLASS
Switch(config-pmap-c)# set dscp af41
Switch(config-pmap-c)# police 5000000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_BULK_DATA_CLASS
Switch(config-pmap-c)# set dscp af11
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_TRANSACTION_CLASS
Switch(config-pmap-c)# set dscp af21
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_SCAVANGER_CLASS
Switch(config-pmap-c)# set dscp cs1
Switch(config-pmap-c)# police 10000000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_SIGNALING_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Switch(config-pmap-c)# set dscp default
Switch(config-if)# service-policy input AUTOQOS-SRND4-SOFTPHONE-POLICY
```

例

次の例では、ポートに接続されているスイッチまたはルータが信頼できる装置である場合に、auto-QoS をイネーブルにし、着信パケットで受信した QoS ラベルを信頼する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# auto qos voip trust
```

設定を確認するには、**show auto qos interface** *interface-id* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
debug auto qos	auto-QoS 機能のデバッグをイネーブルにします。
mls qos cos	デフォルトのポート CoS 値を定義するか、あるいはポートのすべての着信パケットにデフォルトの CoS 値を割り当てます。
mls qos map	CoS/DSCP マップまたは DSCP/CoS マップを定義します。

コマンド	説明
mls qos queue-set output buffers	バッファをキューセットに割り当てます。
mls qos srr-queue input bandwidth	Shaped Round Robin（SRR）の重みを入力キューに割り当てます。
mls qos srr-queue input buffers	入力キュー間のバッファを割り当てます。
mls qos srr-queue input cos-map	CoS 値を入力キューにマッピングするか、または CoS 値をキューとしきい値 ID にマッピングします。
mls qos srr-queue input dscp-map	DSCP 値を入力キューにマッピングするか、または DSCP 値をキューとしきい値 ID にマッピングします。
mls qos srr-queue input priority-queue	入力プライオリティ キューを設定し、帯域幅を保証します。
mls qos srr-queue output cos-map	CoS 値を出力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue output dscp-map	DSCP 値を出力キュー、またはキューとしきい値 ID にマッピングします。
mls qos trust	ポートの信頼状態を設定します。
queue-set	ポートをキューセットにマッピングします。
show auto qos	auto-QoS 情報を表示します。
show mls qos interface	ポート レベルで QoS 情報を表示します。
srr-queue bandwidth shape	シェーピングされた重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅シェーピングをイネーブルにします。
srr-queue bandwidth share	共有する重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅の共有をイネーブルにします。

boot auto-copy-sw

自動アップグレード プロセスをイネーブルにするには、スタック マスターから **boot auto-copy-sw** グローバル コンフィギュレーション コマンドを使用します。このコマンドにより、Version-Mismatch モードのスイッチは、いずれかのスタック メンバ上で実行中のソフトウェア イメージをコピーするか、スイッチ スタックのフラッシュ メモリの tar ファイル イメージをコピーして、自動的にアップグレードされます。自動アップグレード プロセス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。

boot auto-copy-sw

no boot auto-copy-sw

構文の説明

このコマンドには、引数またはキーワードはありません。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

Version-Mismatch モードのスイッチは、スタック上のバージョンと異なるマイナー バージョン番号を持つスイッチです。Version-Mismatch モードのスイッチは、完全に機能しているメンバとしてはスタックに加入できません。スタックが Version-Mismatch モードのスイッチにコピーできるイメージを保有している場合、自動アップグレード プロセスを使用することで、スタック メンバから Version-Mismatch モードのスイッチにイメージを自動でコピーできます。その場合、スイッチは Version-Mismatch モードを終了し、再起動後に完全に機能しているメンバとしてスタックに加入します。

自動アップグレード プロセスは、Version-Mismatch モードのスイッチだけに影響します。既存のスタック メンバには影響しません。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。
show version	ハードウェアおよびファームウェアのバージョン情報を表示します。

boot auto-download-sw

boot auto-download-sw 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、ソフトウェアの自動アップグレードのために使用する URL パス名を指定します。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。

boot auto-download-sw *source-url*

no boot auto-download-sw

構文の説明

source-url	自動アップグレードのためのソース URL エイリアス。次のオプションがサポートされています。 • スタンドアロン スイッチまたはスタック マスター上のローカル フラッシュ ファイル システムの構文： **flash:** スタック メンバ上のローカル フラッシュ ファイル システムの構文： **flash** *member number***:** • FTP の構文： **ftp:**[[//*username*[**:***password*]**@***location*]/*directory*]/*image-name***.tar** • HTTP サーバの構文： **http:**//[[*username***:***password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name***.tar** • セキュア HTTP サーバの構文： **https:**//[[*username***:***password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name***.tar** • Remote Copy Protocol（RCP）の構文： **rcp:**[[//*username***@***location*]/*directory*]/*image-name***.tar** • TFTP の構文： **tftp:**[[//*location*]/*directory*]/*image-name***.tar** *image-name***.tar** は、スイッチにダウンロードし、インストールするソフトウェア イメージです。

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

コマンド履歴

リリース	変更内容
12.2(35)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、ソフトウェアの自動アップグレードのために使用する URL パスを指定します。

このコマンドを使用して、バージョンのミスマッチの場合にアクセスするマスタースイッチの URL を設定できます。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot buffersize

NVRAM サイズを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **boot buffersize** グローバル コンフィギュレーション コマンドを使用します。このコマンド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。

boot buffersize *size*

no boot buffersize

構文の説明

size	NVRAM バッファ サイズ（KB） 有効な範囲は 4096 ～ 1048576 です。

デフォルト

デフォルトの NVRAM バッファ サイズは 512 KB 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

コマンド履歴

リリース	変更内容
12.2(55)SE	このコマンドが追加されました。

使用上のガイドライン

デフォルトの NVRAM バッファ サイズは 512 KB です。コンフィギュレーション ファイルが大きすぎて NVRAM に保存できない場合があります。一般的に、この状態はスイッチ スタック内に多くのスイッチがある場合に発生します。より大きいコンフィギュレーション ファイルをサポートできるように、NVRAM バッファのサイズを設定できます。新しい NVRAM バッファ サイズは、現在および新しいすべてのメンバ スイッチに同期されます。

NVRAM バッファ サイズを設定後、スイッチまたはスイッチ スタックをリロードします。

スイッチをスタックに追加し、NVRAM サイズが異なる場合、新しいスイッチはスタックに同期化し、自動的にリロードされます。

例

次の例では、NVRAM バッファ サイズを設定する方法を示します。

```
Switch(config)# boot buffersize 524288
Switch(config)# end
```

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot config-file

システム設定の不揮発性コピーの読み込みおよび書き込みを行うために、Cisco IOS が使用するファイル名を指定するには、スタンドアロン スイッチ上で **boot config-file** グローバル コンフィギュレーション 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。

boot config-file flash:/*file-url*

no boot config-file

構文の説明

flash:/*file-url*	コンフィギュレーション ファイルのパス（ディレクトリ）および名前です。

デフォルト

デフォルトのコンフィギュレーション ファイルは、flash:config.text 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、スタンドアロン スイッチからだけ正常に動作します。

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

このコマンドは、CONFIG_FILE 環境変数の設定を変更します。詳細は、付録 A「Catalyst 3750 スイッチ ブート ローダー コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot enable-break

自動ブート プロセスの中断をイネーブルにするには、スタンドアロン スイッチ上で **boot enable-break** グローバル コンフィギュレーション 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。

boot enable-break

no boot enable-break

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル。コンソール上で Break キーを押しても自動ブート プロセスを中断することはできません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、スタンドアロン スイッチからだけ正常に動作します。

このコマンドを入力すると、フラッシュ ファイル システムが初期化された後で Break キーを押して、自動ブート プロセスを中断できます。

（注）　このコマンドの設定に関係なく、スイッチ前面パネルの MODE ボタンを押すと、いつでも自動ブート プロセスを中断することができます。

このコマンドは、ENABLE_BREAK 環境変数の設定を変更します。詳細は、付録 A「Catalyst 3750 スイッチ ブート ローダー コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot helper

boot helper 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、ブート ローダー初期化中に動的にファイルをロードして、ブート ローダーの機能を拡張したり、パッチを当てたりします。このコマンド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。

boot helper *filesystem*:/*file-url* ...

no boot helper

構文の説明

filesystem:	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスには **flash:** を使用します。
/*file-url*	ローダー初期化中に動的にロードするためのパス（ディレクトリ）およびロード可能なファイルのリストです。イメージ名はセミコロンで区切ります。

デフォルト

ヘルパー ファイルはロードされません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

この変数は、内部開発およびテスト専用です。

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

このコマンドは、HELPER 環境変数の設定を変更します。詳細は、付録 A「Catalyst 3750 スイッチ ブート ローダー コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot helper-config-file

boot helper-config-file 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、Cisco IOS ヘルパー イメージが使用するコンフィギュレーション ファイルの名前を指定します。このコマンドが設定されていない場合は、CONFIG_FILE 環境変数によって指定されたファイルが、ロードされたすべてのバージョンの Cisco IOS に使用されます。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。

boot helper-config-file *filesystem*:/*file-url*

no boot helper-config file

構文の説明

filesystem:	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスには **flash:** を使用します。
/*file-url*	ロードするパス（ディレクトリ）およびヘルパー コンフィギュレーション ファイル

デフォルト

ヘルパー コンフィギュレーション ファイルは指定されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

この変数は、内部開発およびテスト専用です。

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

このコマンドは、HELPER_CONFIG_FILE 環境変数の設定を変更します。詳細は、付録 A「Catalyst 3750 スイッチ ブート ローダー コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot manual

次回ブート サイクル中にスイッチの手動起動をイネーブルにするには、スタンドアロン スイッチ上で **boot manual** グローバル コンフィギュレーション 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。

boot manual

no boot manual

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

手動による起動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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、スタンドアロン スイッチからだけ正常に動作します。

システムを次回再起動すると、スイッチはブート ローダー モードで起動します。これは *switch:* プロンプトによってわかります。システムを起動するには、**boot** ブート ローダー コマンドを使用して起動可能なイメージの名前を指定します。

このコマンドは、MANUAL_BOOT 環境変数の設定を変更します。詳細は、付録 A「Catalyst 3750 スイッチ ブート ローダー コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot private-config-file

プライベート コンフィギュレーションの不揮発性コピーの読み込みおよび書き込みを行うために Cisco IOS が使用するファイル名を指定するには、スタンドアロン スイッチ上で **boot private-config-file** グローバル コンフィギュレーション 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。

boot private-config-file *filename*

no boot private-config-file

構文の説明

filename	プライベート コンフィギュレーション ファイルの名前

デフォルト

デフォルトのコンフィギュレーション ファイルは、*private-config* 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、スタンドアロン スイッチからだけ正常に動作します。

ファイル名は、大文字と小文字を区別します。

例

次の例では、プライベート コンフィギュレーション ファイルの名前を *pconfig* と指定する方法を示します。

```
Switch(config)# boot private-config-file pconfig
```

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot system

boot system 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、次回のブート サイクル中にロードする Cisco IOS イメージを指定します。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。

boot system {*filesystem*:/*file-url* ...| **switch** {*number* | **all**}}

no boot system

no boot system switch {*number* | **all**}

構文の説明

filesystem:	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスには **flash:** を使用します。
/*file-url*	ブート可能なイメージのパス（ディレクトリ）および名前。各イメージ名はセミコロンで区切ります。
switch	Cisco IOS イメージがロードされるスイッチを指定します。
number	スタック メンバを指定します（1 ～9 の範囲で、1 つのスタック メンバだけを指定する）。
all	すべてのスタック メンバを指定します。

デフォルト

スイッチは、BOOT 環境変数内の情報を使用して、自動的にシステムを起動しようとします。この変数が設定されていない場合、スイッチは、フラッシュ ファイル システム全体に再帰的に縦型検索し、最初の実行可能イメージをロードして実行しようとします。ディレクトリの縦型検索では、検出した各サブディレクトリを完全に検索してから元のディレクトリでの検索を続けます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(25)SEA	**switch** {*number* | **all**} キーワードが追加されました。**boot system** コマンドは現在、スイッチ スタックおよびスタンドアロン スイッチ上で正常に動作します。

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

スタック マスター上で **boot system** *filesystem:/file-url* コマンドを入力した場合、指定したソフトウェア イメージは、次回のブート サイクルの際に、スタック マスター上でだけロードされます。

スタック マスター上で、次回のブート サイクル中に指定のスタック メンバでソフトウェア イメージがロードされるように指定するには、**boot system switch** *number* コマンドを使用します。次回のブート サイクル中にすべてのスタック メンバ上でソフトウェア イメージがロードされるように指定するには、**boot system switch all** コマンドを使用します。

boot system switch *number* コマンドまたは **boot system switch all** コマンドをスタック マスター上で入力すると、スタック マスターはスタック メンバ（スタック マスターを除く）上にソフトウェア イメージが存在しているかどうか確認します。スタック メンバ上（スタック メンバ 1 など）にソフトウェア イメージが存在しない場合、次のようなエラー メッセージが表示されます。

```
%Command to set boot system switch all xxx on switch=1 failed
```

スタック マスター上で **boot system switch** *number* コマンドを入力した場合、*number* 変数に 1 つのスタック メンバだけを指定できます。*number* 変数に複数のスタック メンバを入力することはサポートされていません。

archive download-sw 特権 EXEC コマンドを使用してシステム イメージを保存している場合、**boot system** コマンドを使用する必要はありません。**boot system** コマンドは自動的に処理され、ダウンロードされたイメージがロードされます。

このコマンドは、BOOT 環境変数の設定を変更します。詳細は、付録 A「Catalyst 3750 スイッチ ブート ローダー コマンド」を参照してください。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

cdp forward

CDP トラフィックの入力および出力スイッチ ポートを指定するには、**cdp forward** グローバル コンフィギュレーション 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。

cdp forward ingress *port-id* **egress** *port-id*

no cdp forward ingress *port-id*

構文の説明

ingress *port-id*	IP Phone から CDP パケットを受信するスイッチ ポートを指定します。
egress *port-id*	Cisco TelePresence System に CDP パケットを転送するスイッチ ポートを指定します。

デフォルト

スイッチを通る CDP パケットのデフォルト パスは、任意の入力ポートから Cisco TelePresence System に接続された出力ポートです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(53)SE	このコマンドが追加されました。

使用上のガイドライン

TelePresence E911 IP Phone がサポートされた CDP 対応の電話機だけを使用する必要があります。

スイッチ スタック内の任意の 2 つのポートを経由した Cisco TelePresence System 内で、IP Phone とコーデックを接続できます。

例

```
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# cdp forward ingress gigabitethernet2/0/1 egress gigabitethernet2/0/12
Switch(config)# cdp forward ingress gigabitethernet2/0/2 egress gigabitethernet2/0/13
Switch(config)# end
Switch# show running-config | include cdp
cdp forward ingress GigabitEthernet2/0/1 egress GigabitEthernet2/0/12
cdp forward ingress GigabitEthernet2/0/2 egress GigabitEthernet2/0/13
Switch# show cdp forward
Ingress         Egress         # packets         # packets
Port            Port           forwarded         dropped
-------------------------------------------------------------
 Gi2/0/1        Gi2/0/12            0                 0
 Gi2/0/2        Gi2/0/13            0                 0
```

関連コマンド

コマンド	説明
show cdp forward	CDP フォワーディング テーブルを表示します。

channel-group

channel-group インターフェイス コンフィギュレーション コマンドを使用して、EtherChannel グループにイーサネット ポートを割り当てたり、EtherChannel モードをイネーブルにしたり、この両方を行ったりします。イーサネット ポートを EtherChannel グループから削除する場合は、このコマンドの **no** 形式を使用します。

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

no channel-group

PAgP モード：
channel-group *channel-group-number* **mode {**{**auto** [**non-silent**]} | {**desirable** [**non-silent}}**

LACP モード：
channel-group *channel-group-number* **mode** {**active** | **passive**}

on モード：
channel-group *channel-group-number* **mode on**

構文の説明

channel-group-number	チャネル グループ番号を指定します。指定できる範囲は 1 ～ 48 です。
mode	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。 active モードは、ポートをネゴシエーション ステートにします。このステートでは、ポートは LACP パケットを送信することによって、他のポートとのネゴシエーションを開始します。チャネルは、active モードまたは passive モードの別のポート グループで形成されます。
auto	Port Aggregation Protocol（PAgP; ポート集約プロトコル）装置が検出された場合に限り、PAgP をイネーブルにします。 auto モードは、ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。チャネルは、desirable モードの別のポート グループでだけ形成されます。**auto** がイネーブルの場合、サイレント動作がデフォルトになります。
desirable	無条件に PAgP をイネーブルにします。 desirable モードは、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。この場合、ポートは PAgP パケットを送信することによって、他のポートとのネゴシエーションを開始します。EtherChannel は、desirable モードまたは auto モードの別のポート グループで形成されます。**desirable** がイネーブルの場合は、デフォルトでサイレント動作となります。
non-silent	（任意）他の装置からのトラフィックが予想されている場合に PAgP モードで **auto** または **desirable** キーワードとともに使用されます。

on	**on** モードをイネーブルにします。 **on** モードでは、使用可能な EtherChannel が存在するのは、両方の接続ポート グループが **on** モードになっている場合だけです。
passive	LACP 装置が検出された場合に限り、LACP をイネーブルにします。 passive モードは、ポートをネゴシエーション ステートにします。この場合、ポートは受信した LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。チャネルは、active モードの別のポート グループでだけ形成されます。

デフォルト

チャネル グループは割り当てることができません。

モード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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**active** キーワードおよび **passive** キーワードが追加されました。
12.2(25)SE	*channel-group-number* 範囲が 1 ～ 12 から 1 ～ 48 に変更されました。
12.2(25)SEC	LACP はクロススタック EtherChannel をネゴシエートできるようになりました。

使用上のガイドライン

レイヤ 2 EtherChannel の場合、物理ポートをチャネル グループに割り当てる前に、先に **interface port-channel** 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ポートチャネル インターフェイスを作成しておく必要はありません。代わりに、**channel-group** インターフェイス コンフィギュレーション コマンドを使用できます。論理インターフェイスがまだ作成されていない場合は、チャネル グループが最初の物理ポートを取得した時点で、自動的にポートチャネル インターフェイスが作成されます。最初にポートチャネル インターフェイスを作成する場合は、*channel-group-number* を *port-channel-number* と同じ番号にしても、新しい番号にしてもかまいません。新しい番号を使用した場合、**channel-group** コマンドは動的に新しいポート チャネルを作成します。

チャネル グループの一部である物理ポートに割り当てられた IP アドレスをディセーブルにする必要はありませんが、これをディセーブルにすることを強く推奨します。

interface port-channel コマンドの次に **no switchport** インターフェイス コンフィギュレーション コマンドを使用して、レイヤ 3 のポート チャネルを作成できます。インターフェイスをチャネル グループに適用する前に、ポート チャネルの論理インターフェイスを手動で設定してください。

EtherChannel を設定した後、ポートチャネル インターフェイスに加えられた設定の変更は、そのポートチャネル インターフェイスに割り当てられたすべての物理ポートに適用されます。物理ポートに適用された設定の変更は、設定を適用したポートだけに有効です。EtherChannel 内のすべてのポートのパラメータを変更するには、ポートチャネル インターフェイスに対してコンフィギュレーション コマンドを適用します。たとえば、spanning-tree コマンドを使用して、レイヤ 2 EtherChannel をトランクとして設定します。

auto モードまたは **desirable** モードとともに **non-silent** を指定しなかった場合は、サイレントが指定されているものと見なされます。サイレント モードを設定するのは、PAgP 非対応で、かつほとんどパケットを送信しない装置にスイッチを接続する場合です。サイレント パートナーの例は、トラフィッ

クを生成しないファイル サーバ、またはパケット アナライザなどです。この場合、物理ポート上で稼動している PAgP は、そのポートを動作可能にしません。ただし、PAgP は動作可能で、チャネル グループにポートを付与したり、伝送用ポートを使用したりできます。リンクの両端はサイレントに設定することはできません。

on モードでは、使用可能な EtherChannel が存在するのは、**on** モードのポート グループが、**on** モードの別のポート グループに接続する場合だけです。

注意　**on** モードの使用には注意が必要です。これは手動の設定であり、EtherChannel の両端のポートには、同一の設定が必要です。グループの設定を誤ると、パケット損失またはスパニング ツリー ループが発生することがあります。

クロススタック EtherChannel は、最大 2 つの 10 ギガビット イーサネット インターフェイスをサポートします。

EtherChannel は、PAgP と LACP の両方のモードには設定しないでください。PAgP および LACP を実行している EtherChannel グループは、同一のスイッチ、またはスタックにある異なるスイッチ上で共存できます（クロススタック構成ではできません）。個々の EtherChannel グループは PAgP または LACP のいずれかを実行できますが、相互運用することはできません。

channel-protocol インターフェイス コンフィギュレーション コマンドを使用してプロトコルを設定した場合、設定値は、**channel-group** インターフェイス コンフィギュレーション コマンドによっては上書きされません。

アクティブまたはアクティブでない EtherChannel メンバであるポートを IEEE 802.1x ポートとして設定しないでください。EtherChannel ポートで IEEE 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x 認証はイネーブルになりません。

セキュア ポートを EtherChannel の一部として、または EtherChannel ポートをセキュア ポートとしては設定しないでください。

設定の注意事項の一覧については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring EtherChannels」の章を参照してください。

注意　物理 EtherChannel ポート上で、レイヤ 3 のアドレスをイネーブルにしないでください。物理 EtherChannel ポート上でブリッジ グループを割り当てることは、ループが発生する原因になるため、行わないでください。

例

次の例では、単一のスイッチ上で、EtherChannel を設定する方法を示します。VLAN 10 のスタティック アクセス ポート 2 つを PAgP モード **desirable** であるチャネル 5 に割り当てます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2//1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable
Switch(config-if-range)# end
```

次の例では、単一のスイッチ上で、EtherChannel を設定する方法を示します。VLAN 10 のスタティック アクセス ポート 2 つを LACP モード **active** であるチャネル 5 に割り当てます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2//1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
```

```
Switch(config-if-range)# end
```

次の例では、クロススタック EtherChannel を設定する方法を示します。LACP パッシブ モードを使用して、VLAN 10 内のスタティックアクセス ポートとしてスタック メンバ 2 のポートを 2 つ、スタック メンバ 3 のポートを 1 つチャネル 5 に割り当てます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/4 -5
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode passive
Switch(config-if-range)# exit
Switch(config)# interface gigabitethernet3/0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# channel-group 5 mode passive
Switch(config-if)# exit
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
channel-protocol	チャネリングを管理するため、ポート上で使用されるプロトコルを制限します。
interface port-channel	ポート チャネルへのアクセスや、ポート チャネルの作成を行います。
show etherchannel	チャネルの EtherChannel 情報を表示します。
show lacp	LACP チャネル グループ情報を表示します。
show pagp	PAgP チャネル グループ情報を表示します。
show running-config	現在の動作設定を表示します。

channel-protocol

channel-protocol インターフェイス コンフィギュレーション コマンドを使用して、チャネリングを管理するために、ポート上で使用されるプロトコルを制限します。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。

channel-protocol {lacp | pagp}

no channel-protocol

構文の説明

lacp	Link Aggregation Control Protocol（LACP）で EtherChannel を設定します。
pagp	Port Aggregation Protocol（PAgP）で EtherChannel を設定します。

デフォルト

EtherChannel に割り当てられているプロトコルはありません。

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

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

channel-protocol コマンドは、チャネルを LACP または PAgP に制限するためだけに使用します。**channel-protocol** コマンドを使用してプロトコルを設定する場合、設定は **channel-group** インターフェイス コンフィギュレーション コマンドで上書きされることはありません。

channel-group インターフェイス コンフィギュレーション コマンドは、EtherChannel のパラメータ設定に使用してください。また、**channel-group** コマンドは、EtherChannel に対しモードを設定することもできます。

EtherChannel グループ上で、PAgP および LACP モードの両方をイネーブルにすることはできません。

PAgP と LACP には互換性がありません。両方ともチャネルの終端は同じプロトコルを使用する必要があります。

例

次の例では、EtherChannel を管理するプロトコルとして LACP を指定する方法を示します。

```
Switch(config-if)# channel-protocol lacp
```

設定を確認するには、**show etherchannel** [*channel-group-number*] **protocol** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
channel-group	EtherChannel グループにイーサネット ポートを割り当てます。
show etherchannel protocol	EtherChannel のプロトコル情報を表示します。

cisp enable

cisp enable 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、スイッチの Client Information Signalling Protocol（CISP）をイネーブルにすることで、スイッチがサプリカント スイッチに対するオーセンティケータとして動作するようにします。

cisp enable

no cisp enable

構文の説明

cisp enable	CISP をイネーブルにします。

デフォルト

デフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

オーセンティケータとサプリカント スイッチの間のリンクはトランクです。両方のスイッチで VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）をイネーブルにする場合は、VTP ドメイン名が同一であり、VTP モードが サーバである必要があります。

VTP モードを設定する場合は、MD5 チェックサムの不一致エラーにならないようにするために、次の点を確認してください。

- VLAN が異なる 2 台のスイッチに設定されていないこと。同じドメインに VTP サーバが 2 台存在することがこの状態の原因になることがあります。
- 両方のスイッチで、設定のリビジョン番号が異なっていること。

例

次の例では、CISP をイネーブルにする方法を示します。

```
switch(config)# cisp enable
```

関連コマンド

コマンド	説明
dot1x credentials（グローバル コンフィギュレーション）*profile*	プロファイルをサプリカント スイッチに設定します。
show cisp	指定されたインターフェイスの CISP 情報を表示します。

class

指定のクラス マップ名のトラフィックを分類する一致条件を（**police**、**set**、および **trust** ポリシー マップ クラス コンフィギュレーション コマンドを使用して）定義するには、**class** ポリシー マップ コンフィギュレーション コマンドを使用します。既存のクラス マップを削除する場合は、このコマンドの **no** 形式を使用します。

class {**class-map-name** | *class-default*}

no class {**class-map-name** | *class-default*}

構文の説明

class-map-name	クラス マップ名です。
class-default	分類されていないパケットに一致するシステムのデフォルト クラスです。

デフォルト

ポリシー マップ クラス マップは定義されていません。

コマンド モード

ポリシー マップ コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(55)SE	**class-default** キーワードが追加されました。

使用上のガイドライン

class コマンドを使用する前に、**policy-map** 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ポリシー マップを識別し、ポリシー マップ コンフィギュレーション モードを開始する必要があります。ポリシー マップを指定すると、ポリシー マップ内で新規クラスのポリシーを設定したり、既存クラスのポリシーを変更したりすることができます。**service-policy** インターフェイス コンフィギュレーション コマンドを使用して、ポリシー マップをポートへ添付することができます。

class コマンドを入力すると、ポリシー マップ クラス コンフィギュレーション モードに入り、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。

- **exit** : ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシー マップ コンフィギュレーション モードに戻ります。
- **no** : コマンドをデフォルト設定に戻します。
- **police** : 分類したトラフィックのポリサーまたは集約ポリサーを定義します。ポリサーは、帯域幅の限度およびその限度を超過した場合に実行するアクションを指定します。詳細については、**police** および **police aggregate** ポリシー マップ クラス コマンドを参照してください。
- **set** : 分類したトラフィックに割り当てる値を指定します。詳細は、**set** コマンドを参照してください。
- **trust** : **class** コマンドまたは **class-map** コマンドで分類したトラフィックの信頼状態を定義します。詳細は、**trust** コマンドを参照してください。

ポリシー マップ コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

class コマンドは、**class-map** グローバル コンフィギュレーション コマンドと同じ機能を実行します。他のポートと共有していない新しい分類が必要な場合は、**class** コマンドを使用します。多数のポート間でマップを共有する場合には、**class-map** コマンドを使用します。

class class-default ポリシー マップ コンフィギュレーション コマンドを使用して、デフォルト クラスを設定できます。分類されていないトラフィック（トラフィック クラスで指定された一致基準を満たさないトラフィック）は、デフォルト トラフィックとして処理されます。

例

次の例では、*policy1* という名前のポリシー マップを作成する方法を示します。このコマンドが入力方向に添付された場合、*class1* で定義されたすべての着信トラフィックの照合を行い、IP Differentiated Service Code Point（DSCP）を 10 に設定し、平均レート 1 Mb/s、バースト 20 KB のトラフィックをポリシングします。プロファイルを超えるトラフィックは、ポリシング設定 DSCP マップから取得した DSCP 値がマークされてから送信されます。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
```

次の例では、ポリシー マップにデフォルトのトラフィック クラスを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# class-map cm-3
Switch(config-cmap)# match ip dscp 30
Switch(config-cmap)# match protocol ipv6
Switch(config-cmap)# exit
Switch(config)# class-map cm-4
Switch(config-cmap)# match ip dscp 40
Switch(config-cmap)# match protocol ip
Switch(config-cmap)# exit
Switch(config)# policy-map pm3
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-3
Switch(config-pmap-c) set dscp 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-4
Switch(config-pmap-c)# trust cos
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

設定を確認するには、**show policy-map** 特権 EXEC コマンドを入力します。

次の例では、**class-default** が最初に設定された場合でも、デフォルトのトラフィック クラスをポリシー マップ pm3 の終わりに自動的に配置する方法を示します。

```
Switch# show policy-map pm3
  Policy Map pm3
    Class cm-3
      set dscp 4
    Class cm-4
      trust cos
    Class class-default
      set dscp 10
Switch#
```

関連コマンド

コマンド	説明
class-map	名前を指定したクラスとパケットとの照合に使用されるクラス マップを作成します。
police	分類したトラフィックにポリサーを定義します。
policy-map	複数のポートに接続可能なポリシー マップを作成または変更して、サービス ポリシーを指定します。
set	パケットに DSCP 値または IP precedence 値を設定することによって、IP トラフィックを分類します。
show policy-map	Quality of Service（QoS）ポリシー マップを表示します。
trust	**class** ポリシー マップ コンフィギュレーション コマンドまたは **class-map** 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分類されたトラフィックの信頼状態を定義します。

class-map

パケットと名前を指定したクラスとの照合に使用するクラス マップを作成し、クラスマップ コンフィギュレーション モードを開始するには、**class-map** グローバル コンフィギュレーション コマンドを使用します。既存のクラス マップを削除し、グローバル コンフィギュレーション モードに戻るには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

match-all	（任意）このクラス マップ内のすべての一致ステートメントの論理積をとります。クラス マップ内のすべての基準が一致する必要があります。
match-any	（任意）このクラス マップ内の一致ステートメントの論理和をとります。1 つ以上の条件が一致していなければなりません。
class-map-name	クラス マップ名です。

デフォルト

クラス マップは定義されていません。

match-all または **match-any** のどちらのキーワードも指定されていない場合、デフォルトは **match-all** 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

クラス マップ一致基準を作成または変更するクラスの名前を指定し、クラス マップ コンフィギュレーション モードを開始する場合は、このコマンドを使用します。

グローバルに名前が付けられたポートごとに適用されるサービス ポリシーの一部としてパケットの分類、マーキング、および集約ポリシングを定義する場合は、**class-map** コマンドおよびそのサブコマンドを使用します。

Quality of Service（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 コマンドを利用することができます。

- **description**：クラス マップを説明します（最大 200 文字）。**show class-map** 特権 EXEC コマンドは、クラスマップの説明と名前を表示します。
- **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。
- **match**：分類基準を設定します。詳細は、**match**（クラスマップ コンフィギュレーション）コマンドを参照してください。
- **no**：クラス マップから一致ステートメントを削除します。

- **rename**：現在のクラス マップの名前を変更します。クラス マップ名をすでに使用されている名前に変更すると、「`A class-map with this name already exists`」というメッセージが表示されます。

物理ポート単位でパケット分類を定義するため、クラス マップごとに 1 つずつに限り **match** コマンドがサポートされています。この状況では、**match-all** キーワードと **match-any** キーワードは同じです。

1 つのクラス マップで設定できる Access Control List（ACL; アクセス コントロール リスト）は 1 つだけです。ACL には複数の Access Control Entry（ACE; アクセス コントロール エントリ）を含めることができます。

例

次の例では、クラス マップ *class1* に 1 つの一致基準（アクセス リスト *103*）を設定する方法を示します。

```
Switch(config)# access-list 103 permit ip any any dscp 10
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# exit
```

次の例では、クラス マップ *class1* を削除する方法を示します。

```
Switch(config)# no class-map class1
```

show class-map 特権 EXEC コマンドを入力すると、設定を確認できます。

関連コマンド

コマンド	説明
class	指定されたクラスマップ名のトラフィック分類一致条件（**police**、**set**、および **trust** ポリシー マップ クラス コンフィギュレーション コマンドによる）を定義します。
match（クラスマップ コンフィギュレーション）	トラフィックを分類するための一致条件を定義します。
policy-map	複数のポートに接続可能なポリシー マップを作成または変更して、サービス ポリシーを指定します。
show class-map	QoS クラス マップを表示します。

clear dot1x

スイッチまたは指定したポートの IEEE 802.1x 情報をクリアするには、**clear dot1x** 特権 EXEC コマンドを使用します。

clear dot1x {**all** | **interface** *interface-id*}

構文の説明

all	スイッチのすべての IEEE 802.1x 情報をクリアします。
interface *interface-id*	指定されたインターフェイスの IEEE 802.1x 情報をクリアします。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

clear dot1x all コマンドを使用して、すべての情報をクリアできます。また、**clear dot1x interface** *interface-id* コマンドを使用して、指定されたインターフェイスの情報だけをクリアできます。

例

次の例では、すべての IEEE 802.1x 情報をクリアする方法を示します。

```
Switch# clear dot1x all
```

次の例では、指定されたインターフェイスの IEEE 802.1x 情報をクリアする方法を示します。

```
Switch# clear dot1x interface gigabithethernet1/0/1
Switch# clear dot1x interface gigabithethernet1/1
```

情報が削除されたかどうかを確認するには、**show dot1x** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show dot1x	スイッチまたは指定されたポートの IEEE 802.1x 統計情報、管理ステータス、および動作ステータスを表示します。

clear eap sessions

スイッチまたは指定したポートの Extensible Authentication Protocol（EAP）セッション情報をクリアするには、**clear eap sessions** 特権 EXEC コマンドを使用します。

clear eap sessions [**credentials** *name* [**interface** *interface-id*] | **interface** *interface-id* | **method** *name* | **transport** *name*] [**credentials** *name* | **interface** *interface-id* | **transport** *name*] ...

構文の説明

credentials **name**	指定されたプロファイルの EAP クレデンシャル情報をクリアします。
interface *interface-id*	指定されたインターフェイスの EAP 情報をクリアします。
method **name**	指定された方式の EAP 情報をクリアします。
transport *name*	指定された下位レベルの EAP トランスポート情報をクリアします。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

clear eap sessions コマンドを使用して、すべてのカウンタをクリアできます。キーワードを使用して、特定の情報だけをクリアできます。

例

次の例では、すべての EAP 情報をクリアする方法を示します。

```
Switch# clear eap
```

次の例では、指定されたプロファイルの EAP セッション クレデンシャル情報をクリアする方法を示します。

```
Switch# clear eap sessions credential type1
```

情報が削除されたかどうかを確認するには、**show dot1x** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show eap	スイッチまたは指定されたポートの EAP のレジストレーション情報およびセッション情報を表示します。

clear errdisable interface

errdisable になっていた VLAN を再度イネーブルにするには、**clear errdisable interface** 特権 EXEC コマンドを使用します。

clear errdisable interface *interface-id* **vlan** [*vlan-list*]

構文の説明

vlan list	（任意）再びイネーブルにする VLAN のリストを指定します。vlan-list を指定しない場合は、すべての VLAN が再びイネーブルになります。

コマンド デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(37)SE	このコマンドが追加されました。

使用上のガイドライン

shutdown および **no shutdown** のインターフェイス コンフィギュレーション コマンドを使用してポートを再びイネーブルにするか、**clear errdisable interface** コマンドを使用して VLAN の errdisable をクリアできます。

例

次の例では、ポート 2 で error-disabled になっているすべての VLAN を再びイネーブルにする方法を示します。

```
Switch# clear errdisable interface GigabitEthernet4/0/2 vlan
```

関連コマンド

コマンド	説明
errdisable detect cause	特定の原因、またはすべての原因に対して errdisable 検出をイネーブルにします。
errdisable recovery	回復メカニズム変数を設定します。
show errdisable detect	errdisable 検出ステータスを表示します。
show errdisable recovery	errdisable 回復タイマー情報を表示します。
show interfaces status err-disabled	errdisable ステートになっているインターフェイスのリストのインターフェイス ステータスを表示します。

clear arp inspection log

ダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査のログ バッファをクリアするには、**clear ip arp inspection log** 特権 EXEC コマンドを使用します。

clear ip arp inspection log

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

例

次の例では、ログ バッファの内容をクリアする方法を示します。

```
Switch# clear ip arp inspection log
```

ログがクリアされたかどうかを確認するには、**show ip arp inspection log** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
arp access-list	ARP ACL を定義します。
ip arp inspection log-buffer	ダイナミック ARP 検査ロギング バッファを設定します。
ip arp inspection vlan logging	VLAN 単位で記録するパケットのタイプを制御します。
show inventory log	ダイナミック ARP 検査ログ バッファの設定と内容を表示します。

clear ip arp inspection statistics

ダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査の統計情報をクリアするには、**clear ip arp inspection statistics** 特権 EXEC コマンドを使用します。

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

構文の説明

vlan *vlan-range*	（任意）指定された 1 つ以上の VLAN の統計情報をクリアします。 VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

例

次の例では、VLAN 1 の統計情報をクリアする方法を示します。

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

統計情報が削除されたかどうかを確認するには、**show ip arp inspection statistics vlan 1** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show inventory statistics	すべての VLAN または指定された VLAN の転送済みパケット、ドロップ済みパケット、MAC 検証に失敗したパケット、および IP 検証に失敗したパケットの統計情報を表示します。

clear ip dhcp snooping

DHCP スヌーピング バインディング データベース、DHCP スヌーピング バインディング データベース エージェントの統計情報または DHCP スヌーピング統計カウンタをクリアするには、**clear ip dhcp snooping** 特権 EXEC コマンドを使用します。

clear ip dhcp snooping {**binding** {***** | *ip-address* | **interface** *interface-id* | **vlan** *vlan-id*} | **database statistics** | **statistics**}

構文の説明

binding	DHCP スヌーピング バインディング データベースをクリアします。
*****	すべての自動バインディングをクリアします。
ip-address	バインディング エントリ IP アドレスをクリアします。
interface *interface-id*	バインディング入力インターフェイスをクリアします。
vlan *vlan-id*	バインディング エントリ VLAN をクリアします。
database statistics	DHCP スヌーピング バインディング データベース エージェントの統計情報をクリアします。
statistics	DHCP スヌーピング統計カウンタをクリアします。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。
12.2(37)SE	**statistics** キーワードが導入されました。
12.2(44)SE	*****、*ip-address*、**interface** *interface-id*、および **vlan** *vlan-id* キーワードが追加されました。

使用上のガイドライン

clear ip dhcp snooping database statistics コマンドを入力すると、スイッチは統計情報をクリアする前にバインディング データベースおよびバインディング ファイル内のエントリを更新しません。

例

次の例では、DHCP スヌーピング バインディング データベース エージェントの統計情報をクリアする方法を示します。

統計情報がクリアされたかどうかを確認するには、**show ip dhcp snooping database** 特権 EXEC コマンドを入力します。`Switch#` **`clear ip dhcp snooping database statistics`**

次の例では、DHCP スヌーピング統計カウンタをクリアする方法を示します。

`Switch#` **`clear ip dhcp snooping statistics`**

統計情報がクリアされたかどうかを確認するには、**show ip dhcp snooping statistics** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip dhcp snooping	VLAN 上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping database	DHCP スヌーピング バインディング データベース エージェントまたはバインディング ファイルを設定します。
show ip dhcp snooping binding	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 バインディング データベース エージェントの統計情報を表示します。
show ip dhcp snooping statistics	DHCP スヌーピングの統計情報を表示します。

clear ipc

Interprocess Communication（IPC; プロセス間通信）プロトコルの統計情報をクリアするには、**clear ipc** 特権 EXEC コマンドを使用します。

clear ipc {**queue-statistics** | **statistics**}

構文の説明

queue-statistics	IPC キューの統計情報をクリアします。
statistics	IPC の統計情報をクリアします。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(18)SE	このコマンドが追加されました。

使用上のガイドライン

clear ipc statistics コマンドを使用してすべての統計情報をクリアできますが、**clear ipc queue-statistics** コマンドを使用してキューの統計情報だけをクリアすることもできます。

例

次の例では、すべての統計情報をクリアする方法を示します。

```
Switch# clear ipc statistics
```

次の例では、キューの統計情報だけをクリアする方法を示します。

```
Switch# clear ipc queue-statistics
```

統計情報が削除されたかどうかを確認するには、**show ipc rpc** または **show ipc session** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ipc {**rpc** | **session**}	IPC マルチキャスト ルーティングの統計情報を表示します。

clear ipv6 dhcp conflict

Dynamic Host Configuration Protocol for IPv6（DHCPv6）サーバ データベースからアドレス競合をクリアするには、**clear ipv6 dhcp conflict** 特権 EXEC コマンドを使用します。

clear ipv6 dhcp conflict {* | *IPv6-address*}

（注）このコマンドは、スイッチでデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートが設定されている場合に限り使用可能です。

構文の説明

*	すべてのアドレス競合をクリアします。
IPv6-address	競合するアドレスを含むホスト IPv6 アドレスをクリアします。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(46)SE	このコマンドが追加されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6 {default | vlan}** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

競合を検出するように DHCPv6 サーバを設定する場合、DHCPv6 サーバは ping を使用します。クライアントは近隣探索を使用してクライアントを検出し、DECLINE メッセージを介してサーバに報告します。アドレス競合が検出されると、このアドレスはプールから削除されます。管理者がこのアドレスを競合リストから削除するまでこのアドレスは割り当てることができません。

アドレス パラメータとしてアスタリスク（*）文字を使用すると、DHCP はすべての競合をクリアします。

例

次の例では、DHCPv6 サーバ データベースからすべてのアドレス競合をクリアする方法を示します。

```
Switch# clear ipv6 dhcp conflict *
```

関連コマンド

コマンド	説明
show ipv6 dhcp conflict	DHCPv6 サーバによって検出された、またはクライアントから DECLINE メッセージにより報告されたアドレス競合を表示します。

clear l2protocol-tunnel counters

プロトコル トンネル ポートのプロトコル カウンタをクリアするには、**clear l2protocol-tunnel counters** 特権 EXEC コマンドを使用します。

clear l2protocol-tunnel counters [*interface-id*]

構文の説明

interface-id	（任意）プロトコル カウンタをクリアするインターフェイス（物理インターフェイスまたはポート チャネル）を指定します。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(25)SE	このコマンドが追加されました。

使用上のガイドライン

スイッチまたは指定されたインターフェイスのプロトコル トンネル カウンタをクリアするには、このコマンドを使用します。

例

次の例では、インターフェイスのレイヤ 2 プロトコル トンネル カウンタをクリアする方法を示します。

```
Switch# clear l2protocol-tunnel counters gigabitethernet1/0/3
```

関連コマンド

コマンド	説明
show l2protocol-tunnel	レイヤ 2 プロトコル トンネリングが設定されたポートに関する情報を表示します。

clear lacp

Link Aggregation Control Protocol（LACP）チャネル グループのカウンタをクリアするには、**clear lacp** 特権 EXEC コマンドを使用します。

clear lacp {*channel-group-number* **counters** | **counters**}

構文の説明

channel-group-number	（任意）チャネル グループ番号。指定できる範囲は 1 ～ 48 です。
counters	トラフィックのカウンタをクリアします。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。
12.2(25)SE	*channel-group-number* 範囲が 1 ～ 12 から 1 ～ 48 に変更されました。

使用上のガイドライン

clear lacp counters コマンドを使用することで、カウンタをすべてクリアできます。また、指定のチャネル グループのカウンタだけをクリアする場合には、**clear lacp** *channel-group-number* **counters** コマンドを使用します。

例

次の例では、すべてのチャネル グループ情報をクリアする方法を示します。

```
Switch# clear lacp counters
```

次の例では、グループ 4 の LACP トラフィックのカウンタをクリアする方法を示します。

```
Switch# clear lacp 4 counters
```

情報が削除されたかどうかを確認するには、**show lacp counters** または **show lacp 4 counters** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show lacp	LACP チャネル グループ情報を表示します。

clear mac address-table

特定のダイナミック アドレス、特定のインターフェイス上のすべてのダイナミック アドレス、スタック メンバ上のすべてのダイナミック アドレス、または特定の VLAN 上のすべてのダイナミック アドレスを MAC アドレス テーブルから削除するには、**clear mac-address-table** 特権 EXEC コマンドを使用します。このコマンドはまた MAC アドレス通知グローバル カウンタもクリアします。

clear mac address-table {**dynamic** [**address** *mac-addr* | **interface** *interface-id* | **vlan** *vlan-id*] | **notification**}

構文の説明

dynamic	すべてのダイナミック MAC アドレスを削除します。
dynamic address *mac-addr*	（任意）指定されたダイナミック MAC アドレスを削除します。
dynamic 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ダイナミック MAC アドレスを削除します。
dynamic vlan *vlan-id*	（任意）指定された VLAN のすべてのダイナミック MAC アドレスを削除します。指定できる範囲は 1 ～ 4094 です。
notification	履歴テーブルの通知をクリアし、カウンタをリセットします。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(19)EA1	**clear mac-address-table**（ハイフン付き）コマンドは、**clear mac address-table**（ハイフンなし）コマンドに替わりました。

例

次の例では、ダイナミック アドレス テーブルから特定の MAC アドレスを削除する方法を示します。

```
Switch# clear mac address-table dynamic address 0008.0070.0007
```

show mac address-table 特権 EXEC コマンドを入力することにより、情報が削除されたかどうかを確認できます。

関連コマンド

コマンド	説明
mac address-table notification	MAC アドレス通知機能をイネーブルにします。
show mac access-group	MAC アドレス テーブルのスタティック エントリおよびダイナミック エントリを表示します。
show mac address-table notification	すべての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対する MAC アドレス通知設定を表示します。
snmp trap mac-notification change	特定のインターフェイス上の Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）MAC アドレス通知トラップをイネーブルにします。

clear mac address-table move update

MAC アドレス テーブルの移行更新関連カウンタをクリアするには、**clear mac address-table move update** 特権 EXEC コマンドを使用します。

clear mac address-table move update

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

例

次の例では、MAC アドレス テーブル移行更新関連カウンタをクリアする方法を示します。

```
Switch# clear mac address-table move update
```

show mac address-table move update 特権 EXEC コマンドを入力することにより、情報がクリアされたかどうかを確認できます。

関連コマンド

コマンド	説明
mac address-table move update {receive | transmit}	スイッチ上の MAC アドレス テーブル移行更新を設定します。
show mac address-table move update	スイッチに MAC アドレス テーブル移行更新情報を表示します。

clear nmsp statistics

Network Mobility Services Protocol（NMSP; ネットワーク モビリティ サービス プロトコル）の統計情報をクリアするには、**clear nmsp statistics** 特権 EXEC コマンドを使用します。このコマンドは、スイッチで暗号化ソフトウェア イメージが実行されている場合にだけ利用できます。

clear nmsp statistics

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

例

次の例では、NMSP の統計情報をクリアする方法を示します。

```
Switch# clear nmsp statistics
```

show nmsp statistics 特権 EXEC コマンドを入力することにより、情報が削除されたかどうかを確認できます。

関連コマンド

コマンド	説明
show nmsp	NMSP 情報を表示します。

clear pagp

Port Aggregation Protocol（PAgP）チャネル グループ情報を表示するには、**clear pagp** 特権 EXEC コマンドを使用します。

clear pagp {*channel-group-number* **counters** | **counters**}

構文の説明

channel-group-number	（任意）チャネル グループ番号。指定できる範囲は 1 ～ 48 です。
counters	トラフィックのカウンタをクリアします。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(25)SE	*channel-group-number* 範囲が 1 ～ 12 から 1 ～ 48 に変更されました。

使用上のガイドライン

すべてのカウンタをクリアするには、**clear pagp counters** コマンドを使用します。また、**clear pagp** *channel-group-number* **counters** コマンドを使用すると、指定のチャネル グループのカウンタだけをクリアできます。

例

次の例では、すべてのチャネル グループ情報をクリアする方法を示します。

```
Switch# clear pagp counters
```

次の例では、グループ 10 の PAgP トラフィックのカウンタをクリアする方法を示します。

```
Switch# clear pagp 10 counters
```

情報が削除されたかどうかを確認するには、**show pagp** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show pagp	PAgP チャネル グループ情報を表示します。

clear port-security

MAC アドレス テーブルからすべてのセキュア アドレスを削除するか、スイッチまたはインターフェイス上の特定のタイプ（設定済み、ダイナミック、またはスティッキ）のすべてのセキュア アドレスを削除するには、**clear port-security** 特権 EXEC コマンドを使用します。

clear port-security {**all** | **configured** | **dynamic** | **sticky**} [[**address** *mac-addr* | **interface** *interface-id*] [**vlan** {*vlan-id* | {**access** | **voice**}}]]

構文の説明

all	すべてのセキュア MAC アドレスを削除します。
configured	設定済みセキュア MAC アドレスを削除します。
dynamic	ハードウェアによって自動学習されたセキュア MAC アドレスを削除します。
sticky	自動学習または設定済みセキュア MAC アドレスを削除します。
address *mac-addr*	（任意）指定されたダイナミック セキュア 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 VLAN 上のすべてのダイナミック セキュア MAC アドレスを削除します。
vlan	（任意）指定された VLAN から指定されたセキュア MAC アドレスを削除します。**vlan** キーワードを入力後、次のいずれかのオプションを入力します。 • *vlan-id* : トランク ポート上で、クリアする必要のあるアドレスの VLAN の VLAN ID を指定します。 • **access** : アクセス ポートで、アクセス VLAN 上の指定されたセキュア MAC アドレスをクリアします。 • **voice** : アクセス ポートで、音声 VLAN 上の指定されたセキュア MAC アドレスをクリアします。 （注）　**voice** キーワードは、音声 VLAN がポートに設定されてそのポートがアクセス VLAN でない場合に限り利用可能です。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(25)SEA	このコマンドが追加されました。
12.2(25)SEB	**access** および **voice** キーワードが追加されました。

例

次の例では、MAC アドレス テーブルからすべてのセキュア アドレスを削除する方法を示します。

```
Switch# clear port-security all
```

次の例では、MAC アドレス テーブルから特定の設定済みセキュア アドレスを削除する方法を示します。

```
Switch# clear port-security configured address 0008.0070.0007
```

次の例では、特定のインターフェイスで学習されたすべてのダイナミック セキュア アドレスを削除する方法を示します。

```
Switch# clear port-security dynamic interface gigabitethernet1/0/1
```

次の例では、アドレス テーブルからすべてのダイナミック セキュア アドレスを削除する方法を示します。

```
Switch# clear port-security dynamic
```

show port-security 特権 EXEC コマンドを入力することにより、情報が削除されたかどうかを確認できます。

関連コマンド

コマンド	説明
switchport port-security	インターフェイス上でポート セキュリティをイネーブルにします。
switchport port-security mac-address *mac-address*	セキュア MAC アドレスを設定します。
switchport port-security maximum *value*	セキュア インターフェイスにセキュア MAC アドレスの最大数を設定します。
show port-security	インターフェイスまたはスイッチに定義されたポート セキュリティ設定を表示します。

clear spanning-tree counters

スパニング ツリーのカウンタをクリアするには、**clear spanning-tree counters** 特権 EXEC コマンドを使用します。

clear spanning-tree counters [**interface** *interface-id*]

構文の説明

interface *interface-id*	（任意）指定のインターフェイスのスパニング ツリー カウンタをすべてクリアします。有効なインターフェイスとしては、物理ポート、VLAN、およびポート チャネルがあります。指定できる VLAN 範囲は 1 ～ 4094 です。ポート チャネル範囲は 1 ～ 48 です。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

interface-id が指定されていない場合は、すべてのインターフェイスのスパニング ツリー カウンタがクリアされます。

例

次の例では、すべてのインターフェイスのスパニング ツリー カウンタをクリアする方法を示します。

```
Switch# clear spanning-tree counters
```

関連コマンド

コマンド	説明
show spanning-tree	スパニング ツリー ステート情報を表示します。

clear spanning-tree detected-protocols

すべてのインターフェイスまたは指定されたインターフェイスで、プロトコル移行プロセスを再開する（近接スイッチと強制的に再ネゴシエーションさせる）には、**clear spanning-tree detected-protocols** 特権 EXEC コマンドを使用します。

clear spanning-tree detected-protocols [**interface** *interface-id*]

構文の説明

interface *interface-id*	（任意）指定されたインターフェイスでプロトコル移行プロセスを再開します。有効なインターフェイスとしては、物理ポート、VLAN、およびポート チャネルがあります。指定できる VLAN 範囲は 1 ～ 4094 です。ポート チャネル範囲は 1 ～ 48 です。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

Rapid Per-VLAN Spanning-Tree Plus（Rapid PVST+）プロトコルまたは Multiple Spanning-Tree Protocol（MSTP）が稼動するスイッチは、組み込み済みのプロトコル移行メカニズムをサポートしています。それによって、スイッチはレガシー IEEE 802.1D スイッチと相互に動作できるようになります。Rapid PVST+ スイッチまたは MSTP スイッチが、プロトコルのバージョンが 0 に設定されているレガシー IEEE 802.1D コンフィギュレーション UniDirectional Link Detection（UDLD; 単一方向リンク検出）を受信した場合は、そのポートで IEEE 802.1D BPDU だけを送信します。Multiple Spanning-Tree（MST）スイッチが、レガシー BPDU、別のリージョンに関連付けられた MST BPDU（バージョン 3）、または Rapid Spanning-Tree（RST; 高速スパニング ツリー）BPDU（バージョン 2）を受信したときは、そのポートがリージョンの境界にあることを検知します。

ただし、スイッチは、IEEE 802.1D BPDU を受信しなくなった場合であっても、自動的には Rapid PVST+ モードまたは MSTP モードには戻りません。これは、レガシー スイッチが指定スイッチでなければ、リンクから削除されたかどうかを学習できないためです。この状況では、**clear spanning-tree detected-protocols** コマンドを使用します。

例

次の例では、ポートでプロトコル移行プロセスを再開する方法を示します。

```
Switch# clear spanning-tree detected-protocols interface gigabitethernet2/0/1
```

関連コマンド

コマンド	説明
show spanning-tree	スパニング ツリー ステート情報を表示します。
spanning-tree link-type	デフォルト リンクタイプ設定を上書きし、スパニング ツリーがフォワーディング ステートに高速移行できるようにします。

clear vmps statistics

VLAN Query Protocol（VQP）クライアントが保持する統計情報をクリアするには、**clear vmps statistics** 特権 EXEC コマンドを使用します。

clear vmps statistics

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

例

次の例では、VLAN Membership Policy Server（VMPS; VLAN メンバシップ ポリシー サーバ）統計情報をクリアする方法を示します。

```
Switch# clear vmps statistics
```

情報が削除されたかどうかを確認するには、**show vmps statistics** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show vmps	VQP バージョン、再確認間隔、再試行回数、VMPS IP アドレス、および現在のサーバとプライマリ サーバを表示します。

clear vtp counters

VLAN Trunking Protocol（VTP）およびプルーニング カウンタをクリアするには、**clear vtp counters** 特権 EXEC コマンドを使用します。

clear vtp counters

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

例

次の例では、VTP カウンタをクリアする方法を示します。

```
Switch# clear vtp counters
```

情報が削除されたかどうかを確認するには、**show vtp counters** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show vtp	VTP 管理ドメイン、ステータス、カウンタの一般情報を表示します。

cluster commander-address

このコマンドは、スタンドアロン クラスタ メンバ スイッチから 入力する必要はありません。クラスタ コマンド スイッチは、メンバ スイッチがクラスタに加入した場合に、MAC アドレスをそのメンバ スイッチに自動的に提供します。クラスタ メンバ スイッチは、この情報および他のクラスタ情報をその実行コンフィギュレーション ファイルに追加します。デバッグまたはリカバリ手順の間だけスイッチをクラスタから削除する場合は、クラスタ メンバ スイッチ コンソール ポートから、このグローバル コンフィギュレーション コマンドの **no** 形式を使用します。

cluster commander-address *mac-address* [**member** *number* **name** *name*]

no cluster commander-address

構文の説明

mac-address	クラスタ コマンド スイッチの MAC アドレス
member *number*	（任意）設定されたクラスタ メンバ スイッチの番号。指定できる範囲は 0 ～ 15 です。
name *name*	（任意）設定されたクラスタの名前（最大 31 文字）

デフォルト

このスイッチはどのクラスタのメンバでもありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、クラスタ コマンド スイッチ上でだけ使用できます。

各クラスタ メンバは、クラスタ コマンド スイッチを 1 つしか持てません。

クラスタ メンバ スイッチは、*mac-address* パラメータによりシステム リロード中にクラスタ コマンド スイッチの ID を保持します。

特定のクラスタ メンバ スイッチで **no** 形式を入力すると、デバッグまたはリカバリ手順の間そのクラスタ メンバ スイッチをクラスタから削除できます。通常は、メンバがクラスタ コマンド スイッチと通信ができなくなった場合にだけ、クラスタ メンバ スイッチ コンソール ポートからこのコマンドを使用することになります。通常のスイッチ構成では、クラスタ コマンド スイッチで **no cluster member** *n* グローバル コンフィギュレーション コマンドを入力することによってだけ、クラスタ メンバ スイッチを削除することを推奨します。

スタンバイ クラスタ コマンド スイッチがアクティブになった場合（クラスタ コマンド スイッチになった場合）、このスイッチは cluster commander-address 行をその設定から削除します。

例

次の例では、実行中のクラスタ メンバの設定から、その出力を一部示します。

```
Switch(config)# show running-configuration

<output truncated>

cluster commander-address 00e0.9bc0.a500 member 4 name my_cluster

<output truncated>
```

次の例では、クラスタ メンバ コンソールでクラスタからメンバを削除する方法を示します。

```
Switch # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# no cluster commander-address
```

設定を確認するには、**show cluster** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
debug cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。

cluster discovery hop-count

候補スイッチの拡張検出用にホップカウントの制限を設定するには、クラスタ コマンド スイッチ上で **cluster discovery hop-count** グローバル コンフィギュレーション 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。

cluster discovery hop-count *number*

no cluster discovery hop-count

構文の説明

number	クラスタ コマンド スイッチが候補の検出を制限するクラスタ エッジからのホップの数。指定できる範囲は 1 ～ 7 です。

デフォルト

ホップ カウントは 3 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、クラスタ コマンド スイッチ上でだけ使用できます。このコマンドは、クラスタ メンバ スイッチでは機能しません。

ホップ カウントが 1 に設定された場合、拡張検出はディセーブルになります。クラスタ コマンド スイッチは、クラスタのエッジから 1 ホップの候補だけを検出します。クラスタのエッジとは、最後に検出されたクラスタのメンバ スイッチと最初に検出された候補スイッチの間の点です。

例

次の例では、ホップ カウント制限を 4 に設定する方法を示します。このコマンドは、クラスタ コマンド スイッチ上から実行します。

```
Switch(config)# cluster discovery hop-count 4
```

設定を確認するには、**show cluster** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。
show cluster candidates	候補スイッチのリストを表示します。

cluster enable

このコマンド対応スイッチをクラスタ コマンド スイッチとしてイネーブルにし、クラスタ名を割り当て、任意でメンバ番号を割り当てるには、コマンド対応スイッチ上で **cluster enable** グローバル コンフィギュレーション コマンドを使用します。すべてのメンバを削除して、このクラスタ コマンド スイッチを候補スイッチにするには、このコマンドの **no** 形式を使用します。

cluster enable *name* [*command-switch-member-number*]

no cluster enable

構文の説明

name	クラスタ名（最大 31 文字）。指定できる文字は、英数字、ダッシュ、および下線だけです。
command-switch-member-number	（任意）クラスタのクラスタ コマンド スイッチにメンバ番号を割り当てます。指定できる範囲は 0 ～ 15 です。

デフォルト

このスイッチはクラスタ コマンド スイッチではありません。

クラスタ名は定義されません。

スイッチがクラスタ コマンド スイッチである場合、メンバ番号は 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、どのクラスタにも属していない任意のコマンド対応スイッチ上で入力します。装置がすでにクラスタのメンバとして設定されている場合、コマンドはエラーとなります。

クラスタ コマンド スイッチをイネーブルにするときには、クラスタに名前を付けてください。スイッチがすでにクラスタ コマンド スイッチとして設定されており、クラスタ名が以前の名前と異なっている場合、コマンドはクラスタ名を変更します。

例

次の例では、クラスタ コマンド スイッチをイネーブルにし、クラスタに名前を付け、クラスタ コマンド スイッチ メンバ番号を 4 に設定する方法を示します。

```
Switch(config)# cluster enable Engineering-IDF4 4
```

設定を確認するには、クラスタ コマンド スイッチで **show cluster** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。

cluster holdtime

スイッチ（コマンドまたはクラスタ メンバ スイッチのいずれか）が、他のスイッチのハートビート メッセージを受信しなくなってからそのスイッチのダウンを宣言するまでの期間を秒単位で設定するには、クラスタ コマンド スイッチ上で **cluster holdtime** グローバル コンフィギュレーション コマンドを使用します。期間をデフォルト値に設定する場合は、このコマンドの **no** 形式を使用します。

cluster holdtime *holdtime-in-secs*

no cluster holdtime

構文の説明

holdtime-in-secs	スイッチ（コマンドまたはクラスタ メンバ スイッチ）が、他のスイッチのダウンを宣言するまでの期間（秒）。指定できる範囲は 1 ～ 300 秒です。

デフォルト

デフォルトのホールド時間は 80 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

クラスタ コマンド スイッチ上でだけ、このコマンドと **cluster timer** 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ください。クラスタ内のすべてのスイッチ間で設定の一貫性が保たれるように、クラスタ コマンド スイッチはこの値をそのすべてのクラスタ メンバに伝達します。

ホールドタイムは通常インターバル タイマー（**cluster timer**）の倍数として設定されます。たとえば、スイッチのダウンを宣言するまでには、「ホールド タイムをインターバル タイムで割った秒数」回のハートビート メッセージが連続して受信されなかったことになります。

例

次の例では、クラスタ コマンド スイッチでインターバル タイマーおよびホールド タイム時間を変更する方法を示します。

```
Switch(config)# cluster timer 3
Switch(config)# cluster holdtime 30
```

設定を確認するには、**show cluster** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。

cluster member

クラスタに候補を追加するには、クラスタ コマンド スイッチ上で **cluster member** グローバル コンフィギュレーション コマンドを使用します。メンバをクラスタから削除するには、このコマンドの **no** 形式を使用します。

cluster member [*n*] **mac-address** *H.H.H* [**password** *enable-password*] [**vlan** *vlan-id*]

no cluster member *n*

構文の説明

n	クラスタ メンバを識別する番号。指定できる範囲は 0 ～ 15 です。
mac-address *H.H.H*	クラスタ メンバ スイッチの MAC アドレス（16 進数）
password *enable-password*	候補スイッチのパスワードをイネーブルにします。候補スイッチにパスワードがない場合、パスワードは必要ありません。
vlan *vlan-id*	（任意）クラスタ コマンド スイッチが候補をクラスタに追加するときに使用される VLAN ID。指定できる範囲は 1 ～ 4094 です。

デフォルト

新しくイネーブルになったクラスタ コマンド スイッチには、関連するクラスタ メンバはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、候補をクラスタに追加したり、メンバをクラスタから削除したりする場合にクラスタ コマンド スイッチでだけ入力できます。このコマンドをクラスタ コマンド スイッチ以外のスイッチで入力すると、スイッチはコマンドを拒否し、エラー メッセージを表示します。

スイッチをクラスタから削除する場合はメンバ番号を入力してください。ただし、スイッチをクラスタに追加する場合には、メンバ番号を入力する必要はありません。クラスタ コマンド スイッチは、次に利用可能なメンバ番号を選択し、これをクラスタに加入しているスイッチに割り当てます。

候補スイッチがクラスタに加入した場合には、認証を行うためにそのスイッチのイネーブル パスワードを入力してください。パスワードは、実行コンフィギュレーションまたはスタートアップ コンフィギュレーションには保存されません。候補スイッチがクラスタのメンバになった後、そのパスワードはクラスタ コマンド スイッチ パスワードと同じになります。

スイッチが、設定されたホスト名を持たない場合、クラスタ コマンド スイッチは、メンバ番号をクラスタ コマンド スイッチ ホスト名に追加し、これをクラスタ メンバ スイッチに割り当てます。

VLAN ID を指定していない場合、クラスタ コマンド スイッチは自動的に VLAN を選択し、候補をクラスタに追加します。

例

次の例では、スイッチをメンバ 2、MAC アドレス 00E0.1E00.2222、パスワード *key* としてクラスタに追加する方法を示しています。クラスタ コマンド スイッチは、VLAN 3 を経由して候補をクラスタに追加します。

```
Switch(config)# cluster member 2 mac-address 00E0.1E00.2222 password key vlan 3
```

次の例では、MAC アドレス 00E0.1E00.3333 のスイッチをクラスタに追加する方法を示します。このスイッチにはパスワードはありません。クラスタ コマンド スイッチは、次に利用可能なメンバ番号を選択し、これをクラスタに加入しているスイッチに割り当てます。

```
Switch(config)# cluster member mac-address 00E0.1E00.3333
```

設定を確認するには、クラスタ コマンド スイッチで **show cluster members** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。
show cluster candidates	候補スイッチのリストを表示します。
show cluster members	クラスタ メンバに関する情報を表示します。

cluster outside-interface

クラスタの Network Address Translation（NAT; ネットワーク アドレス変換）の外部インターフェイスを設定し、IP アドレスのないメンバがクラスタの外部にある装置と通信できるようにするには、クラスタ コマンド スイッチ上で **cluster outside-interface** グローバル コンフィギュレーション 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。

cluster outside-interface *interface-id*

no cluster outside-interface

構文の説明

interface-id	外部インターフェイスとして機能するインターフェイス。有効なインターフェイスとしては、物理インターフェイス、ポート チャネル、または VLAN があります。ポート チャネル範囲は 1 ～ 48 です。指定できる VLAN 範囲は 1 ～ 4094 です。

デフォルト

デフォルトの外部インターフェイスは、クラスタ コマンド スイッチによって自動的に選択されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、クラスタ コマンド スイッチ上でだけ入力できます。クラスタ メンバ スイッチでコマンドを入力すると、エラー メッセージが表示されます。

例

次の例では、VLAN 1 に外部インターフェイスを設定する方法を示します。

```
Switch(config)# cluster outside-interface vlan 1
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	現在の動作設定を表示します。

cluster run

スイッチ上でクラスタリングをイネーブルにするには、**cluster run** グローバル コンフィギュレーション コマンドを使用します。スイッチでクラスタリングをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

cluster run

no cluster run

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

すべてのスイッチでクラスタリングがイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

クラスタ コマンド スイッチ上で **no cluster run** コマンドを入力すると、クラスタ コマンド スイッチはディセーブルになります。クラスタリングはディセーブルになり、スイッチは候補スイッチになることができません。

クラスタ メンバ スイッチで **no cluster run** コマンドを入力すると、このメンバ スイッチはクラスタから削除されます。クラスタリングはディセーブルになり、スイッチは候補スイッチになることができません。

クラスタに属していないスイッチで **no cluster run** コマンドを入力すると、クラスタリングはそのスイッチ上でディセーブルになります。このスイッチは候補スイッチになることができません。

例

次の例では、クラスタ コマンド スイッチでクラスタリングをディセーブルにする方法を示します。

```
Switch(config)# no cluster run
```

設定を確認するには、**show cluster** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。

cluster standby-group

既存の Hot Standby Router Protocol（HSRP; ホット スタンバイ ルータ プロトコル）にクラスタをバインドして、クラスタ コマンド スイッチ冗長をイネーブルにするには、**cluster standby-group** グローバル コンフィギュレーション コマンドを使用します。routing-redundancy キーワードを入力することで、同一の HSRP グループが、クラスタ コマンド スイッチの冗長性およびルーティングの冗長性に対して使用できるようになります。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。

cluster standby-group *HSRP-group-name* [**routing-redundancy**]

no cluster standby-group

構文の説明

HSRP-group-name	クラスタにバインドされる HSRP グループの名前。設定できるグループ名は 32 文字までです。
routing-redundancy	（任意）同一の HSRP スタンバイ グループをイネーブルにし、クラスタ コマンド スイッチの冗長性およびルーティングの冗長性に対して使用します。

デフォルト

クラスタは、どの HSRP グループにもバインドされません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、クラスタ コマンド スイッチ上でだけ入力できます。クラスタ メンバ スイッチでこれを入力すると、エラー メッセージが表示されます。

クラスタ コマンド スイッチは、クラスタ HSRP バインディング情報をすべてのクラスタ HSRP 対応メンバに伝播します。各クラスタ メンバ スイッチはバインディング情報を NVRAM（不揮発性 RAM）に保存します。HSRP グループ名は、有効なスタンバイ グループである必要があります。そうでない場合、エラーが発生してコマンドが終了します。

クラスタにバインドする HSRP スタンバイ グループのすべてのメンバに同じグループ名を使用する必要があります。バインドされる HSRP グループのすべてのクラスタ HSRP 対応メンバに同じ HSRP グループ名を使用してください （クラスタを HSRP グループにバインドしない場合には、クラスタ コマンダおよびメンバに異なる名前を使用できます）。

例

次の例では、*my_hsrp* という名前の HSRP グループをクラスタにバインドする方法を示します。このコマンドは、クラスタ コマンド スイッチ上から実行します。

```
Switch(config)# cluster standby-group my_hsrp
```

次の例では、同じ HSRP グループ名 *my_hsrp* を使用して、ルーティング冗長とクラスタ冗長を確立する方法を示します。

```
Switch(config)# cluster standby-group my_hsrp routing-redundancy
```

次の例では、このコマンドがクラスタ コマンド スイッチから実行され、指定された HSRP スタンバイ グループが存在しない場合のエラー メッセージを示します。

```
Switch(config)# cluster standby-group my_hsrp
%ERROR: Standby (my_hsrp) group does not exist
```

次の例では、このコマンドがクラスタ メンバ スイッチで実行された場合のエラー メッセージを示します。

```
Switch(config)# cluster standby-group my_hsrp routing-redundancy
%ERROR: This command runs on a cluster command switch
```

設定を確認するには、**show cluster** 特権 EXEC コマンドを入力します。出力は、クラスタ内の冗長性がイネーブルになったかどうかを示します。

関連コマンド

コマンド	説明
standby ip	インターフェイスで HSRP をイネーブルにします。
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。
show standby	スタンバイ グループ情報を表示します。

cluster timer

ハートビート メッセージの間隔を秒単位で設定するには、クラスタ コマンド スイッチ上で **cluster timer** グローバル コンフィギュレーション コマンドを使用します。デフォルト値の間隔を設定する場合は、このコマンドの **no** 形式を使用します。

cluster timer *interval-in-secs*

no cluster timer

構文の説明

interval-in-secs	ハートビート メッセージ間の間隔（秒）。指定できる範囲は 1 ～ 300 秒です。

デフォルト

8 秒間隔です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドと **cluster holdtime** グローバル コンフィギュレーション コマンドは、クラスタ コマンド スイッチ上に限り入力してください。クラスタ内のすべてのスイッチ間で設定の一貫性が保たれるように、クラスタ コマンド スイッチはこの値をそのすべてのクラスタ メンバに伝達します。

ホールドタイムは通常ハートビート インターバル タイマー（**cluster timer**）の倍数として設定されます。たとえば、スイッチのダウンを宣言するまでには、「ホールド タイムをインターバル タイムで割った秒数」回のハートビート メッセージが連続して受信されなかったことになります。

例

次の例では、クラスタ コマンド スイッチでハートビート間隔のタイマーおよび期間を変更する方法を示します。

```
Switch(config)# cluster timer 3
Switch(config)# cluster holdtime 30
```

設定を確認するには、**show cluster** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。

define interface-range

インターフェイス範囲のマクロを作成するには、**define interface-range** グローバル コンフィギュレーション コマンドを使用します。定義されたマクロを削除するには、このコマンドの **no** 形式を使用します。

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

no define interface-range *macro-name interface-range*

構文の説明

macro-name	インターフェイス範囲マクロの名前（最大 32 文字）
interface-range	インターフェイス範囲。インターフェイス範囲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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

マクロ名は、最大 32 文字の文字列です。

マクロには、最大 5 つの範囲を含めることができます。

ある範囲内のすべてのインターフェイスは同じタイプ、つまり、すべてがファスト イーサネット ポート、すべてがギガビット イーサネット ポート、すべてが EtherChannel ポート、またはすべてが VLAN のいずれかでなければなりません。ただし、マクロ内では複数のインターフェイス タイプを組み合わせることができます。

interface-range を入力する場合は、次のフォーマットを使用します。

- *type* {*first-interface*} - {*last-interface*}
- *interface-range* を入力するときは、最初のインターフェイス番号とハイフンの間にスペースを入れます。たとえば、**gigabitethernet 1/0/1 - 2** は有効な範囲ですが、**gigabitethernet 1/0/1-2** は有効な範囲ではありません。

type および *interface* の有効値は次のとおりです。

- **vlan** *vlan-id* - *vlan-id*（vlan-id の範囲は 1 ～ 4094）

  VLAN インターフェイスは、**interface vlan** コマンドで設定する必要があります（**show running-config** 特権 EXEC コマンドは、設定された VLAN インターフェイスを表示します）。**show running-config** コマンドで表示されない VLAN インターフェイスは、*interface-range* では使用できません。
- **port-channel** *port-channel-number*、ここで、*port-channel-number* は 1 ～ 48 です。
- **fastethernet** stack member/module/{*first port*} - {*last port*}
- **gigabitethernet** stack member/module/{*first port*} - {*last port*}

物理インターフェイス

- stack member は、スタック内のスイッチ識別に使用する番号です。番号に指定できる範囲は 1 ～ 9 で、スタック メンバの最初の初期化の際に、スイッチに割り当てられます。
- モジュールは常に 0 です。
- 使用可能範囲は、*type stack member*/**0**/*number* - *number* です（例：**gigabitethernet 1/0/1/1 - 2**）。

範囲を定義するときは、ハイフン（-）の前にスペースが必要です。次に例を示します。

- **gigabitethernet1/0/1/1 - 2**

複数の範囲を入力することもできます。複数の範囲を定義するときは、カンマ（,）の前の最初のエントリの後にスペースを入力する必要があります。カンマの後のスペースは任意になります。次に例を示します。

- **fastethernet1/0/1/3, gigabitethernet**1/0/1/1 **- 2**
- **fastethernet1/0/1/3 -4, gigabitethernet**1/0/1/1 **- 2**

例

次の例では、複数のインターフェイス マクロを作成する方法を示します。

```
Switch(config)# define interface-range macro1 fastethernet1/01 - 2, gigabitethernet1/0/1 - 2
```

関連コマンド

コマンド	説明
interface range	複数のポートで 1 つのコマンドを同時に実行します。
show running-config	定義されたマクロを含む現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」> 「File Management Commands」> 「Configuration File Management Commands」を選択してください。

delete

フラッシュ メモリ デバイス上のファイルまたはディレクトリを削除するには、**delete** 特権 EXEC コマンドを使用します。

delete [**/force**] [**/recursive**] *filesystem***:***/file-url*

構文の説明

/force	（任意）削除を確認するプロンプトを抑制します。
/recursive	（任意）指定されたディレクトリおよびそのディレクトリに含まれるすべてのサブディレクトリおよびファイルを削除します。
*filesystem***:**	フラッシュ ファイル システムのエイリアスです。 スタック メンバまたはスタック マスター上のローカル フラッシュ ファイル システムの構文： **flash:** スタック マスターから、スタック メンバ上のローカル フラッシュ ファイル システムの構文： **flash** *member number***:** **（注）**
/file-url	削除するパス（ディレクトリ）およびファイル名

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

/force キーワードを使用すると、削除プロセスにおいて削除の確認を要求するプロンプトが、最初の 1 回だけとなります。

/force キーワードを指定せずに **/recursive** キーワードを使用すると、ファイルごとに削除の確認を要求するプロンプトが表示されます。

プロンプト動作は、**file prompt** グローバル コンフィギュレーション コマンドの設定によって異なります。デフォルトでは、スイッチは、破壊的なファイル操作に関する確認をプロンプトで要求します。このコマンドの詳細については、『*Cisco IOS Command Reference for Release 12.1*』を参照してください。

例

次の例では、新しいイメージのダウンロードが正常に終了した後で、古いソフトウェア イメージを含むディレクトリを削除する方法を示します。

```
Switch# delete /force /recursive flash:/old-image
```

dir *filesystem***:** 特権 EXEC コマンドを入力することにより、ディレクトリが削除されたかどうかを確認できます。

関連コマンド

コマンド	説明
archive download-sw	新しいイメージをスイッチにダウンロードし、既存のイメージを上書きまたは保存します。

deny（ARP アクセスリスト コンフィギュレーション）

DHCP バインディングとの照合に基づいて Address Resolution Protocol（ARP; アドレス解決プロトコル）パケットを拒否するには、**deny** ARP アクセス リスト コンフィギュレーション コマンドを使用します。アクセス リストから指定された Access Control Entry（ACE）を削除するには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

request	（任意）ARP 要求との一致を定義します。**request** を指定しない場合は、すべての ARP パケットに対して照合が行われます。
ip	送信側 IP アドレスを指定します。
any	すべての IP アドレスまたは MAC アドレスを拒否します。
host *sender-ip*	指定された送信側 IP アドレスを拒否します。
sender-ip sender-ip-mask	指定された範囲の送信側 IP アドレスを拒否します。
mac	送信側 MAC アドレスを拒否します。
host *sender-mac*	特定の送信側 MAC アドレスを拒否します。
sender-mac sender-mac-mask	指定された範囲の送信側 MAC アドレスを拒否します。
response ip	ARP 応答の IP アドレス値を定義します。
host *target-ip*	指定されたターゲット IP アドレスを拒否します。
target-ip target-ip-mask	指定された範囲のターゲット IP アドレスを拒否します。
mac	ARP 応答の MAC アドレス値を拒否します。
host *target-mac*	指定されたターゲット MAC アドレスを拒否します。
target-mac target-mac-mask	指定された範囲のターゲット MAC アドレスを拒否します。
log	（任意）ACE と一致するパケットを記録します。

デフォルト

デフォルト設定はありません。ただし、ARP アクセス リストの末尾に暗黙の **deny ip any mac any** コマンドがあります。

コマンド モード

ARP アクセス リスト コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

deny 句を追加すると、一致条件に基づいて ARP パケットをドロップできます。

例

次の例では、ARP アクセス リストを定義し、IP アドレスが 1.1.1.1 で MAC アドレスが 0000.0000.abcd のホストからの ARP 要求と ARP 応答の両方を拒否する方法を示します。

```
Switch(config)# arp access-list static-hosts
Switch(config-arp-nacl)# deny ip host 1.1.1.1 mac host 0000.0000.abcd
Switch(config-arp-nacl)# end
```

設定を確認するには、**show arp access-list** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
arp access-list	ARP ACL を定義します。
ip arp inspection filter vlan	スタティック IP アドレスで設定されたホストからの ARP 要求および応答を許可します。
permit（ARP アクセスリスト コンフィギュレーション）	DHCP バインディングとの一致に基づいて ARP パケットを許可します。
show arp access-list	ARP アクセス リストに関する詳細を表示します。

deny（IPv6 アクセスリスト コンフィギュレーション）

IPv6 アクセス リスト コンフィギュレーション モードで、**deny** コマンドを使用して IPv6 アクセス リストの拒否条件を設定します。拒否条件を削除するには、このコマンドの **no** 形式を使用します。

deny {*protocol*} {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**fragments**] [**log**] [**log-input**] [**sequence** *value*] [**time-range** *name*]

no deny {*protocol*} {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**fragments**] [**log**] [**log-input**] [**sequence** *value*] [**time-range** *name*]

Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）

deny icmp {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*] | *icmp-message*] [**dscp** *value*] [**log**] [**log-input**] [**sequence** *value*] [**time-range** *name*]

Transmission Control Protocol（TCP; 伝送制御プロトコル）

deny tcp {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**ack**] [**dscp** *value*] [**established**] [**fin**] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**psh**] [**range** {*port* | *protocol*}] [**rst**] [**sequence** *value*] [**syn**] [**time-range** *name*] [**urg**]

User Datagram Protocol（UDP）

deny udp {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**range** {*port* | *protocol*}] [**sequence** *value*] [**time-range** *name*]

（注）　このコマンドは、スイッチ スタックでデュアル IPv4/IPv6 SDM テンプレートが設定されている場合に限り使用可能です。

構文の説明

protocol	インターネット プロトコルの名前または番号。**ahp**、**esp**、**icmp**、**ipv6**、**pcp**、**sctp**、**tcp**、または **udp** キーワードの 1 つ、あるいは IPv6 プロトコル番号を示す 0 ～ 255 の範囲の整数にすることができます。
source-ipv6-prefix/*prefix-length*	拒否条件を設定する送信元 IPv6 ネットワークまたはネットワークのクラス。 この引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。 **（注）** CLI ヘルプでは /0 ～ /128 のプレフィクス長が表示されますが、スイッチは集約可能なグローバル ユニキャストおよびリンク ローカル ホスト アドレスの /0 ～ /64 のプレフィクス、および Extended Universal Identifier（EUI）ベースの /128 プレフィクスに対してだけ IPv6 アドレス照合をサポートします。
any	IPv6 プレフィクス ::/0 の省略形。
host *source-ipv6-address*	拒否条件を設定する送信元 IPv6 ホスト アドレス。 この *source-ipv6-address* 引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。
operator [*port-number*]	（任意）指定のプロトコルの送信元または宛先ポートを比較する演算子を指定します。演算子は、**lt**（less than：未満）、**gt**（greater than：より大きい）、**eq**（equal：一致）、**neq**（not equal：不一致）、**range**（inclusive range：包含範囲）です。 *source-ipv6-prefix*/*prefix-length* 引数の後ろに演算子が置かれた場合、送信元ポートと一致する必要があります。 *destination-ipv6-prefix/prefix-length* 引数の後ろに演算子が置かれた場合、宛先ポートと一致する必要があります。 **range** 演算子には 2 つのポート番号が必要です。他のすべての演算子は 1 つのポート番号が必要です。 任意の *port-number* 引数は 10 進数、または TCP あるいは UDP ポートの名前です。ポート番号の範囲は 0 ～ 65535 です。TCP ポート名は TCP をフィルタリングする場合に限り使用できます。UDP ポート名は UDP をフィルタリングする場合に限り使用できます。
destination-ipv6-prefix/*prefix-length*	拒否条件を設定する宛先 IPv6 ネットワークまたはネットワークのクラス。 この引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。 **（注）** CLI ヘルプでは /0 ～ /128 のプレフィクス長が表示されますが、スイッチは集約可能なグローバル ユニキャストおよびリンク ローカル ホスト アドレスの /0 ～ /64 のプレフィクス、および EUI ベースの /128 プレフィクスに対してだけ IPv6 アドレス照合をサポートします。
host *destination-ipv6-address*	拒否条件を設定する宛先 IPv6 ホスト アドレス。 この *destination-ipv6-address* 引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。
dscp *value*	（任意）各 IPv6 パケット ヘッダーのトラフィック クラス フィールドのトラフィック クラス値と Differentiated Service Code Point（DSCP）値を照合します。指定できる範囲は 0 ～ 63 です。

fragments	（任意）フラグメント拡張ヘッダーに 0 以外のフラグメント オフセットが含まれる場合、非初期フラグメント パケットを照合します。**fragments** キーワードは、プロトコルが **ipv6** で *operator* [*port-number*] 引数が指定されていない場合に限り、指定できるオプションです。
log	（任意）エントリと一致するパケットに関する情報ロギング メッセージをコンソールに送信します （コンソールに送信するメッセージ レベルは **logging console** コマンドで制御します）。 メッセージには、アクセス リスト名、シーケンス番号、パケットが拒否されたかどうか、プロトコル（TCP、UDP、ICMP または番号のいずれか）、適正な場合には送信元/宛先アドレス、送信元/宛先ポート番号が含まれます。メッセージは、一致した最初のパケットに対して生成され、その後、5 分間隔で拒否されたパケット数を含めて生成されます。 **（注）**　ロギングはポート ACL ではサポートされません。
log-input	（任意）**log** キーワードと同じ機能を提供します（ただし、ロギング メッセージには受信インターフェイスも表示されます）。
sequence *value*	（任意）アクセス リスト ステートメントのシーケンス番号を指定します。指定できる範囲は 1 ～ 4294967295 です。
time-range *name*	（任意）拒否ステートメントに適用する時間範囲を指定します。時間範囲の名前と制限事項は、**time-range** コマンドと、**absolute** または **periodic** コマンドによってそれぞれ指定します。
icmp-type	（任意）ICMP パケットのフィルタリングに ICMP メッセージ タイプを指定します。ICMP パケットは ICMP メッセージ タイプによってフィルタリングできます。メッセージ タイプの番号は 0 ～ 255 です。
icmp-code	（任意）ICMP パケットのフィルタリングに ICMP メッセージ コードを指定します。ICMP メッセージ タイプによってフィルタリングされる ICMP パケットは、ICMP メッセージ コードによってもフィルタリングできます。メッセージ コードの番号は 0 ～ 255 です。
icmp-message	（任意）ICMP パケットのフィルタリングに ICMP メッセージ名を指定します。ICMP パケットは、ICMP メッセージ名、または ICMP メッセージ タイプおよびコードによってフィルタリングできます。使用可能な名前については、「使用上のガイドライン」の項を参照してください。
ack	（任意）TCP プロトコルの場合に限り ACK ビットを設定します。
established	（任意）TCP プロトコルの場合に限り、接続が確立済みであることを意味します。TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われます。接続するための初期 TCP データグラムの場合は照合しません。
fin	（任意）TCP プロトコルの場合に限り、FIN ビットを設定します。送信元からのデータはこれ以上ありません。
neq {*port* | *protocol*}	（任意）指定のポート番号上にないパケットだけを照合します。
psh	（任意）TCP プロトコルの場合に限り、PSH ビットを設定します。
range {*port* | *protocol*}	（任意）ポート番号範囲のパケットだけを照合します。
rst	（任意）TCP プロトコルの場合に限り RST ビットを設定します。
syn	（任意）TCP プロトコルの場合に限り SYN ビットを設定します。
urg	（任意）TCP プロトコルの場合に限り URG ビットを設定します。

（注）　**flow-label**、**routing** および **undetermined-transport** キーワードはコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

デフォルト

IPv6 アクセス リストは定義されていません。

コマンド モード

IPv6 アクセス リスト コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

deny（IPv6 アクセス リスト コンフィギュレーション モード）コマンドは、IPv6 固有である点を除き、**deny**（IPv4 アクセス リスト コンフィギュレーション モード）コマンドと類似しています。

IPv6 アクセス リスト コンフィギュレーション モードを開始し、パケットがアクセス リストを通過する条件を定義するには、**ipv6 access-list** コマンドの後ろに **deny**（IPv6）コマンドを使用します。

protocol 引数に IPv6 を指定すると、パケットの IPv6 ヘッダーに対して照合を行います。

デフォルトでは、アクセス リストの最初のステートメントの番号は 10 で、その次のステートメントからは 10 ずつ増加します。

リスト全体を再入力しないで、**permit**、**deny**、または **remark** ステートメントを既存のアクセス リストに追加できます。リストの最後以外の場所に新しいステートメントを追加するには、挿入する場所を示す、既存の 2 つのエントリ番号の間にある適切なエントリ番号を持った新しいステートメントを作成します。

（注）　すべての IPv6 ACL には最後の一致条件として、暗黙の **permit icmp any any nd-na**、**permit icmp any any nd-ns**、および **deny ipv6 any any** ステートメントがあります。このうち 2 つの **permit** 条件は、ICMPv6 近隣探索を許可します。ICMPv6 近隣探索を許可しないで **icmp any any nd-na** または **icmp any any nd-ns** を拒否するには、明示的な拒否エントリが ACL 内にある必要があります。暗黙的な **deny ipv6 any any** ステートメントを有効にするには、IPv6 ACL に 1 つ以上のエントリを含める必要があります。

IPv6 近隣探索プロセスでは、IPv6 ネットワーク レイヤ サービスを使用します。したがって、デフォルトでは IPv6 ACL により、IPv6 近隣探索パケットのインターフェイス上での送受信が暗黙的に許可されます。IPv4 では、IPv6 近隣探索プロセスと同等の Address Resolution Protocol（ARP; アドレス解決プロトコル）は、別のデータリンク レイヤ プロトコルを使用します。したがってデフォルトでは、IPv4 ACL により、ARP パケットのインターフェイス上での送受信が暗黙的に許可されます。

source-ipv6-prefix/*prefix-length* と *destination-ipv6-prefix*/*prefix-length* の両方の引数をトラフィック フィルタリングに使用します （送信元プレフィクスはトラフィックの送信元に基づいて、宛先プレフィクスはトラフィックの宛先に基づいてトラフィックをフィルタリングします）。

スイッチは集約可能なグローバル ユニキャストおよびリンク ローカル ホスト アドレスの /0 ～ /64 のプレフィクスと EUI ベースの /128 プレフィクスだけをサポートします。

fragments キーワードは、プロトコルが **ipv6** で *operator* [*port-number*] 引数が指定されていない場合に限り、指定できるオプションです。

次に、ICMP メッセージ名を表示します。

beyond-scope	destination-unreachable
echo-reply	echo-request
header	hop-limit
mld-query	mld-reduction
mld-report	nd-na
nd-ns	next-header
no-admin	no-route
packet-too-big	parameter-option
parameter-problem	port-unreachable
reassembly-timeout	renum-command
renum-result	renum-seq-number
router-advertisement	router-renumbering
router-solicitation	time-exceeded
unreachable	

例

次の例では、CISCO という名の IPv6 アクセス リストを設定し、そのアクセス リストをレイヤ 3 インターフェイス上の発信トラフィックに適用する方法を示します。リストの最初の拒否エントリは、5000 より大きい宛先 TCP ポート番号を持ったパケットすべてがインターフェイスで送信されるのを防ぎます。リストの 2 番目の拒否エントリは、5000 未満の送信元 UDP ポート番号を持ったパケットすべてがインターフェイスで送信されるのを防ぎます。また、この 2 番目の拒否エントリは、すべての一致をコンソールに表示します。リストの最初の許可エントリは、すべての ICMP パケットのインターフェイスでの送信を許可します。リストの 2 番目の許可エントリは、その他すべてのトラフィックのインターフェイスでの送信を許可します。すべてのパケットを拒否する暗黙の条件が各 IPv6 アクセス リストの末尾にあるため、この 2 番目の許可エントリが必要となります。

```
Switch(config)# ipv6 access-list CISCO
Switch(config-ipv6-acl)# deny tcp any any gt 5000
Switch config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# permit any any
Switch(config-ipv6-acl)# exit
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter CISCO out
```

関連コマンド

コマンド	説明
ipv6 access-list	IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ipv6 traffic-filter	インターフェイス上の着信または発信 IPv6 トラフィックをフィルタリングします。

コマンド	説明
permit（IPv6 アクセス リスト コンフィギュレーション）	IPv6 アクセス リストに許可条件を設定します。
show ipv6 access-list	現在のすべての IPv6 アクセス リストの内容を表示します。

deny（MAC アクセスリスト コンフィギュレーション）

条件が一致した場合に、非 IP トラフィックの転送を回避するには、**deny** MAC アクセス リスト コンフィギュレーション コマンドを使用します。拒否条件を名前付き MAC アクセス リストから削除するには、このコマンドの **no** 形式を使用します。

{**deny** | **permit**} {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **cos** *cos* | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* |**mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**]

no {**deny** | **permit**} {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **cos** *cos* | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**]

構文の説明

any	あらゆる送信元または宛先 MAC アドレスを拒否するために指定するキーワードです。
host *src MAC-addr* | *src-MAC-addr mask*	ホスト MAC アドレスと任意のサブネット マスクを定義します。パケットの送信元アドレスが定義されたアドレスに一致する場合、そのアドレスからの非 IP トラフィックは拒否されます。
host *dst-MAC-addr* | *dst-MAC-addr mask*	宛先 MAC アドレスと任意のサブネット マスクを定義します。パケットの宛先アドレスが定義されたアドレスに一致する場合、そのアドレスへの非 IP トラフィックは拒否されます。
type mask	（任意）パケットの Ethertype 番号と、Ethernet II または Subnetwork Access Protocol（SNAP）カプセル化を使用して、パケットのプロトコルを識別します。 *type* には、0 ～ 65535 の 16 進数を指定できます。 *mask* は、一致をテストする前に Ethertype に適用される *don’t care* ビットのマスクです。
aarp	（任意）データリンク アドレスをネットワーク アドレスにマッピングする Ethertype AppleTalk Address Resolution Protocol を選択します。
amber	（任意）EtherType DEC-Amber を選択します。
cos *cos*	（任意）プライオリティを設定するため、0 ～ 7 までの Class of Service（CoS; サービス クラス）値を選択します。CoS に基づくフィルタリングは、ハードウェアでだけ実行可能です。**cos** オプションが設定されているかどうかを確認する警告メッセージが表示されます。
dec-spanning	（任意）EtherType Digital Equipment Corporation（DEC）スパニング ツリーを選択します。
decnet-iv	（任意）EtherType DECnet Phase IV プロトコルを選択します。
diagnostic	（任意）EtherType DEC-Diagnostic を選択します。
dsm	（任意）EtherType DEC-DSM を選択します。
etype-6000	（任意）EtherType 0x6000 を選択します。
etype-8042	（任意）EtherType 0x8042 を選択します。
lat	（任意）EtherType DEC-LAT を選択します。
lavc-sca	（任意）EtherType DEC-LAVC-SCA を選択します。

lsap *lsap-number mask*	（任意）パケットの LSAP 番号（0 ～ 65535）と 802.2 カプセル化を使用して、パケットのプロトコルを識別します。 *mask* は、一致をテストする前に LSAP 番号に適用される *don’t care* ビットのマスクです。
mop-console	（任意）EtherType DEC-MOP Remote Console を選択します。
mop-dump	（任意）EtherType DEC-MOP Dump を選択します。
msdos	（任意）EtherType DEC-MSDOS を選択します。
mumps	（任意）EtherType DEC-MUMPS を選択します。
netbios	（任意）EtherType DEC-Network Basic Input/Output System（NETBIOS）を選択します。
vines-echo	（任意）Banyan Systems による EtherType Virtual Integrated Network Service（VINES）を選択します。
vines-ip	（任意）EtherType VINES IP を選択します。
xns-idp	（任意）10 進数、16 進数、または 8 進数の任意の Ethertype である EtherType Xerox Network Systems（XNS）プロトコル スイート（0 ～ 65535）を選択します。

（注）　**appletalk** は、コマンドラインのヘルプ ストリングには表示されますが、一致条件としてはサポートされていません。

IPX トラフィックをフィルタリングするには、使用されている IPX カプセル化のタイプに応じて、*type mask* または **lsap** *lsap mask* キーワードを使用します。表 2-9 に、Novell 用語と Cisco IOS 用語での IPX カプセル化タイプに対応するフィルタ条件を一覧表示します。

表 2-9　IPX フィルタ基準

IPX カプセル化タイプ		
Cisco IOS 名	**Novel 名**	**フィルタ基準**
arpa	Ethernet II	Ethertype 0x8137
snap	Ethernet-snap	Ethertype 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

デフォルト

このコマンドには、デフォルトはありません。ただし、名前付き MAC ACL のデフォルト アクションは拒否です。

コマンド モード

MAC アクセス リスト コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

MAC アクセス リスト コンフィギュレーション モードを開始するには、**mac access-list extended** グローバル コンフィギュレーション コマンドを使用します。

host キーワードを使用した場合、アドレス マスクは入力できません。**host** キーワードを使用しない場合は、アドレス マスクを入力する必要があります。

Access Control Entry（ACE）がアクセス コントロール リストに追加された場合、リストの最後には暗黙の **deny-any-any** 条件が存在します。つまり、一致がない場合にはパケットは拒否されます。ただし、最初の ACE が追加される前に、リストはすべてのパケットを許可します。

名前付き MAC 拡張アクセス リストの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、すべての送信元から MAC アドレス 00c0.00a0.03fa への NETBIOS トラフィックを拒否する名前付き MAC 拡張アクセス リストを定義する方法を示します。このリストに一致するトラフィックは拒否されます。

```
Switch(config-ext-macl)# deny any host 00c0.00a0.03fa netbios.
```

次の例では、名前付き MAC 拡張アクセス リストから拒否条件を削除する方法を示します。

```
Switch(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
```

次の例では、Ethertype 0x4321 のすべてのパケットを拒否します。

```
Switch(config-ext-macl)# deny any any 0x4321 0
```

設定を確認するには、**show access-lists** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mac access-list extended	非 IP トラフィック用に MAC アドレス ベースのアクセス リストを作成します。
permit（MAC アクセスリスト コンフィギュレーション）	条件が一致した場合に非 IP トラフィックが転送されるのを許可します。
show access-lists	スイッチに設定された ACL を表示します。

diagnostic monitor

diagnostic monitor 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、ヘルス モニタリング診断テストを設定します。テストをディセーブルにし、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。

diagnostic monitor switch {*num*} **test** {*test-id* | *test-id-range* | **all**}

diagnostic monitor interval switch {*num*} **test** {*test-id* | *test-id-range* | **all**} *hh:mm:ss milliseconds day*

diagnostic monitor syslog

diagnostic monitor threshold switch {*num*} **test** {*test-id* | *test-id-range* | **all**} **count failure** *count*

no diagnostic monitor switch {*num*} **test** {*test-id* | *test-id-range* | **all**}

no diagnostic monitor interval switch {*num*} **test** {*test-id* | *test-id-range* | **all**}

no diagnostic monitor syslog

no diagnostic monitor threshold switch {*num*} **test** {*test-id* | *test-id-range* | **all**} **failure count**

構文の説明

switch *num*	モジュール番号を指定します。指定できる範囲は 1 ～ 9 です。
test	実行するテストを指定します。
test-id	実行するテストの識別番号。その他の情報については、「使用上のガイドライン」の項を参照してください。
test-id-range	実行するテストの識別番号の範囲。その他の情報については、「使用上のガイドライン」の項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。
interval	テストを実行する間隔を指定します。
hh:mm:ss	テストの時間間隔を指定します。形式については、「使用上のガイドライン」の項を参照してください。
milliseconds	時間（ミリ秒）を指定します。指定できる値は 0 ～ 999 です。
day	テストの間隔（日数）を指定します。形式については、「使用上のガイドライン」の項を参照してください。
Syslog	ヘルス モニタ診断テストが失敗した場合に Syslog メッセージを生成します。
threshold	障害しきい値を指定します。
failure count *count*	障害しきい値のカウントを指定します。

デフォルト

- モニタリングはディセーブルです。
- **syslog** がイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

テストをスケジューリングする場合、次の注意事項があります。

- *test-id* : テスト ID のリストを表示するには、**show diagnostic content** 特権 EXEC コマンドを入力します。
- *test-id-range* : テスト ID のリストを表示するには、**show diagnostic content** コマンドを入力します。カンマおよびハイフンで区切られた整数で範囲を入力します（例：1,3-6 はテスト ID 1、3、4、5 および 6）。
- *hh* : 時間（0 ～ 23）を入力します。
- *mm* : 分（0 ～ 60）を入力します。
- *ss* : 秒（0 ～ 60）を入力します。
- *milliseconds* : ミリ秒（0 ～ 999）を入力します。
- *day* : 0 ～ 20 の数字として日を入力します。

diagnostic monitor switch {*num*} **test** {*test-id* | *test-id-range* | **all**} 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。

- すべての接続ポートをディセーブルにし、ネットワーク トラフィックを隔離します。テスト中はテスト パケットを送出できません。
- システムまたはテスト済みモジュールをリセットした後で、システムを通常の動作モードに戻します。

（注）スタックのスイッチにリロードされた属性がある診断テストを実行している場合、ケーブル接続の設定に応じてスタックをパーティションで区切ることができます。スタックをパーティションで区切らないようにするには、**show switch detail** 特権 EXEC コマンドを入力して、スタック設定を確認する必要があります。

例

次の例では、2 分ごとに指定したテストを行うように設定する方法を示します。

```
Switch(config)# diagnostic monitor interval switch 1 test 1 00:02:00 0 1
```

次の例では、ヘルス モニタが以前にイネーブルになっていない場合に、指定されたスイッチでテストを実行する方法を示します。

```
Switch(config)# diagnostic monitor switch 1 test 1
```

次の例では、スイッチ上でテスト モニタリング用の障害しきい値を設定する方法を示します。

```
Switch(config)# diagnostic monitor threshold switch 1 test 1 failure count 50
```

次の例では、ヘルス モニタ 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方法を示します。

```
Switch(config)# diagnostic monitor syslog
```

関連コマンド

コマンド	説明
show diagnostic	オンライン診断テストの結果を表示します。

diagnostic schedule

diagnostic schedule 特権 EXEC コマンドを使用して、診断テストのスケジューリングを設定します。スケジューリングを削除し、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。

diagnostic schedule switch *num* **test** {*test-id* | *test-id-range* | **all** | **basic** | **non-disruptive**} {**daily** *hh*:*mm* | **on** *mm dd yyyy hh*:*mm* | **weekly** *day-of-week hh*:*mm*}

no diagnostic schedule switch *num* **test** {*test-id* | *test-id-range* | **all** | **basic** | **non-disruptive**} {**daily** *hh*:*mm* | **on** *mm dd yyyy hh*:*mm* | **weekly** *day-of-week hh*:*mm*}

構文の説明

switch *num*	スイッチ番号を指定します。指定できる範囲は 1 ～ 9 です。
test	スケジューリングするテストを指定します。
test-id	実行するテストの識別番号。その他の情報については、「使用上のガイドライン」の項を参照してください。
test-id-range	実行するテストの識別番号の範囲。その他の情報については、「使用上のガイドライン」の項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。
basic	基本的なオンデマンドの診断テストを実行します。
non-disruptive	ノンディスラプティブ ヘルスモニタ テストを実行します。
daily *hh*:*mm*	テストベースの診断タスクのスケジュール（日単位）を指定します。形式については、「使用上のガイドライン」の項を参照してください。
on *mm dd yyyy hh*:*mm*	テストベースの診断タスクのスケジュールを指定します。形式については、「使用上のガイドライン」の項を参照してください。
weekly *day-of-week hh*:*mm*	テストベースの診断タスクのスケジュール（週単位）を指定します。形式については、「使用上のガイドライン」の項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

コマンド履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

テストをスケジューリングする場合、次の注意事項があります。

- *test-id* : テスト ID のリストを表示するには、**show diagnostic content** コマンドを入力します。
- *test-id-range* : テスト ID のリストを表示するには、**show diagnostic content** コマンドを入力します。カンマおよびハイフンで区切られた整数で範囲を入力します（例 : 1,3-6 はテスト ID 1、3、4、5 および 6）。
- *hh*:*mm* : 2 桁の数字（24 時間表記）で時間および分を入力します。コロン（**:**）が必要です。

- *mm*：January、February ～ December のように、月を入力します（大文字または小文字のいずれかを使用）。
- *dd*：2 桁の数字で日を入力します。
- *yyyy*：4 桁の数字で年を入力します。
- *day-of-week*：Monday、Tuesday ～ Sunday のように、曜日を入力します（大文字または小文字のいずれかを使用）。

例

次の例では、特定のスイッチに対して特定の日時に診断テストをスケジューリングする方法を示します。

```
Switch(config)# diagnostic schedule switch 1 test 1,2,4-6 on january 3 2006 23:32
```

次の例では、指定されたスイッチで毎週特定の時間に診断テストを行うようスケジューリングする方法を示します。

```
Switch(config)# diagnostic schedule switch 1 test 1,2,4-6 weekly friday 09:23
```

関連コマンド

コマンド	説明
show diagnostic	オンライン診断テストの結果を表示します。

diagnostic start

指定した診断テストを実行するには、**diagnostic start** ユーザ コマンドを使用します。

diagnostic start switch *num* **test** {*test-id* | *test-id-range* | **all** | **basic** | **non-disruptive**}

構文の説明

switch *num*	スイッチ番号を指定します。指定できる範囲は 1 ～ 9 です。
test	実行するテストを指定します。
test-id	実行するテストの識別番号。その他の情報については、「使用上のガイドライン」の項を参照してください。
test-id-range	実行するテストの識別番号の範囲。その他の情報については、「使用上のガイドライン」の項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。
basic	基本的なオンデマンドの診断テストを実行します。
non-disruptive	ノンディスラプティブ ヘルスモニタ テストを実行します。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

テスト ID のリストを表示するには、**show diagnostic content** コマンドを入力します。

test-id-range をカンマおよびハイフンで区切られた整数で入力します（例：1,3-6 はテスト ID 1、3、4、5、および 6）。

例

次の例では、特定のスイッチで診断テストを実行する方法を示します。

```
Switch> diagnostic start switch 1 test 1
Switch>
06:27:50: %DIAG-6-TEST_RUNNING: Switch 1: Running TestPortAsicStackPortLoopback{ID=1} ...
(switch-1)
06:27:51: %DIAG-6-TEST_OK: Switch 1: TestPortAsicStackPortLoopback{ID=1} has completed
successfully (switch-1)
```

次の例では、正常なシステム動作を阻害するスイッチに診断テスト 2 を開始する方法を示します。

```
Switch> diagnostic start switch 1 test 2
Switch 1: Running test(s) 2 will cause the switch under test to reload after completion of
the test list.
Switch 1: Running test(s) 2 may disrupt normal system operation
Do you want to continue?[no]: y
Switch>
16:43:29: %STACKMGR-2-STACK_LINK_CHANGE: Stack Port 2 Switch 2 has changed to state DOWN
```

```
16:43:30: %STACKMGR-2-STACK_LINK_CHANGE: Stack Port 1 Switch 9 has changed to state DOWN
16:43:30: %STACKMGR-2-SWITCH_REMOVED: Switch 1 has been REMOVED from the stack
Switch#
16:44:35: %STACKMGR-2-STACK_LINK_CHANGE: Stack Port 1 Switch 2 has changed to state UP
16:44:37: %STACKMGR-2-STACK_LINK_CHANGE: Stack Port 2 Switch 2 has changed to state UP
16:44:45: %STACKMGR-2-SWITCH_ADDED: Switch 1 has been ADDED to the stack
16:45:00: %STACKMGR-3-SWITCH_READY: Switch 1 is READY
16:45:00: %STACKMGR-2-STACK_LINK_CHANGE: Stack Port 1 Switch 1 has changed to state UP
16:45:00: %STACKMGR-2-STACK_LINK_CHANGE: Stack Port 2 Switch 1 has changed to state UP
00:00:20: %STACKMGR-2-SWITCH_ADDED: Switch 1 has been ADDED to the stack (Switch-1)
00:00:20: %STACKMGR-2-SWITCH_ADDED: Switch 2 has been ADDED to the stack (Switch-1)
00:00:25: %SPANTREE-3-EXTENDED_SYSID: Extended SysId enabled for type vlan (Switch-1)
00:00:29: %SYS-3-CONFIG_I: Configured from memory by console (Switch-1)
00:00:29: %STACKMGR-3-SWITCH_READY: Switch 2 is READY (Switch-1)
00:00:29: %STACKMGR-3-MASTER_READY: Master Switch 2 is READY (Switch-1)
00:00:30: %STACKMGR-3-SWITCH_READY: Switch 1 is READY (Switch-1)
00:00:30: %DIAG-6-TEST_RUNNING: Switch 1: Running TestPortAsicLoopback{ID=2} ...
(Switch-1)
00:00:30: %DIAG-6-TEST_OK: Switch 1: TestPortAsicLoopback{ID=2} has completed successfully
(Switch-1)
```

次のメッセージは、テストを実行することによりスタック接続性が失われる場合に表示されます。

```
Switch 3: Running test(s) 2 will cause the switch under test to reload after completion of
the test list.
Switch 3: Running test(s) 2 may disrupt normal system operation
Do you want to continue?[no]:
```

次のメッセージは、テストを実行することによりスタックの分離が発生する場合に表示されます。

```
Switch 4: Running test(s) 2 will cause the switch under test to reload after completion of
the test list.
Switch 4: Running test(s) 2 will partition stack
Switch 4: Running test(s) 2 may disrupt normal system operation
Do you want to continue?[no]:
```

関連コマンド

コマンド	説明
show diagnostic	オンライン診断テストの結果を表示します。

dot1x

IEEE 802.1x 認証をグローバルにイネーブルにするには、**dot1x** グローバル コンフィギュレーション 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 {**critical** {**eapol** | **recovery delay** *milliseconds*} | {**guest-vlan supplicant**} | **system-auth-control**}

no dot1x {**critical** {**eapol** | **recovery delay**} | {**guest-vlan supplicant**} | **system-auth-control**}

（注）　**credentials** *name* キーワードは、コマンドラインのヘルプ ストリングには表示されますが、サポートされていません。

構文の説明

critical {**eapol** | **recovery delay** *milliseconds*}	アクセス不能な認証バイパス パラメータを設定します。詳細は、**dot1x critical**（グローバル コンフィギュレーション）コマンドを参照してください。
guest-vlan supplicant	スイッチでオプションのゲスト VLAN の動作をグローバルにイネーブルにします。
system-auth-control	スイッチで IEEE 802.1x 認証をグローバルにイネーブルにします。

デフォルト

IEEE 802.1x 認証はディセーブルで、オプションのゲスト VLAN の動作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

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。
12.2(25)SE	**guest-vlan supplicant** キーワードが追加されました。
12.2(25)SEE	**critical** {**eapol** | **recovery delay** *milliseconds*} キーワードが追加されました。

使用上のガイドライン

IEEE 802.1x 認証をグローバルにイネーブルにする前に、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）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。方式リストには、ユーザの認証に使用する、順序と認証方式が記述されています。

スイッチの IEEE 802.1x 認証をグローバルにイネーブルにする前に、IEEE 802.1x 認証および EtherChannel が設定されているインターフェイスから EtherChannel の設定を削除します。

EAP-Transparent LAN Service（TLS）および EAP-MD5 で IEEE 802.1x を認証する Cisco Access Control Server（ACS）アプリケーションが稼動する装置を使用し、スイッチが Cisco IOS Release 12.1(14)EA1 を実行している場合、装置が ACS バージョン 3.2.1 以上で稼動していることを確認します。

guest-vlan supplicant キーワードを使用して、スイッチでオプションの IEEE 802.1x ゲスト VLAN の動作をグローバルにイネーブルにできます。詳細は、**dot1x guest-vlan** コマンドを参照してください。

例

次の例では、スイッチで IEEE 802.1x 認証をグローバルにイネーブルにする方法を示します。

```
Switch(config)# dot1x system-auth-control
```

次の例では、スイッチでオプションのゲスト VLAN の動作をグローバルにイネーブルにする方法を示します。

```
Switch(config)# dot1x guest-vlan supplicant
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x critical（グローバルコンフィギュレーション）	スイッチ上で、アクセス不能な認証バイパス機能のパラメータを設定します。
dot1x guest-vlan	アクティブ VLAN をイネーブルにし、IEEE 802.1x ゲスト VLAN として指定します。
dot1x port-control	ポートの認証ステートの手動制御をイネーブルにします。
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x auth-fail max-attempts

ポートが制限 VLAN に移行されるまでに許容される最大の認証試行回数を設定するには、**dot1x auth-fail max-attempts** 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。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 auth-fail max-attempts *max-attempts*

no dot1x auth-fail max-attempts

構文の説明

max-attempts	ポートが制限 VLAN に移行するまでに許容される最大の認証試行回数を指定します。指定できる範囲は 1 ～ 3 です。デフォルト値は 3 です。

デフォルト

デフォルト値は 3 回です。

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

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

VLAN で許容される最大の認証試行回数を再設定する場合、変更内容は再認証タイマーが期限切れになった後で反映されます。

例

次の例では、ポート 3 の制限 VLAN にポートが移行する前に許容される最大の認証試行回数を *2* に設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/01/3
Switch(config-if)# dot1x auth-fail max-attempts 2
Switch(config-if)# end
Switch(config)# end
Switch#
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x auth-fail vlan [*vlan id*]	オプションの制限 VLAN の機能をイネーブルにします。
dot1x max-reauth-req [*count*]	ポートが無許可ステートに移行する前に、スイッチが認証プロセスを再起動する最大回数を設定します。
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x auth-fail vlan

ポートで制限 VLAN をイネーブルにするには、**dot1x auth-fail vlan** 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。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 auth-fail vlan *vlan-id*

no dot1x auth-fail vlan

構文の説明

vlan-id	VLAN を 1 ～ 4094 の範囲で指定します。

デフォルト

制限 VLAN 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

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

次のように設定されたポートで制限 VLAN を設定できます。

- シングルホスト（デフォルト）モード
- 認証用 auto モード

再認証をイネーブルにする必要があります。ディセーブルになっていると、制限 VLAN のポートは再認証要求を受け取りません。再認証プロセスを開始するには、制限 VLAN がポートからリンクダウン イベントまたは Extensible Authentication Protocol（EAP）ログオフ イベントを受け取る必要があります。ホストがハブを介して接続されている場合、ホストが切断されているとポートがリンクダウン イベントを受け取ることができず、次の再認証試行が行われるまで新しいホストが検出されないことがあります。

サプリカントが認証に失敗すると、ポートは制限 VLAN に移行し、EAP *認証成功* メッセージがサプリカントに送信されます。サプリカントには実際の認証失敗が通知されないため、この制限ネットワーク アクセスに混乱が生じることがあります。EAP の成功メッセージは、次の理由で送信されます。

- EAP の成功メッセージが送信されない場合、サプリカントは 60 秒ごと（デフォルト）に EAP 開始メッセージを送信して認証を行おうとします。
- 一部のホスト（たとえば、Windows XP を実行中のデバイス）は、EAP の成功メッセージを受け取るまで Dynamic Host Configuration Protocol（DHCP）を実装できません。

サプリカントは、認証から EAP 成功メッセージを受け取った後で不正なユーザ名とパスワードの組み合わせをキャッシュし、再認証のたびにその情報を使用する可能性があります。サプリカントが正しいユーザ名とパスワードの組み合わせを送信するまで、ポートは制限 VLAN のままになります。

レイヤ 3 ポートに使用する内部 VLAN は、制限 VLAN として設定することはできません。

VLAN を制限 VLAN と音声 VLAN の両方に設定することはできません。そのように設定すると、syslog メッセージが生成されます。

制限 VLAN ポートが無許可ステートに移行すると、認証プロセスが再起動されます。サプリカントが再度認証プロセスに失敗すると、認証は保持ステートで待機します。サプリカントが正常に再認証された後、すべての IEEE 802.1x ポートが再初期化され、通常の IEEE 802.1x ポートとして扱われます。

制限 VLAN を異なる VLAN として再設定すると、制限 VLAN のポートも移行し、そのポートは現在認証されたステートのままになります。

制限 VLAN をシャットダウンするか VLAN データベースから削除すると、制限 VLAN のポートはただちに無許可ステートに移行し、認証プロセスが再起動します。制限 VLAN 設定がまだ存在するため、認証は保持ステートで待機しません。制限 VLAN が非アクティブである間も、制限 VLAN がアクティブになったときにポートがただちに制限 VLAN になるように、すべての認証試行がカウントされます。

制限 VLAN は、シングルホスト モード（デフォルトのポート モード）でだけサポートされます。そのため、ポートが制限 VLAN になると、サプリカントの MAC アドレスが MAC アドレス テーブルに追加され、ポートに表示される他の MAC アドレスは、すべてセキュリティ違反として扱われます。

例

次の例では、ポート 1 で制限 VLAN を設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/01/3
Switch(config-if)# dot1x auth-fail vlan 40
Switch(config-if)# end
Switch#
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x auth-fail max-attempts [*max-attempts*]	サプリカントを制限 VLAN に割り当てる前に、試行可能な認証回数を設定します。
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x control-direction

Wake-on-LAN（WoL）機能を搭載した IEEE 802.1x 認証をイネーブルにし、ポート制御を単一方向または双方向に設定するには、**dot1x control-direction** 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。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 control-direction {**both** | **in**}

no dot1x control-direction

構文の説明

both	ポートの双方向制御をイネーブルにします。ポートは、ホストにパケットを送受信できません。
in	ポートの単一方向制御をイネーブルにします。ポートは、ホストにパケットを送信できますが、受信はできません。

デフォルト

ポートは双方向モード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

コマンド履歴

リリース	変更内容
12.2(25)SEC	このコマンドが追加されました。

使用上のガイドライン

デフォルト設定の双方向モードに戻すには、このコマンドの **both** キーワードまたは **no** 形式を使用します。

WoL の詳細については、ソフトウェア コンフィギュレーション ガイドの「Configuring IEEE802.1x Port-Based Authentication」の章の「Using IEEE 802.1x Authentication with Wake-on-LAN」の項を参照してください。

例

次の例では、単一方向制御をイネーブルにする方法を示します。

```
Switch(config-if)# dot1x control-direction in
```

次の例では、双方向制御をイネーブルにする方法を示します。

```
Switch(config-if)# dot1x control-direction both
```

設定を確認するには、**show dot1x all** 特権 EXEC コマンドを入力します。

show dot1x all 特権 EXEC コマンド出力は、ポート名とポートのステートを除き、すべてのスイッチで同一です。ホストがポートに接続されていてまだ認証されていない場合、次のように表示されます。

```
Supplicant MAC 0002.b39a.9275
AuthSM State = CONNECTING
BendSM State = IDLE
PortStatus = UNAUTHORIZED
```

dot1x control-direction in インターフェイス コンフィギュレーション コマンドを入力して単一方向制御をイネーブルにする場合、これが **show dot1x all** コマンド出力で次のように表示されます。

```
ControlDirection  = In
```

dot1x control-direction in インターフェイス コンフィギュレーション コマンドを入力しても、設定の競合によりポートでこのモードをサポートできない場合、**show dot1x all** コマンド出力で次のように表示されます。

```
ControlDirection  = In (Disabled due to port settings)
```

関連コマンド

コマンド	説明
show dot1x [**all** | **interface** *interface-id*]	指定したインターフェイスに対する制御方向のポート設定ステータスを表示します。

dot1x credentials（グローバル コンフィギュレーション）

dot1x credentials 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、サプリカント スイッチでプロファイルを設定します。

dot1x credentials *profile*

no dot1x credentials *profile*

構文の説明

profile	サプリカント スイッチのプロファイルを指定します。

デフォルト

スイッチにプロファイルは設定されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

このスイッチをサプリカントにするには、オーセンティケータとして別のスイッチをセットアップしてある必要があります。

例

次の例では、スイッチをサプリカントとして設定する方法を示します。

```
Switch(config)# dot1x credentials profile
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
cisp enable	Client Information Signalling Protocol（CISP）をイネーブルにします。
show cisp	指定されたインターフェイスの CISP 情報を表示します。

dot1x critical（グローバル コンフィギュレーション）

dot1x critical 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、アクセス不能な認証バイパス機能のパラメータ（クリティカル認証または Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）失敗ポリシーともいう）を設定します。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 critical {**eapol** | **recovery delay** *milliseconds*}

no dot1x critical {**eapol | recovery delay**}

構文の説明

eapol	スイッチによりクリティカルなポートが critical-authentication ステートに置かれた場合、EAPOL-Success メッセージを送信するようスイッチを指定します。
recovery delay *milliseconds*	リカバリ遅延期間（ミリ秒）を設定します。指定できる範囲は 1 ～ 10000 ミリ秒です。

デフォルト

クリティカルなポートを critical-authentication ステートに置くことによってそのクリティカルなポートの認証に成功した場合に、スイッチは EAPOL-Success メッセージをホストに送信しません。

リカバリ遅延期間は、1000 ミリ秒（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

コマンド履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

クリティカルなポートが critical-authentication ステートに置かれた場合、スイッチが EAPOL-Success メッセージを送信するよう指定するには、**eapol** キーワードを使用します。

使用不能な RADIUS サーバが使用可能になった場合にスイッチがクリティカルなポートを再初期化するために待機するリカバリ遅延期間を設定するには、**recovery delay** *milliseconds* キーワードを使用します。デフォルトのリカバリ遅延期間は 1000 ミリ秒です。ポートは、秒単位で再初期化できます。

アクセス不能な認証バイパスをポート上でイネーブルにするには、**dot1x critical** 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。スイッチがクリティカルなポートに割り当てるアクセス VLAN を設定するには、**dot1x critical vlan** *vlan-id* 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。

例

次の例では、リカバリ遅延期間として 200 をスイッチに設定する方法を示します。

```
Switch# dot1x critical recovery delay 200
```

設定を確認するには、**show dot1x** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x critical（インターフェイス コンフィギュレーション）	アクセス不能な認証バイパス機能をイネーブルにし、この機能にアクセス VLAN を設定します。
show dot1x	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x critical（インターフェイス コンフィギュレーション）

dot1x critical インターフェイス コンフィギュレーション コマンドを使用して、アクセス不能な認証バイパス機能（クリティカル認証または Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）失敗ポリシーともいう）をイネーブルにします。ポートが critical-authentication ステートに置かれた場合にスイッチがクリティカルなポートに割り当てるアクセス VLAN を設定することもできます。この機能をディセーブルにするか、または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。

dot1x critical [**recovery action reinitialize** | **vlan** *vlan-id*]

no dot1x critical [**recovery** | **vlan**]

構文の説明

recovery action reinitialize	アクセス不能な認証バイパスのリカバリ機能をイネーブルにし、認証サーバが使用可能になった場合にリカバリ アクションによりポートを認証するよう指定します。
vlan *vlan-id*	スイッチがクリティカルなポートに割り当てることのできるアクセス VLAN を指定します。指定できる範囲は 1 ～ 4094 です。

デフォルト

アクセス不能認証バイパス機能はディセーブルです。

リカバリ アクションは設定されていません。

アクセス VLAN 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

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。
12.2(25)SEE	**vlan** *vlan-id* キーワードが追加されました。

使用上のガイドライン

ポートが critical-authentication ステートに置かれた場合にスイッチがクリティカルなポートに割り当てるアクセス VLAN を指定するには、**vlan** *vlan-id* キーワードを使用します。指定された VLAN タイプは、次のようにポート タイプに適合している必要があります。

- クリティカルなポートがアクセス ポートの場合、VLAN はアクセス VLAN でなければなりません。
- クリティカルなポートがプライベート VLAN のホスト ポートである場合、VLAN はセカンダリ プライベート VLAN でなければなりません。
- クリティカルなポートがルーテッド ポートの場合、VLAN を指定できます（指定は任意）。

クライアントで Windows XP を稼動し、クライアントが接続されているクリティカル ポートが critical-authentication ステートである場合、Windows XP はインターフェイスが認証されていないことを報告します。

Windows XP クライアントで DHCP が設定され、DHCP サーバからの IP アドレスがある場合、クリティカル ポートで EAP 認証成功メッセージを受信しても DHCP 設定プロセスを再初期化しません。

アクセス不能認証バイパス機能および制限 VLAN を IEEE802.1x ポート上に設定できます。スイッチが制限 VLAN でクリティカル ポートの再認証を試行し、RADIUS サーバがすべて使用できない場合、ポートの状態はクリティカル認証ステートに移行し、ポートは制限 VLAN のままとなります。

アクセス不能認証バイパス機能とポート セキュリティは、同じスイッチ ポートに設定できます。

例

次の例では、アクセス不能認証バイパス機能をポート上でイネーブルにする方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/01/3
Switch(config-if)# dot1x critical
Switch(config-if)# end
Switch(config)# end
Switch#
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x critical（グローバル コンフィギュレーション）	スイッチ上で、アクセス不能な認証バイパス機能のパラメータを設定します。
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x default

IEEE 802.1x パラメータをデフォルト値にリセットするには、**dot1x default** 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。

dot1x default

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルト値は次のとおりです。

- ポート単位の IEEE 802.1x プロトコルのイネーブル ステートはディセーブルです（force-authorized）。
- 再認証の試行間隔の秒数は 3600 秒です。
- 定期的な再認証はディセーブルです。
- 待機時間は 60 秒です。
- 再伝送時間は 30 秒です。
- 最高再伝送回数は 2 回です。
- ホスト モードはシングル ホストです。
- クライアントの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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	このコマンドは、インターフェイス コンフィギュレーション モードに変更されました。

例

次の例では、ポート上の IEEE 802.1x パラメータをリセットする方法を示します。

```
Switch(config-if)# dot1x default
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x fallback

IEEE 802.1x 認証をサポートしないクライアントに対し、Web 認証をフォールバック方式として使用するようにポートを設定するには、**dot1xfallback** 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。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 fallback *profile*

no dot1x fallback

構文の説明

profile	IEEE 802.1x 認証をサポートしていないクライアントのフォールバック プロファイルを指定します。

デフォルト

フォールバックはイネーブルではありません。

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

コマンド履歴

リリース	変更内容
12.2(35)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドを入力する前に、スイッチ ポートで **dot1x port-control** auto インターフェイス コンフィギュレーション コマンドを入力する必要があります。

例

次の例では、IEEE 802.1x 認証用に設定されているスイッチ ポートにフォールバック プロファイルを指定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/01/3
Switch(config-if)# dot1x fallback profile1
Switch(config-fallback-profile)# exit
Switch(config)# end
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。
fallback profile	Web 認証のフォールバック プロファイルを作成します。
ip admission	ポートで Web 認証をイネーブルにします。
ip admission name proxy http	スイッチで Web 認証をグローバルにイネーブルにします。

dot1x guest-vlan

アクティブな VLAN を IEEE 802.1x のゲスト VLAN として指定するには、**dot1x guest-vlan** 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。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 guest-vlan *vlan-id*

no dot1x guest-vlan

構文の説明

vlan-id	アクティブ VLAN を IEEE 802.1x ゲスト VLAN として指定します。指定できる範囲は 1 ～ 4094 です。

デフォルト

ゲスト VLAN は設定されません。

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

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。
12.2(25)SE	このコマンドは、デフォルトのゲスト VLAN の動作を変えるように変更されました。

使用上のガイドライン

次のいずれかのスイッチ ポートにゲスト VLAN を設定できます。

- 非プライベート VLAN に属するスタティックアクセス ポート
- セカンダリ プライベート VLAN に属するプライベート VLAN ポート。スイッチ ポートに接続されるすべてのホストは、端末状態の妥当性の評価に成功したかどうかにかかわらず、プライベート VLAN に割り当てられます。スイッチが、スイッチのプライマリおよびセカンダリ プライベート VLAN の対応付けを使用してプライマリ プライベート VLAN を判別します。

スイッチの IEEE 802.1x ポートごとにゲスト VLAN を設定して、現在 IEEE 802.1x 認証を実行していないクライアント（スイッチに接続されているデバイスまたはワークステーション）へのサービスを制限できます。こうしたユーザは IEEE 802.1x 認証のためにシステムをアップグレードできますが、Windows 98 システムなどのホストでは IEEE 802.1x に対応できません。

IEEE 802.1x ポートでゲスト VLAN をイネーブルにした場合、認証サーバが Extensible Authentication Protocol over LAN（EAPOL）Request/Identity フレームに対する応答を受信しない、あるいは EAPOL パケットがクライアントから送信されないと、スイッチではクライアントをゲスト VLAN に割り当てます。

スイッチは EAPOL パケット履歴を保持します。リンクの存続時間内に別の EAPOL パケットがインターフェイス上で検出された場合、ゲスト VLAN 機能はディセーブルになります。ポートがすでにゲスト VLAN ステートにある場合、ポートは無許可ステートに戻り、認証が再開されます。EAPOL 履歴はリンクの損失でリセットされます。

Cisco IOS Release 12.2(25)SE よりも前のスイッチでは、EAPOL パケット履歴を保持していなかったため、インターフェイスで EAPOL パケットが検出されたかどうかに関係なく、ゲスト VLAN への認証アクセスに失敗したクライアントを許可しました。Cisco IOS Release 12.2(25)SE で、このオプションの動作をイネーブルにするには、**dot1x guest-vlan supplicant** グローバル コンフィギュレーション コマンドを使用します。

ただし、Cisco IOS Release 12.2(25)SEE では、**dot1x guest-vlan supplicant** グローバル コンフィギュレーション コマンドはすでにサポートされていません。**dot1x auth-fail vlan** *vlan-id* インターフェイス コンフィギュレーション コマンドを入力すると、制限 VLAN を使用して、認証に失敗したクライアントにネットワーク アクセスを与えることができます。

スイッチ ポートがゲスト VLAN に移行すると、IEEE 802.1x 非対応クライアントはいくつでもアクセスが許可されます。IEEE 802.1x 対応クライアントが、ゲスト VLAN を設定しているポートと同じポートに加入すると、ポートは RADIUS 設定 VLAN またはユーザ設定アクセス VLAN では無許可ステートに移行し、認証が再開されます。

ゲスト VLAN は、シングルホスト モードおよびマルチホスト モードの IEEE 802.1x ポート上でサポートされます。

Remote Switched Port Analyzer（RSPAN）VLAN、プライマリ プライベート VLAN、または音声 VLAN 以外のアクティブなすべての VLAN は、IEEE 802.1x のゲスト VLAN として設定できます。ゲスト VLAN の機能は、内部 VLAN（ルーテッド ポート）またはトランク ポート上ではサポートされません。サポートされるのはアクセス ポートだけです。

DHCP クライアントが接続されている IEEE 802.1x ポートのゲスト VLAN を設定した後、DHCP サーバからホスト IP アドレスを取得する必要があります。クライアント上の DHCP プロセスが時間切れとなり、DHCP サーバからホスト IP アドレスを取得しようとする前に、スイッチ上の IEEE 802.1x 認証プロセスを再起動する設定を変更できます。IEEE 802.1x 認証プロセスの設定を減らします（**dot1x timeout quiet-period** および **dot1x timeout tx-period** インターフェイス コンフィギュレーション コマンド）。設定の減少量は、接続された IEEE 802.1x クライアントのタイプによって異なります。

スイッチは *MAC 認証バイパス* をサポートします。MAC 認証バイパスは IEEE 802.1x ポートでイネーブルの場合、スイッチは、EAPOL メッセージ交換を待機している間に IEEE802.1x 認証が期限切れになると、クライアントの MAC アドレスに基づいてクライアントを許可できます。スイッチは、IEEE 802.1x ポート上のクライアントを検出した後で、クライアントからのイーサネット パケットを待機します。スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。認証に失敗すると、スイッチはポートにゲスト VLAN を割り当てます（指定されていない場合）。詳細については、ソフトウェア コンフィギュレーション ガイドの「Configuring IEEE802.1x Port-Based Authentication」の章の「Using IEEE 802.1x Authentication with MAC Authentication Bypass」の項を参照してください。

例

次の例では、VLAN 5 を IEEE 802.1x ゲスト VLAN として指定する方法を示します。

```
Switch(config-if)# dot1x guest-vlan 5
```

次の例では、スイッチの待機時間を 3 秒に設定し、スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を 15 に設定する方法、および IEEE 802.1x ポートが DHCP クライアントに接続されているときに VLAN 2 を IEEE 802.1x ゲスト VLAN としてイネーブルにする方法を示します。

```
Switch(config-if)# dot1x timeout quiet-period 3
Switch(config-if)# dot1x timeout tx-period 15
Switch(config-if)# dot1x guest-vlan 2
```

次の例では、オプションのゲスト VLAN の動作をイネーブルにし、VLAN 5 を IEEE 802.1x ゲスト VLAN として指定する方法を示します。

```
Switch(config)# dot1x guest-vlan supplicant
Switch(config)# interface gigabitethernet1/01/3
Switch(config-if)# dot1x guest-vlan 5
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x	オプションのゲスト VLAN のサプリカント機能をイネーブルにします。
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x host-mode

IEEE802.1x 許可ポート上で、シングルホスト（クライアント）または複数のホストを許可するには、**dot1x host-mode** 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。IEEE802.1x 許可ポート上で、マルチドメイン認証（MDA）をイネーブルにするには、**multi-domain** キーワードを使用します。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 host-mode {**multi-host** | **single-host** | **multi-domain**}

no dot1x host-mode [**multi-host** | **single-host** | **multi-domain**}

構文の説明

multi-host	スイッチでマルチホスト モードをイネーブルにします。
single-host	スイッチでシングルホスト モードをイネーブルにします。
multi-domain	スイッチ ポートで MDA をイネーブルにします。

デフォルト

デフォルト設定は、シングルホスト モードです。

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

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。**dot1x multiple-hosts** インターフェイス コンフィギュレーション コマンドに替わるものです。
12.2(35)SE	**multi-domain** キーワードが追加されました。

使用上のガイドライン

このコマンドを使用すると、IEEE 802.1x 対応ポートを単一のクライアントに限定したり、複数のクライアントを IEEE 802.1x 対応ポートに接続したりすることができます。マルチホスト モードでは、接続されたホストのうち 1 つだけが許可されれば、すべてのホストのネットワーク アクセスが許可されます。ポートが無許可ステートになった場合（再認証が失敗した場合、または Extensible Authentication Protocol over LAN（EAPOL）-Logoff メッセージを受信した場合）には、接続されたすべてのクライアントがネットワーク アクセスを拒否されます。

ポートで MDA をイネーブルにするには、**multi-domain** キーワードを使用します。MDA はポートをデータ ドメインと音声ドメインの両方に分割します。MDA により、データ装置と IP Phone などの音声装置（シスコ製品またはシスコ以外の製品）の両方が同じ IEEE 802.1x 対応ポート上で許可されます。

このコマンドを入力する前に、指定のポートで **dot1x port-control** インターフェイス コンフィギュレーション コマンドが **auto** に設定されていることを確認します。

例

次の例では、IEEE 802.1x 認証をグローバルにイネーブルにして、ポートの IEEE 802.1x 認証をイネーブルにし、マルチホスト モードをイネーブルにする方法を示します。

```
Switch(config)# dot1x system-auth-control
Switch(config)# interface gigabitethernet1/01/3
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
```

次の例では、IEEE 802.1x 認証をグローバルにイネーブルにし、IEEE 802.1x 認証をイネーブルにし、指定されたポートで MDA をイネーブルにする方法を示します。

```
Switch(config)# dot1x system-auth-control
Switch(config)# interface gigabitethernet1/01/3
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x initialize

ポート上で新しく認証セッションを初期化する前に、指定の IEEE 802.1x 対応ポートを、手動で無許可ステートに戻すには、**dot1x initialize** 特権 EXEC コマンドを使用します。

dot1x initialize [**interface** *interface-id*]

構文の説明

interface *interface-id*	（任意）ポートを初期化します。

デフォルト

デフォルト設定はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IEEE 802.1x ステート マシンを初期化し、新たな認証環境を設定します。このコマンドを入力した後、ポートの状態は無許可になります。

このコマンドには、**no** 形式はありません。

例

次の例では、ポートを手動で初期化する方法を示します。

```
Switch# dot1x initialize interface gigabitethernet2/01/2
```

show dot1x [**interface** *interface-id*] 特権 EXEC コマンドを入力することにより、ポート ステータスが無許可になっていることを確認できます。

関連コマンド

コマンド	説明
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x mac-auth-bypass

MAC 認証バイパス機能をイネーブルにするには、**dot1x mac-auth-bypass** 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。MAC 認証バイパス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。

dot1x mac-auth-bypass [**eap** | **timeout inactivity** *value*]

no dot1x mac-auth-bypass

構文の説明

eap	（任意）認証に Extensible Authentication Protocol（EAP）を使用するようスイッチを設定します。
timeout inactivity *value*	（任意）接続されたホストが無許可ステートになる前に非アクティブである秒数を設定します。指定できる範囲は 1 ～ 65535 です。

デフォルト

MAC 認証バイパス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

コマンド履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。
12.2(35)SE	**timeout inactivity** *value* キーワードが追加されました。

使用上のガイドライン

特に言及されない限り、MAC 認証バイパス機能の使用上のガイドラインは IEEE802.1x 認証の使用上のガイドラインと同じです。

ポートが MAC アドレスで認証された後で、ポートから MAC 認証バイパス機能をディセーブルにした場合、ポート ステートには影響ありません。

ポートが未許可ステートであり、クライアント MAC アドレスが認証サーバ データベースにない場合、ポートは未許可ステートのままです。ただし、クライアント MAC アドレスがデータベースに追加されると、スイッチは MAC 認証バイパス機能を使用してポートを再認証できます。

ポートが認証ステートにない場合、再認証が行われるまでポートはこのステートを維持します。

リンクのライフタイム中に EAPOL パケットがインターフェイス上で検出された場合、スイッチは、そのインターフェイスに接続されているデバイスが IEEE 802.1x 対応サプリカントであることを確認し、（MAC 認証バイパス機能ではなく）IEEE 802.1x 認証を使用してインターフェイスを認証します。

MAC 認証バイパスで認証されたクライアントは再認証できます。

MAC 認証バイパスおよび IEEE 802.lx 認証の相互作用の詳細については、ソフトウェア コンフィギュレーション ガイドの「Configuring IEEE 802.1x Port-Based Authentication」の章の「Understanding IEEE 802.1x Authentication with MAC Authentication Bypass」の項および「IEEE 802.1x Authentication Configuration Guidelines」の項を参照してください。

例

次の例では、MAC 認証バイパスをイネーブルにし、認証に EAP を使用するようスイッチを設定する方法を示します。

```
Switch(config-if)# dot1x mac-auth-bypass eap
```

次の例では、MAC 認証バイパスをイネーブルにし、接続されたホストが 30 秒間非アクティブである場合にタイムアウトを設定する方法を示します。

```
Switch(config-if)# dot1x mac-auth-bypass timeout inactivity 30
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x max-reauth-req

ポートが無許可ステートに変わるまでに、スイッチが認証プロセスを再始動する上限回数を設定するには、**dot1x max-reauth-req** 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。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-reauth-req *count*

no dot1x max-reauth-req

構文の説明

count	ポートが無許可ステートに移行する前に、スイッチが EAPOL-Identity-Request フレームを再送信して認証プロセスを開始する回数を設定します。ポートに 802.1x 非対応のデバイスが接続されている場合、スイッチは、デフォルトでは 2 回の認証試行を行います。ポートにゲスト VLAN が設定されている場合、2 回の再認証試行後、ポートは、デフォルトではゲスト VLAN 上で許可されます。指定できる範囲は 1 ～ 10 です。デフォルト値は 2 です。

デフォルト

デフォルトは 2 回です。

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

コマンド履歴

リリース	変更内容
12.2(18)SE	このコマンドが追加されました。
12.2(25)SEC	*count* 範囲が変更されました。

使用上のガイドライン

このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

例

次の例では、ポートが無許可ステートに移行する前に、スイッチが認証プロセスを再起動する回数を 4 に設定する方法を示します。

```
Switch(config-if)# dot1x max-reauth-req 4
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x max-req	スイッチが認証プロセスを再起動する前に、EAP フレームを認証サーバに送信する最高回数を設定します（応答を受信しないと仮定）。
dot1x timeout tx-period	スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を設定します。
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x max-req

スイッチが認証プロセスを再始動する前に、Extensible Authentication Protocol（EAP）フレームを認証サーバからクライアントに送信する最大回数を設定するには（応答を受信しないことが前提）、**dot1x max-req** 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。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

構文の説明

count	スイッチが、認証プロセスを再起動する前に、EAPOL DATA パケットの再送信を試行する回数です。たとえば、認証プロセスの中間にサプリカントがあり、問題が発生した場合、オーセンティケータは、プロセスを中止する前にデータ要求を 2 回再送信します。指定できる範囲は 1 ～ 10 です。デフォルト値は 2 です。

デフォルト

デフォルトは 2 回です。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	このコマンドは、インターフェイス コンフィギュレーション モードに変更されました。

使用上のガイドライン

このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

例

次の例では、認証プロセスを再起動する前に、スイッチが EAP フレームを認証サーバからクライアントに送信する回数を 5 回に設定する方法を示します。

```
Switch(config-if)# dot1x max-req 5
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x timeout tx-period	スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を設定します。
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x multiple-hosts

このコマンドは、現在は使用されていません。

過去のリリースで、**dot1x multiple-hosts** インターフェイス コンフィギュレーション コマンドは、IEEE 802.1x 許可ポートで複数のホスト（クライアント）を許可するために使用されました。

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**dot1x multiple-hosts** インターフェイス コンフィギュレーション コマンドは、**dot1x host-mode** インターフェイス コンフィギュレーション コマンドに替わりました。

関連コマンド

コマンド	説明
dot1x host-mode	ポートの IEEE 802.1x ホスト モードを設定します。
show dot1x	スイッチまたは指定されたポートの IEEE 802.1x 統計情報、管理ステータス、および動作ステータスを表示します。

dot1x pae

IEEE 802.1x Port Access Entity（PAE）オーセンティケータとしてポートを設定するには、**dot1x pae** 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。IEEE 802.1x 認証をポート上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。

dot1x pae authenticator

no dot1x pae

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ポートは IEEE 802.1x PAE オーセンティケータではありません。IEEE 802.1x 認証はポート上でディセーブルです。

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

コマンド履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

IEEE 802.1x 認証をポート上でディセーブルにする場合は、**no dot1x pae** 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。

dot1x port-control インターフェイス コンフィギュレーション コマンドを入力するなどしてポート上で IEEE 802.1x 認証を設定した場合、スイッチは自動的にポートを IEEE 802.1x オーセンティケータとして設定します。オーセンティケータの PAE 動作は、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを入力した後でディセーブルになります。

例

次の例では、ポートの IEEE 802.1x 認証をディセーブルにする方法を示します。

```
Switch(config-if)# no dot1x pae
```

設定を確認するには、**show dot1x** または **show eap** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show dot1x	スイッチまたは指定されたポートの IEEE 802.1x 統計情報、管理ステータス、および動作ステータスを表示します。
show eap	スイッチまたは指定されたポートの EAP のレジストレーション情報およびセッション情報を表示します。

dot1x port-control

ポートの許可ステートを手動で制御できるようにするには、**dot1x port-control** 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。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 {auto | force-authorized | force-unauthorized}

no dot1x port-control

構文の説明

auto	ポートで IEEE 802.1x 認証をイネーブルにし、スイッチおよびクライアント間の IEEE 802.1x 認証交換に基づきポートを許可または無許可ステートに変更します。
force-authorized	ポートで IEEE 802.1x 認証をディセーブルにすれば、認証情報の交換をせずに、ポートを許可ステートに移行します。ポートはクライアントとの IEEE 802.1x ベース認証を行わずに、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、ポートを強制的に無許可ステートに変更することにより、このポート経由のすべてのアクセスを拒否します。スイッチはポートを介してクライアントに認証サービスを提供できません。

デフォルト

デフォルトの設定は force-authorized 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

特定のポートの IEEE 802.1x 認証をイネーブルにする前に、**dot1x system-auth-control** 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、スイッチの IEEE 802.1x 認証をグローバルにイネーブルにする必要があります。

IEEE 802.1x 標準は、レイヤ 2 のスタティック アクセス ポート、音声 VLAN のポート、およびレイヤ 3 のルーテッド ポート上でサポートされます。

ポートが、次の項目の 1 つとして設定されていない場合に限り **auto** キーワードを使用できます。

- トランク ポート：トランク ポートで IEEE 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートのモードをトランクに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。
- ダイナミック ポート：ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで IEEE 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x 認証はイネーブルになりません。IEEE 802.1x 対応ポートのモードをダイナミックに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。

- ダイナミック アクセス ポート：ダイナミック アクセス（VLAN Query Protocol（VQP））ポートで IEEE 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x 認証はイネーブルになりません。IEEE 802.1x 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラー メッセージが表示され、VLAN 設定は変更されません。
- EtherChannel ポート：アクティブまたはアクティブでない EtherChannel メンバであるポートを IEEE 802.1x ポートとして設定しないでください。EtherChannel ポートで IEEE 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x 認証はイネーブルになりません。
- Switched Port Analyzer（SPAN）および Remote SPAN（RSPAN）宛先ポート：SPAN または RSPAN 宛先ポートであるポートの IEEE 802.1x 認証をイネーブルにすることができます。ただし、そのポートが SPAN または RSPAN 宛先として削除されるまで、IEEE 802.1x 認証はディセーブルのままです。SPAN または RSPAN 送信元ポートでは IEEE 802.1x 認証をイネーブルにすることができます。

スイッチで IEEE 802.1x 認証をグローバルにディセーブルにするには、**no dot1x system-auth-control** グローバル コンフィギュレーション コマンドを使用します。特定のポートの IEEE 802.1x 認証をディセーブルにするか、デフォルトの設定に戻すには、**no dot1x port-control** 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。

例

次の例では、ポートの IEEE 802.1x 認証をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet2/01/2
Switch(config-if)# dot1x port-control auto
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x re-authenticate

指定の IEEE 802.1x 対応ポートの再認証を手動で開始するには、**dot1x re-authenticate** 特権 EXEC コマンドを使用します。

dot1x re-authenticate [**interface** *interface-id*]

構文の説明

interface *interface-id*	（任意）再認証するスタック スイッチ番号、モジュール、およびインターフェイスのポート番号

デフォルト

デフォルト設定はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、再認証試行間隔（re-authperiod）および自動再認証の設定秒数を待たずにクライアントを再認証できます。

例

次の例では、ポートに接続されたデバイスを手動で再認証する方法を示します。

```
Switch# dot1x re-authenticate interface gigabitethernet2/0/2
```

関連コマンド

コマンド	説明
dot1x reauthentication	クライアントの定期的再認証をイネーブルにします。
dot1x timeout reauth-period	再認証の試行の間隔（秒）を設定します。

dot1x re-authentication

このコマンドは、現在は使用されていません。

過去のリリースで、**dot1x re-authentication** グローバル コンフィギュレーション コマンドは、定期的な再認証の試行間隔の合計時間を設定するために使用されました。

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**dot1x re-authentication** インターフェイス コンフィギュレーション コマンドは、**dot1x reauthentication** グローバル コンフィギュレーション コマンドに替わりました。

関連コマンド

コマンド	説明
dot1x reauthentication	再認証の試行の間隔（秒）を設定します。
show dot1x	スイッチまたは指定されたポートの IEEE 802.1x 統計情報、管理ステータス、および動作ステータスを表示します。

dot1x reauthentication

定期的なクライアントの再認証をイネーブルにするには、**dot1x reauthentication** 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。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

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

定期的な再認証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

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。**dot1x re-authentication** グローバル コンフィギュレーション コマンド（ハイフン付き）に替わるものです。

使用上のガイドライン

dot1x timeout reauth-period インターフェイス コンフィギュレーション コマンドを使用して、定期的に再認証を行う間隔の時間量を設定します。

例

次の例では、クライアントの定期的な再認証をディセーブルにする方法を示します。

```
Switch(config-if)# no dot1x reauthentication
```

次の例では、定期的な再認証をイネーブルにし、再認証の間隔を 4000 秒に設定する方法を示します。

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x re-authenticate	すべての IEEE 802.1x 対応ポートの再認証を手動で初期化します。
dot1x timeout reauth-period	再認証の試行の間隔（秒）を設定します。
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x supplicant force-multicast

マルチキャストまたはユニキャスト Extensible Authentication Protocol over LAN（EAPOL）パケットを受信した場合、常にサプリカント スイッチにマルチキャスト EAPOL *だけ*を送信させるようにするには、**dot1x supplicant force-multicast** グローバル コンフィギュレーション 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 supplicant force-multicast

no dot1x supplicant force-multicast

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

サプリカント スイッチは、ユニキャスト EAPOL パケットを受信すると、ユニキャスト EAPOL パケットを送信します。同様に、マルチキャスト EAPOL パケットを受信すると、EAPOL パケットを送信します。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(52)SE	このコマンドが追加されました。

使用上のガイドライン

Network Edge Access Topology（NEAT）がすべてのホスト モードで機能するようにするには、サプリカント スイッチ上でこのコマンドをイネーブルにします。

例

次の例では、サプリカント スイッチがオーセンティケータ スイッチにマルチキャスト EAPOL パケットを送信するように設定する方法を示します。

```
Switch(config)# dot1x supplicant force-multicast
```

関連コマンド

コマンド	説明
cisp enable	スイッチの Client Information Signalling Protocol（CISP）をイネーブルにすることで、スイッチがサプリカント スイッチに対するオーセンティケータとして動作するようにします。
dot1x credentials	ポートに 802.1x サプリカント資格情報を設定します。
dot1x pae supplicant	インターフェイスがサプリカントとしてだけ機能するように設定します。

dot1x test eapol-capable

すべてのスイッチ ポート上の IEEE 802.1x のアクティビティをモニタリングして、IEEE 802.1x をサポートするポートに接続しているデバイスの情報を表示するには、**dot1x test eapol-capable** 特権 EXEC コマンドを使用します。

dot1x test eapol-capable [interface *interface-id*]

構文の説明

interface *interface-id*	（任意）クエリー対象のポートです。

デフォルト

デフォルト設定はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(44)SE	このコマンドが追加されました。

使用上のガイドライン

スイッチ上のすべてのポートまたは特定のポートに接続するデバイスの IEEE 802.1x 機能をテストするには、このコマンドを使用します。

このコマンドには、**no** 形式はありません。

例

次の例では、スイッチ上で IEEE 802.1x の準備チェックをイネーブルにして、ポートに対してクエリーを実行する方法を示します。また、ポートに接続しているデバイスを確認するためのクエリーの実行対象ポートから受信した応答が IEEE 802.1x 対応であることを示します。

```
Switch# dot1x test eapol-capable interface gigabitethernet1/0/13

DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL
capable
```

関連コマンド

コマンド	説明
dot1x test timeout *timeout*	IEEE 802.1x 準備クエリーに対する EAPOL 応答を待機するために使用されるタイムアウトを設定します。

dot1x test timeout

IEEE 802.1x の準備が整っているかどうかを確認するためにクエリーが実行されるポートからの EAPOL 応答の待機に使用するタイムアウトを設定するには、**dot1x test timeout** グローバル コンフィギュレーション コマンドを使用します。

dot1x test timeout *timeout*

構文の説明

timeout	EAPOL 応答を待機する時間（秒）。指定できる範囲は 1 ～ 65535 秒です。

デフォルト

デフォルト設定は 10 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

コマンド履歴

リリース	変更内容
12.2(44)SE	このコマンドが追加されました。

使用上のガイドライン

EAPOL 応答を待機するために使用されるタイムアウトを設定するには、このコマンドを使用します。

このコマンドには、**no** 形式はありません。

例

次の例では、EAPOL 応答を 27 秒間待機するようにスイッチを設定する方法を示します。

```
Switch# dot1x test timeout 27
```

タイムアウト設定のステータスを確認するには、**show run** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x test eapol-capable [**interface** *interface-id*]	すべての、または指定された IEEE 802.1x 対応ポートに接続するデバイスで IEEE 802.1x の準備が整っているかを確認します。

dot1x timeout

IEEE 802.1x のタイマーを設定するには、**dot1x timeout** 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。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 {**quiet-period** *seconds* | **ratelimit-period** *seconds* | **reauth-period** {*seconds* | **server**} | **server-timeout** *seconds* | **supp-timeout** *seconds* | **tx-period** *seconds*}

no dot1x timeout {**quiet-period** | **reauth-period** | **server-timeout** | **supp-timeout** | **tx-period**}

構文の説明

quiet-period *seconds*	スイッチがクライアントとの認証情報の交換に失敗した後、待機状態を続ける秒数。指定できる範囲は 1 ～ 65535 です。
ratelimit-period *seconds*	この期間中に認証に成功したクライアントからの Extensible Authentication Protocol over LAN（EAPOL）パケットをスイッチが無視した秒数。指定できる範囲は 1 ～ 65535 です。
reauth-period {*seconds* | **server**}	再認証の試行の間隔（秒）を設定します。 キーワードの意味は次のとおりです。 • *seconds* : 1 ～ 65535 の範囲で秒数を設定します。デフォルトは 3600 秒です。 • **server** : セッションタイムアウト RADIUS 属性（属性 [27]）の値として秒数を設定します。
server-timeout *seconds*	認証サーバに対して、スイッチのパケット再送信を待機する秒数。 指定できる範囲は 1 ～ 65535 です。しかし、最小設定値である 30 を推奨します。
supp-timeout *seconds*	スイッチが IEEE 802.1x クライアントへパケットを再送信する前に待機する秒数。指定できる範囲は 30 ～ 65535 です。
tx-period *seconds*	スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を設定します。指定できる範囲は 1 ～ 65535 です。

デフォルト

デフォルトの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 5 秒です。

supp-timeout は 30 秒です。

server-timeout は 30 秒です。

rate-limit は、1 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**supp-timeout** および **server-timeout** キーワードが追加され、コマンドはインターフェイス コンフィギュレーション モードに変更されました。
12.2(18)SE	**server-timeout**、**supp-timeout**、および **tx-period** キーワードの範囲が変更されました。
12.2(25)SEC	**tx-period** キーワードの範囲が変更され、**reauth-period server** キーワードが追加されました。
12.2(25)SEE	**ratelimit-period** キーワードが追加されました。
12.2(40)SE	**tx-period** *seconds* の範囲が間違っています。正しい範囲は 1 ～ 65535 です。

使用上のガイドライン

このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

dot1x reauthentication インターフェイス コンフィギュレーション コマンドを使用して定期的な再認証をイネーブルにしただけの場合、**dot1x timeout reauth-period** インターフェイス コンフィギュレーション コマンドは、スイッチの動作に影響します。

待機時間の間、スイッチはどのような認証要求も受け付けず、開始もしません。デフォルトよりも小さい数を入力することによって、ユーザへの応答時間を短縮できます。

ratelimit-period が 0（デフォルト）に設定された場合、スイッチは認証に成功したクライアントからの EAPOL パケットを無視し、それらを RADIUS サーバに転送します。

例

次の例では、定期的な再認証をイネーブルにし、再認証の間隔を 4000 秒に設定する方法を示します。

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```

次の例では、定期的な再認証をイネーブルにし、再認証の間隔の秒数としてセッションタイムアウト RADIUS 属性の値を指定する方法を示します。

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period server
```

次の例では、スイッチの待機時間を 30 秒に設定する方法を示します。

```
Switch(config-if)# dot1x timeout quiet-period 30
```

次の例では、スイッチから認証サーバへの再送信時間を 45 秒に設定する方法を示します。

```
Switch(config)# dot1x timeout server-timeout 45
```

次の例では、EAP request フレームに対するスイッチからクライアントへの再送信時間を 45 秒に設定する方法を示します。

```
Switch(config-if)# dot1x timeout supp-timeout 45
```

次の例では、EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの時間を 60 秒に設定する方法を示します。

```
Switch(config-if)# dot1x timeout tx-period 60
```

次の例では、認証に成功したクライアントからの EAPOL パケットをスイッチが無視する秒数を 30 と設定する方法を示します。

```
Switch(config-if)# dot1x timeout ratelimit-period 30
```

設定を確認するには、**show dot1x** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x max-req	スイッチが、認証プロセスを再始動する前に、EAP-Request/Identity フレームを送信する最高回数を設定します。
dot1x reauthentication	クライアントの定期的再認証をイネーブルにします。
show dot1x	すべてのポートの IEEE 802.1x ステータスを表示します。

dot1x violation-mode

dot1x violation-mode インターフェイス コンフィギュレーション コマンドを使用して、新しいデバイスがポートに接続するとき、または最大数のデバイスがポートに接続されている状態で新しいデバイスがポートに接続するときに発生する違反モードを設定します。

dot1x violation-mode {shutdown | restrict | protect}

no dot1x violation-mode

構文の説明

shutdown	エラーによって、予期しない新たな MAC アドレスが発生するポートまたは仮想ポートがディセーブルになります。
restrict	違反エラーの発生時に Syslog エラーを生成します。
protect	新しい MAC アドレスからパケットをそのままドロップします。これがデフォルト設定です。

デフォルト

デフォルトでは、**dot1x violation-mode protect** がイネーブルになっています。

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

コマンド履歴

リリース	変更内容
12.2(46)SE1	このコマンドが追加されました。

例

次の例では、新しいデバイスをポートに接続するときに、IEEE 802.1x 対応ポートを errdisable に設定して、シャットダウンする方法を示します。

```
Switch(config-if)# dot1x violation-mode shutdown
```

次の例では、新しいデバイスをポートに接続するときに、システム エラー メッセージを生成して、ポートを制限モードに変更するように IEEE 802.1x 対応ポートを設定する方法を示します。

```
Switch(config-if)# dot1x violation-mode restrict
```

次の例では、新しいデバイスをポートに接続するときに、新たに接続されたデバイスを無視するように IEEE 802.1x 対応ポートを設定する方法を示します。

```
Switch(config-if)# dot1x violation-mode protect
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

duplex

ポートの動作のデュプレックス モードを指定するには、**duplex** 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。ポートを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。

duplex {**auto** | **full** | **half**}

no duplex

構文の説明

auto	自動によるデュプレックス設定をイネーブルにします（接続されたデバイス モードにより、ポートが自動的に全二重モードか半二重モードかを判断します）。
full	全二重モードをイネーブルにします。
half	半二重モードをイネーブルにします（10 または 100 Mb/s で動作するインターフェイスに限る）。1000 または 10,000 Mb/s で動作するインターフェイスに対して半二重モードを設定できません。

デフォルト

ファスト イーサネット ポートおよびギガビット イーサネット ポートに対するデフォルトは **auto** です。

100BASE-x（-x は -BX、-FX、-FX-FE、または - LX）Small Form-factor Pluggable（SFP; 着脱可能小型フォーム ファクタ）モジュールのデフォルトは **half** です。

二重オプションは、1000BASE-*x*（-*x* は -BX、-CWDM、-LX、-SX、または -ZX）SFP モジュールではサポートされていません。

ご使用のスイッチでサポートされている SFP モジュールについては、製品のリリース ノート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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(20)SE	100 BASE-FX SFP モジュール用に **half** キーワー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 インターフェイスでは使用できません。

ファスト イーサネット ポートでは、接続された装置がデュプレックス パラメータの自動ネゴシエーションを行わない場合にポートを **auto** に設定すると、**half** を指定するのと同じ効果があります。

ギガビット イーサネット ポートでは、接続装置がデュプレックス パラメータを自動ネゴシエートしないときにポートを **auto** に設定すると、**full** を指定する場合と同じ効果があります。

（注） デュプレックス モードが **auto** で接続されている装置が半二重で動作している場合、半二重モードはギガビット イーサネット インターフェイスでサポートされます。ただし、これらのインターフェイスを半二重モードで動作するように設定することはできません。

特定のポートを全二重または半二重のいずれかに設定できます。このコマンドの適用可能性は、スイッチが接続されているデバイスによって異なります。

両方のラインの終端が自動ネゴシエーションをサポートしている場合、デフォルトの自動ネゴシエーションを使用することを強く推奨します。片方のインターフェイスが自動ネゴシエーションをサポートし、もう片方がサポートしていない場合、両方のインターフェイス上でデュプレックスと速度を設定し、サポートされている側で **auto** の設定を使用してください。

速度が **auto** に設定されている場合、スイッチはリンクの反対側のデバイスと速度設定についてネゴシエートし、速度をネゴシエートされた値に強制的に設定します。デュプレックス設定はリンクの両端での設定が引き継がれますが、これにより、デュプレックス設定に矛盾が生じることがあります。

デュプレックス設定を行うことができるのは、速度が **auto** に設定されている場合です。

注意　インターフェイス速度とデュプレックス モードの設定を変更すると、再設定中にインターフェイスがシャットダウンし、再度イネーブルになる場合があります。

スイッチの速度およびデュプレックスのパラメータの設定に関する注意事項は、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring Interface Characteristics」の章を参照してください。

例

次の例では、インターフェイスを全二重動作に設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# duplex full
```

設定を確認するには、**show interfaces** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces	スイッチのインターフェイスの設定を表示します。
speed	10/100 または 10/100/1000 Mb/s インターフェイスの速度を設定します。

epm access-control open

Access Control List（ACL; アクセス コントロール リスト）が設定されていないポートにオープン ディレクティブを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **epm access-control open** グローバル コンフィギュレーション コマンドを使用します。オープン ディレクティブ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。

epm access-control open

no epm access-control open

構文の説明

このコマンドには、キーワードと引数はありません。

デフォルト

デフォルトのディレクティブが適用されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容

使用上のガイドライン

スタティック ACL が設定されたアクセス ポートに、認可ポリシーのないホストを許可するオープン ディレクティブを設定するには、このコマンドを使用します。このコマンドを設定しない場合、ポートは設定された ACL のポリシーをトラフィックに適用します。ポートにスタティック ACL が設定されていない場合、デフォルトおよびオープンの両方のディレクティブがポートへのアクセスを許可します。

例

次の例では、オープン ディレクティブを設定する方法を示します。

```
Switch(config)# epm access-control open
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	動作設定を表示します。構文情報については、『Cisco IOS Release 12.2 Command Reference』一覧ページへのリンク（http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html）を使用してください。 コマンドに移動するには、「Cisco IOS Commands Master List, Release 12.2」を選択します。

errdisable detect cause

特定の原因またはすべての原因の error-disable 検出をイネーブルにするには、**errdisable detect cause** グローバル コンフィギュレーション コマンドを使用します。errdisable 検出機能をディセーブルにする場合は、このコマンドの **no** 形式を使用します。

errdisable detect cause {**all** | **arp-inspection** | **bpduguard** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **inline-power** | **l2ptguard** | **link-flap** | **loopback** | **pagp-flap** | **security-violation shutdown vlan** | **sfp-config-mismatch**}

no errdisable detect cause {**all** | **arp-inspection** | **bpduguard** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **inline-power** |**l2ptguard** | **link-flap** | **loopback** | **pagp-flap** | **security-violation shutdown vlan** | **sfp-config-mismatch**}

BPDU ガード機能およびポート セキュリティ機能の場合は、このコマンドを使用し、違反の発生時にポート全体をシャットダウンする代わりに、ポートで問題となっている VLAN だけをシャットダウンするようにスイッチをグローバルに設定できます。

VLAN ごとに errdisable 機能をオフにしていて BPDU ガード違反が発生した場合は、ポート全体がディセーブルになります。VLAN ごとに errdisable 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。

errdisable detect cause bpduguard shutdown vlan

no errdisable detect cause bpduguard shutdown vlan

構文の説明

all	すべての errdisable の原因に対して、エラー検出をイネーブルにします。
arp-inspection	ダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査のエラー検出をイネーブルにします。
bpduguard shutdown vlan	BPDU ガードで VLAN ごとに errdisable をイネーブルにします。
dhcp-rate-limit	Dynamic Host Configuration Protocol（DHCP）スヌーピング用のエラー検出をイネーブルにします。
dtp-flap	Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）フラップのエラー検出をイネーブルにします。
gbic-invalid	無効なギガビット インターフェイス コンバータ（GBIC）モジュール用のエラー検出をイネーブルにします。 **（注）** このエラーは、スイッチでの無効な Small Form-Factor Pluggable（SFP）モジュールを意味します。
inline-power	インライン パワーに対し、エラー検出をイネーブルにします。
l2ptguard	レイヤ 2 プロトコル トンネルの errdisable 原因に対し、エラー検出をイネーブルにします。
link-flap	リンクステートのフラップに対して、エラー検出をイネーブルにします。
loopback	検出されたループバックに対して、エラー検出をイネーブルにします。
pagp-flap	Port Aggregation Protocol（PAgP）フラップの errdisable 原因のエラー検出をイネーブルにします。
security-violation shutdown vlan	音声認識 IEEE 802.1x セキュリティをイネーブルにします。
sfp-config-mismatch	SFP 設定の不一致によるエラー検出をイネーブルにします。

コマンド デフォルト

検出はすべての原因に対してイネーブルです。VLAN ごとの errdisable を除くすべての原因について、ポート全体をシャットダウンするように設定されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**loopback** キーワードが追加されました。
12.1(19)EA1	**dhcp-rate-limit** キーワードが追加されました。
12.2(20)SE	**arp-inspection** キーワードが追加されました。
12.2(25)SE	**l2ptguard** キーワードが追加されました。
12.2(37)SE	VLAN ごとのエラー検出機能が追加されました。**inline-power** キーワードおよび **sfp-config-mismatch** キーワードが追加されました。
12.2(46)SE	**security-violation shutdown vlan** キーワードが追加されました。

使用上のガイドライン

原因（**link-flap**、**dhcp-rate-limit** など）は、errdisable ステートが発生した理由です。原因がポートで検出された場合、ポートは errdisable ステート（リンクダウン ステートに類似した動作ステート）となります。

ポートが errdisable になっているときは事実上シャットダウンし、トラフィックはポートで送受信されません。BPDU、音声認識 802.1x セキュリティ、ガードおよびポート セキュリティ機能のため、違反の発生時に、ポート全体でなく、ポート上の障害のある VLAN だけをシャットダウンするようスイッチを設定することができます。

原因に対して **errdisable recovery** 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、原因の回復メカニズムを設定する場合は、すべての原因がタイムアウトになった時点で、ポートは errdisable ステートから抜け出して、処理を再試行できるようになります。回復メカニズムを設定しない場合は、まず **shutdown** コマンドを入力し、次に **no shutdown** コマンドを入力して、ポートを手動で errdisable ステートから回復させる必要があります。

例

次の例では、リンクフラップ errdisable 原因の errdisable 検出をイネーブルにする方法を示します。

```
Switch(config)# errdisable detect cause link-flap
```

次のコマンドでは、VLAN ごとの errdisable で BPDU ガードをグローバルに設定する方法を示します。

```
Switch(config)# errdisable detect cause bpduguard shutdown vlan
```

次のコマンドでは、VLAN ごとの errdisable で音声認識 802.1x セキュリティをグローバルに設定する方法を示します。

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

show errdisable detect 特権 EXEC コマンドを入力すると、設定を確認できます。

関連コマンド

コマンド	説明
show errdisable detect	errdisable 検出情報を表示します。
show interfaces status err-disabled	インターフェイスのステータスまたは errdisable ステートにあるインターフェイスのリストを表示します。
clear errdisable interface	VLAN ごとの errdisable 機能によって errdisable になったポートまたは VLAN から errdisable ステートをクリアします。

errdisable detect cause small-frame

着信 VLAN タグ付きパケットのフレームが小さく（67 バイト以下）、設定された最低速度（しきい値）で到着する場合に、任意のスイッチ ポートを errdisable にできるようにするには、**errdisable detect cause small-frame** グローバル コンフィギュレーション 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。

errdisable detect cause small-frame

no errdisable detect cause small-frame

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

この機能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

コマンド履歴

リリース	変更内容
12.2(44)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、小さいフレームの着信機能をグローバルにイネーブルにします。各ポートのしきい値を設定するには、**small violation-rate** 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。

ポートが自動的に再びイネーブルになるように設定するには、**errdisable recovery cause small-frame** グローバル コンフィギュレーション コマンドを使用します。回復時間を設定するには、**errdisable recovery interval** *interval* グローバル コンフィギュレーション コマンドを使用します。

例

次の例では、小さい着信フレームが設定されたしきい値で到着すると errdisable モードになるスイッチ ポートをイネーブルにする方法を示します。

```
Switch(config)# errdisable detect cause small-frame
```

設定を確認するには、**show interfaces** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
errdisable recovery cause small-frame	回復タイマーをイネーブルにします。
errdisable recovery interval *interval*	指定された errdisable ステートから回復する時間を指定します。
show interfaces	入出力フロー制御を含むスイッチのインターフェイス設定を表示します。
small violation-rate	ポートが errdisable ステートとなる、小さい着信フレームの伝送速度（しきい値）を設定します。

errdisable recovery cause small-frame

小さいフレームが着信してポートが errdisable となった後でポートを自動で再度イネーブルにするための回復タイマーをイネーブルにするには、スイッチ上で **errdisable recovery cause small-frame** グローバル コンフィギュレーション 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。

errdisable recovery cause small-frame

no errdisable recovery cause small-frame

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

この機能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

コマンド履歴

リリース	変更内容
12.2(44)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、errdisable ポートの回復タイマーをイネーブルにします。回復時間を設定するには、errdisable **recovery interval** *interval* 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。

例

次の例では、回復タイマーを設定する方法を示します。

```
Switch(config)# errdisable recovery cause small-frame
```

設定を確認するには、**show interfaces** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
errdisable detect cause small-frame	着信フレームが指定した最小サイズより小さく、指定した伝送速度（しきい値）で到着する場合に、スイッチ ポートを errdisable 状態にします。
show interfaces	入出力フロー制御を含むスイッチのインターフェイス設定を表示します。
small violation-rate	ポートが errdisable ステートとなる、（小さい）着信フレームのサイズを設定します。

errdisable recovery

回復メカニズムの変数を設定するには、**errdisable recovery** グローバル コンフィギュレーション 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。

errdisable recovery {**cause** {**all** | **arp-inspection** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **inline-power** |**l2ptguard** | **link-flap** | **loopback** | **pagp-flap** | **psecure-violation** | **security-violation** | **sfp-mismatch** | **udld** | **vmps**} | {**interval** *interval*}

no errdisable recovery {**cause** {**all** | **arp-inspection** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **inline-power** | **l2ptguard** | **link-flap** | **loopback** | **pagp-flap** | **psecure-violation** | **security-violation** | **sfp-mismatch** | **udld** | **vmps**} | {**interval** *interval*}

構文の説明

cause	特定の原因から回復するように errdisable メカニズムをイネーブルにします。
all	すべての errdisable の原因から回復するタイマーをイネーブルにします。
bpduguard	UniDirectional Link Detection（UDLD; 単一方向リンク検出）ガード errdisable ステートから回復するタイマーをイネーブルにします。
arp-inspection	Address Resolution Protocol（ARP; アドレス解決プロトコル）検査による errdisable ステートから回復するためのタイマーをイネーブルにします。
channel-misconfig	EtherChannel の設定矛盾による errdisable ステートから回復するタイマーをイネーブルにします。
dhcp-rate-limit	DHCP スヌーピング errdisable ステートから回復するタイマーをイネーブルにします。
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 errdisable ステートから回復するタイマーをイネーブルにします。
gbic-invalid	ギガビット インターフェイス コンバータ（GBIC）モジュールを無効な errdisable ステートから回復するタイマーをイネーブルにします。 **（注）** このエラーは無効な Small Form-Factor Pluggable（SFP）の errdisable ステートを意味します。
inline-power	インライン パワーに対し、エラー検出をイネーブルにします。
l2ptguard	レイヤ 2 プロトコル トンネルによる errdisable ステートから回復するためのタイマーをイネーブルにします。
link-flap	リンクフラップ errdisable ステートから回復するタイマーをイネーブルにします。
loopback	ループバック errdisable ステートから回復するタイマーをイネーブルにします。
pagp-flap	Port Aggregation Protocol（PAgP）フラップ errdisable ステートから回復するタイマーをイネーブルにします。
psecure-violation	ポート セキュリティ違反ディセーブル ステートから回復するタイマーをイネーブルにします。
security-violation	IEEE 802.1x 違反ディセーブル ステートから回復するタイマーをイネーブルにします。
sfp-mismatch	SFP 設定の不一致でエラー検出をイネーブルにします。
udld	UniDirectional Link Detection（UDLD; 単方向リンク検出）errdisable ステートから回復するタイマーをイネーブルにします。

vmps	VLAN Membership Policy Server（VMPS; VLAN メンバシップ ポリシー サーバ）errdisable ステートから回復するタイマーをイネーブルにします。
interval *interval*	指定された errdisable ステートから回復する時間を指定します。指定できる範囲は 30 ～ 86400 秒です。すべての原因に同じ間隔が適用されます。デフォルト間隔は 300 秒です。 （注）　errdisable recovery のタイマーは、設定された間隔値からランダムな差で初期化されます。実際のタイムアウト値と設定された値の差は、設定された間隔の 15% まで認められます。

デフォルト

すべての原因に対して回復はディセーブルです。

デフォルトの回復間隔は 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**security-violation** キーワードが追加されました。**gbic-invalid** キーワードは、SFP モジュール ポートでサポートされます。
12.1(19)EA1	**dhcp-rate-limit** キーワードが追加されました。
12.2(18)SE	**channel-misconfig** キーワードが追加されました。
12.2(20)SE	**arp-inspection** キーワードが追加されました。
12.2(25)SE	**l2ptguard** キーワードが追加されました。
12.2(37)SE	VLAN ごとのエラー検出機能が追加されました。**inline-power** キーワードおよび **sfp-mismatch** キーワードが追加されました。

使用上のガイドライン

原因（**link-flap**、**bpduguard** など）は、errdisable ステートが発生した理由として定義されます。原因がポートで検出された場合、ポートは errdisable ステート（リンクダウン ステートに類似した動作ステート）となります。

ポートが errdisable になっているときは事実上シャットダウンし、トラフィックはポートで送受信されません。BPDU ガード機能およびポートセキュリティ機能の場合は、違反の発生時にポート全体をシャットダウンする代わりに、ポートで問題となっている VLAN だけをシャットダウンするようにスイッチを設定できます。

その原因に対して errdisable の回復をイネーブルにしない場合、ポートは、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドが入力されるまで 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、ポートは errdisable ステートから回復し、すべての原因がタイムアウトになったときに処理を再開できるようになります。

原因の回復をイネーブルにしない場合、まず **shutdown** コマンドを入力し、次に **no shutdown** コマンドを入力して、手動でポートを errdisable ステートから回復させる必要があります。

例

次の例では、BPDU ガード errdisable 原因に対して回復タイマーをイネーブルにする方法を示します。

```
Switch(config)# errdisable recovery cause bpduguard
```

次の例では、タイマーを 500 秒に設定する方法を示します。

```
Switch(config)# errdisable recovery interval 500
```

設定を確認するには、**show errdisable recovery** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show errdisable recovery	errdisable 回復タイマーの情報を表示します。
show interfaces status err-disabled	インターフェイスのステータスまたは errdisable ステートにあるインターフェイスのリストを表示します。
clear errdisable interface	VLAN ごとの errdisable 機能によって errdisable になったポートまたは VLAN から errdisable ステートをクリアします。

exception crashinfo

Cisco IOS イメージのエラー時にスイッチで拡張 crashinfo ファイルが作成されるよう設定するには、**exception crashinfo** グローバル コンフィギュレーション 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。

exception crashinfo

no exception crashinfo

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

スイッチが拡張 crashinfo ファイルを作成します。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SEC	このコマンドが追加されました。

使用上のガイドライン

基本 crashinfo ファイルには、失敗した Cisco IOS のイメージ名およびバージョン、プロセッサ レジスタのリスト、およびスタック トレースが含まれます。拡張 crashinfo ファイルには、スイッチの障害の原因を判別するのに役立つその他の追加情報が含まれます。

スタック マスター上で **exception crashinfo** グローバル コンフィギュレーション コマンドを入力すると、すべてのスタック メンバは、スタック メンバ上の Cisco IOS イメージが失敗した場合に拡張 crashinfo ファイルを作成するよう設定されます。

スイッチが拡張 crashinfo ファイルを作成しないように設定するには、**no exception crashinfo** グローバル コンフィギュレーション コマンドを使用します。

例

次の例では、スイッチが拡張 crashinfo ファイルを作成しないように設定する方法を示します。

```
Switch(config)# no exception crashinfo
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	定義されたマクロを含む動作設定を表示します。

fallback profile

Web 認証用にフォールバック プロファイルを作成するには、**fallback profile** グローバル コンフィギュレーション 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。

fallback profile *profile*

no fallback profile

構文の説明

profile	IEEE 802.1x 認証をサポートしていないクライアントのフォールバック プロファイルを指定します。

デフォルト

フォールバック プロファイル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

コマンド履歴

リリース	変更内容
12.2(35)SE	このコマンドが追加されました。

使用上のガイドライン

フォールバック プロファイルは、サプリカントを持たない IEEE 802.1x ポートの IEEE 802.1x フォールバック動作を定義するために使用されます。サポートされる動作は、Web 認証へのフォールバックだけです。

fallback profile コマンドを入力すると、プロファイル コンフィギュレーション モードが開始され、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。

- **ip** : IP コンフィギュレーションを作成します。
- **access-group** : まだ認証されていないホストによって送信されるパケットのアクセス コントロールを指定します。
- **admission** : IP アドミッション ルールを適用します。

例

次の例では、Web 認証で使用されるフォールバック プロファイルの作成方法を示します。

```
Switch# configure terminal
Switch(config)# ip admission name rule1 proxy http
Switch(config)# fallback profile profile1
Switch(config-fallback-profile)# ip access-group default-policy in
Switch(config-fallback-profile)# ip admission rule1
Switch(config-fallback-profile)# exit
Switch(config)# interface gigabitethernet 1/0/1
Switch(config-if)# dot1x fallback profile1
Switch(config-if)# end
```

show running-configuration [**interface** *interface-id*] 特権 EXEC コマンドを入力することにより、設定を確認できます。

関連コマンド

コマンド	説明
dot1x fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
ip admission	スイッチ ポートで Web 認証をイネーブルにします。
ip admission name proxy http	スイッチで Web 認証をグローバルにイネーブルにします。
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。
show fallback profile	スイッチの設定済みプロファイルを表示します。

flowcontrol

インターフェイスに対する受信フロー制御ステートを設定するには、**flowcontrol** 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。ある装置に対してフロー制御 **send** が動作可能でオンになっていて、接続のもう一方の側で輻輳が少しでも検出された場合は、休止フレームを送信することによって、リンクの相手側またはリモート装置に輻輳を通知します。ある装置に対してフロー制御 **receive** がオンで、休止フレームを受信した場合、データ パケットの送信は停止します。こうすることにより、輻輳期間中にデータ パケットの損失を防ぎます。

フロー制御をディセーブルにする場合は、**receive off** キーワードを使用します。

flowcontrol receive {**desired** | **off** | **on**}

（注）　スイッチは、ポーズ フレームを受信できますが、送信はできません。

構文の説明

receive	インターフェイスがリモート装置からフロー制御パケットを受信できるかどうかを設定します。
desired	インターフェイスを、フロー制御パケットを送信する必要がある接続装置またはフロー制御パケットを送信する必要はないが送信することのできる接続装置とともに稼動させることができます。
off	接続装置がフロー制御パケットをインターフェイスへ送信する機能をオフにします。
on	インターフェイスを、フロー制御パケットを送信する必要がある接続装置またはフロー制御パケットを送信する必要はないが送信することのできる接続装置とともに稼動させることができます。

デフォルト

デフォルトは、**flowcontrol receive off** 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このスイッチでは、送信フロー制御の休止フレームはサポートされません。

on および **desired** キーワードは同一の結果になることに注意してください。

flowcontrol コマンドを使用してポートが輻輳中にトラフィック レートを制御するよう設定する場合、フロー制御はポート上で次の条件のうちの 1 つに設定されます。

- **receive on** または **desired** : ポートはポーズ フレームを送信できませんが、ポーズ フレームを送信する必要がある装置、または送信可能な接続装置と連動できます。ポートはポーズ フレームを受信できます。
- **receive off** : フロー制御はどちらの方向にも動作しません。輻輳が生じても、リンクの相手側に通知はなく、どちら側の装置も休止フレームの送受信を行いません。

表 2-10 は、各設定の組み合わせによるローカル ポートおよびリモート ポート上のフロー制御の結果を示したものです。表は **receive desired** キーワードの使用時と **receive on** キーワードの使用時の結果が同一になることを前提としています。

表 2-10　フロー制御設定およびローカル/リモート ポート フロー制御解決

フロー制御設定		フロー制御解決	
ローカル デバイス	リモート デバイス	ローカル デバイス	リモート デバイス
send off/receive on	**send on/receive on**	受信だけ行います。	送受信を行います。
	send on/receive off	受信だけ行います。	送信だけ行います。
	send desired/receive on	受信だけ行います。	送受信を行います。
	send desired/receive off	受信だけ行います。	送信だけ行います。
	send off/receive on	受信だけ行います。	受信だけ行います。
	send off/receive off	送受信を行いません。	送受信を行いません。
send off/receive off	**send on/receive on**	送受信を行いません。	送受信を行いません。
	send on/receive off	送受信を行いません。	送受信を行いません。
	send desired/receive on	送受信を行いません。	送受信を行いません。
	send desired/receive off	送受信を行いません。	送受信を行いません。
	send off/receive on	送受信を行いません。	送受信を行いません。
	send off/receive off	送受信を行いません。	送受信を行いません。

例

次の例では、リモート ポートによってフロー制御がサポートされないようにローカル ポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet 1/0/1
Switch(config-if)# flowcontrol receive off
```

設定を確認するには、**show interfaces** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces	入出力フロー制御を含むスイッチのインターフェイス設定を表示します。

interface port-channel

ポート チャネルの論理インターフェイスにアクセスしたり、作成したりするには、**interface port-channel** グローバル コンフィギュレーション コマンドを使用します。ポート チャネルを削除する場合は、このコマンドの **no** 形式を使用します。

interface port-channel *port-channel-number*

no interface port-channel *port-channel-number*

構文の説明

port-channel-number	ポート チャネル番号。指定できる範囲は 1 ～ 48 です。

デフォルト

ポート チャネル論理インターフェイスは定義されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(25)SE	*port-channel-number* 範囲が 1 ～ 12 から 1 ～ 48 に変更されました。

使用上のガイドライン

レイヤ 2 EtherChannel では、物理ポートをチャネル 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。代わりに、**channel-group** インターフェイス コンフィギュレーション コマンドを使用できます。チャネル グループが最初の物理ポートを獲得すると、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。最初にポートチャネル インターフェイスを作成する場合は、*channel-group-number* を *port-channel-number* と同じ番号にしても、新しい番号にしてもかまいません。新しい番号を使用した場合、**channel-group** コマンドは動的に新しいポート チャネルを作成します。

interface port-channel コマンドの次に **no switchport** インターフェイス コンフィギュレーション コマンドを使用して、レイヤ 3 のポート チャネルを作成できます。インターフェイスをチャネル グループに適用する前に、ポート チャネルの論理インターフェイスを手動で設定してください。

チャネル グループ内の 1 つのポート チャネルだけが許可されます。

注意　ポート チャネル インターフェイスをルーテッド ポートとして使用する場合、チャネル グループに割り当てられた物理ポート上のレイヤ 3 に、アドレスを割り当てないようにしてください。

注意　レイヤ 3 のポート チャネル インターフェイスとして使用されているチャネル グループの物理ポート上で、ブリッジ グループを割り当てることは、ループ発生の原因になるため行わないようにしてください。スパニングツリーもディセーブルにする必要があります。

interface port-channel コマンドを使用する場合は、次の注意事項に従ってください。

- Cisco Discovery Protocol（CDP）を使用する場合には、これを物理ポートでだけ設定してください。ポート チャネル インターフェイスでは設定できません。
- EtherChannel のアクティブ メンバであるポートを IEEE 802.1x ポートとしては設定しないでください。まだアクティブになっていない EtherChannel のポートで IEEE 802.1x をイネーブルにしても、そのポートは EtherChannel に加入しません。

設定の注意事項の一覧については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring EtherChannels」の章を参照してください。

例

次の例では、ポート チャネル番号 5 でポートチャネル インターフェイスを作成する方法を示します。

```
Switch(config)# interface port-channel 5
```

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show etherchannel** *channel-group-number* **detail** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
channel-group	EtherChannel グループにイーサネット ポートを割り当てます。
show etherchannel	チャネルの EtherChannel 情報を表示します。
show running-config	現在の動作設定を表示します。

interface range

インターフェイス レンジ コンフィギュレーション モードを開始し、複数のポートでコマンドを同時に実行するには、**interface range** グローバル コンフィギュレーション コマンドを使用します。インターフェイス範囲を削除する場合は、このコマンドの **no** 形式を使用します。

interface range {*port-range* | **macro** *name*}

no interface range {*port-range* | **macro** *name*}

構文の説明

port-range	ポート範囲。*port-range* の有効値のリストについては、「使用上のガイドライン」の項を参照してください。
macro *name*	マクロ名を指定します。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

インターフェイス範囲を設定するモードを開始して入力した、すべてのインターフェイスのパラメータは、その範囲内のすべてのインターフェイスに対する属性になります。

VLAN については、既存の VLAN Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）でだけ **interface range** コマンドを使用することができます。VLAN の SVI を表示する場合は、**show running-config** 特権 EXEC コマンドを入力します。表示されない VLAN は、**interface range** コマンドで使用することはできません。**interface range** コマンドのもとで入力したコマンドは、この範囲のすべての既存の VLAN SVI に適用されます。

あるインターフェイス範囲に対して行われた設定変更は、すべて NVRAM（不揮発性 RAM）に保存されますが、インターフェイス範囲自体は NVRAM に保存されません。

インターフェイス範囲は 2 つの方法で入力できます。

- 最大 5 つまでのインターフェイス範囲を指定。
- 定義済みのインターフェイス範囲マクロ設定を指定。

範囲内のすべてのインターフェイスは同じタイプ、つまり、すべてがファスト イーサネット ポート、すべてがギガビット イーサネット ポート、すべてが EtherChannel ポート、またはすべてが VLAN のいずれかでなければなりません。ただし、各範囲をカンマ（,）で区切ることにより、1 つのコマンドで最大 5 つのインターフェイス範囲を定義できます。

port-range タイプおよびインターフェイスの有効値は次のとおりです。

- **vlan** *vlan-ID* : *vlan-ID*（vlan ID の範囲は 1 ～ 4094）
- **fastethernet** module/{*first port*} - {*last port*}（module は常に **0**）
- **gigabitethernet** stack member/module/{*first port*} - {*last port*}（module は常に **0**）

  物理インターフェイス

  - stack member は、スタック内のスイッチ識別に使用する番号です。番号に指定できる範囲は 1 ～ 9 で、スタック メンバの最初の初期化の際に、スイッチに割り当てられます。
  - モジュールは常に 0 です。
  - 使用可能範囲は、*type* **stack member**/*0*/*number* - **number** です（例 : gigabitethernet1/0/1 - 2）
- **port-channel** *port-channel-number* - *port-channel-number*、*port-channel-number* は 1 ～ 48 です。

（注）　ポート チャネルの **interface range** コマンドを使用した場合、範囲内の最初と最後のポート チャネル番号はアクティブなポート チャネルである必要があります。

範囲を定義するときは、最初の入力とハイフン（-）の間にスペースが必要です。

```
interface range gigabitethernet1/0/1 -2
```

範囲を複数定義するときでも、最初のエントリとカンマ（,）の間にスペースを入れる必要があります。

```
interface range fastethernet1/0/1 - 2, gigabitethernet1/0/1 - 2
```

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。

また、*port-range* で単一インターフェイスを指定することもできます。つまりこのコマンドは、**interface** *interface-id* グローバル コンフィギュレーション コマンドに類似しています。

インターフェイスの範囲の設定に関する詳細は、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、**interface range** コマンドを使用して、インターフェイス範囲コンフィギュレーション モードを開始し、2 つのポートにコマンドを入力する方法を示します。

```
Switch(config)# interface range gigabitethernet1/0/1 - 2
```

次の例では、同じ機能に対して 1 つのポート範囲マクロ *macro1* を使用する方法を示します。この利点は、*macro1* を削除するまで再利用できることです。

```
Switch(config)# define interface-range macro1 gigabitethernet1/0/1 - 2
Switch(config)# interface range macro macro1
Switch(config-if-range)#
```

関連コマンド

コマンド	説明
define interface-range	インターフェイス範囲のマクロを作成します。
show running-config	スイッチで現在の動作設定情報を表示します。

interface vlan

動的な Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）を作成、またはこれにアクセスし、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 vlan** グローバル コンフィギュレーション 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*

構文の説明

vlan-id	VLAN 番号。指定できる範囲は 1 ～ 4094 です。

デフォルト

デフォルトの VLAN インターフェイスは VLAN 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

SVI は、特定の VLAN に対して、初めて **interface vlan** *vlan-id* コマンドを入力したときに作成されます。*vlan-id* は、ISL（スイッチ間リンク）または IEEE 802.1Q カプセル化トランクのデータ フレームに関連付けられた VLAN タグ、またはアクセス ポートに設定された VLAN ID に相当します。

（注）物理ポートと関連付けられていない場合、SVI を作成してもアクティブにはなりません。

no interface vlan *vlan-id* コマンドを入力して SVI を削除すると、削除されたインターフェイスは、それ以降、**show interfaces** 特権 EXEC コマンドの出力には表示されません。

（注）VLAN 1 インターフェイスを削除することはできません。

削除した SVI は、削除したインターフェイスに対して **interface vlan** *vlan-id* コマンドを入力することで、元に戻すことができます。インターフェイスはバックアップとなりますが、それまでの設定は削除されます。

スイッチ スタック上で設定された SVI の数と、設定された他の機能の数の相互関係によっては、ハードウェア制限により、CPU 使用率に影響が出る可能性があります。**sdm prefer** グローバル コンフィギュレーション コマンドを使用し、システムのハードウェア リソースを、テンプレートおよび機能テーブルに基づいて再度割り当てることができます。詳細は、**sdm prefer** コマンドを参照してください。

例

次の例では、VLAN ID 23 の新しい SVI を作成し、インターフェイス コンフィギュレーション モードを開始する方法を示します。

```
Switch(config)# interface vlan 23
Switch(config-if)#
```

show interfaces および **show interfaces vlan** *vlan-id* 特権 EXEC コマンドを入力することによって、設定を確認できます。

関連コマンド

コマンド	説明
show interfaces vlan *vlan-id*	すべてのインターフェイスまたは指定の VLAN の管理ステータスおよび動作ステータスを表示します。

ip access-group

レイヤ 2 またはレイヤ 3 インターフェイスへのアクセスを制御するには、**ip access-group** 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。インターフェイスからすべてまたは指定のアクセス 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。

ip access-group {*access-list-number* | *name*} {**in** | **out**}

no ip access-group [*access-list-number* | *name*] {**in** | **out**}

構文の説明

access-list-number	IP Access Control List（ACL; アクセス コントロール リスト）の番号です。指定できる範囲は、1 ～ 199 または 1300 ～ 2699 です。
name	**ip access-list** グローバル コンフィギュレーション コマンドで指定された IP ACL 名です。
in	入力パケットに対するフィルタリングを指定します。
out	発信パケットに対するフィルタリングを指定します。このキーワードは、レイヤ 3 のインターフェイス上に限り有効です。

デフォルト

アクセス リストは、インターフェイスには適用されません。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	コマンドのサポートがレイヤ 2 インターフェイスまで拡張されました。

使用上のガイドライン

名前付きまたは番号付きの標準 / 拡張 IP アクセス リストをインターフェイスに適用できます。名前を付けてアクセス リストを定義するには、**ip access-list** グローバル コンフィギュレーション コマンドを使用します。番号付きアクセス リストを定義するには、**access list** グローバル コンフィギュレーション コマンドを使用します。1 ～ 99 および 1300 ～ 1999 の範囲の番号付き標準アクセス リスト、または 100 ～ 199 および 2000 ～ 2699 の範囲の番号付き拡張アクセス リストを使用できます。

このコマンドを使用し、アクセス リストをレイヤ 2 またはレイヤ 3 のインターフェイスに適用できます。ただし、レイヤ 2 のインターフェイス（ポート ACL）には、次のような制限があることに注意してください。

- ACL は受信方向のレイヤ 2 ポートにだけ適用できます。
- インターフェイスごとに 1 つの IP ACL と 1 つの MAC ACL だけを適用できます。
- レイヤ 2 のインターフェイスはロギングをサポートしていません。**log** キーワードが IP ACL で指定された場合、無視されます。
- レイヤ 2 のインターフェイスに適用された IP ACL は、IP パケットだけをフィルタにかけます。非 IP パケットをフィルタリングするには、MAC 拡張 ACL とともに **mac access-group** 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。

ユーザは同一のスイッチ上で、ルータ ACL、入力ポート ACL、VLAN マップを使用できます。ただし、ポートの ACL はルータの ACL、または VLAN マップより優先されます。

- 入力ポートの ACL がインターフェイスに適用され、さらにインターフェイスがメンバとなっている VLAN に VLAN マップが適用された場合、ACL のポート上で受信した着信パケットは、そのポート ACL でフィルタリングされます。その他のパケットは、VLAN マップによってフィルタリングされます。
- 入力ルータの ACL および入力ポートの ACL が SVI に存在している場合、ポートの ACL が適用されたポート上で受信された着信パケットには、ポート ACL のフィルタが適用されます。他のポートで受信した着信のルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- 出力ルータの ACL および入力ポートの ACL が SVI に存在している場合、ポートの ACL が適用されたポート上で受信された着信パケットには、ポート ACL のフィルタが適用されます。発信するルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- VLAN マップ、入力ルータの ACL、および入力ポートの ACL が SVI に存在している場合、ポートの ACL が適用されたポート上で受信された着信パケットには、ポート ACL のフィルタだけが適用されます。他のポートで受信した着信のルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけが適用されます。
- VLAN マップ、出力ルータの ACL、および入力ポートの ACL が SVI に存在している場合、ポートの ACL が適用されたポート上で受信された着信パケットには、ポート ACL のフィルタだけが適用されます。発信するルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけが適用されます。

IP の ACL は、送信側または受信側のレイヤ 3 インターフェイス両方に適用できます。

レイヤ 3 のインターフェイスでは、IP の ACL を各方向に 1 つ適用できます。

VLAN インターフェイス上の各方向（入力および出力）に VLAN マップおよびルータの ACL を 1 つずつに限り設定できます。

標準入力アクセス リストでは、スイッチは、パケットを受信すると、パケットの送信元アドレスをアクセス リストに比較して検査します。IP 拡張アクセス リストでは、任意で、宛先 IP アドレス、プロトコル タイプ、ポート番号などのパケット内の他のフィールドを検査することができます。アクセス リストがパケットを許可する場合に、スイッチはパケットの処理を続行します。アクセス リストがパケットを拒否する場合は、スイッチはそのパケットをドロップします。アクセス リストがレイヤ 3 のインターフェイスに適用された場合、パケットのドロップにともない（デフォルト設定）、Internet Control Message Protocol（ICMP）の Host Unreachable のメッセージが生成されます。ICMP Host Unreachable メッセージは、レイヤ 2 インターフェイスでドロップされたパケットに対しては生成されません。

通常の発信アクセス リストでは、パケットを受信して、それを制御されたインターフェイスへ送信した後、スイッチがアクセス リストと照合することでパケットを確認します。アクセス リストがパケットを許可した場合、スイッチはパケットを送信します。アクセス リストがパケットを拒否した場合、スイッチはパケットをドロップし、デフォルトの設定では、ICMP Host Unreachable メッセージが生成されます。

指定したアクセス リストが存在しない場合は、すべてのパケットが通過します。

例

次の例では、ポートの入力パケットに IP アクセス リスト 101 を適用する方法を示します。

```
Switch(config)# interface gigabitethernet 1/0/1
Switch(config-if)# ip access-group 101 in
```

show ip interface、**show access-lists**、または **show ip access-lists** 特権 EXEC コマンドを入力することにより、設定を確認できます。

関連コマンド

コマンド	説明
access list	番号付き ACL を設定します。
ip access-list	名前付き ACL を設定します。
show access-lists	スイッチで設定された ACL を表示します。
show ip access-lists	スイッチで設定された IP ACL を表示します。
show ip interface	インターフェイスのステータスと設定に関する情報を表示します。

ip address

レイヤ 2 スイッチの IP アドレスや、各 Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）またはレイヤ 3 スイッチのルーテッド ポートの IP アドレスを設定するには、**ip address** 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。IP アドレスを削除したり、IP 処理をディセーブルにしたりするには、このコマンドの **no** 形式を使用します。

ip address *ip-address subnet-mask* [**secondary**]

no ip address [*ip-address subnet-mask*] [**secondary**]

構文の説明

ip-address	IP アドレス。
subnet-mask	関連する IP サブネットのマスク。
secondary	（任意）設定されたアドレスをセカンダリ IP アドレスに指定します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。

デフォルト

IP アドレス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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

Telnet のセッションで、スイッチの IP アドレスを削除した場合、スイッチの接続が切断されます。

ホストは、Internet Control Message Protocol（ICMP）Mask Request メッセージを使用して、サブネット マスクを判別できます。ルータは、この要求に対して ICMP Mask Reply メッセージで応答します。

no ip address コマンドを使って IP アドレスを削除することで、特定のインターフェイス上の IP プロセスをディセーブルにできます。スイッチが、その IP アドレスのうちの 1 つを使用している他のホストを検出した場合、コンソールにエラー メッセージを送信します。

オプションで **secondary** キーワードを使用することで、セカンダリ アドレスの番号を無制限に指定することができます。システムがセカンダリの送信元アドレスのルーティングの更新以外にデータグラムを生成しないということを除けば、セカンダリ アドレスはプライマリ アドレスのように処理されます。IP ブロードキャストと ARP 要求は、IP ルーティング テーブル内のインターフェイス ルートと同様に、適切に処理されます。

（注）ネットワーク セグメント上のすべてのルータがセカンダリのアドレスを使用した場合、同一のセグメント上にある他のデバイスも、同一のネットワークまたはサブネットからセカンダリ アドレスを使用しなければなりません。ネットワーク セグメント上のセカンダリ アドレスの使用に矛盾があると、ただちにルーティング ループが引き起こされる可能性があります。

Open Shortest Path First（OSPF）のルーティングの場合、インターフェイスのすべてのセカンダリ アドレスが、プライマリ アドレスと同一の OSPF 領域にあることを確認してください。

スイッチが、Bootstrap Protocol（BOOTP）または Dynamic Host Configured Protocol（DHCP）サーバから IP アドレスを受信し、そのスイッチ IP アドレスを **no ip address** コマンドで削除した場合、IP 処理はディセーブルとなり、BOOTP サーバまたは DHCP サーバが再びアドレスを割り当てることはできません。

スイッチは、各ルーテッド ポートおよび SVI に割り当てられた IP アドレスを持つことができます。設定できるルーテッド ポートおよび SVI の数はソフトウェアでは制限されていません。ただし、この数と設定された他の機能の数との相互関係によっては、ハードウェア制限により、CPU 使用率に影響が出る可能性があります。**sdm prefer** グローバル コンフィギュレーション コマンドを使用し、システムのハードウェア リソースを、テンプレートおよび機能テーブルに基づいて再度割り当てることができます。詳細は、**sdm prefer** コマンドを参照してください。

例

次の例では、サブネット ネットワークでレイヤ 2 スイッチの IP アドレスを設定する方法を示します。

```
Switch(config)# interface vlan 1
Switch(config-if)# ip address 172.20.128.2 255.255.255.0
```

次の例では、レイヤ 3 スイッチ上のポートに IP アドレスを設定する方法を示します。

```
Switch(config)# ip multicast-routing
Switch(config)# interface gigabitethernet6/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.20.128.2 255.255.255.0
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	スイッチの実行コンフィギュレーションを表示します。

ip admission

Web 認証をイネーブルにするには、**ip admission** 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。このコマンドは、fallback-profile モードでも使用できます。Web 認証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 admission *rule*

no ip admission

構文の説明

rule	IP アドミッション ルールをインターフェイスに適用します。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(35)SE	このコマンドが追加されました。

使用上のガイドライン

ip admission コマンドにより、スイッチ ポートに Web 認証ルールが適用されます。

例

次の例では、スイッチ ポートに Web 認証ルールを適用する方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip admission rule1
```

次の例では、IEEE 802.1x 対応のスイッチ ポートで使用するフォールバック プロファイルに Web 認証ルールを適用する方法を示します。

```
Switch# configure terminal
Switch(config)# fallback profile profile1
Switch(config)# ip admission name rule1
Switch(config)# end
```

関連コマンド

コマンド	説明
dot1x fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
fallback profile	ポートで Web 認証をイネーブルにします。
ip admission name proxy http	スイッチで Web 認証をグローバルにイネーブルにします。
show ip admission	Network Admission Control（NAC）のキャッシュされたエントリまたは NAC 設定についての情報を表示します。 詳細については、Cisco.com で『*Network Admission Control Software Configuration Guide*』を参照してください。

ip admission name proxy http

Web 認証をイネーブルにするには、**ip admission name proxy http** グローバル コンフィギュレーション コマンドを使用します。Web 認証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 admission name proxy http

no ip admission name proxy http

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

Web 認証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

コマンド履歴

リリース	変更内容
12.2(35)SE	このコマンドが追加されました。

使用上のガイドライン

ip admission name proxy http コマンドにより、Web 認証がスイッチ上でグローバルにイネーブルになります。

スイッチで Web 認証をグローバルにイネーブルにしてから、**ip access-group in** および **ip admission** *web-rule* インターフェイス コンフィギュレーション コマンドを使用して、特定のインターフェイスで Web 認証をイネーブルにします。

例

次の例では、スイッチ ポートで Web 認証だけを設定する方法を示します。

```
Switch# configure terminal
Switch(config) ip admission name http-rule proxy http
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 101 in
Switch(config-if)# ip admission rule
Switch(config-if)# end
```

次の例では、スイッチ ポートでのフォールバック メカニズムとして、Web 認証とともに IEEE 802.1x 認証を設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ip admission name rule2 proxy http
Switch(config)# fallback profile profile1
Switch(config)# ip access group 101 in
Switch(config)# ip admission name rule2
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x fallback profile1
Switch(config-if)# end
```

関連コマンド

コマンド	説明
dot1x fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
fallback profile	Web 認証のフォールバック プロファイルを作成します。
ip admission	ポートで Web 認証をイネーブルにします。
show ip admission	Network Admission Control（NAC）のキャッシュされたエントリまたは NAC 設定についての情報を表示します。詳細については、Cisco.com で『*Network Admission Control Software Configuration Guide*』を参照してください。

ip arp inspection filter vlan

ダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査がイネーブルの場合に、スタティック IP アドレスが設定されたホストからの ARP 要求および応答を許可または拒否するには、**ip arp inspection filter vlan** グローバル コンフィギュレーション 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 filter *arp-acl-name* **vlan** *vlan-range* [**static**]

no ip arp inspection filter *arp-acl-name* **vlan** *vlan-range* [**static**]

構文の説明

arp-acl-name	ARP Access Control List（ACL; アクセス コントロール リスト）の名前
vlan-range	VLAN の番号または範囲。 VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。
static	（任意）ARP ACL 内の暗黙の拒否を明示的な拒否として取り扱い、ACL 内の前の句に一致しないパケットをドロップするために、**static** を指定します。DHCP バインディングは使用されません。 このキーワードを指定しない場合は、パケットを拒否する明示的な拒否が ACL 内にないことを意味し、パケットが ACL 内の句に一致しないと DHCP バインディングがパケットの許可または拒否を決定します。

デフォルト

VLAN には、定義された ARP ACL が適用されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

ARP ACL を VLAN に適用してダイナミック ARP 検査を行う場合は、IP/MAC バインディングを含む ARP パケットだけが ACL と比較されます。ACL がパケットを許可すると、スイッチがパケットを転送します。それ以外のすべてのパケット タイプは、検証されずに、入力 VLAN 内でブリッジングされます。

スイッチが ACL 内の明示的な拒否ステートメントによってパケットを拒否すると、パケットがドロップされます。スイッチが暗黙の拒否ステートメントによってパケットを拒否すると、パケットは DHCP バインディングのリストと照合されます。ただし、ACL がスタティック（パケットがバインディングと比較されない）である場合を除きます。

ARP ACL を定義、または定義済みのリストの末尾に句を追加するには、**arp access-list** *acl-name* グローバル コンフィギュレーション コマンドを使用します。

例

次の例では、ダイナミック ARP 検査用に ARP ACL *static-hosts* を VLAN 1 に適用する方法を示します。

```
Switch(config)# ip arp inspection filter static-hosts vlan 1
```

設定を確認するには、**show ip arp inspection vlan 1** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
arp access-list	ARP ACL を定義します。
deny（**ARP アクセスリスト コンフィギュレーション**）	DHCP バインディングとの照合に基づいて ARP パケットを拒否します。
permit（**ARP アクセスリスト コンフィギュレーション**）	DHCP バインディングとの一致に基づいて ARP パケットを許可します。
show arp access-list	ARP アクセス リストに関する詳細を表示します。
show inventory vlan *vlan-range*	指定された VLAN のダイナミック ARP 検査の設定および動作ステートを表示します。

ip arp inspection limit

インターフェイス上の着信 Address Resolution Protocol（ARP; アドレス解決プロトコル）要求および応答のレートを制限するには、**ip arp inspection limit** 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。DoS 攻撃が発生した場合にダイナミック ARP 検査によってスイッチ リソースのすべてが消費されないようにします。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

構文の説明

rate *pps*	1 秒間に処理される着信パケット数の上限を指定します。範囲は、0 ～ 2048 pps です。
burst interval *seconds*	（任意）インターフェイスで高速 ARP パケットをモニタリングするインターバルを秒単位で指定します。範囲は 1 ～ 15 秒です。
none	処理可能な着信 ARP パケットのレートに上限を指定しません。

デフォルト

1 秒間に 15 台の新規ホストに接続するホストが配置されたスイッチド ネットワークの場合、信頼できないインターフェイスのレートは 15 pps に設定されます。

信頼できるすべてのインターフェイスでは、レートは無制限です。

バースト インターバルは 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

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

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。複数のダイナミック ARP 検査対応 VLAN でパケットを処理するようにトランクに適切なレートを設定するか、**none** キーワードを使用してレートを無制限にします。

スイッチが、設定されているレートを超えるレートのパケットを、バーストの秒数を超える連続する秒数受信すると、インターフェイスが errdisable ステートになります。

インターフェイス上のレート制限を明示的に設定しない限り、インターフェイスの信頼状態を変更することは、レート制限を信頼状態のデフォルト値に変更することになります。レート制限を設定すると、信頼状態が変更された場合でもインターフェイスはレート制限を保ちます。**no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを入力すると、インターフェイスはデフォルトのレート制限に戻ります。

トランク ポートは、集約が反映されるように、より大きいレートに設定する必要があります。着信パケットのレートが、ユーザが定義したレートを超えると、スイッチはインターフェイスを errdisable ステートにします。errdisable 回復機能は、回復の設定に従ってポートを errdisable ステートから自動的に移行させます。

レート制限は、スイッチ スタックの各スイッチで別々に算出されます。クロススタック EtherChannel の場合、これは実際のレート制限が設定値よりも高い可能性があることを意味します。たとえば、レート制限が 30 pps に設定された EtherChannel で、スイッチ 1 に 1 つのポート、およびスイッチ 2 に 1 つのポートがある場合、EtherChannel が errdisable にならずに、各ポートは 29 pps でパケットを受信できます。

EtherChannel ポートの着信 ARP パケットのレートは、すべてのチャネル メンバの着信 ARP パケット レートの合計と同じです。EtherChannel ポートのレート制限は、必ずすべてのチャネル メンバの着信 ARP パケットのレートを調べてから設定してください。

例

次の例では、ポート上の着信 ARP 要求のレートを 25 pps 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 5 秒間に設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip arp inspection limit rate 25 burst interval 5
```

設定を確認するには、**show ip arp inspection interfaces** *interface-id* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show inventory interfaces	指定されたインターフェイスまたはすべての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。

ip arp inspection log-buffer

ダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査のロギング バッファを設定するには、**ip arp inspection log-buffer** グローバル コンフィギュレーション 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 log-buffer {**entries** *number* | **logs** *number* **interval** *seconds*}

no ip arp inspection log-buffer {**entries** | **logs**}

構文の説明

entries *number*	バッファに記録されるエントリ数。指定できる範囲は 0 ～ 1024 です。
logs *number* **interval** *seconds*	システム メッセージを生成するために、指定された間隔で必要なエントリ数 **logs** *number* に指定できる範囲は 0 ～ 1024 です。値 0 は、エントリはログ バッファに配置されるものの、システム メッセージは生成されないことを意味します。 指定できる **interval** *seconds* の範囲は 0 ～ 86400 秒（1 日）です。値が 0 の場合、システム メッセージがただちに生成され、ログ バッファは常に空の状態です。

デフォルト

ダイナミック ARP がイネーブル化されると、拒否またはドロップされた ARP パケットが記録されます。

ログ エントリ数は、32 です。

システム メッセージ数は、1 秒あたり 5 に制限されています。

ロギングレート インターバルは、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

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

0 の値は、**logs** および **interval** キーワードの両方で許可されていません。

logs および **interval** の設定は、相互に作用します。**logs** *number* X が **interval** *seconds* Y より大きい場合、X 割る Y（X/Y）のシステム メッセージが毎秒送信されます。そうでない場合、1 つのシステム メッセージが Y 割る X（Y/X）秒ごとに送信されます。たとえば、**logs** *number* が 20 で、**interval** *seconds* が 4 の場合、スイッチはログ バッファにエントリがある間、5 エントリのシステム メッセージを毎秒生成します。

ログ バッファ エントリは、複数のパケットを表すことができます。たとえば、インターフェイスが同一の VLAN 上のパケットを同一の ARP パラメータで多数受信すると、スイッチは、ログ バッファ内の 1 つのエントリとしてパケットを結合し、1 つのエントリとしてシステム メッセージを生成します。

ログ バッファがオーバーフローする場合は、ログ イベントがログ バッファに収まらないことを意味しており、**show ip arp inspection log** 特権 EXEC コマンドの出力が影響を受けます。パケット数および時間以外のすべてのデータの代わりに -- が表示されます。このエントリには、これ以外の統計情報が提供されません。出力にこのようなエントリが表示される場合、ログ バッファ内のエントリ数を増やすか、ロギング レートを増やします。

ロギング バッファ コンフィギュレーションは、スイッチ スタックの各スタック メンバに適用されます。各スタック メンバでは、**logs** *number* が指定されていて、設定されたレートでシステム メッセージを生成します。たとえば、間隔（レート）が 1 エントリ / 秒の場合、メンバが 5 つのスタックでは、1 秒あたり最大 5 つのシステム メッセージが生成されます。

例

次の例では、最大 45 のエントリを保持できるようにロギング バッファを設定する方法を示します。

```
Switch(config)# ip arp inspection log-buffer entries 45
```

次の例では、ロギング レートを 4 秒あたり 20 のログ エントリに設定する方法を示します。この設定では、スイッチはログ バッファにエントリがある間、5 エントリのシステム メッセージを毎秒生成します。

```
Switch(config)# ip arp inspection log-buffer logs 20 interval 4
```

設定を確認するには、**show ip arp inspection log** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
arp access-list	ARP ACL を定義します。
clear ip arp inspection log	ダイナミック ARP 検査ログ バッファをクリアします。
ip arp inspection vlan logging	VLAN 単位で記録するパケットのタイプを制御します。
show inventory log	ダイナミック ARP 検査ログ バッファの設定と内容を表示します。

ip arp inspection trust

検査対象の着信 Address Resolution Protocol（ARP; アドレス解決プロトコル）パケットを決定する信頼状態を、インターフェイスに設定するには、**ip arp inspection trust** 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。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 trust

no ip arp inspection trust

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

インターフェイスは、信頼できない状態です。

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

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

スイッチは、信頼できるインターフェイス上で受信した ARP パケットを確認せず、単純にパケットを転送します。

信頼できないインターフェイスでは、スイッチはすべての ARP 要求と応答を代行受信します。ローカル キャッシュを更新し、該当する宛先にパケットを転送する前に、代行受信したパケットが有効な IP/MAC アドレス バインディングを持つかどうかを検証します。スイッチは、無効なパケットをドロップし、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログ バッファに記録します。

例

次の例では、ポートを信頼できる状態に設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip arp inspection trust
```

設定を確認するには、**show ip arp inspection interfaces** *interface-id* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip arp inspection log-buffer	ダイナミック ARP 検査ロギング バッファを設定します。
show inventory interfaces	指定されたインターフェイスまたはすべての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。
show inventory log	ダイナミック ARP 検査ログ バッファの設定と内容を表示します。

ip arp inspection validate

ダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査の特定のチェックを実行するには、**ip arp inspection validate** グローバル コンフィギュレーション 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 validate {[**src-mac**] [**dst-mac**] [**ip** [**allow zeros**]]}

no ip arp inspection validate [**src-mac**] [**dst-mac**] [**ip** [**allow zeros**]]

構文の説明

src-mac	イーサネット ヘッダー内の送信元 MAC アドレスと、ARP 本体内の送信側 MAC アドレスを比較します。このチェックは、ARP 要求と応答の両方に対して行われます。 このチェックがイネーブルの場合、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、ドロップされます。
dst-mac	イーサネット ヘッダー内の宛先 MAC アドレスと、ARP 本体内のターゲット MAC アドレスを比較します。このチェックは、ARP 応答に対して行われます。 このチェックがイネーブルの場合、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、ドロップされます。
ip	ARP 本体内で、無効な予期しない IP アドレスを比較します。このようなアドレスには、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。 送信側 IP アドレスは、すべての ARP 要求および応答と比較されます。ターゲット IP アドレスは ARP 応答でだけチェックされます。
allow-zeros	送信側アドレスが 0.0.0.0（ARP プローブ）である ARP が拒否されないように、IP 検証テストを変更します。

デフォルト

チェックは行われません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。
12.2(37)SE	allow-zero キーワードが追加されました。

使用上のガイドライン

少なくとも 1 つのキーワードを指定する必要があります。コマンドを実行するたびに、その前のコマンドの設定は上書きされます。つまり、コマンドが **src-mac** および **dst-mac** の検証をイネーブルにし、2 番目のコマンドが IP 検証だけをイネーブルにすると、2 番目のコマンドによって **src-mac** および **dst-mac** の検証がディセーブルになります。

allow-zeros キーワードは、次の方法で ARP Access Control List（ACL; アクセス コントロール リスト）と連動します。

- ARP ACL が ARP プローブを拒否するように設定されている場合は、**allow-zero** キーワードが指定されていても、ARP プローブはドロップされます。

- ARP プローブを明確に許可する ARP ACL を設定し、**ip arp inspection validate ip** コマンドを設定する場合、**allow-zeros** キーワードを入力しない限り、ARP プローブはドロップされます。

このコマンドの **no** 形式を使用すると、指定されたチェックだけがディセーブルになります。どのオプションもイネーブルにしない場合は、すべてのチェックがディセーブルになります。

例

次の例では、送信元 MAC の検証をイネーブルにする方法を示します。

```
Switch(config)# ip arp inspection validate src-mac
```

設定を確認するには、**show ip arp inspection vlan** *vlan-range* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show inventory vlan *vlan-range*	指定された VLAN のダイナミック ARP 検査の設定および動作ステートを表示します。

ip arp inspection vlan

VLAN 単位で、ダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査をイネーブルにするには、**ip arp inspection vlan** グローバル コンフィギュレーション 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 vlan *vlan-range*

no ip arp inspection vlan *vlan-range*

構文の説明

vlan-range	VLAN の番号または範囲。 VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。

デフォルト

すべての VLAN で ARP 検査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

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

ダイナミック ARP 検査をイネーブルにする VLAN を指定する必要があります。

ダイナミック ARP 検査は、アクセス ポート、トランク ポート、EtherChannel ポートおよびプライベート VLAN ポートでサポートされます。

例

次の例では、VLAN 1 でダイナミック ARP 検査をイネーブルにする方法を示します。

```
Switch(config)# ip arp inspection vlan 1
```

設定を確認するには、**show ip arp inspection vlan** *vlan-range* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
arp access-list	ARP ACL を定義します。
show inventory vlan *vlan-range*	指定された VLAN のダイナミック ARP 検査の設定および動作ステートを表示します。

ip arp inspection vlan logging

VLAN 単位でロギングされるパケットのタイプを制御するには、**ip arp inspection vlan logging** グローバル コンフィギュレーション 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** {**all** | **none** | **permit**} | **arp-probe**}

no ip arp inspection vlan *vlan-range* **logging** {**acl-match** | **dhcp-bindings** | **arp-probe**}

構文の説明

vlan-range	ロギングに対して設定された VLAN を指定します。 VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。
acl-match {**matchlog** | **none**}	Access Control List（ACL; アクセス コントロール リスト）との一致に基づいたパケットのロギングを指定します。 キーワードの意味は次のとおりです。 • **matchlog** : Access Control Entries（ACE）に指定されたロギング設定に基づいてパケットを記録します。このコマンドに **matchlog** キーワード、**permit** または **deny** ARP アクセス リスト コンフィギュレーション コマンドに **log** キーワードを指定すると、ACL によって許可または拒否された Address Resolution Protocol（ARP; アドレス解決プロトコル）パケットが記録されます。 • **none** : ACL に一致するパケットを記録しません。
dhcp-bindings {**permit** | **all** | **none**}	Dynamic Host Configuration Protocol（DHCP）バインディングとの一致に基づいたパケットのロギングを指定します。 キーワードの意味は次のとおりです。 • **all** : DHCP バインディングに一致するすべてのパケットを記録します。 • **none** : DHCP バインディングに一致するパケットを記録しません。 • **permit** : DHCP バインディングに許可されたパケットを記録します。
arp-probe	具体的に許可されたパケットが ARP プローブである場合に、パケットのロギングを指定します。

デフォルト

拒否またはドロップされたパケットは、すべて記録されます。ARP プローブ パケットは記録されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。
12.2(37)SE	**arp-probe** キーワードが追加されました。

使用上のガイドライン

logged の用語は、エントリがログ バッファに置かれ、システム メッセージが生成されることを意味します。

acl-match キーワードと **dhcp-bindings** キーワードは連携しています。ACL の一致を設定すると、DHCP バインディングの設定はディセーブルになりません。ロギング基準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。いずれのオプションも指定しない場合は、ARP パケットが拒否されたときに、すべてのロギング タイプが記録されるようにリセットされます。使用できるオプションは、次の 2 つです。

- **acl-match**：拒否されたパケットが記録されるように、ACL との一致に関するロギングがリセットされます。
- **dhcp-bindings**：拒否されたパケットが記録されるように、DHCP バインディングとの一致に関するロギングがリセットされます。

acl-match キーワードと **dhcp-bindings** キーワードのどちらも指定されないと、拒否されたすべてのパケットが記録されます。

ACL の末尾にある暗黙の拒否には、**log** キーワードが含まれません。つまり、**ip arp inspection filter vlan** グローバル コンフィギュレーション コマンドで **static** キーワードを使用した場合、ACL は DHCP バインディングを上書きします。ARP ACL の末尾で明示的に **deny ip any mac any log** ACE を指定しない限り、拒否された一部のパケットが記録されない場合があります。

例

次の例では、ACL 内の **permit** コマンドと一致するパケットを記録するように、VLAN 1 の ARP 検査を設定する方法を示します。

```
Switch(config)# arp access-list test1
Switch(config-arp-nacl)# permit request ip any mac any log
Switch(config-arp-nacl)# permit response ip any any mac any any log
Switch(config-arp-nacl)# exit
Switch(config)# ip arp inspection vlan 1 logging acl-match matchlog
```

設定を確認するには、**show ip arp inspection vlan** *vlan-range* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
arp access-list	ARP ACL を定義します。
clear ip arp inspection log	ダイナミック ARP 検査ログ バッファをクリアします。
ip arp inspection log-buffer	ダイナミック ARP 検査ロギング バッファを設定します。
show inventory log	ダイナミック ARP 検査ログ バッファの設定と内容を表示します。
show inventory vlan *vlan-range*	指定された VLAN のダイナミック ARP 検査の設定および動作ステートを表示します。

ip device tracking probe

Address Resolution Protocol（ARP; アドレス解決プロトコル）プローブの IP デバイス トラッキング テーブルを設定するには、**ip device tracking probe** グローバル コンフィギュレーション コマンドを使用します。ARP プローブ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 device tracking probe {**count** | **interval** | **use-svi**}

no ip device tracking probe {**count** | **interval** | **use-svi**}

構文の説明

count *number*	スイッチが ARP プローブを送信する回数を設定します。指定できる範囲は 1 ～ 255 です。
interval *seconds*	スイッチが応答を待ち、ARP プローブを再送信するまでの秒数を設定します。指定できる範囲は 30 ～ 1814400 秒です。
use-svi	Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）IP アドレスを ARP プローブのソースとして使用します。

コマンド デフォルト

カウント番号は 3 です。

30 秒間隔です。

ARP プローブのデフォルト ソース IP アドレスはレイヤ 3 インターフェイスで、スイッチポートでは 0.0.0.0 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

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。
12.2(55)SE	**use-svi** キーワードが追加されました。

使用上のガイドライン

スイッチが ARP プローブを送信する回数を設定するには、**count** キーワード オプションを使用します。指定できる範囲は 1 ～ 255 です。

スイッチが応答を待ち、ARP プローブを再送信するまでの秒数を設定するには、**interval** キーワード オプションを使用します。指定できる範囲は 30 ～ 1814400 秒です。

スイッチ ポートのデフォルト ソース IP アドレス 0.0.0.0 が使用され、ARP プローブがドロップする場合に、IP デバイス トラッキング テーブルが SVI IP アドレスを ARP プローブに使用するように設定するには、**use-svi** キーワード オプションを使用します。

IP デバイス トラッキング テーブル内のエントリに関する情報を表示するには、**show ip device tracking all** コマンドを使用します。このコマンドの詳細については、『Cisco IOS Security Command Reference, Release 12.4T』を参照してください。

例

次の例では、SVI を ARP プローブのソースとして設定する方法を示します。

```
Switch(config)# ip device tracking probe use-svi
Switch(config)#
```

関連コマンド

コマンド	説明
show ip device tracking all	IP デバイス トラッキング テーブル内のエントリに関する情報を表示します。

ip device tracking

IP デバイス トラッキングをイネーブルにするには、**ip device tracking** グローバル コンフィギュレーション 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 device tracking

no ip device tracking

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

IP デバイス トラッキング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

コマンド履歴

12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

IP デバイス トラッキングがイネーブルの場合、IP デバイス トラッキング プローブの間隔とカウントを設定し、**ip device tracking probe** コマンドを使用して ARP プローブ アドレスを設定できます。

IP デバイス トラッキング テーブル内のエントリに関する情報を表示するには、**show ip device tracking all** コマンドを使用します。このコマンドの詳細については、『Cisco IOS Security Command Reference, Release 12.4T』を参照してください。

例

次の例では、デバイス トラッキングをイネーブルにする方法を示します。

```
Switch(config)# ip device tracking
Switch(config)#
```

関連コマンド

コマンド	説明
ip device tracking probe	ARP プローブの IP デバイス トラッキング テーブルを設定します。
show ip device tracking all	IP デバイス トラッキング テーブル内のエントリに関する情報を表示します。

ip dhcp snooping

DHCP スヌーピングをグローバルにイネーブルにするには、**ip dhcp snooping** グローバル コンフィギュレーション 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 snooping

no ip dhcp snooping

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

DHCP スヌーピングは、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

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。

使用上のガイドライン

DHCP スヌーピング設定を有効にするには、DHCP 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。

ip dhcp snooping vlan *vlan-id* 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 VLAN 上でスヌーピングをイネーブルにするまで DHCP スヌーピングはアクティブになりません。

例

次の例では、DHCP スヌーピングをイネーブルにする方法を示します。

```
Switch(config)# ip dhcp snooping
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip dhcp snooping vlan	VLAN 上で DHCP スヌーピングをイネーブルにします。
show ip igmp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

ip dhcp snooping binding

DHCP スヌーピング バインディング データベースを設定して、バインディング エントリをデータベースに追加するには、**ip dhcp snooping binding** 特権 EXEC コマンドを使用します。バインディング データベースからエントリを削除するには、このコマンドの **no** 形式を使用します。

ip dhcp snooping binding *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* **expiry** *seconds*

no ip dhcp snooping binding *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*

構文の説明

mac-address	MAC アドレスを指定します。
vlan *vlan-id*	VLAN 番号を指定します。指定できる範囲は 1 ～ 4094 です。
ip-address	IP アドレスを指定します。
interface *interface-id*	バインディング エントリを追加または削除するインターフェイスを指定します。
expiry *seconds*	バインディング エントリが無効になるまでのインターバル（秒）を指定します。指定できる範囲は 1 ～ 4294967295 です。

デフォルト

デフォルトのデータベースは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、スイッチをテストまたはデバッグするときに使用します。

DHCP スヌーピング バインディング データベースでは、各データベース エントリ（別名、バインディング）には、IP アドレス、関連付けられた MAC アドレス、リース時間（16 進数）、バインディングが適用されるインターフェイス、およびインターフェイスが所属する VLAN が含まれます。データベースには、8192 のバインディングを含めることができます。

設定されたバインディングだけを表示するには、**show ip dhcp snooping binding** 特権 EXEC コマンドを使用します。動的および静的に設定されたバインディングを表示するには、**show ip source binding** 特権 EXEC コマンドを使用します。

例

次の例では、VLAN 1 のポートに、有効期限が 1000 秒の DHCP バインディング設定を生成する方法を示します。

```
Switch# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface
gigabitethernet1/0/1 expiry 1000
```

設定を確認するには、**show ip dhcp snooping binding** または **show ip dhcp source binding** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip dhcp snooping	VLAN 上で 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 バインディング データベース内の動的に設定されたバインディングおよび設定情報を表示します。
show ip source binding	DHCP スヌーピング バインディング データベース内の動的および静的に設定されたバインディングを表示します。

ip dhcp snooping database

DHCP スヌーピング バインディング データベース エージェントを設定するには、**ip dhcp snooping database** グローバル コンフィギュレーション コマンドを使用します。エージェントのディセーブル化、タイムアウト値のリセット、または書き込み遅延値のリセットを行うには、このコマンドの **no** 形式を使用します。

ip dhcp snooping database {{**flash**[*number*]**:**/*filename* | **ftp:**//*user:password@host/filename* | **http:**//*[[username:password]@]{hostname* | *host-ip}[/directory]/image-name*.**tar** | **rcp:**//*user@host/filename* | **tftp:**//*host/filename*} | **timeout** *seconds* | **write-delay** *seconds*}

no ip dhcp snooping database [**timeout** | **write-delay**]

構文の説明

flash[*number*]**:**/*filename*	データベース エージェントまたはバインディング ファイルがフラッシュ メモリにあることを指定します。 **（注）**　（任意）スタック マスターのスタック メンバ番号を指定するには、*number* パラメータを使用します。*number* に指定できる範囲は 1 ～ 9 です。
ftp://*user*:*password*@*host*/*filename*	データベース エージェントまたはバインディング ファイルが FTP サーバにあることを指定します。
http://*[[username:password]@]{hostname* | *host-ip}[/directory]/image-name*.**tar**	データベース エージェントまたはバインディング ファイルが FTP サーバにあることを指定します。
rcp://*user@host/filename*	データベース エージェントまたはバインディング ファイルが Remote Copy Protocol（RCP）サーバにあることを指定します。
tftp://*host/filename*	データベース エージェントまたはバインディング ファイルが TFTP サーバにあることを指定します。
timeout *seconds*	データベース転送プロセスを打ち切るまでの時間（秒）を指定します。 デフォルト値は 300 秒です。指定できる範囲は 0 ～ 86400 です。無期限の期間を定義するには、0 を使用します。これは転送を無期限に試行することを意味します。
write-delay *seconds*	バインディング データベースが変更された後に、転送を遅らせる期間（秒）を指定します。デフォルト値は 300 秒です。指定できる範囲は 15 ～ 86400 です。

デフォルト

データベース エージェントまたはバインディング ファイルの URL は、定義されていません。

タイムアウト値は、300 秒（5 分）です。

書き込み遅延値は、300 秒（5 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

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

DHCP スヌーピング バインディング データベースには、8192 のバインディングを含めることができます。

データベース内のリース時間を正確な時間にするには、Network Time Protocol（NTP; ネットワーク タイム プロトコル）をイネーブルにし、次の機能を設定することを強く推奨します。

- NTP 認証
- NTP ピアおよびサーバ アソシエーション
- NTP ブロードキャスト サービス
- NTP アクセス制限
- NTP パケット送信元 IP アドレス

NTP が設定されている場合、スイッチのシステム クロックが NTP と同期化されたときにだけ、スイッチがバインディングの変更内容をバインディング ファイルに書き込みます。

NVRAM（不揮発性 RAM）とフラッシュ メモリの両方のストレージ容量には限りがあるため、バインディング ファイルを TFTP サーバ上に保存することを推奨します。スイッチがネットワークベースの URL（TFTP や FTP など）の設定済み URL 内のバインディング ファイルにバインディングを書き込む前に、この URL に空のファイルを作成しておく必要があります。

DHCP スヌーピング バインディング データベースをスタック マスター NVRAM に保存するには、**ip dhcp snooping database flash**[*number*]**:**/*filename* コマンドを使用します。データベースは、スタック メンバ NVRAM に保存されません。

ip dhcp snooping database timeout コマンドに 0 秒を設定し、データベースを TFTP ファイルに書き込んでいるときに、TFTP サーバがダウンした場合、データベース エージェントは転送を無期限に続けようとします。この転送が進行中の間、他の転送は開始されません。サーバがダウンしている場合、ファイルを書き込むことができないため、これはあまり重要ではありません。

エージェントをディセーブルにするには、**no ip dhcp snooping database** コマンドを使用します。

タイムアウト値をリセットするには、**no ip dhcp snooping database timeout** コマンドを使用します。

書き込み遅延値をリセットするには、**no ip dhcp snooping database write-delay** コマンドを使用します。

例

次の例では、IP アドレス 10.1.1.1 の *directory* という名前のディレクトリ内にバインディング ファイルを保存する方法を示します。TFTP サーバに *file* という名前のファイルが存在しなければなりません。

```
Switch(config)# ip dhcp snooping database tftp://10.1.1.1/directory/file
```

次の例では、*スタック マスター* NVRAM に file01.txt というバインディング ファイルを保存する方法を示します。

```
Switch(config)# ip dhcp snooping database flash:file01.txt
```

設定を確認するには、**show ip dhcp snooping database** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip dhcp snooping	VLAN 上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping binding	DHCP スヌーピング バインディング データベースを設定します。
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 オプション 82 データ挿入をイネーブルにするには、**ip dhcp snooping information option** グローバル コンフィギュレーション コマンドを使用します。DHCP オプション 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

no ip dhcp snooping information option

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

DHCP オプション 82 データは挿入されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。

使用上のガイドライン

DHCP スヌーピング設定を有効にするには、**ip dhcp snooping** 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 DHCP 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。

オプション 82 機能がイネーブルの場合、スイッチがホストからの DHCP 要求を受信すると、オプション 82 情報がパケットに追加されます。オプション 82 情報には、スイッチ MAC アドレス（リモート ID サブオプション）、およびパケットが受信された **vlan-mod-port**（回線 ID サブオプション）のポート ID が含まれます。スイッチは、オプション 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。

DHCP サーバがパケットを受信する場合、リモート ID、回線 ID、または両方を使用して IP アドレスを割り当てるとともに、単一のリモート ID または回線 ID に割り当てることができる IP アドレス数の制限などのポリシーを適用することができます。次に DHCP サーバは、DHCP 応答内にオプション 82 フィールドをエコーします。

スイッチによって要求がサーバにリレーされた場合、DHCP サーバは応答をスイッチにユニキャストします。クライアントとサーバが同一サブネットにある場合、サーバは応答をブロードキャストします。スイッチは、リモート ID または回線 ID フィールドを検査し、オプション 82 データが最初から挿入されていたかを確認します。スイッチは、オプション 82 フィールドを削除し、DHCP 要求を送信した DHCP ホストに接続するスイッチ ポートにパケットを転送します。

例

次の例では、DHCP オプション 82 データ挿入をイネーブルにする方法を示します。

```
Switch(config)# ip dhcp snooping information option
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

ip dhcp snooping information option allow-untrusted

エッジ スイッチに接続されている信頼できないポートで受信するか、オプション 82 情報を持つ DHCP パケットを受け入れるようにアグリゲーション スイッチを設定するには、アグリゲーション スイッチで **ip dhcp snooping information option allow-untrusted** グローバル コンフィギュレーション 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 snooping information option allow-untrusted

no ip dhcp snooping information option allow-untrusted

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

スイッチは、エッジ スイッチに接続されている信頼できないポートで受信する、オプション 82 情報を持つ DHCP パケットをドロップします。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SEA	このコマンドが追加されました。

使用上のガイドライン

ホストに接続されたエッジ スイッチが、ネットワークのエッジで DHCP オプション 82 情報を挿入するように設定したい場合があります。また集約スイッチでは、DHCP スヌーピング、IP ソース ガード、またはダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査などの DHCP セキュリティ機能をイネーブルにすることもできます。ただし、アグリゲーション スイッチで DHCP スヌーピングをイネーブルにすると、スイッチは信頼できないポートで受信されたオプション 82 情報を持つパケットをドロップし、信頼できるインターフェイスに接続されたデバイスの DHCP スヌーピング バインディングを学習しません。

ホストに接続されたエッジ スイッチがオプション 82 情報を挿入する場合に、アグリゲーション スイッチで DHCP スヌーピングを使用するには、アグリゲーション スイッチで **ip dhcp snooping information option allow-untrusted** コマンドを入力します。アグリゲーション スイッチは信頼できないポートで DHCP スヌーピング パケットを受信しますが、ホストのバインディングを学習できます。アグリゲーション スイッチで DHCP セキュリティ機能をイネーブルにすることも可能です。アグリゲーション スイッチが接続されているエッジ スイッチ上のポートは、信頼できるポートとして設定する必要があります。

（注）　信頼できないデバイスが接続されたアグリゲーション スイッチに **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、信頼できないデバイスがオプション 82 情報をスプーフィングする可能性があります。

例

次の例では、アクセス スイッチが、エッジ スイッチからの信頼できないパケットのオプション 82 情報を確認せずに、パケットを受け入れるように設定する方法を示します。

```
Switch(config)# ip dhcp snooping information option allow-untrusted
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

ip dhcp snooping information option format remote-id

オプション 82 リモート ID サブオプションを設定するには、**ip dhcp snooping information option format remote-id** グローバル コンフィギュレーション コマンドを使用します。デフォルトのリモート ID サブオプションを設定するには、このコマンドの **no** 形式を使用します。

ip dhcp snooping information option format remote-id [string *ASCII-string* | **hostname]**

no ip dhcp snooping information option format remote-id

構文の説明

string *ASCII-string*	1 ～ 63 の ASCII 文字（スペースなし）を使用して、リモート ID を指定します。
hostname	スイッチのホスト名をリモート ID として指定します。

デフォルト

スイッチの MAC アドレスは、リモート ID 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

コマンド履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

DHCP スヌーピング設定を有効にするには、**ip dhcp snooping** 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 DHCP 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。

オプション 82 機能がイネーブルの場合、デフォルトのリモート ID サブオプションはスイッチの MAC アドレスです。このコマンドを使用すると、スイッチのホスト名または 63 個の ASCII 文字列（スペースなし）のいずれかをリモート ID として設定できます。

（注）ホスト名が 63 文字を超える場合、リモート ID 設定では 63 文字以降は省略されます。

例

次の例では、オプション 82 リモート ID サブオプションを設定する方法を示します。

```
Switch(config)# ip dhcp snooping information option format remote-id hostname
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip dhcp snooping vlan information option format-type circuit-id string	オプション 82 サーキット ID サブオプションを設定します。
show ip dhcp snooping	DHCP スヌーピング設定を表示します。

ip dhcp snooping limit rate

インターフェイスが 1 秒あたりに受信することのできる DHCP メッセージの数を設定するには、**ip dhcp snooping limit rate** 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。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 snooping limit rate *rate*

no ip dhcp snooping limit rate

構文の説明

rate	インターフェイスが 1 秒あたりに受信することのできる DHCP メッセージの数。指定できる範囲は 1 ～ 2048 です。

デフォルト

DHCP スヌーピング レート制限は、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

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。
12.2(18)SE	変更された指定範囲は 1 ～ 2048 です。

使用上のガイドライン

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の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内の複数の VLAN 上（一部はスヌーピングされない場合があります）の DHCP トラフィックを集約するので、インターフェイス レート制限を高い値に調整する必要があることに注意してください。

レート制限を超えた場合、インターフェイスが errdisable になります。**errdisable recovery dhcp-rate-limit** 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エラー回復をイネーブルにした場合、インターフェイスはすべての原因が時間切れになった際に動作を再試行します。エラー回復メカニズムがイネーブルでない場合、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力するまでインターフェイスは errdisable ステートのままです。

例

次の例は、インターフェイス上でメッセージ レート制限を 1 秒あたり 150 メッセージに設定する方法を示します。

```
Switch(config-if)# ip dhcp snooping limit rate 150
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
errdisable recovery	回復メカニズムを設定します。
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

ip dhcp snooping trust

Dynamic Host Configuration Protocol（DHCP）スヌーピングのためにポートを信頼性があるものとして設定するには、**ip dhcp snooping trust** 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。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 snooping trust

no ip dhcp snooping trust

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

DHCP スヌーピング信頼は、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

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。

使用上のガイドライン

DHCP サーバ、その他のスイッチ、またはルータに接続されたポートを信頼できるポートとして設定します。DHCP クライアントに接続されたポートを信頼できないポートとして設定します。

例

次の例では、ポート上で DHCP スヌーピング信頼をイネーブルにする方法を示します。

```
Switch(config-if)# ip dhcp snooping trust
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

ip dhcp snooping verify

スイッチが、信頼性のないポート上で 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 アドレスと一致することを確認するよう設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip dhcp snooping verify** グローバル コンフィギュレーション コマンドを使用します。スイッチが MAC アドレスを確認しないように設定するには、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

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

スイッチは、パケットのクライアント ハードウェア アドレスと一致する信頼されないポートで受信した DHCP パケットの送信元 MAC アドレスを確認します。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(18)SE	このコマンドが追加されました。

使用上のガイドライン

サービスプロバイダー ネットワークで、スイッチが信頼できないポートの DHCP クライアントからパケットを受信した場合、スイッチは自動的に送信元 MAC アドレスと DHCP クライアント ハードウェア アドレスが一致するかを確認します。アドレスが一致する場合、スイッチはパケットを転送します。アドレスが一致しない場合、スイッチはパケットをドロップします。

例

次の例では、MAC アドレス確認をディセーブルにする方法を示します。

```
Switch(config)# no ip dhcp snooping verify mac-address
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピング設定を表示します。

ip dhcp snooping vlan

VLAN で Dynamic Host Configuration Protocol（DHCP）スヌーピングをイネーブルにするには、**ip dhcp snooping vlan** グローバル コンフィギュレーション 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 snooping vlan *vlan-range*

no ip dhcp snooping vlan *vlan-range*

構文の説明

vlan-range	DHCP スヌーピングをイネーブルにする VLAN ID または VLAN 範囲を指定します。指定できる範囲は 1 ～ 4094 です。 VLAN ID 番号によって特定される単一の VLAN ID、それぞれをカンマで区切った一連の VLAN ID、ハイフンを間に挿入した VLAN ID の範囲、または先頭および末尾の VLAN ID で区切られた VLAN ID の範囲を入力することができます。これらはスペースで区切ります。

デフォルト

すべての VLAN 上で DHCP スヌーピングがディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。

使用上のガイドライン

VLAN 上で DHCP スヌーピングをイネーブルにする前に、まず DHCP 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。

例

次の例では、DHCP スヌーピングを VLAN 10 でイネーブルにする方法を示します。

```
Switch(config)# ip dhcp snooping vlan 10
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

ip dhcp snooping vlan information option format-type circuit-id string

オプション 82 回線 ID サブオプションを設定するには、**ip dhcp snooping vlan information option format-type circuit-id string** 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。デフォルトのサーキット ID サブオプションを設定するには、このコマンドの **no** 形式を使用します。

ip dhcp snooping vlan *vlan-id* **information option format-type circuit-id** [**override**] **string** *ASCII-string*

no ip dhcp snooping vlan *vlan-id* **information option format-type circuit-id** [**override**] **string**

構文の説明

vlan *vlan-id*	VLAN ID を指定します。指定できる範囲は 1 ～ 4094 です。
override	（任意）3 ～ 63 の ASCII 文字（スペースなし）を使用して、上書き文字列を指定します。
string *ASCII-string*	3 ～ 63 の ASCII 文字（スペースなし）を使用して、サーキット ID を指定します。

デフォルト

vlan-mod-port 形式のスイッチ VLAN およびポート ID は、デフォルトのサーキット ID 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

コマンド履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。
12.2(52)SE	**override** キーワードが追加されました。

使用上のガイドライン

DHCP スヌーピング設定を有効にするには、**ip dhcp snooping** 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 DHCP 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。

オプション 82 機能がイネーブルの場合、デフォルトのサーキット ID サブオプションは、**vlan-mod-port** 形式のスイッチ VLAN およびポート ID です。このコマンドを使用すると、サーキット ID となる ASCII 文字列を設定できます。**vlan-mod-port** フォーマット タイプを無効にし、その代わりにサーキット ID を使用して、加入者情報を定義する場合、**override** キーワードを使用します。

（注）　スイッチ上で文字数の多いサーキット ID を設定する場合、NVRAM（不揮発性 RAM）またはフラッシュ メモリに長い文字列が与える影響を考慮してください。サーキット ID 設定がその他のデータと組み合わされた場合、NVRAM またはフラッシュ メモリの容量を超えてしまい、エラー メッセージが表示されます。

例

次の例では、オプション 82 サーキット ID サブオプションを設定する方法を示します。

```
Switch(config-if)# ip dhcp snooping vlan 250 information option format-type circuit-id
string customerABC-250-0-0
```

次の例では、オプション 82 サーキット ID 上書きサブオプションを設定する方法を示します。

```
Switch(config-if)# ip dhcp snooping vlan 250 information option format-type circuit-id
override string testcustomer
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

（注）　リモート ID 設定を含むグローバル コマンド出力だけを表示するには、**show ip dhcp snooping** ユーザ EXEC コマンドを使用します。サーキット ID として設定したインターフェイス単位または VLAN 単位の文字列は表示されません。

関連コマンド

コマンド	説明
ip dhcp snooping information option format remote-id	オプション 82 リモート ID サブオプションを設定します。
show ip dhcp snooping	DHCP スヌーピング設定を表示します。

ip igmp filter

インターフェイスに Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）を適用することで、レイヤ 2 インターフェイス上のすべてのホストが 1 つまたは複数の IP マルチキャスト グループに加入できるかどうかを制御するには、**ip igmp filter** 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。インターフェイスから指定されたプロファイルを削除するには、このコマンドの **no** 形式を使用します。

ip igmp filter *profile number*

no ip igmp filter

構文の説明

profile number	適用する IGMP プロファイル番号。指定できる範囲は 1 ～ 4294967295 です。

デフォルト

IGMP のフィルタは適用されていません。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

IGMP フィルタはレイヤ 2 の物理インターフェイスだけに適用できます。ルーテッド ポート、Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）、または EtherChannel グループに属するポートに対して IGMP フィルタを適用することはできません。

IGMP のプロファイルは 1 つまたは複数のポート インターフェイスに適用できますが、1 つのポートに対して 1 つのプロファイルだけ適用できます。

例

次の例では、IGMP プロファイル 22 をポートに適用する方法を示します。

```
Switch(config)# interface gigabitethernet1//2
Switch(config-if)# ip igmp filter 22
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを使用してインターフェイスを指定します。

関連コマンド

コマンド	説明
ip igmp profile	指定された IGMP プロファイル番号を設定します。
show ip dhcp snooping statistics	指定された IGMP プロファイルの特性を表示します。
show running-config interface *interface-id*	スイッチのインターフェイス上の実行コンフィギュレーションを（インターフェイスに適用している IGMP プロファイルがある場合はそれを含み）表示します。

ip igmp max-groups

レイヤ 2 インターフェイスが加入可能な Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）グループの最大数を設定したり、転送テーブル内でエントリが最大数に達する場合の IGMP スロットリング動作を設定したりするには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip igmp max-groups** 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。最大数をデフォルト値（無制限）に戻すか、デフォルトのスロットリング アクション（レポートをドロップ）に戻すには、このコマンドの **no** 形式を使用します。

ip igmp max-groups {*number* | **action** {**deny** | **replace**}}

no ip igmp max-groups {*number* | **action**}

構文の説明

number	インターフェイスが参加できる IGMP グループの最大数。指定できる範囲は 0 ～ 4294967294 です。デフォルトの設定に制限はありません。
action deny	エントリの最大数が IGMP スヌーピング転送テーブルにある場合は、次の IGMP 加入レポートをドロップします。これがデフォルトのアクションになります。
action replace	最大数のエントリが IGMP スヌーピング転送テーブルにある場合、IGMP レポートを受信した既存のグループを新しいグループに置き換えます。

デフォルト

デフォルトの最大グループ数は制限なしです。

インターフェイス上に IGMP グループ エントリの最大数があることをスイッチが学習した後の、デフォルトのスロットリング アクションでは、インターフェイスが受信する次の IGMP レポートをドロップし、インターフェイスに IGMP グループのエントリを追加しません。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(19)EA1	**action** {**deny** | **replace**} キーワードが追加されました。

使用上のガイドライン

このコマンドは、レイヤ 2 物理インターフェイスおよび論理 EtherChannel インターフェイスでだけ使用できます。ルーテッド ポート、Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）、または EtherChannel グループに属するポートに対して IGMP 最大グループ数を設定することはできません。

IGMP スロットリング アクションを設定する場合には、次の注意事項に従ってください。

- スロットリング アクションを **deny** として設定して最大グループ制限を設定する場合、以前転送テーブルにあったエントリは、削除されませんが期限切れになります。これらのエントリの期限が切れた後で、エントリの最大数が転送テーブルにある場合は、インターフェイス上で受信された次の IGMP レポートをスイッチがドロップします。
- スロットリング アクションを **replace** として設定して最大グループ制限を設定する場合、以前転送テーブルにあったエントリは削除されます。最大数のエントリが転送テーブルにある場合、スイッチはランダムに選択したマルチキャスト エントリを受信した IGMP レポートと置き換えます。

- 最大グループ制限がデフォルト（制限なし）に設定されている場合、**ip igmp max-groups** {**deny** | **replace**} コマンドを入力しても無効です。

例

次の例では、ポートが加入できる IGMP グループ数を 25 に制限する方法を示します。

```
Switch(config)# interface gigabitethernet1//2
Switch(config-if)# ip igmp max-groups 25
```

次の例では、最大数のエントリが転送テーブルにあるときに、IGMP レポートを受信した既存のグループを新しいグループと置き換えるように設定する方法を示します。

```
Switch(config)# interface gigabitethernet1//2
Switch(config-if)# ip igmp max-groups action replace
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを使用してインターフェイスを指定します。

関連コマンド

コマンド	説明
show running-config interface *interface-id*	インターフェイスが参加できる IGMP グループの最大数やスロットリング アクションなど、スイッチのインターフェイス上で実行コンフィギュレーションを表示します。

ip igmp profile

Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）プロファイルを作成し、IGMP プロファイル コンフィギュレーション モードを開始するには、**ip igmp profile** グローバル コンフィギュレーション コマンドを使用します。このモードで、スイッチポートからの IGMP メンバシップ レポートをフィルタリングするための IGMP プロファイルの設定を指定できます。IGMP プロファイルを削除するには、このコマンドの **no** 形式を使用します。

ip igmp profile *profile number*

no ip igmp profile *profile number*

構文の説明

profile number	設定する IGMP プロファイル番号。指定できる範囲は 1 ～ 4294967295 です。

デフォルト

IGMP プロファイルは定義されていません。設定された場合、デフォルトの IGMP プロファイルとの一致機能は、一致するアドレスを拒否する設定になります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

IGMP プロファイル コンフィギュレーション モードでは、次のコマンドを使用することでプロファイルを作成できます。

- deny : 一致するアドレスを拒否します（デフォルト設定の状態）。
- exit : IGMP プロファイル コンフィギュレーション モードを終了します。
- no : コマンドを無効にする、またはデフォルトにリセットします。
- permit : 一致するアドレスを許可します。
- range : プロファイルに対する IP アドレスの範囲を指定します。1 つの IP アドレス、またはアドレスの最初と最後で範囲を指定することもできます。

  範囲を入力する場合、低い方の IP マルチキャスト アドレスを入力してからスペースを入力し、次に高い方の IP マルチキャスト アドレスを入力します。

IGMP のプロファイルを、1 つまたは複数のレイヤ 2 インターフェイスに適用できますが、各インターフェイスに適用できるプロファイルは 1 つだけです。

例

次の例では、IP マルチキャスト アドレスの範囲を指定した IGMP プロファイル 40 の設定方法を示します。

```
Switch(config)# ip igmp profile 40
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 233.1.1.1 233.255.255.255
```

設定を確認するには、**show ip igmp profile** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip igmp filter	指定のインターフェイスに対し、IGMP を適用します。
show ip dhcp snooping statistics	すべての IGMP プロファイルまたは指定の IGMP プロファイル番号の特性を表示します。

ip igmp snooping

Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）スヌーピングをスイッチ上でグローバルにイネーブル、または VLAN ごとにイネーブルにするには、**ip igmp snooping** グローバル コンフィギュレーション 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 [**vlan** *vlan-id*]

no ip igmp snooping [**vlan** *vlan-id*]

構文の説明

vlan *vlan-id*	（任意）指定された VLAN で IGMP スヌーピングをイネーブルにします。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。

デフォルト

スイッチ上で、IGMP スヌーピングはグローバルにイネーブルです。

VLAN インターフェイス上で、IGMP スヌーピングはイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

IGMP スヌーピングがグローバルにイネーブルである場合は、すべての既存 VLAN インターフェイスでイネーブルになります。IGMP スヌーピングがグローバルにディセーブルである場合、すべての既存 VLAN インターフェイスで IGMP スヌーピングがディセーブルになります。

VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

例

次の例では、IGMP スヌーピングをグローバルにイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping
```

次の例では、IGMP スヌーピングを VLAN 1 でイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping vlan 1
```

設定を確認するには、**show ip igmp snooping** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip igmp snooping report-suppression	IGMP レポート抑制をイネーブルにします。
show ip dhcp snooping statistics	スヌーピング設定を表示します。
show ip igmp snooping groups	IGMP スヌーピング マルチキャスト情報を表示します。
show ip igmp snooping mrouter	IGMP スヌーピング ルータ ポートを表示します。
show ip igmp snooping querier	スイッチ上に設定された IGMP クエリアの設定および動作情報を表示します。

ip igmp snooping last-member-query-interval

Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）の設定可能な Leave タイマーをグローバルにまたは VLAN ベースごとにイネーブルにするには、**ip igmp snooping last-member-query-interval** グローバル コンフィギュレーション 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 [**vlan** *vlan-id*] **last-member-query-interval** *time*

no ip igmp snooping [**vlan** *vlan-id*] **last-member-query-interval**

構文の説明t

vlan *vlan-id*	（任意）指定された VLAN で IGMP スヌーピングおよび Leave タイマーをイネーブルにします。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。
time	秒単位のタイムアウト間隔。指定できる範囲は 100 ～ 32768 ミリ秒です。

デフォルト

デフォルトのタイムアウト設定は 1000 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

コマンド履歴

リリース	変更内容
12.2(25)SEB	このコマンドが追加されました。
12.2(46)SE	*time* の範囲が 100 ～ 32768 に変更されました。

使用上のガイドライン

IGMP スヌーピングがグローバルにイネーブルである場合は、IGMP スヌーピングはすべての既存 VLAN インターフェイスでイネーブルになります。IGMP スヌーピングがグローバルにディセーブルである場合は、IGMP スヌーピングはすべての既存 VLAN インターフェイスでディセーブルになります。

VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

VLAN 上に Leave タイマーを設定すると、グローバル設定を上書きします。

IGMP 設定可能な Leave タイムは、IGMP バージョン 2 を実行するデバイスでだけサポートされます。

設定は、NVRAM（不揮発性 RAM）に保存されます。

例

次の例では、IGMP Leave タイマーを 2000 ミリ秒でグローバルにイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping last-member-query-interval 2000
```

次の例では、VLAN 1 上で IGMP Leave タイマーを 3000 ミリ秒に設定する方法を示します。

```
Switch(config)# ip igmp snooping vlan 1 last-member-query-interval 3000
```

設定を確認するには、**show ip igmp snooping** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピングをイネーブルにします。
ip igmp snooping vlan immediate-leave	IGMP 即時脱退処理をイネーブルにします。
ip igmp snooping vlan mrouter	レイヤ 2 ポートをマルチキャスト ルータ ポートとして設定します。
ip igmp snooping vlan static	レイヤ 2 ポートをグループのメンバとして設定します。
show ip igmp snooping	IGMP スヌーピング設定を表示します。

ip igmp snooping querier

レイヤ 2 ネットワークの Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）クエリア機能をグローバルにイネーブルにするには、**ip igmp snooping querier** グローバル コンフィギュレーション コマンドを使用します。キーワードとともにコマンドを入力すると、VLAN インターフェイスの IGMP クエリア機能をイネーブルにし、設定できます。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 querier [**vlan** *vlan-id*] [**address** *ip-address* | **max-response-time** *response-time* | **query-interval** *interval-count* | **tcn query** [**count** *count* | **interval** *interval*] | **timer expiry** | **version** *version*]

no ip igmp snooping querier [**vlan** *vlan-id*] [**address** | **max-response-time** | **query-interval** | **tcn query** { **count** *count* | **interval** *interval*} | **timer expiry** | **version**]

構文の説明

vlan *vlan-id*	（任意）指定された VLAN で IGMP スヌーピングおよび IGMP クエリア機能をイネーブルにします。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。
address *ip-address*	（任意）送信元 IP アドレスを指定します。IP アドレスを指定しない場合、クエリアは IGMP クエリアに設定されたグローバル IP アドレスを使用します。
max-response-time *response-time*	（任意）IGMP クエリア レポートを待機する最長時間を設定します。指定できる範囲は 1 ～ 25 秒です。
query-interval *interval-count*	（任意）IGMP クエリアの間隔を設定します。指定できる範囲は 1 ～ 18000 秒です。
tcn query[**count** *count* | **interval** *interval*]	（任意）Topology Change Notification（TCN; トポロジ変更通知）に関連するパラメータを設定します。キーワードの意味は次のとおりです。 • **count** *count* : TCN 時間間隔に実行される TCN クエリーの数を設定します。指定できる範囲は 1 ～ 10 です。 • **interval** *interval* : TCN クエリーの時間間隔を設定します。指定できる範囲は 1 ～ 255 です。
timer expiry	（任意）IGMP クエリアが期限切れになる時間を設定します。指定できる範囲は 60 ～ 300 秒です。
version *version*	（任意）クエリア機能が使用する IGMP バージョン番号を選択します。選択できる番号は 1 または 2 です。

デフォルト

IGMP スヌーピング クエリア機能は、スイッチでグローバルにイネーブルです。

イネーブルになっている場合、マルチキャスト対応デバイスから IGMP トラフィックを検出すると、IGMP スヌーピング クエリアはディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SEA	このコマンドが追加されました。

使用上のガイドライン

クエリアとも呼ばれる IGMP クエリー メッセージを送信するデバイスの IGMP バージョンおよび IP アドレスを検出するために IGMP スヌーピングをイネーブルにするには、このコマンドを使用します。

デフォルトでは、IGMP スヌーピング クエリアは、IGMP *バージョン 2*（IGMPv2）を使用するデバイスを検出するよう設定されていますが、IGMP *バージョン 1*（IGMPv1）を使用しているクライアントは検出しません。デバイスが IGMPv2 を使用している場合、**max-response-time** 値を手動で設定できます。デバイスが IGMPv1 を使用している場合は、**max-response-time** を設定できません （値を設定できず、0 に設定されています）。

IGMPv1 を実行している RFC に準拠していないデバイスは、**max-response-time** 値としてゼロ以外の値を持つ IGMP 一般クエリー メッセージを拒否することがあります。デバイスで IGMP 一般クエリー メッセージを受け入れる場合、IGMP スヌーピング クエリアが IGMPv1 を実行するように設定します。

VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

例

次の例では、IGMP スヌーピング クエリア機能をグローバルにイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping querier
```

次の例では、IGMP スヌーピング クエリアの最大応答時間を 25 秒に設定する方法を示します。

```
Switch(config)# ip igmp snooping querier max-response-time 25
```

次の例では、IGMP スヌーピング クエリアの時間間隔を 60 秒に設定する方法を示します。

```
Switch(config)# ip igmp snooping querier query-interval 60
```

次の例では､IGMP スヌーピング クエリアの TCN クエリー カウントを 25 に設定する方法を示します。

```
Switch(config)# ip igmp snooping querier tcn count 25
```

次の例では、IGMP スヌーピング クエリアのタイムアウトを 60 秒に設定する方法を示します。

```
Switch(config)# ip igmp snooping querier timeout expiry 60
```

次の例では、IGMP スヌーピング クエリア機能をバージョン 2 に設定する方法を示します。

```
Switch(config)# ip igmp snooping querier version 2
```

設定を確認するには、**show ip igmp snooping** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip igmp snooping report-suppression	IGMP レポート抑制をイネーブルにします。
show ip igmp snooping	IGMP スヌーピング設定を表示します。
show ip igmp snooping groups	IGMP スヌーピング マルチキャスト情報を表示します。
show ip igmp snooping mrouter	IGMP スヌーピング ルータ ポートを表示します。

ip igmp snooping report-suppression

Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）レポート抑制をイネーブルにするには、**ip igmp snooping report-suppression** グローバル コンフィギュレーション コマンドを使用します。IGMP レポート抑制をディセーブルにして、すべての IGMP レポートをマルチキャスト ルータへ転送するには、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

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

IGMP レポート抑制はイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。

使用上のガイドライン

IGMP レポート抑制は、マルチキャスト クエリーに IGMPv1 レポートと IGMPv2 レポートがある場合にだけサポートされます。この機能は、クエリーに IGMPv3 レポートが含まれている場合はサポートされません。

スイッチは IGMP レポート抑制を使用して、マルチキャスト ルータ クエリーごとに IGMP レポートを 1 つだけマルチキャスト デバイスに転送します。IGMP ルータ抑制がイネーブル（デフォルト）である場合、スイッチは最初の IGMP レポートをグループのすべてのポートからすべてのマルチキャスト ルータに送信します。スイッチは、グループの残りの IGMP レポートをマルチキャスト ルータに送信しません。この機能により、マルチキャスト デバイスにレポートが重複して送信されることを防ぎます。

マルチキャスト ルータ クエリーに IGMPv1 および IGMPv2 レポートに対する要求だけが含まれている場合、スイッチは最初の IGMPv1 レポートまたは IGMPv2 レポートだけを、グループのすべてのホストからすべてのマルチキャスト ルータに送信します。マルチキャスト ルータ クエリーに IGMPv3 レポートの要求も含まれる場合は、スイッチはグループのすべての IGMPv1、IGMPv2、および IGMPv3 レポートをマルチキャスト デバイスに転送します。

no ip igmp snooping report-suppression コマンドを入力して IGMP レポート抑制をディセーブルにした場合、すべての IGMP レポートがすべてのマルチキャスト ルータに送信されます。

例

次の例では、レポート抑制をディセーブルにする方法を示します。

```
Switch(config)# no ip igmp snooping report-suppression
```

設定を確認するには、**show ip igmp snooping** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピングをイネーブルにします。
show ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピング設定を表示します。

ip igmp snooping tcn

Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）Topology Change Notification（TCN）の動作を設定するには、**ip igmp snooping tcn** グローバル コンフィギュレーション 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 tcn {**flood query count** *count* | **query solicit**}

no ip igmp snooping tcn {**flood query count** | **query solicit**}

構文の説明

flood query count *count*	マルチキャスト トラフィックがフラッディングする IGMP の一般的クエリー数を指定します。指定できる範囲は 1 ～ 10 です。
query solicit	TCN イベント中に発生したフラッド モードから回復するプロセスの速度を上げるために、IGMP Leave メッセージ（グローバル脱退）を送信します。

デフォルト

TCN フラッド クエリー カウントは 2 です。

TCN クエリー要求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

コマンド履歴

リリース	変更内容
12.2(25)SEB	このコマンドが追加されました。

使用上のガイドライン

TCN イベント後にマルチキャスト トラフィックがフラッディングする時間を制御するには、**ip igmp snooping tcn flood query count** グローバル コンフィギュレーション コマンドを使用します。**ip igmp snooping tcn flood 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 つの一般的クエリーの受信後にフラッディングが停止します。カウントを 7 に設定すると、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ディングは、7 つの一般的クエリーを受信するまで継続します。グループは、TCN イベント中に受信した一般的クエリーに基づいて学習されます。

スパニング ツリー ルートかどうかにかかわらず、グローバル Leave メッセージを送信するようにスイッチをイネーブルにするには、**ip igmp snooping tcn query solicit** グローバル コンフィギュレーション コマンドを使用します。また、このコマンドは、TCN イベント中に発生したフラッド モードから回復するプロセスの速度を上げます。

例

次の例では、マルチキャスト トラフィックがフラッディングする IGMP の一般的クエリー数を 7 に指定する方法を示します。

```
Switch(config)# no ip igmp snooping tcn flood query count 7
```

設定を確認するには、**show ip igmp snooping** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピングをイネーブルにします。
ip igmp snooping tcn flood	インターフェイスのフラッディングを IGMP スヌーピング スパニング ツリー TCN 動作として指定します。
show ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピング設定を表示します。

ip igmp snooping tcn flood

マルチキャスト フラッディングを Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）スヌーピング スパニングツリー Topology Change Notification（TCN）の動作として設定するには、**ip igmp snooping tcn flood** 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。マルチキャスト 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 tcn flood

no ip igmp snooping tcn flood

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

マルチキャスト フラッディングは、スパニング ツリー TCN のイベント中、インターフェイス上でイネーブルです。

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

コマンド履歴

リリース	変更内容
12.2(25)SEB	このコマンドが追加されました。

使用上のガイドライン

スイッチが TCN を受信すると、2 つの一般的なクエリーが受信されるまで、マルチキャスト トラフィックはすべてのポートに対してフラッディングします。異なるマルチキャスト グループに加入している接続ホストを持つポートがスイッチに多数ある場合、フラッディングがリンクの容量を超過し、パケット損失を招くことがあります。

ip igmp snooping tcn flood query count *count* 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、フラッディング クエリー カウントを変更できます。

例

次の例では、インターフェイス上でマルチキャスト フラッディングをディセーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1//2
Switch(config-if)# no ip igmp snooping tcn flood
```

設定を確認するには、**show ip igmp snooping** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピングをイネーブルにします。
ip igmp snooping tcn	スイッチで IGMP TCN 動作を設定します。
show ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピング設定を表示します。

ip igmp snooping vlan immediate-leave

VLAN ごとに Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）スヌーピング即時脱退処理をイネーブルにするには、**ip igmp snooping immediate-leave** グローバル コンフィギュレーション 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 vlan *vlan-id* **immediate-leave**

no ip igmp snooping vlan *vlan-id* **immediate-leave**

構文の説明

vlan-id	指定された VLAN で IGMP スヌーピングおよび即時脱退機能をイネーブルにします。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。

デフォルト

IGMP の即時脱退処理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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

VLAN の各ポート上で 1 つのレシーバの最大値が設定されている場合に限り、即時脱退処理の機能を設定してください。設定は、NVRAM（不揮発性 RAM）に保存されます。

即時脱退機能をサポートするのは、IGMP バージョン 2 が稼動しているホストだけです。

例

次の例では、VLAN 1 で IGMP 即時脱退処理をイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping vlan 1 immediate-leave
```

設定を確認するには、**show ip igmp snooping** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip igmp snooping report-suppression	IGMP レポート抑制をイネーブルにします。
show ip igmp snooping	スヌーピング設定を表示します。
show ip igmp snooping groups	IGMP スヌーピング マルチキャスト情報を表示します。
show ip igmp snooping mrouter	IGMP スヌーピング ルータ ポートを表示します。
show ip igmp snooping querier	スイッチ上に設定された IGMP クエリアの設定および動作情報を表示します。

ip igmp snooping vlan mrouter

マルチキャスト ルータ ポートを追加したり、マルチキャスト学習方式を設定したりするには、**ip igmp snooping mrouter** グローバル コンフィギュレーション 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 vlan *vlan-id* **mrouter** {**interface** *interface-id* | **learn** {**cgmp** | **pim-dvmrp**}}

no ip igmp snooping vlan *vlan-id* **mrouter** {**interface** *interface-id* | **learn** {**cgmp** | **pim-dvmrp**}}

構文の説明

vlan-id	IGMP スヌーピングをイネーブルにして、指定した VLAN のポートをマルチキャスト ルータ ポートとして追加します。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。
interface *interface-id*	ネクストホップ インターフェイスをマルチキャスト ルータに指定します。キーワードの意味は次のとおりです。 • **fastethernet** *interface number*：ファスト イーサネット IEEE 802.3 インターフェイス • **gigabitethernet** *interface number*：ギガビット イーサネット IEEE 802.3z インターフェイス • **port-channel** *interface number*：チャネル インターフェイス。指定できる範囲は 0 ～ 48 です。
learn {**cgmp** | **pim-dvmrp**}	マルチキャスト ルータの学習方式を指定します。キーワードの意味は次のとおりです。 • **cgmp**：Cisco Group Management Protocol（CGMP）パケットでのスヌーピングによりスイッチがマルチキャスト ルータ ポートを学習するように設定します。 • **pim-dvmrp**：IGMP クエリーおよび Protocol-Independent Multicast-Distance Vector Multicast Routing Protocol（PIM-DVMRP）パケットでのスヌーピングによりスイッチがマルチキャスト ルータ ポートを学習するように設定します。

デフォルト

デフォルトでは、マルチキャスト ルータ ポートはありません。

デフォルトの学習方式は **pim-dvmrp** です。IGMP クエリーおよび PIM-DVMRP パケットをスヌーピングします。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

CGMP の学習方式は制御トラフィックの削減に役立ちます。

設定は、NVRAM（不揮発性 RAM）に保存されます。

例

次の例では、ポートをマルチキャスト ルータ ポートとして設定する方法を示します。

```
Switch(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet1/0/22
```

次の例では、マルチキャスト ルータの学習方式を CGMP として指定する方法を示します。

```
Switch(config)# ip igmp snooping vlan 1 mrouter learn cgmp
```

設定を確認するには、**show ip igmp snooping** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip igmp snooping report-suppression	IGMP レポート抑制をイネーブルにします。
show ip igmp snooping	スヌーピング設定を表示します。
show ip igmp snooping groups	IGMP スヌーピング マルチキャスト情報を表示します。
show ip igmp snooping mrouter	IGMP スヌーピング ルータ ポートを表示します。
show ip igmp snooping querier	スイッチ上に設定された IGMP クエリアの設定および動作情報を表示します。

ip igmp snooping vlan static

Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）スヌーピングをイネーブルにし、レイヤ 2 ポートをマルチキャスト グループのメンバとしてスタティックに追加するには、**ip igmp snooping static** グローバル コンフィギュレーション コマンドを使用します。スタティックなマルチキャスト グループのメンバとして指定されたポートを削除するには、このコマンドの **no** 形式を使用します。

ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*

no ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*

構文の説明

vlan-id	指定した VLAN で IGMP スヌーピングをイネーブルにします。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。
ip-address	指定のグループ IP アドレスを持ったマルチキャスト グループのメンバとして、レイヤ 2 ポートを追加します。
interface *interface-id*	メンバ ポートのインターフェイスを指定します。キーワードの意味は次のとおりです。 • **fastethernet** *interface number*：ファスト イーサネット IEEE 802.3 インターフェイス • **gigabitethernet** *interface number*：ギガビット イーサネット IEEE 802.3z インターフェイス • **port-channel** *interface number*：チャネル インターフェイス。指定できる範囲は 0 ～ 48 です。

デフォルト

デフォルトでは、マルチキャスト グループのメンバとしてスタティックに設定されたポートはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

設定は、NVRAM（不揮発性 RAM）に保存されます。

例

次の例では、インターフェイス上のホストをスタティックに設定する方法を示します。

```
Switch(config)# ip igmp snooping vlan 1 static 0100.5e02.0203 interface
gigabitethernet1/0/1
Configuring port gigabitethernet1/0/1 on group 0100.5e02.0203
```

設定を確認するには、**show ip igmp snooping** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip igmp snooping report-suppression	IGMP レポート抑制をイネーブルにします。
show ip igmp snooping	スヌーピング設定を表示します。
show ip igmp snooping groups	IGMP スヌーピング マルチキャスト情報を表示します。
show ip igmp snooping mrouter	IGMP スヌーピング ルータ ポートを表示します。
show ip igmp snooping querier	スイッチ上に設定された IGMP クエリアの設定および動作情報を表示します。

ip snap forwarding

Subnetwork Access Protocol（SNAP）カプセル化を使用した IP Version 4（IPv4）および IP Version 6（IPv6）フレームの転送をイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチ上で **ip snap forwarding** グローバル コンフィギュレーション コマンドを使用します。このフレームの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。

ip snap forwarding

no ip snap forwarding

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

スイッチは、SNAP カプセル化を使用した IPv4 および IPv6 フレームを転送しません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SEC	このコマンドが追加されました。

使用上のガイドライン

SNAP カプセル化を使用した IPv4 および IPv6 フレームの転送をイネーブルにするには、**ip snap forwarding** グローバル コンフィギュレーション コマンドを使用します。

スタックに加入しているスイッチが SNAP カプセル化を使用した IPv4 および IPv6 フレームの転送をサポートしない場合、スタックのすべてのスイッチは IPv4 および IPv6 フレームを転送せず、転送機能がディセーブルになります。

例

次の例では、SNAP カプセル化を使用した IPv4 および IPv6 フレームの転送をイネーブルにする方法を示します。

```
Switch(config)# ip snap forwarding
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	スイッチの実行コンフィギュレーションを表示します。

ip source binding

スイッチ上のスタティックな IP 送信元バインディングを設定するには、**ip source binding** グローバル コンフィギュレーション コマンドを使用します。スタティック バインディ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。

ip source binding *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*

no source binding *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*

構文の説明

mac-address	MAC アドレスを指定します。
vlan *vlan-id*	VLAN 番号を指定します。指定できる範囲は 1 ～ 4094 です。
ip-address	IP アドレスを指定します。
interface *interface-id*	IP 送信元バインディングを追加または削除するインターフェイスを指定します。

デフォルト

IP 送信元バインディング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

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

スタティック IP 送信元バインディング エントリには、IP アドレス、関連付けられた MAC アドレス、および関連付けられた VLAN 番号が含まれます。エントリは、MAC アドレスおよび VLAN 番号に基づいています。IP アドレスだけの変更でエントリを変更する場合は、スイッチは新しいエントリを作成せずに、エントリを更新します。

例

次の例では、スタティック IP 送信元バインディングを追加する方法を示します。

```
Switch(config)# ip source binding 0001.1234.1234 vlan 1 172.20.50.5 interface
gigabitethernet1/0/1
```

次の例では、スタティック バインディングを追加してから、その IP アドレスを変更する方法を示します。

```
Switch(config)# ip source binding 0001.1357.0007 vlan 1 172.20.50.25 interface
gigabitethernet1/0/1
Switch(config)# ip source binding 0001.1357.0007 vlan 1 172.20.50.30 interface
gigabitethernet1/0/1
```

コマンド設定を確認するには、**show ip source binding** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip verify source	インターフェイス上の IP 送信元ガードをイネーブルにします。
show ip source binding	スイッチ上の IP 送信元バインディングを表示します。
show ip verify source	スイッチ上または特定のインターフェイス上の IP ソース ガードの設定を表示します。

ip ssh

Secure Shell（SSH; セキュア シェル）version 1（SSHv1）または SSH version 2（SSHv2）を実行するようにスイッチを設定するには、**ip ssh** グローバル コンフィギュレーション コマンドを使用します。このコマンドは、スイッチで暗号化ソフトウェア イメージが実行されている場合にだけ利用できます。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 ssh version [**1** | **2**]

no ip ssh version [**1** | **2**]

構文の説明

1	（任意）スイッチが SSHv1 を実行するように設定します。
2	（任意）スイッチが SSH バージョン 2（SSHv2）を実行するように設定します。

デフォルト

デフォルトのバージョンは、SSH クライアントでサポートされる最新の SSH バージョンです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。

使用上のガイドライン

このコマンドを入力しない場合、またはキーワードを指定しないときは、SSH サーバは SSH クライアントがサポートする最新の SSH バージョンを選択します。たとえば、SSH クライアントが SSHv1 および SSHv2 をサポートする場合、SSH サーバは SSHv2 を選択します。

スイッチは、SSHv1 または SSHv2 サーバをサポートします。また、SSHv1 クライアントもサポートします。SSH サーバおよび SSH クライアントの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

SSHv1 サーバによって生成された Rivest、Shamir、Adelman（RSA）キー ペアは、SSHv2 サーバで使用できます。その逆の場合も同様です。

例

次の例では、スイッチが SSH バージョン 2 を実行するように設定する方法を示します。

```
Switch(config)# ip ssh version 2
```

設定を確認するには、**show ip ssh** または **show ssh** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ip ssh	SSH サーバがイネーブルであるかどうかを表示すると同時に、SSH サーバのバージョンおよび設定情報を表示します。
show ssh	SSH サーバのステータスを表示します。

ip sticky-arp（グローバル コンフィギュレーション）

プライベート VLAN に属する Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）上で sticky Address Resolution Protocol（ARP; アドレス解決プロトコル）をイネーブルにするには、**ip sticky-arp** グローバル コンフィギュレーション コマンドを使用します。sticky 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

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

sticky ARP は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

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

sticky ARP エントリとは、プライベート VLAN SVI によって学習されるエントリです。これらのエントリは、期限切れになることはありません。

ip sticky-arp グローバル コンフィギュレーション コマンドは、プライベート VLAN に属する SVI でだけサポートされます。

- プライベート VLAN を設定する場合、sticky ARP はスイッチでイネーブルです（デフォルト）。

  ip sticky-arp *インターフェイス* コンフィギュレーション コマンドを入力する場合、このコマンドは作用しません。

  no ip sticky-arp *インターフェイス* コンフィギュレーション コマンドを入力する場合、sticky ARP はインターフェイス上でディセーブルになりません。

（注）　プライベート VLAN インターフェイスの ARP エントリを表示し、確認するには、**show arp** 特権 EXEC コマンドを使用するよう推奨します。

- スイッチをデバイスから取り外し、MAC アドレスは異なるが IP アドレスが同じである別のデバイスに接続する場合、ARP エントリは作成されず、次のメッセージが表示されます。

```
*Mar 2 00:26:06.967: %IP-3-STCKYARPOVR: Attempt to overwrite Sticky ARP entry:
20.6.2.1, hw: 0000.0602.0001 by hw: 0000.0503.0001
```

- デバイスの MAC アドレスを変更する場合は、**no arp** *ip-address* 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、プライベート VLAN インターフェイス ARP エントリを手動で削除する必要があります。
- プライベート VLAN ARP エントリを追加するには、**arp** *ip-address hardware-address* **type** グローバル コンフィギュレーション コマンドを使用します。
- スイッチ上で sticky ARP をディセーブルにするには、**no sticky-arp** グローバル コンフィギュレーション コマンドを使用します。
- スイッチ上で sticky ARP がディセーブルのときに、インターフェイス上で sticky ARP をディセーブルにするには、**no sticky-arp** 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。

例

sticky ARP をディセーブルにする方法：

```
Switch(config)# no ip sticky-arp
```

設定を確認するには、**show arp** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
arp	ARP テーブルに永続的エントリを追加します。
show arp	ARP テーブル内のエントリを表示します。

ip sticky-arp（インターフェイス コンフィギュレーション）

Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）またはレイヤ 3 インターフェイス上で sticky Address Resolution Protocol（ARP; アドレス解決プロトコル）をイネーブルにするには、**ip sticky-arp** 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。sticky 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

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

sticky ARP は、プライベート VLAN SVI 上でイネーブルになります。

sticky ARP は、レイヤ 3 インターフェイスおよび標準 SVI 上でディセーブルになります。

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

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

sticky ARP エントリとは、SVI およびレイヤ 3 インターフェイス上で学習されるエントリです。これらのエントリは、期限切れになることはありません。

ip sticky-arp インターフェイス コンフィギュレーション コマンドは、次の上でだけサポートされます。

- レイヤ 3 インターフェイス
- 標準 VLAN に属する SVI
- プライベート VLAN に属する SVI

レイヤ 3 インターフェイスまたは標準 VLAN に属する SVI 上で

- sticky ARP をイネーブルにするには、**sticky-arp** 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。
- sticky ARP をディセーブルにするには、**no sticky-arp** 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。

プライベート VLAN SVI 上で

- プライベート VLAN を設定する場合、sticky ARP はスイッチでイネーブルです（デフォルト）。

  ip sticky-arp *インターフェイス* コンフィギュレーション コマンドを入力する場合、このコマンドは作用しません。

  no ip sticky-arp *インターフェイス* コンフィギュレーション コマンドを入力する場合、sticky ARP はインターフェイス上でディセーブルになりません。

（注）　プライベート VLAN インターフェイスの ARP エントリを表示し、確認するには、**show arp** 特権 EXEC コマンドを使用するよう推奨します。

- スイッチをデバイスから取り外し、MAC アドレスは異なるが IP アドレスが同じである別のデバイスに接続する場合、ARP エントリは作成されず、次のメッセージが表示されます。

```
*Mar 2 00:26:06.967: %IP-3-STCKYARPOVR: Attempt to overwrite Sticky ARP entry:
20.6.2.1, hw: 0000.0602.0001 by hw: 0000.0503.0001
```

- デバイスの MAC アドレスを変更する場合は、**no arp** *ip-address* 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、プライベート VLAN インターフェイス ARP エントリを手動で削除する必要があります。
- プライベート VLAN ARP エントリを追加するには、**arp** *ip-address hardware-address* **type** グローバル コンフィギュレーション コマンドを使用します。
- スイッチ上で sticky ARP をディセーブルにするには、**no sticky-arp** グローバル コンフィギュレーション コマンドを使用します。
- インターフェイス上で sticky ARP をディセーブルにするには、**no sticky-arp** 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。

例

標準 SVI 上で sticky ARP をイネーブルにする方法：

```
Switch(config-if)# ip sticky-arp
```

レイヤ 3 インターフェイスまたは SVI 上で sticky ARP をディセーブルにする方法：

```
Switch(config-if)# no ip sticky-arp
```

設定を確認するには、**show arp** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
arp	ARP テーブルに永続的エントリを追加します。
show arp	ARP テーブル内のエントリを表示します。

ip verify source

インターフェイスで IP ソース ガードをイネーブルにするには、**ip verify source** 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。IP ソース 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。

ip verify source [**port-security**]

no ip verify source

構文の説明

port-security	（任意）IP および MAC アドレス フィルタリングによる IP ソース ガードをイネーブルにします。 **port-security** キーワードを入力しない場合、IP アドレス フィルタリングによる IP ソース ガードがイネーブルになります。

デフォルト

IP 送信元ガ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

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

送信元 IP アドレス フィルタリングによる IP ソース ガードをイネーブルにするには、**ip verify source** 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。

送信元 IP および MAC アドレス フィルタリングによる IP ソース ガードをイネーブルにするには、**ip verify source port-security** 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。

送信元 IP および MAC アドレス フィルタリングによる IP ソース ガードをイネーブルにするには、インターフェイスのポート セキュリティをイネーブルにする必要があります。

例

次の例では、送信元 IP アドレス フィルタリングによる IP ソース ガードをイネーブルにする方法を示します。

```
Switch(config-if)# ip verify source
```

次の例では、送信元 IP および MAC アドレス フィルタリングによる IP ソース ガードをイネーブルにする方法を示します。

```
Switch(config-if)# ip verify source port-security
```

コマンド設定を確認するには、**show ip source binding** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip source binding	スイッチにスタティック バインディングを設定します。
show ip verify source	スイッチ上または特定のインターフェイス上の IP ソース ガードの設定を表示します。

ipv6 access-list

IPv6 アクセス リストを定義し、スイッチを IPv6 アクセス リスト コンフィギュレーション モードにするには、**ipv6 access-list** グローバル コンフィギュレーション コマンドを使用します。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。

ipv6 access-list *access-list-name*

no ipv6 access-list *access-list-name*

（注）　このコマンドは、スイッチ スタックでデュアル IPv4/IPv6 SDM テンプレートが設定されている場合に限り使用可能です。

構文の説明

access-list-name	IPv6 アクセス リスト名。名前にはスペースまたは引用符を含めることはできません。また、数字で始めることはできません。

デフォルト

IPv6 アクセス リスト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

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

IPv6 固有である点を除くと、**ipv6 access-list** コマンドは **ip access-list** コマンドと類似しています。

（注）　IPv6 Access Control List（ACL; アクセス コントロール リスト）は一意な名前によって定義されます（IPv6 は番号付けされた ACL をサポートしません）。IPv4 ACL と IPv6 ACL は同じ名前を共有できません。

IPv6 オプション ヘッダーに基づいた IPv6 トラフィックのフィルタリングに関する情報と任意の上位層プロトコル タイプ情報の詳細については、**ipv6 access-list** および **permit（IPv6 アクセスリスト コンフィギュレーション）** のコマンドを参照してください。変換された IPv6 ACL の設定例については、「例」の項を参照してください。

（注）すべての IPv6 ACL には最後の一致条件として、暗黙の **permit icmp any any nd-na**、**permit icmp any any nd-ns**、および **deny ipv6 any any** ステートメントがあります。このうち 2 つの **permit** 条件は、ICMPv6 近隣探索を許可します。ICMPv6 近隣探索を許可しないで **icmp any any nd-na** または **icmp any any nd-ns** を拒否するには、明示的な拒否エントリが ACL 内にある必要があります。暗黙的な **deny ipv6 any any** ステートメントを有効にするには、IPv6 ACL に 1 つ以上のエントリを含める必要があります。

IPv6 近隣探索プロセスでは、IPv6 ネットワーク レイヤ サービスを使用します。したがって、デフォルトでは IPv6 ACL により、IPv6 近隣探索パケットのインターフェイス上での送受信が暗黙的に許可されます。IPv4 では、IPv6 近隣探索プロセスと同等の Address Resolution Protocol（ARP; アドレス解決プロトコル）は、別のデータリンク レイヤ プロトコルを使用します。したがってデフォルトでは、IPv4 ACL により、ARP パケットのインターフェイス上での送受信が暗黙的に許可されます。

IPv6 ACL を IPv6 インターフェイスに適用するには、**access-list-name** 引数を指定して *ipv6 traffic-filter* 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。着信および発信 IPv6 ACL をレイヤ 3 物理インターフェイス、またはルーテッド ACL のスイッチ仮想インターフェイスに適用することはできますが、ポート ACL のレイヤ 2 インターフェイスに適用できるのは着信 IPv6 ACL だけです。

（注）**ipv6 traffic-filter** コマンドでインターフェイスに適用された IPv6 ACL は、スイッチによって転送されるトラフィックはフィルタリングしますが、スイッチによって生成されたトラフィックはフィルタリングしません。

例

次の例では、スイッチを IPv6 アクセス リスト コンフィギュレーション モードにし、list2 という名の IPv6 ACL を設定し、その ACL をインターフェイス上の発信トラフィックに適用します。最初の ACL エントリは、ネットワーク FE80:0:0:2::/64 からのすべてのパケット（送信元 IPv6 アドレスの最初の 64 ビットとして、リンクローカル プレフィクス FE80:0:0:2 のあるパケット）がインターフェイスから送信されるのを防ぎます。ACL の 2 番目のエントリは、その他すべてのトラフィックがインターフェイスから送信されるのを許可します。すべてのパケットを拒否する暗黙の条件が各 IPv6 ACL の末尾にあるので、この 2 番目のエントリが必要となります。

```
Switch(config)# ipv6 access-list list2
Switch(config-ipv6-acl)# deny FE80:0:0:2::/64 any
Switch(config-ipv6-acl)# permit any any
Switch(config-ipv6-acl)# exit
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter list2 out
```

（注）暗黙の拒否条件に依存するか、または **deny any any** ステートメントを指定してトラフィックをフィルタリングする IPv6 ACL には、プロトコル パケットのフィルタリングを避けるため、リンクローカル アドレスに対する **permit** ステートメントを含める必要があります。また、**deny** ステートメントを使用してトラフィックをフィルタリングする IPv6 ACL では、**permit any any** ステートメントをリストの最後のステートメントとして使用する必要があります。

関連コマンド

コマンド	説明
deny（IPv6 アクセスリスト コンフィギュレーション）	IPv6 アクセス リストに拒否条件を設定します。
ipv6 traffic-filter	インターフェイス上の着信または発信 IPv6 トラフィックをフィルタリングします。
permit（IPv6 アクセスリスト コンフィギュレーション）	IPv6 アクセス リストに許可条件を設定します。
show ipv6 access-list	現在のすべての IPv6 アクセス リストの内容を表示します。

ipv6 address dhcp

Dynamic Host Configuration Protocol for IPv6（DHCPv6）サーバからインターフェイス上の IPv6 アドレスを取得するには、**ipv6 address dhcp** 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。インターフェイスから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。

ipv6 address dhcp [rapid-commit]

no ipv6 address dhcp [rapid-commit]

（注）　このコマンドは、スイッチ スタックでデュアル IPv4/IPv6 SDM テンプレートが設定されている場合に限り使用可能です。

構文の説明

rapid-commit	（任意）アドレス割り当てに 2 つのメッセージ交換方式を許可します。

デフォルト

デフォルト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

コマンド履歴

リリース	変更内容
12.2(46)SE	このコマンドが追加されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

ipv6 address dhcp インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイスは DHCP プロトコルを使用して IPv6 アドレスを動的に学習できます。

rapid-commit キーワードは、アドレス割り当ておよびその他の設定について、2 つのメッセージ交換を使用できるようにします。これをイネーブルにすると、クライアントは送信請求メッセージに rapid-commit オプションを含めます。

例

次の例では、IPv6 アドレスを要求して、rapid-commit オプションをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# ipv6 address dhcp rapid-commit
```

設定を確認するには、**show ipv6 dhcp interface** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ipv6 dhcp interface	DHCPv6 インターフェイス情報を表示します。

ipv6 dhcp client request vendor

Dynamic Host Configuration Protocol for IPv6（DHCPv6）サーバのオプションを要求するように IPv6 クライアントを設定するには、**ipv6 dhcp client request** 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。要求を削除するには、このコマンドの **no** 形式を使用します。

ipv6 dhcp client request vendor

no ipv6 dhcp client request vendor

（注）　このコマンドは、スイッチ スタックでデュアル IPv4/IPv6 SDM テンプレートが設定されている場合に限り使用可能です。

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルト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

コマンド履歴

リリース	変更内容
12.2(46)SE	このコマンドが追加されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

ベンダー固有オプションを要求するには、**ipv6 dhcp client request vendor** 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。イネーブルにすると、IPv6 アドレスを DHCP から取得するときにだけこのコマンドの確認が行われます。インターフェイスが IPv6 アドレスを取得した後でこのコマンドを入力しても、次回クライアントが DHCP から IPv6 アドレスを取得するまでこのコマンドは有効になりません。

例

次の例では、ベンダー固有オプションの要求をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# ipv6 dhcp client request vendor-specific
```

関連コマンド

コマンド	説明
ipv6 address dhcp	DHCP からインターフェイスの IPv6 アドレスを取得します。

ipv6 dhcp ping packets

Dynamic Host Configuration Protocol for IPv6（DHCPv6）サーバが ping 操作の一部としてプール アドレスに送信するパケットの数を指定するには、**ipv6 dhcp ping packets** グローバル コンフィギュレーション コマンドを使用します。サーバがプール アドレスに ping を送信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。

ipv6 dhcp ping packets *number*

no ipv6 dhcp ping packets

（注）　このコマンドは、スイッチ スタックでデュアル IPv4/IPv6 SDM テンプレートが設定されている場合に限り使用可能です。

構文の説明

number	アドレスが要求元のクライアントに割り当てられる前に送信された ping パケット数。指定できる範囲は 0 ～ 10 です。

デフォルト

デフォルト値は 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

コマンド履歴

リリース	変更内容
12.2(46)SE	このコマンドが追加されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

DHCPv6 サーバは、要求元クライアントにアドレスを割り当てる前にプール アドレスに ping を送信します。ping の応答がない場合、サーバはアドレスが使用されていない可能性が高いと想定し、アドレスを要求元クライアントに割り当てます。

number 引数を 0 に設定すると、DHCPv6 サーバの ping 操作がオフになります。

例

次の例では、DHCPv6 サーバによる 2 回の ping 試行を指定する方法を示します（その後、ping 試行を停止します）。

```
Switch(config)# ipv6 dhcp ping packets 2
```

関連コマンド

コマンド	説明
clear ipv6 dhcp conflict	DHCPv6 サーバ データベースからアドレス競合をクリアします。
show ipv6 dhcp conflict	DHCPv6 サーバによって検出された、またはクライアントから DECLINE メッセージにより報告されたアドレス競合を表示します。

ipv6 dhcp pool

Dynamic Host Configuration Protocol for IPv6（DHCPv6）プール コンフィギュレーション モードを開始するには、**ipv6 dhcp pool** グローバル コンフィギュレーション 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 dhcp pool *poolname*

no ipv6 dhcp pool *poolname*

（注）　このコマンドは、スイッチ スタックでデュアル IPv4/IPv6 SDM テンプレートが設定されている場合に限り使用可能です。

構文の説明

poolname	DHCPv6 プールのユーザ定義名。プール名には象徴的な文字列（Engineering など）または整数（0 など）を使用できます。

デフォルト

デフォルト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

コマンド履歴

リリース	変更内容
12.2(46)SE	コマンドが導入され、**address prefix**、**lifetime**、**link-address**、および **vendor-specific** キーワードがコマンドのサブモードに追加されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

ipv6 dhcp pool コマンドは、DHCPv6 プール コンフィギュレーション モードをイネーブルにします。使用できるコンフィギュレーション コマンドは、次のとおりです。

- **address prefix** *IPv6-prefix* : アドレス割り当てのアドレス プレフィクスを設定します。このアドレスはコロンで区切られた 16 ビット値を使用した 16 進数形式である必要があります。
- **lifetime** *t1 t2* : IPv6 アドレスの*有効*間隔（秒）および*優先*間隔（秒）を設定します。指定できる範囲は 5 ～ 4294967295 秒です。有効なデフォルト値は 2 日です。優先されるデフォルト値は 1 日です。有効ライフタイムは優先ライフタイムと同じかそれより長い必要があります。間隔を指定しない場合は、**infinite** を指定します。
- **link-address** *IPv6-prefix* : リンク アドレス IPv6 プレフィクスを設定します。着信インターフェイスのアドレスまたはパケット内のリンク アドレスが指定した IPv6 プレフィクスと一致する場合、サーバは設定情報プールを使用します。このアドレスはコロンで区切られた 16 ビット値を使用した 16 進数形式である必要があります。

- **vendor-specific** : DHCPv6 ベンダー固有コンフィギュレーション モードをイネーブルにします。使用できるコンフィギュレーション コマンドは、次のとおりです。
  - *vendor-id* : ベンダー固有の ID 番号を指定します。この番号は、ベンダーの IANA プライベート エンタープライズ番号です。指定できる範囲は 1 ～ 4294967295 です。
  - **suboption** *number* : ベンダー固有のサブオプション番号を設定します。指定できる範囲は 1 ～ 65535 です。IPv6 アドレス、ASCII テキスト、または 16 進文字列をサブオプション パラメータで定義されているように入力します。

DHCPv6 設定情報プールを作成してから、**ipv6 dhcp server** インターフェイス コンフィギュレーション コマンドを使用してプールとインターフェイス上のサーバを関連付けます。ただし、情報プールを設定しない場合は、**ipv6 dhcp server** インターフェイス コンフィギュレーション コマンドを使用して DHCPv6 サーバ機能をインターフェイスでイネーブルにする必要があります。

DHCPv6 プールとインターフェイスを関連付けると、関連付けられているインターフェイス上の要求を処理するのはそのプールだけとなります。プールは、他のインターフェイスについても処理を行います。DHCPv6 プールとインターフェイスを関連付けない場合は、すべてのインターフェイスに対する要求を処理できます。

IPv6 アドレス プレフィクスを使用しないということは、プールは設定されているオプションだけを返すことを指します。

link-address キーワードを使用すると、必ずしもアドレスを割り当てなくてもリンク アドレスの照合を行うことができます。プール内の複数のリンク アドレス コンフィギュレーション コマンドを使用して、複数のリレーのプールを照合できます。

アドレス プール情報またはリンク情報のいずれかについて最長一致が行われるため、あるプールについてはアドレスを割り当てるように設定して、サブプレフィクスの別のプールについては設定されたオプションだけを返すように設定できます。

例

次の例では、engineering という IPv6 アドレス プレフィクスを持つプールを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool engineering
Switch(config-dhcpv6)# address prefix 2001:1000::0/64
Switch(config-dhcpv6)# end
```

次の例では、*testgroup* という 3 つのリンク アドレス プレフィクスおよび 1 つの IPv6 アドレス プレフィクスを持つプールを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool testgroup
Switch(config-dhcpv6)# link-address 2001:1001::0/64
Switch(config-dhcpv6)# link-address 2001:1002::0/64
Switch(config-dhcpv6)# link-address 2001:2000::0/48
Switch(config-dhcpv6)# address prefix 2001:1003::0/64
Switch(config-dhcpv6)# end
```

次の例では、350 というベンダー固有オプションを持つプールを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool 350
Switch(config-dhcpv6)# vendor-specific 9
Switch(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Switch(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Switch(config-dhcpv6-vs)# end
```

関連コマンド

コマンド	説明
ipv6 dhcp server	インターフェイスで DHCPv6 サービスをイネーブルにします。
show ipv6 dhcp pool	DHCPv6 設定プール情報を表示します。

ipv6 dhcp server

インターフェイスで Dynamic Host Configuration Protocol for IPv6（DHCPv6）サービスをイネーブルにするには、**ipv6 dhcp server** 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。インターフェイスで DHCPv6 サービス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 dhcp server [*poolname* | **automatic**] [**rapid-commit**] [**preference** *value*] [**allow-hint**]

no ipv6 dhcp server [*poolname* | **automatic**] [**rapid-commit**] [**preference** *value*] [**allow-hint**]

（注）　このコマンドは、スイッチ スタックでデュアル IPv4/IPv6 SDM テンプレートが設定されている場合に限り使用可能です。

構文の説明

poolname	（任意）IPv6 DHCP プールのユーザ定義名。プール名には象徴的な文字列（Engineering など）または整数（0 など）を使用できます。
automatic	（任意）サーバが、クライアントにアドレスを割り当てるときに使用するプールを自動的に決定できるようにします。
rapid-commit	（任意）2 つのメッセージ交換方式を許可します。
preference *value*	（任意）サーバにより送信されるアドバタイズ メッセージのプリファレンス オプションで伝送されるプリファレンス値。指定できる範囲は 0 ～ 255 です。デフォルトのプリファレンス値は 0 です。
allow-hint	（任意）サーバが SOLICIT メッセージ内のクライアント提案を考慮するかどうかを指定します。デフォルトでは、サーバはクライアントのヒントを無視します。

デフォルト

デフォルトでは、DHCPv6 パケットはインターフェイス上で処理されません。

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

コマンド履歴

リリース	変更内容
12.2(46)SE	コマンドが導入され、**automatic** キーワードが追加されました。

使用上のガイドライン

ipv6 dhcp server インターフェイス コンフィギュレーション コマンドは、指定されたインターフェイスで DHCPv6 サービスをイネーブルにします。

automatic キーワードは、クライアントにアドレスを割り当てるときに使用するプールを自動的に決定できるようにします。サーバが IPv6 DHCP パケットを受信すると、サーバはそのパケットを DHCP リレーから受信したか、クライアントから直接受信したかを判別します。リレーからパケットを受信した場合、サーバは、クライアントに最も近い最初のリレーと関連付けられているパケット内部のリンク アドレス フィールドを確認します。サーバは、このリンク アドレスと、すべてのアドレス プレフィクスおよび IPv6 DHCP プールのリンク アドレス設定とを照合して、最長のプレフィクス一致を探します。サーバは最長一致と関連付けられているプールを選択します。

パケットをクライアントから直接受信した場合、サーバは同じ照合を行いますが、照合を行うときに着信インターフェイスに設定されているすべての IPv6 アドレスを使用します。そして再度、サーバは最長のプレフィクス照合を選択します。

rapid-commit キーワードは、2 つのメッセージ交換を使用できるようにします。

preference キーワードを 0 以外の値とともに設定すると、サーバはプリファレンス オプションを追加して、アドバタイズ メッセージのプリファレンス値を伝送します。この動作は、クライアントによるサーバの選択に影響を与えます。プリファレンス オプションを含まないアドバタイズ メッセージのプリファレンス値は 0 であると見なされます。クライアントが、プリファレンス値が 255 であるアドバタイズ メッセージを受信する場合、クライアントはメッセージの送信元であるサーバに要求メッセージを即時に送信します。

allow-hint キーワードを指定する場合、サーバは送信請求メッセージおよび要求メッセージの有効なクライアント提案アドレスを割り当てます。プレフィクス アドレスは、関連付けられているローカル プレフィクス アドレス プール内にあり、デバイスに割り当てられていない場合は有効です。**allow-hint** キーワードを指定しない場合、サーバはクライアント ヒントを無視して、プール内のフリー リストにあるアドレスが割り当てられます。

DHCPv6 クライアント、サーバ、およびリレー機能は、インターフェイス上で相互に排他的です。これらの機能の 1 つがすでにイネーブルになっているときに同じインターフェイスで別の機能を設定しようとすると、スイッチは次のメッセージのいずれかを返します。

```
Interface is in DHCP client mode
Interface is in DHCP server mode
Interface is in DHCP relay mode
```

例

次の例では、*testgroup* というプールの DHCPv6 をイネーブルにします。

```
Switch(config-if)# ipv6 dhcp server testgroup
```

関連コマンド

コマンド	説明
ipv6 dhcp pool	DHCPv6 プールを設定して、DHCPv6 プール コンフィギュレーション モードを開始します。
show ipv6 dhcp interface	DHCPv6 インターフェイス情報を表示します。

ipv6 mld snooping

IP version 6（IPv6）Multicast Listener Discovery（MLD）スヌーピングをグローバルまたは指定の VLAN 上でイネーブルにするには、**ipv6 mld snooping** グローバル コンフィギュレーション コマンドをキーワードなしで使用します。MLD スヌーピングを、スイッチ、スイッチ スタック、または VLAN 上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。

ipv6 mld snooping [**vlan** *vlan-id*]

no ipv6 mld snooping [**vlan** *vlan-id*]

（注）　このコマンドは、スイッチでデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートが設定されている場合に限り使用可能です。

構文の説明

vlan *vlan-id*	（任意）指定の VLAN で IPv6 MLD スヌーピングをイネーブルまたはディセーブルにします。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。

デフォルト

スイッチ上で、MLD スヌーピングはグローバルにディセーブルです。

すべての VLAN で MLD スヌーピングはイネーブルです。ただし、VLAN スヌーピングが実行される前に、MLD 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。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

MLD スヌーピングがグローバルにディセーブルである場合、すべての既存の VLAN インターフェイスで MLD スヌーピングがディセーブルになります。MLD スヌーピングをグローバルにイネーブルにすると、デフォルトの状態（イネーブル）であるすべての VLAN インターフェイス上で MLD スヌーピングがイネーブルになります。VLAN 設定は、MLD スヌーピングがディセーブルのインターフェイス上のグローバル コンフィギュレーションを上書きします。

MLD スヌーピングがグローバルにディセーブルである場合、VLAN 上で MLD スヌーピングをイネーブルにできません。MLD スヌーピングがグローバルにイネーブルである場合、個々の VLAN 上で MLD スヌーピングをディセーブルにできます。

IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ～ 4094）を使用する場合、スイッチが VLAN 上でクエリーを受信できるようにするため、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの拡張 VLAN でイネーブルにする必要があります。標準範囲 VLAN（1 ～ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。

1002 ～ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

例

次の例では、MLD スヌーピングをグローバルにイネーブルにする方法を示します。

```
Switch(config)# ipv6 mld snooping
```

次の例では、MLD スヌーピングを VLAN でディセーブルにする方法を示します。

```
Switch(config)# no ipv6 mld snooping vlan 11
```

設定を確認するには、**show ipv6 mld snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。
show ipv6 mld snooping	MLD スヌーピング設定を表示します。

ipv6 mld snooping last-listener-query-count

クライアントがエージング アウトになる前に送信される IP version 6（IPv6）Multicast Listener Discovery（MLD）Multicast Address Specific Queries（MASQ）を設定するには、**ipv6 mld snooping last-listener-query-count** グローバル コンフィギュレーション コマンドを使用します。クエリー カウントをデフォルト設定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。

ipv6 mld snooping [**vlan** *vlan-id*] **last-listener-query-count** *integer_value*

no ipv6 mld snooping [**vlan** *vlan-id*] **last-listener-query-count**

（注）このコマンドは、スイッチでデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートが設定されている場合に限り使用可能です。

構文の説明

vlan *vlan-id*	（任意）指定の VLAN で last-listener クエリー カウントを設定します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
integer_value	指定できる範囲は 1 ～ 7 です。

コマンド デフォルト

デフォルトのグローバル カウントは 2 です。

デフォルトの VLAN カウントは 0 です（グローバル カウントを使用します）。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

MLD スヌーピングでは、IPv6 マルチキャスト ルータはマルチキャスト グループに所属するホストにクエリーを定期的に送信します。ホストがマルチキャスト グループを脱退する場合、ホストは静かに脱退する、または Multicast Listener Done メッセージでクエリーに応答できます（IGMP Leave メッセージに相当）。即時脱退が設定されていない場合（1 つのグループに対し複数のクライアントが同じポート上に存在する場合は設定しない）、設定された last-listener クエリー カウントにより、MLD クライアントが期限切れになる前に送信する MASQ の数が決定します。

last-listener クエリー カウントが VLAN 用に設定されている場合、このカウントはグローバルに設定された値より優先されます。VLAN カウントが設定されていない（デフォルトの 0 に設定されている）場合は、グローバル カウントが使用されます。

1002 ～ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

例

次の例では、last-listener クエリー カウントをグローバルに設定する方法を示します。

```
Switch(config)# ipv6 mld snooping last-listener-query-count 1
```

次の例では、last-listener クエリー カウントを VLAN 10 に設定する方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 10 last-listener-query-count 3
```

設定を確認するには、**show ipv6 mld snooping** [**vlan** *vlan-id*] ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping last-listener-query-interval	IPv6 MLD スヌーピング last-listener クエリー間隔を設定します。
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。
show ipv6 mld snooping querier	MLD スヌーピング設定を表示します。

ipv6 mld snooping last-listener-query-interval

スイッチまたは VLAN で IP version 6（IPv6）Multicast Listener Discovery（MLD）スヌーピングの last-listener クエリー間隔を設定するには、**ipv6 mld snooping last-listener-query-interval** グローバル コンフィギュレーション コマンドを使用します。この時間間隔は、Multicast Address Specific Query（MASQ）マルチキャスト グループからポートを削除する前にマルチキャスト ルータが待機する最大時間です。クエリー時間をデフォルト設定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。

ipv6 mld snooping [**vlan** *vlan-id*] **last-listener-query-interval** *integer_value*

no ipv6 mld snooping [**vlan** *vlan-id*] **last-listener-query-interval**

（注）　このコマンドは、スイッチでデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートが設定されている場合に限り使用可能です。

構文の説明

vlan *vlan-id*	（任意）指定の VLAN で last-listener クエリー時間を設定します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
integer_value	MASQ を送信した後マルチキャスト グループからポートを削除する前にマルチキャスト ルータが待機する時間（1000 秒単位）を設定します。指定できる範囲は 100 ～ 32,768 です。デフォルト値は 1000（1 秒）です。

コマンド デフォルト

デフォルトのグローバル クエリー間隔（最大応答時間）は 1000（1 秒）です。

デフォルトの VLAN クエリー間隔（最大応答時間）は 0 です（グローバル カウントが使用されます）。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

MLD スヌーピングでは、IPv6 マルチキャスト ルータが MLD Leave メッセージを受信すると、マルチキャスト グループに所属するホストにクエリーを送信します。一定の時間、ポートから MASQ への応答がない場合、ルータはマルチキャスト アドレスのメンバシップ データベースからそのポートを削除します。last listener クエリー間隔は、応答のないポートをマルチキャスト グループから削除する前にルータが待機する最大時間です。

VLAN クエリー間隔が設定されていると、グローバル クエリー間隔より優先されます。VLAN 間隔が 0 に設定されていると、グローバル値が使用されます。

1002 ～ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

例

次の例では、last-listener クエリー間隔を 2 秒にグローバルに設定する方法を示します。

```
Switch(config)# ipv6 mld snooping last-listener-query-interval 2000
```

次の例では、VLAN 1 用の last-listener クエリー間隔を 5.5 秒に設定する方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 1 last-listener-query-interval 5500
```

設定を確認するには、**show ipv6 MLD snooping** [**vlan** *vlan-id*] ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping last-listener-query-count	IPv6 MLD スヌーピング last-listener クエリー カウントを設定します。
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。
show ipv6 mld snooping querier	IPv6 MLD スヌーピング last-listener クエリー間隔を設定します。

ipv6 mld snooping listener-message-suppression

IP version 6（IPv6）Multicast Listener Discovery（MLD）スヌーピング リスナー メッセージ抑制をイネーブルにするには、**ipv6 mld snooping listener-message-suppression** グローバル コンフィギュレーション コマンドを使用します。MLD スヌーピング リスナー メッセージ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 listener-message-suppression

no ipv6 mld snooping listener-message-suppression

（注）　このコマンドは、スイッチでデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートが設定されている場合に限り使用可能です。

コマンド デフォルト

デフォルトでは、MLD スヌーピング リスナー メッセージ抑制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

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

MLD スヌーピング リスナー メッセージ抑制は、IGMP レポート抑制に相当します。イネーブルの場合、グループに対する受信 MLDv1 レポートはレポート転送時間ごとに 1 回だけ IPv6 マルチキャスト ルータに転送されます。これにより、重複レポートの転送を避けられます。

例

次の例では、MLD スヌーピング リスナー メッセージ抑制をイネーブルにする方法を示します。

```
Switch(config)# ipv6 mld snooping listener-message-suppression
```

次の例では、MLD スヌーピング リスナー メッセージ抑制をディセーブルにする方法を示します。

```
Switch(config)# no ipv6 mld snooping listener-message-suppression
```

設定を確認するには、**show ipv6 mld snooping** [**vlan** *vlan-id*] ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping	IPv6 MLD スヌーピングをイネーブルにします。
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。
show ipv6 mld snooping	MLD スヌーピング設定を表示します。

ipv6 mld snooping robustness-variable

応答のないリスナーを削除するまでにスイッチが送信する IP version 6（IPv6）Multicast Listener Discovery（MLD）クエリーの数を設定するには、**ipv6 mld snooping robustness-variable** グローバル コンフィギュレーション コマンドを使用します。VLAN ごとに設定するには、VLAN ID を入力します。変数をデフォルト設定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。

ipv6 mld snooping [**vlan** *vlan-id*] **robustness-variable** *integer_value*

no ipv6 mld snooping [**vlan** *vlan-id*] **robustness-variable**

（注）　このコマンドは、スイッチでデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートが設定されている場合に限り使用可能です。

構文の説明

vlan *vlan-id*	（任意）指定の VLAN にロバストネス変数を設定します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
integer_value	指定できる範囲は 1 ～ 3 です。

コマンド デフォルト

デフォルトのグローバル ロバストネス変数（リスナーを削除する前のクエリー数）は、2 です。

デフォルトの VLAN ロバストネス変数（マルチキャスト アドレスが期限切れになる前のクエリー数）は 0 です。リスナーの期限の判断には、グローバル ロバストネス変数が使用されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

ロバストネスは、ポートをマルチキャスト グループから削除する前に送信された応答がなかった MLDv1 クエリー数の点から測定されます。設定された回数送信された MLDv1 クエリーに対して受信した MLDv1 レポートがない場合、ポートが削除されます。グローバル値により、スイッチが応答しないリスナーを削除する前に待機するクエリー数が決定し、VLAN 値が設定されていない VLAN すべてに適用します。

VLAN に設定されたロバストネス値はグローバル値より優先されます。VLAN ロバストネス値が 0（デフォルト）の場合、グローバル値が使用されます。

1002 ～ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

例

次の例では、スイッチが応答しないリスナー ポートを削除する前に 3 個のクエリーを送信するようグローバル ロバストネス変数を設定する方法を示します。

```
Switch(config)# ipv6 mld snooping robustness-variable 3
```

次の例では、VLAN 1 にロバストネス変数を設定する方法を示します。この値は VLAN のグローバルコンフィギュレーションより優先されます。

```
Switch(config)# ipv6 mld snooping vlan 1 robustness-variable 1
```

設定を確認するには、**show ipv6 MLD snooping** [**vlan** *vlan-id*] ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping last-listener-query-count	IPv6 MLD スヌーピング last-listener クエリー カウントを設定します。
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。
show ipv6 mld snooping	MLD スヌーピング設定を表示します。

ipv6 mld snooping tcn

IP version 6（IPv6）Multicast Listener Discovery（MLD）Topology Change Notification（TCN）を設定するには、**ipv6 mld snooping tcn** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定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。

ipv6 mld snooping tcn {**flood query count** *integer_value* | **query solicit**}

no ipv6 mld snooping tcn {**flood query count** *integer_value* | **query solicit**}

（注）このコマンドは、スイッチでデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートが設定されている場合に限り使用可能です。

構文の説明

flood query count *integer_value*	フラッディング クエリー カウントを設定します。これは、クエリーの受信を要求したポートだけにマルチキャスト データを転送する前に送信されるクエリー数です。指定できる範囲は 1 ～ 10 です。
query solicit	TCN クエリーの送信請求をイネーブルにします。

コマンド デフォルト

TCN クエリー送信請求はディセーブルです。

イネーブルの場合、デフォルトのフラッディング クエリー カウントは 2 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

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

例

次の例では、TCN クエリー送信請求をイネーブルにする方法を示します。

```
Switch(config)# ipv6 mld snooping tcn query solicit.
```

次の例では、フラッディング クエリー カウントを 5 に設定する方法を示します。

```
Switch(config)# ipv6 mld snooping tcn flood query count 5.
```

設定を確認するには、**show ipv6 MLD snooping** [**vlan** *vlan-id*] ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。
show ipv6 mld snooping	MLD スヌーピング設定を表示します。

ipv6 mld snooping vlan

VLAN インターフェイスで IP version 6（IPv6）Multicast Listener Discovery（MLD）スヌーピング パラメータを設定するには、**ipv6 mld snooping vlan** グローバル コンフィギュレーション コマンドを使用します。パラメータをデフォルト設定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。

ipv6 mld snooping vlan *vlan-id* [**immediate-leave** | **mrouter interface** *interface-id* | **static** *ipv6-multicast-address* **interface** *interface-id*]

no ipv6 mld snooping vlan *vlan-id* [**immediate-leave** | **mrouter interface** *interface-id* | **static** *ip-address* **interface** *interface-id*]

（注）　このコマンドは、スイッチでデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートが設定されている場合に限り使用可能です。

構文の説明

vlan *vlan-id*	VLAN 番号を指定します。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。
immediate-leave	（任意）VLAN インターフェイス上で、MLD の即時脱退処理をイネーブルにします。この機能をインターフェイス上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。
mrouter interface	（任意）マルチキャスト ルータ ポートを設定します。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。
static *ipv6-multicast-address*	（任意）指定の IPv6 マルチキャスト アドレスでマルチキャスト グループを設定します。
interface *interface-id*	レイヤ 2 ポートをグループに追加します。マルチキャスト ルータまたはスタティック インターフェイスは、物理ポートまたはインターフェイス範囲 1 ～ 48 の**ポートチャネル** インターフェイスになることができます。

コマンド デフォルト

MLD スヌーピング即時脱退処理はディセーブルです。

デフォルトでは、スタティック IPv6 マルチキャスト グループは設定されていません。

デフォルトでは、マルチキャスト ルータ ポートはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

VLAN の各ポート上に 1 つのレシーバだけが存在する場合、即時脱退処理の機能だけを設定してください。設定は、NVRAM（不揮発性 RAM）に保存されます。

static キーワードは MLD メンバ ポートを静的に設定するために使用されます。

設定およびスタティック ポートとグループは、NVRAM に保存されます。

IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ～ 4094）を使用する場合、Catalyst 3750 または Catalyst 3560 スイッチが VLAN 上でクエリーを受信できるようにするため、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの拡張 VLAN でイネーブルにする必要があります。標準範囲 VLAN（1 ～ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。

1002 ～ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

例

次の例では、VLAN 1 で MLD 即時脱退処理をイネーブルにする方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 1 immediate-leave
```

次の例では、VLAN 1 で MLD 即時脱退処理をディセーブルにする方法を示します。

```
Switch(config)# no ipv6 mld snooping vlan 1 immediate-leave
```

次の例では、ポートをマルチキャスト ルータ ポートとして設定する方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 1 mrouter interface gigabitethernet1/01/2
```

次の例では、スタティック マルチキャスト グループを設定する方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 2 static FF12::34 interface gigabitethernet1/01/2
```

設定を確認するには、**show ipv6 mld snooping vlan** *vlan-id* ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping	IPv6 MLD スヌーピングをイネーブルにします。
ipv6 mld snooping vlan	VLAN で IPv6 MLD スヌーピングを設定します。
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。
show ipv6 mld snooping	IPv6 MLD スヌーピング設定を表示します。

ipv6 traffic-filter

インターフェイス上で IPv6 トラフィックをフィルタリングするには、**ipv6 traffic-filter** 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。フィルタリングできるトラフィックのタイプと方向は、スイッチ スタックで稼動するイメージによって異なります。インターフェイスでの IPv6 トラフィックのフィル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。

ipv6 traffic-filter *access-list-name* {**in** | **out**}

no ipv6 traffic-filter *access-list-name* {**in** | **out**}

（注）　このコマンドは、スイッチ スタックでデュアル IPv4/IPv6 SDM テンプレートが設定されている場合に限り使用可能です。

構文の説明

access-list-name	IPv6 アクセス名を指定します。
in	着信 IPv6 トラフィックを指定します。
out	発信 IPv6 トラフィックを指定します。 （注）　**out** キーワードはレイヤ 2 インターフェイス（ポート ACL）ではサポートされません。

デフォルト

インターフェイス上での IPv6 トラフィックのフィルタリングは設定されません。

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

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。
12.2(35)SE	IP サービスおよび IP ベース イメージの着信レイヤ 3 管理トラフィック（ルータ ACL）のサポートが追加されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

物理インターフェイス（レイヤ 2 またはレイヤ 3 ポート）、レイヤ 3 ポート チャネル、または Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）で **ipv6 traffic-filter** コマンドを使用できます。

ACL をレイヤ 3 インターフェイス（ポート ACL）の発信または着信トラフィックに、あるいはレイヤ 2 インターフェイス（ルータ ACL）の着信トラフィックに適用できます。

*いずれか*のポート ACL（IPv4、IPv6、または MAC）がインターフェイスに適用された場合、そのポート ACL を使用してパケットをフィルタリングし、ポート VLAN の SVI に適用されたルータ ACL は無視されます。

例

次の例では、*cisco* という名のアクセス リストの定義に従って、IPv6 設定のインターフェイスで着信 IPv6 トラフィックをフィルタリングする方法を示します。

```
Switch (config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter cisco in
```

関連コマンド

コマンド	説明
ipv6 access-list	IPv6 アクセス リストを定義し、定義されたアクセス リストに拒否または許可条件を設定します。
show ipv6 access-list	現在のすべての IPv6 アクセス リストの内容を表示します。
show ipv6 interface	IPv6 用に設定され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。

l2protocol-tunnel

アクセス ポート、IEEE 802.1Q トンネル ポート、またはポート チャネルでレイヤ 2 プロトコルのトンネリングをイネーブルにするには、**l2protocol-tunnel** 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。Cisco Discovery Protocol（CDP）、Spanning Tree Protocol（STP; スパニング ツリー プロトコル）、または VLAN Trunking Protocol（VTP）パケットのトンネリングをイネーブルにできます。また、Port Aggregation Protocol（PAgP）、Link Aggregation Control Protocol（LACP）、または UniDirectional Link Detection（UDLD; 単一方向リンク検出）パケットのポイントツーポイント トンネリングをイネーブルにできます。インターフェイスでトンネリングをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

l2protocol-tunnel [**cdp** | **stp** | **vtp**] [**point-to-point** [**pagp** | **lacp** | **udld**]] | [**shutdown-threshold** [**cdp** | **stp** | **vtp**] [**point-to-point** [**pagp** | **lacp** | **udld**]]] *value*] | [**drop-threshold** [**cdp** | **stp** | **vtp**] [**point-to-point** [**pagp** | **lacp** | **udld**]] *value*]

no l2protocol-tunnel [**cdp** | **stp** | **vtp**] [**point-to-point** [**pagp** | **lacp** | **udld**]] | [**shutdown-threshold** [**cdp** | **stp** | **vtp**] [**point-to-point** [**pagp** | **lacp** | **udld**]]] | [**drop-threshold** [**cdp** | **stp** | **vtp**] [**point-to-point** [**pagp** | **lacp** | **udld**]]]

構文の説明

l2protocol-tunnel	CDP、STP、および VTP パケットのポイントツーマルチポイント トンネリングをイネーブルにします。
cdp	（任意）CDP のトンネリングをイネーブルにします。または、CDP のシャットダウンしきい値またはドロップしきい値を指定します。
stp	（任意）STP のトンネリングをイネーブルにします。または、STP のシャットダウンしきい値またはドロップしきい値を指定します。
vtp	（任意）VTP のトンネリングをイネーブルにします。または、VTP のシャットダウンしきい値またはドロップしきい値を指定します。
point-to-point	（任意）PAgP、LACP、および UDLD パケットのポイントツーポイント トンネリングをイネーブルにします。
pagp	（任意）PAgP のポイントツーポイント トンネリングをイネーブルにします。または、PAgP のシャットダウンしきい値またはドロップしきい値を指定します。
lacp	（任意）LACP のポイントツーポイント トンネリングをイネーブルにします。または、LACP のシャットダウンしきい値またはドロップしきい値を指定します。
udld	（任意）UDLD のポイントツーポイント トンネリングをイネーブルにします。または、UDLD のシャットダウンしきい値またはドロップしきい値を指定します。
shutdown-threshold	（任意）インターフェイスがシャットダウンするまでに受信されるシャットダウンしきい値をレイヤ 2 プロトコル pps（パケット/秒）の最大レートで設定します。

drop-threshold	（任意）インターフェイスがパケットをドロップするまでに受信されるドロップしきい値をレイヤ 2 プロトコル pps（パケット / 秒）の最大レートで設定します。
value	インターフェイスがシャットダウンするまでにカプセル化に対して受信されるしきい値を pps（パケット / 秒）で指定します。または、インターフェイスがパケットをドロップするまでのしきい値を指定します。指定できる範囲は 1 ～ 4096 です。デフォルトでは、しきい値は設定されていません。

デフォルト

デフォルトでは、レイヤ 2 プロトコルのトンネリングは設定されていません。

デフォルトでは、レイヤ 2 プロトコル パケット数のシャットダウンしきい値は設定されていません。

デフォルトでは、レイヤ 2 プロトコル パケット数のドロップしきい値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

コマンド履歴

リリース	変更内容
12.2(25)SE	このコマンドが追加されました。

使用上のガイドライン

レイヤ 2 パケットをトンネリングするには、このコマンドを入力する必要があります（必要な場合は、プロトコル タイプを指定）。

このコマンドをポート チャネルで入力する場合、チャネル内のすべてのポートが同じ設定になる必要があります。

サービス プロバイダー ネットワーク内のレイヤ 2 プロトコル トンネリングは、レイヤ 2 の情報が確実にネットワーク内のすべてのカスタマー ロケーションに伝播するようにします。プロトコル トンネリングがイネーブルになると、ネットワーク内の伝送用に、プロトコル パケットがシスコの既知のマルチキャスト アドレスでカプセル化されます。パケットが宛先に到着すると、既知の MAC アドレスがレイヤ 2 プロトコル MAC アドレスに置き換えられます。

CDP、STP、および VTP のレイヤ 2 プロトコル トンネリングは、個別にまたは 3 つすべてのプロトコルに対してイネーブルにできます。

サービス プロバイダー ネットワークでは、ポイントツーポイント ネットワーク トポロジをエミュレートして EtherChannel の作成を強化するのに、レイヤ 2 プロトコル トンネルを使用できます。PAgP または LACP のプロトコル トンネリングがサービス プロバイダーのスイッチでイネーブルにされている場合、リモート カスタマー スイッチは、Protocol Data Unit（PDU; プロトコル データ ユニット）を受信し、EtherChannel の自動作成をネゴシエートできます。

PAgP、LACP、および UDLD パケットのトンネリングをイネーブルにするには、ポイントツーポイント ネットワーク トポロジが必要になります。リンクダウン検出時間を減らすには、PAgP または LACP パケットのトンネリングをイネーブルにするときにインターフェイスで UDLD もイネーブルにする必要があります。

PAgP、LACP、および UDLD のポイントツーポイント プロトコル トンネリングは、個別にまたは 3 つすべてのプロトコルに対してイネーブルにできます。

注意　PAgP、LACP、および UDLD トンネリングは、ポイントツーポイント トポロジをエミュレートすることだけを目的としています。設定を間違えたことによりトンネリング パケットが多くのポートに送信されると、ネットワーク障害が発生する可能性があります。

shutdown-threshold キーワードを入力して、シャットダウンするまでにインターフェイスで受信されるプロトコルの pps（パケット / 秒）数を制御します。このキーワードにプロトコル オプションが指定されていない場合は、しきい値が各トンネリング レイヤ 2 プロトコル タイプに適用されます。インターフェイスにドロップしきい値も設定する場合は、シャットダウンしきい値がドロップしきい値以上でなければなりません。

シャットダウンしきい値に到達すると、インターフェイスが errdisable になります。**errdisable recovery cause l2ptguard** グローバル コンフィギュレーション コマンドを入力し、エラー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開します。**l2ptguard** でエラー回復メカニズムをイネーブルにしない場合、インターフェイスは、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドが入力されるまで errdisable ステートのままになります。

drop-threshold キーワードを入力して、インターフェイスがパケットをドロップするまでにインターフェイスで受信されるプロトコルの pps（パケット / 秒）数を制御します。このキーワードにプロトコル オプションが指定されていない場合は、しきい値が各トンネリング レイヤ 2 プロトコル タイプに適用されます。インターフェイスにシャットダウンしきい値も設定する場合は、ドロップしきい値がシャットダウンしきい値以下でなければなりません。

ドロップしきい値に到達すると、受信されるレートがドロップしきい値を下回るまでインターフェイスがレイヤ 2 プロトコル パケットをドロップします。

設定は、NVRAM（不揮発性 RAM）に保存されます。

レイヤ 2 プロトコル トンネリングに関する詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、CDP パケットのプロトコル トンネリングをイネーブルにし、シャットダウンしきい値を 50 pps に設定する方法を示します。

```
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)# l2protocol-tunnel shutdown-threshold cdp 50
```

次の例では、STP パケットのプロトコル トンネリングをイネーブルにし、ドロップしきい値を 400 pps に設定する方法を示します。

```
Switch(config-if)# l2protocol-tunnel stp
Switch(config-if)# l2protocol-tunnel drop-threshold stp 400
```

次の例では、PAgP および UDLD パケットのポイントツーポイント プロトコル トンネリングをイネーブルにし、PAgP ドロップしきい値を 1000 pps に設定する方法を示します。

```
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
```

関連コマンド

コマンド	説明
l2protocol-tunnel cos	すべてのトンネリング レイヤ 2 プロトコル パケットに対して Class of Service（CoS）値を設定します。
show errdisable recovery	errdisable 回復タイマーの情報を表示します。
show l2protocol-tunnel	レイヤ 2 プロトコル トンネリングが設定されたポートに関する情報（ポート、プロトコル、CoS、およびしきい値を含む）を表示します。

l2protocol-tunnel cos

トンネリングされたレイヤ 2 プロトコル パケットすべてに、Class of Service（CoS）値を設定するには、**l2protocol-tunnel cos** グローバル コンフィギュレーション 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 *value*

no l2protocol-tunnel cos

構文の説明

value	トンネリング レイヤ 2 プロトコル パケットの CoS プライオリティ値を指定します。CoS 値がインターフェイスのデータ パケットに対して設定されている場合、デフォルトでこの CoS 値が使用されます。インターフェイスに CoS 値が設定されていない場合は、デフォルトは 5 です。指定できる範囲は 0 ～ 7 です。7 が最も高いプライオリティです。

デフォルト

デフォルトでは、インターフェイス上のデータに対して設定された CoS 値が使用されます。CoS 値が設定されていない場合は、すべてのトンネリング レイヤ 2 プロトコル パケットのデフォルトは 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

コマンド履歴

リリース	変更内容
12.2(25)SE	このコマンドが追加されました。

使用上のガイドライン

イネーブルの場合、トンネリング レイヤ 2 プロトコル パケットがこの CoS 値を使用します。

NVRAM（不揮発性 RAM）に値が保存されます。

例

次の例では、レイヤ 2 プロトコル トンネルの CoS 値を 7 に設定する方法を示します。

```
Switch(config)# l2protocol-tunnel cos 7
```

関連コマンド

コマンド	説明
show l2protocol-tunnel	レイヤ 2 プロトコル トンネリングが設定されたポートに関する情報（CoS を含む）を表示します。

lacp port-priority

Link Aggregation Control Protocol（LACP）のポート プライオリティを設定するには、**lacp port-priority** 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。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 port-priority *priority*

no lacp port-priority

構文の説明

priority	LACP のポート プライオリティ。指定できる範囲は 1 ～ 65535 です。

デフォルト

デフォルト値は 32768 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

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

lacp port-priority インターフェイス コンフィギュレーション コマンドは、LACP チャネル グループに 9 つ以上のポートがある場合、バンドルされるポートと、ホット スタンバイ モードに置かれるポートを判別します。

LACP チャネル グループは、同じタイプのイーサネット ポートを 16 個まで保有できます。最大 8 個をアクティブに、最大 8 個をスタンバイ モードにできます。

ポート プライオリティの比較では、数値が*小さい*ほどプライオリティが*高く*なります。LACP チャネル グループに 9 つ以上のポートがある場合、LACP ポート プライオリティの数値が小さい（つまり、高いプライオリティ値の）9 つのポートがチャネル グループにバンドルされ、それより低いプライオリティのポートはホットスタンバイ モードに置かれます。LACP ポート プライオリティが同じポートが 2 つ以上ある場合（たとえば、そのいずれもデフォルト設定の 65535 に設定されている場合）、ポート番号の内部値によりプライオリティが決定します。

（注）　LACP リンクを制御するスイッチ上にポートがある場合に限り、LACP ポート プライオリティは有効です。リンクを制御するスイッチの判別については、**lacp system-priority** グローバル コンフィギュレーション コマンドを参照してください。

LACP ポート プライオリティおよび内部ポート番号値を表示するには、**show lacp internal** 特権 EXEC コマンドを使用します。

物理ポート上の LACP の設定に関する情報については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring EtherChannels」の章を参照してください。

例

次の例では、ポートで LACP ポート プライオリティを設定する方法を示します。

```
Switch(config)# interface gigabitethernet2/01
Switch(config-if)# lacp port-priority 1000
```

設定を確認するには、**show lacp** [*channel-group-number*] **internal** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
channel-group	EtherChannel グループにイーサネット ポートを割り当てます。
lacp system-priority	LACP システム プライオリティを設定します。
show lacp [*channel-group-number*] **internal**	すべてのチャネル グループまたは指定のチャネル グループの内部情報を表示します。

lacp system-priority

Link Aggregation Control Protocol（LACP）のシステム プライオリティを設定するには、**lacp system-priority** グローバル コンフィギュレーション 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 system-priority *priority*

no lacp system-priority

構文の説明

priority	LACP のシステム プライオリティ。指定できる範囲は 1 ～ 65535 です。

デフォルト

デフォルト値は 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

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

lacp system-priority コマンドでは、ポート プライオリティを制御する LACP リンクのスイッチが判別されます。

LACP チャネル グループは、同じタイプのイーサネット ポートを 16 個まで保有できます。最大 8 個をアクティブに、最大 8 個をスタンバイ モードにできます。LACP チャネルグループに 9 つ以上のポートがある場合、リンクの制御側終端にあるスイッチは、ポート プライオリティを使用して、チャネルにバンドルするポートおよびホットスタンバイ モードに置くポートを判別します。他のスイッチ上のポート プライオリティ（リンクの非制御側終端）は無視されます。

プライオリティの比較においては、数値が小さいほどプライオリティが高くなります。したがって、LACP システム プライオリティの数値が小さい（プライオリティ値の高い）システムが制御システムとなります。どちらのスイッチも同じ LACP システム プライオリティである場合（たとえば、どちらもデフォルト設定の 32768 が設定されている場合）、LACP システム ID（スイッチの MAC アドレス）により制御するスイッチが判別されます。

lacp system-priority コマンドは、スイッチ上のすべての LACP EtherChannel に適用されます。

ホットスタンバイ モード（ポート ステート フラグの H で出力に表示）にあるポートを判断するには、**show etherchannel summary** 特権 EXEC コマンドを使用します。

物理ポート上の LACP の設定の詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring EtherChannels」の章を参照してください。

例

次の例では、LACP のシステム プライオリティを設定する方法を示します。

```
Switch(config)# lacp system-priority 20000
```

設定を確認するには、**show lacp sys-id** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
channel-group	EtherChannel グループにイーサネット ポートを割り当てます。
lacp port-priority	LACP ポート プライオリティを設定します。
show lacp sys-id	LACP によって使用されるシステム識別子を表示します。

link state group

リンクステート グループのメンバとしてポートを設定するには、**link state group** 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。リンクステート グループからポートを削除するには、このコマンドの **no** 形式を使用します。

link state group [*number*] {**upstream** | **downstream**}

no link state group [*number*] {**upstream** | **downstream**}

構文の説明

number	（任意）リンクステート グループ番号を指定します。グループ番号は、1 ～ 10 です。デフォルトは 1 です。
upstream	ポートを特定のリンクステート グループのアップストリーム ポートとして設定します。
downstream	ポートを特定のリンクステート グループのダウンストリーム ポートとして設定します。

デフォルト

デフォルトのグループは group 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

コマンド履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

指定されたリンク ステート グループのアップストリームまたはダウンストリーム インターフェイスとしてポートを設定するには、**link state group** 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。グループ番号が省略されている場合、デフォルトのグループ番号は 1 です。

リンクステート トラッキングをイネーブルにするには、*link-state group* を作成し、リンクステート グループに割り当てるインターフェイスを指定します。ポートの集合（EtherChannel）、アクセス モードまたはトランク モードの単一の物理ポート、またはルーテッド ポートをインターフェイスに指定できます。リンクステート グループでは、これらのインターフェイスはまとめてバンドルされます。*ダウンストリーム インターフェイス*は、*アップストリーム インターフェイス*にバインドされます。サーバに接続されたインターフェイスはダウンストリーム インターフェイスと呼ばれ、ディストリビューション スイッチおよびネットワーク装置に接続されたインターフェイスはアップストリーム インターフェイスと呼ばれます。

ダウンストリーム インターフェイスとアップストリーム インターフェイス間の連動の詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring EtherChannels and Link-State Tracking」の章を参照してください。

設定上の問題を回避するために、次の注意事項に従ってください。

- アップストリーム インターフェイスとして定義されているインターフェイスを、同じまたは異なるリンクステート グループ内でダウンストリーム インターフェイスとして定義することはできません。その逆も同様です。

- インターフェイスは、複数のリンクステート グループのメンバにはなれません。
- スイッチごとに設定できるのは、10 個のリンクステート グループだけです。

例

次の例では、group 2 でインターフェイスを **upstream** として設定する方法を示します。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/0/11 - 14
Switch(config-if-range)# link state group 2 downstream
Switch(config-if-range)# end
Switch(config-if)# end
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
link state track	リンクステート グループをイネーブルにします。
show link state group	リンクステート グループ情報を表示します。
show running-config	現在の動作設定を表示します。

link state track

リンクステート グループをイネーブルにするには、**link state track** ユーザ EXEC コマンドを使用します。リンクステート グルー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。

link state track [*number*]

no link state track [*number*]

構文の説明

number	（任意）リンクステート グループ番号を指定します。グループ番号は、1 ～ 10 です。デフォルト値は 1 です。

デフォルト

リンクステート トラッキングは、すべてのグループ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

コマンド履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

リンクステート グループをイネーブルにするには、**link state track** グローバルコンフィギュレーション コマンドを使用します。

例

次の例では、リンクステート グループの group 2 をイネーブルにする方法を示します。

```
Switch(config)# link state track 2
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
link state track	リンクステート グループのメンバとしてインターフェイスを設定します。
show link state group	リンクステート グループ情報を表示します。
show running-config	現在の動作設定を表示します。

location（グローバル コンフィギュレーション）

エンドポイントのロケーション情報を設定するには、**location** グローバル コンフィギュレーション コマンドを使用します。ロケーション情報を削除する場合は、このコマンドの **no** 形式を使用します。

location {**admin-tag** *string* | **civic-location identifier** *id* | **elin-location** *string* **identifier** *id*}

no location {**admin-tag** *string* | **civic-location identifier** *id* | **elin-location** *string* **identifier** *id*}

構文の説明

admin-tag	管理タグまたはサイト情報を設定します。
civic-location	都市ロケーション情報を設定します。
elin-location	緊急ロケーション情報（ELIN）を設定します。
identifier *id*	都市ロケーションまたは elin ロケーションの ID を指定します。指定できる ID 範囲は 1 ～ 4095 です。 （注）　LLDP-MED TLV での都市ロケーションの ID は 250 バイト以下に制限されます。スイッチ設定中に使用できるバッファ スペースに関するエラー メッセージを回避するには、各都市ロケーション ID に指定されたすべての都市ロケーション情報の全体の長さが 250 バイトを超えないようにします。
string	サイト情報またはロケーション情報を英数字形式で指定します。

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

コマンド履歴

リリース	変更内容
12.2(40)SE	このコマンドが追加されました。

使用上のガイドライン

location civic-location identifier id グローバル コンフィギュレーション コマンドを入力後、都市ロケーション コンフィギュレーション モードが開始されます。このモードでは、都市ロケーションおよび郵便ロケーション情報を入力することができます。

都市ロケーション ID は 250 バイトを超えてはなりません。

ロケーション TLV をディセーブルにするには、**no lldp med-tlv-select location** 情報インターフェイス コンフィギュレーション コマンドを使用します。デフォルトでは、ロケーション TLV はイネーブルに設定されています。詳細情報については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring LLDP and LLDP-MED」の章を参照してください。

例

次の例では、スイッチに都市ロケーション情報を設定する方法を示します。

```
Switch(config)# location civic-location identifier 1
Switch(config-civic)# number 3550
Switch(config-civic)# primary-road-name "Cisco Way"
Switch(config-civic)# city "San Jose"
Switch(config-civic)# state CA
Switch(config-civic)# building 19
Switch(config-civic)# room C6
Switch(config-civic)# county "Santa Clara"
Switch(config-civic)# country US
Switch(config-civic)# end
```

設定を確認するには、**show location civic-location** 特権 EXEC コマンドを入力します。
次の例では、スイッチ上で緊急ロケーション情報を設定する方法を示します。

```
Switch (config)# location elin-location 14085553881 identifier 1
```

設定を確認するには、**show location elin** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
location（インターフェイス コンフィギュレーション）	インターフェイスにロケーション情報を設定します。
show location	エンドポイントのロケーション情報を表示します。

location（インターフェイス コンフィギュレーション）

インターフェイスのロケーション情報を入力するには、**location** インターフェイス コマンドを使用します。インターフェイスのロケーション情報を削除するには、このコマンドの **no** 形式を使用します。

location {**additional-location-information** *word* | **civic-location-id** *id* | **elin-location-id** *id*}

no location {**additional-location-information** *word* | **civic-location-id** *id* | **elin-location-id** *id*}

構文の説明

additional-location-information	ロケーションまたは場所に関する追加情報を設定します。
word	追加のロケーション情報を指定する語またはフレーズを指定します。
civic-location-id	インターフェイスにグローバル都市ロケーション情報を設定します。
elin-location-id	インターフェイスに緊急ロケーション情報を設定します。
id	都市ロケーションまたは elin ロケーションの ID を指定します。指定できる ID 範囲は 1 ～ 4095 です。 **（注）** LLDP-MED TLV での都市ロケーションの ID は 250 バイト以下に制限されます。スイッチ設定中に使用できるバッファ スペースに関するエラー メッセージを回避するには、各都市ロケーション ID に指定されたすべての都市ロケーション情報の全体の長さが 250 バイトを超えないようにします。

デフォルト

このコマンドにはデフォルト設定はありません。

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

コマンド履歴

リリース	変更内容
12.2(40)SE	このコマンドが追加されました。

使用上のガイドライン

location civic-location-id id インターフェイス コンフィギュレーション コマンドを入力すると、都市ロケーション コンフィギュレーション モードに入ります。このモードでは、追加のロケーション情報を入力することができます。

都市ロケーション ID は 250 バイトを超えてはなりません。

例

次の例では、インターフェイスに都市ロケーション情報を入力する方法を示します。

```
Switch(config-if)# interface gigabitethernet1/0/1
Switch(config-if)# location civic-location-id 1
Switch(config-if)# end
```

設定を確認するには、**show location civic-location** 特権 EXEC コマンドを入力します。

次の例では、インターフェイスに緊急ロケーション情報を入力する方法を示します。

```
Switch(config-if)# interface gigabitethernet1/0/1
Switch(config-if)# location elin-location-id 1
Switch(config-if)# end
```

設定を確認するには、**show location elin interface** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
location（グローバル コンフィギュレーション）	エンドポイントにロケーション情報を設定します。
show location	エンドポイントのロケーション情報を表示します。

logging event

インターフェイス リンク ステータス変更の通知をイネーブルにするには、**logging event** 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。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。

logging event {**bundle-status** | **link-status** | **spanning-tree** | **status** | **trunk status**}

no logging event {**bundle-status** | **link-status** | **spanning-tree** | **status** | **trunk status**}

構文の説明

bundle-status	BUNDLE および UNBUNDLE メッセージの通知をイネーブルにします。
link-status	インターフェイス データ リンク ステータス変更の通知をイネーブルにします。
spanning-tree	スパニングツリー イベントの通知をイネーブルにします。
status	スパニングツリー ステート変更メッセージの通知をイネーブルにします。
trunk-status	トランクステータス メッセージの通知をイネーブルにします。

デフォルト

イベント ロギング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

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

例

次の例では、スパニングツリー ロギングをイネーブルにする方法を示します。

```
Switch(config-if)# logging event spanning-tree
```

logging event power-inline-status

Power over Ethernet（PoE）イベントのロギングをイネーブルにするには、**logging event power-inline-status** 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。PoE 状態イベントのロギングをディセーブルにする場合は、このコマンドの **no** 形式を使用しますが、このコマンドの **no** 形式を使用しても、PoE エラー イベントはディセーブルになりません。

logging event power-inline-status

no logging event power-inline-status

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

PoE イベントのロギ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

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。

使用上のガイドライン

logging event power-inline-status コマンドは、PoE インターフェイスでだけ使用できます。

例

次の例では、ポート上で PoE イベントのロギングをイネーブルにする方法を示します。

```
Switch(config-if)# interface gigabitethernet1/0/1
Switch(config-if)# logging event power-inline-status
Switch(config-if)#
```

関連コマンド

コマンド	説明
power inline	指定した PoE ポートまたはすべての PoE ポートの電力管理モードを設定します。
show controllers power inline	指定した PoE コントローラのレジスタ値を表示します。

logging file

ロギング ファイルのパラメータを設定するには、**logging file** グローバル コンフィギュレーション 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 file *filesystem*:*filename* [*max-file-size* | **nomax** [*min-file-size*]] [*severity-level-number* | *type*]

no logging file *filesystem*:*filename* [*severity-level-number* | *type*]

構文の説明

filesystem:*filename*	フラッシュ ファイル システムのエイリアスです。ログ メッセージを持つファイルのパスおよび名前を含みます。 スタック メンバまたはスタック マスター上のローカル フラッシュ ファイル システムの構文： **flash:** スタック マスターから、スタック メンバ上のローカル フラッシュ ファイル システムの構文： **flash** *member number* **（注）**
max-file-size	（任意）ログ ファイルの最大サイズを指定します。指定できる範囲は 4096 ～ 2147483647 です。
nomax	（任意）最大ファイル サイズ（2147483647）を指定します。
min-file-size	（任意）ログ ファイルの最小サイズを指定します。指定できる範囲は 1024 ～ 2147483647 です。
severity-level-number	（任意）ログ ファイルの重大度のレベルを指定します。指定できる範囲は 0 ～ 7 です。各レベルの意味については *type* オプションを参照してください。
type	（任意）ログ タイプを指定します。次のキーワードが有効です。 • **emergencies**：システムは使用不可（重大度 0） • **alerts**：早急な対応が必要（重大度 1） • **critical**：危険な状態（重大度 2） • **errors**：エラーが発生している状態（重大度 3） • **warnings**：警告状態（重大度 4） • **notifications**：通常ではあるが、重要なメッセージ（重大度 5） • **informational**：通知メッセージ（重大度 6） • **debugging**：デバッグ メッセージ（重大度 7）

デフォルト

ファイル サイズは最小で 2048 バイト、最大で 4096 バイトになります。

デフォルトの重大度のレベルは 7（**debugging** メッセージ：数字的に低いレベル）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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

ログ ファイルは ASCII テキストの形式で、スタンドアロン スイッチの内部バッファに格納されます。スイッチ スタックの場合、スタック マスター上の内部バッファに格納されます。スタンドアロン スイッチまたはスタック マスターに障害が発生した場合、事前に **logging file flash:***filename* 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、フラッシュ メモリに保存していない限り、ログは失われます。

logging file flash:*filename* グローバル コンフィギュレーション コマンドで、ログをフラッシュ メモリに保存した後は、**more flash:***filename* 特権 EXEC コマンドを使用してその内容を表示できます。

最小ファイル サイズが、最大ファイル サイズから 1024 引いた数より大きい場合、コマンドはその最小ファイルを拒否し、最大ファイル サイズから 1024 引いたサイズで設定されます。

level を指定すると、そのレベルのメッセージおよび数字的に低いレベルのメッセージが表示されます。

例

次の例では、フラッシュ メモリ内のファイルに情報レベルのログ メッセージを保存する方法を示します。

```
Switch(config)# logging file flash:logfile informational
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	スイッチの実行コンフィギュレーションを表示します。

mab request format attribute 32

スイッチ上で VLAN ID ベースの MAC 認証をイネーブルにするには、**mab request format attribute 32 vlan access-vlan** グローバル コンフィギュレーション 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。

mab request format attribute 32 vlan access-vlan

no mab request format attribute 32 vlan access-vlan

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

VLAN-ID ベースの MAC 認証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

コマンド履歴

リリース	変更内容
12.2(52)SE	このコマンドが追加されました。

使用上のガイドライン

RADIUS サーバがホスト MAC アドレスと VLAN に基づいて新しいユーザを認証できるようにするには、このコマンドを使用します。

Microsoft IAS RADIUS サーバを使用したネットワークでこの機能を使用します。Cisco ACS はこのコマンドを無視します。

例

次の例では、スイッチで VLAN-ID ベースの MAC 認証をイネーブルにする方法を示します。

```
Switch(config)# mab request format attribute 32 vlan access-vlan
```

関連コマンド

コマンド	説明
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートの再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。

コマンド	説明
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータと再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートにすでに最大数のデバイスが接続しているときに、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
mab	ポートの MAC-based 認証をイネーブルにします。
mab eap	Extensible Authentication Protocol（EAP）を使用するようポートを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

mac access-group

MAC Access Control List（ACL; アクセス コントロール リスト）をレイヤ 2 インターフェイスに適用するには、**mac access-group** 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。インターフェイスからすべてまたは指定の MAC ACL を削除するには、このコマンドの **no** 形式を使用します。MAC ACL を作成するには、**mac access-list extended** グローバル コンフィギュレーション コマンドを使用します。

mac access-group {*name*} **in**

no mac access-group {*name*}

構文の説明

name	名前付き MAC アクセス リストを指定します。
in	ACL が入力方向に適用されるように指定します。出力 ACL はレイヤ 2 インターフェイスではサポートされていません。

デフォルト

MAC ACL は、インターフェイスには適用されません。

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（レイヤ 2 インターフェイスだけ）

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

MAC ACL は入力レイヤ 2 インターフェイスにだけ適用できます。レイヤ 3 インターフェイスには適用できません。

レイヤ 2 インターフェイスでは、IP アクセス リストを使用して IP トラフィックをフィルタリングし、MAC アクセス リストを使用して非 IP トラフィックをフィルタリングできます。インターフェイスに IP ACL と MAC ACL の両方を適用すると、同じレイヤ 2 インターフェイスで IP トラフィックと非 IP トラフィックの両方をフィルタリングできます。同じレイヤ 2 インターフェイスには、IP アクセス リストと MAC アクセス リストを 1 つずつしか適用できません。

MAC ACL がすでにレイヤ 2 インターフェイスに設定されており、新しい MAC ACL をインターフェイスに適用した場合、以前に設定されていた ACL は新しい ACL で置換されます。

スイッチ上でレイヤ 2 インターフェイスに ACL を適用する場合に、そのスイッチに対してレイヤ 3 ACL が適用されているか、またはインターフェイスがメンバである VLAN に VLAN マップが適用されていれば、レイヤ 2 インターフェイスに適用された ACL が有効になります。

スイッチは、MAC ACL が適用されたインターフェイス上で入力パケットを受信すると、その ACL 内の一致条件を調べます。条件が一致すると、スイッチは ACL に従ってパケットを転送またはドロップします。

指定された ACL が存在しない場合、スイッチはすべてのパケットを転送します。

MAC 拡張 ACL を設定する方法の詳細については、このリリースのソフトウェア コンフィギュレーション ガイドの「Configuring Network Security with ACLs」の章を参照してください。

例

次の例では、*macacl2* と名付けられた MAC 拡張 ACL をインターフェイスに適用する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mac access-group macacl2 in
```

設定を確認するには、**show mac access-group** 特権 EXEC コマンドを入力します。スイッチに設定された ACL を表示するには、**show access-lists** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show access-lists	スイッチで設定される ACL を表示します。
show link state group	スイッチで設定される MAC ACL を表示します。
show running-config	スイッチの実行コンフィギュレーションを表示します。

mac access-list extended

非 IP トラフィックの MAC アドレスに基づいたアクセス リストを作成するには、**mac access-list extended** グローバル コンフィギュレーション コマンドを使用します。このコマンドを使用すると、拡張 MAC アクセス リスト コンフィギュレーション モードに入ります。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 access-list extended *name*

no mac access-list extended *name*

構文の説明

name	MAC 拡張アクセス リストに名前を割り当てます。

デフォルト

デフォルトでは、MAC アクセス リストは作成されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

MAC 名前付き拡張リストは、VLAN マップおよびクラス マップとともに使用されます。

名前付き MAC 拡張 ACL は、VLAN マップまたはレイヤ 2 インターフェイスに適用できます。レイヤ 3 インターフェイスには適用できません。

mac access-list extended コマンドを入力すると、MAC アクセス リスト コンフィギュレーション モードがイネーブルになります。使用できるコンフィギュレーション コマンドは、次のとおりです。

- **default**：コマンドをそのデフォルトに設定します。
- **deny**：パケットを拒否するように指定します。詳細については、deny（MAC アクセスリスト コンフィギュレーション）の MAC アクセス リスト コンフィギュレーション コマンドを参照してください。
- **exit**：MAC アクセス リスト コンフィギュレーション モードを終了します。
- **no**：コマンドを無効にするか、デフォルト値を設定します。
- **permit**：パケットを転送するように指定します。詳細は、permit（MAC アクセスリスト コンフィギュレーション）コマンドを参照してください。

MAC 拡張アクセス リストの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、名前付き MAC 拡張アクセス リスト *mac1* を作成し、拡張 MAC アクセス リスト コンフィギュレーション モードを開始する方法を示します。

```
Switch(config)# mac access-list extended mac1
Switch(config-ext-macl)#
```

次の例では、名前付き MAC 拡張アクセス リスト *mac1* を削除する方法を示します。

```
Switch(config)# no mac access-list extended mac1
```

設定を確認するには、**show access-lists** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
deny（MAC アクセス リスト コンフィギュレーション） **permit（MAC アクセスリスト コンフィギュレーション）**	MAC ACL を設定します（拡張 MAC アクセス リスト コンフィギュレーション モード）。
show access-lists	スイッチで設定されるアクセス リストを表示します。
vlan access-map	VLAN マップを定義し、アクセス マップ コンフィギュレーション モードに入ります。このモードでは、照合する MAC ACL と実行するアクションを指定できます。

mac address-table aging-time

ダイナミック エントリが使用または更新された後、MAC アドレス テーブル内に維持される時間を設定するには、**mac address-table aging-time** グローバル コンフィギュレーション 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。エージング タイムはすべての VLAN、または指定の VLAN に対して適用されます。

mac address-table aging-time {**0** | *10-1000000*} [**vlan** *vlan-id*]

no mac address-table aging-time {**0** | *10-1000000*} [**vlan** *vlan-id*]

構文の説明

0	この値はエージングをディセーブルにします。スタティック アドレスは、期限切れになることもテーブルから削除されることもありません。
10-1000000	エージング タイム（秒）。指定できる範囲は 10 ～ 1000000 秒です。
vlan *vlan-id*	（任意）エージング タイムを適用する VLAN ID を指定します。指定できる範囲は 1 ～ 4094 です。

デフォルト

デフォルト値は 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(19)EA1	**mac-address-table aging-time**（ハイフン付き）コマンドが、**mac address-table aging-time**（ハイフンなし）コマンドに替わりました。

使用上のガイドライン

ホストが継続して送信しない場合、エージング タイムを長くして、より長い時間ダイナミック エントリを記録してください。時間を長くすることで、ホストが再送信した場合にフラッディングが起こりにくくなります。

特定の VLAN を指定しない場合、このコマンドはすべての VLAN に対してエージング タイムを設定します。

例

次の例では、すべての VLAN にエージング タイムを 200 秒に設定する方法を示します。

```
Switch(config)# mac address-table aging-time 200
```

show mac address-table aging-time 特権 EXEC コマンドを入力すると、設定を確認できます。

関連コマンド

コマンド	説明
show mac address-table aging-time	すべての VLAN または指定された VLAN の、MAC アドレス テーブルのエージング タイムを表示します。

mac address-table learning vlan

VLAN で MAC アドレス学習をイネーブルにするには、**mac address-table learning** グローバル コンフィギュレーション コマンドを使用します。これがデフォルトの状態になります。VLAN で MAC アドレス学習をディセーブルにして、MAC アドレスを学習できる VLAN を制御するには、このコマンドの **no** 形式を使用します。

mac address-table learning vlan *vlan-id*

no mac address-table learning vlan *vlan-id*

構文の説明

vlan-id	1 つの VLAN ID、またはハイフンあるいはカンマで区切った VLAN ID の範囲を指定します。有効な VLAN ID は 1 ～ 4094 です。VLAN は VLAN 内部には指定できません。

デフォルト

デフォルトでは、MAC アドレス学習はすべての VLAN 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

コマンド履歴

リリース	変更内容
12.2(46)SE1	このコマンドが追加されました。

使用上のガイドライン

VLAN で MAC アドレス学習を制御する場合、MAC アドレスを学習できる VLAN、さらにポートを制御することで、利用可能な MAC アドレス テーブル スペースを管理できます。

1 つの VLAN ID（たとえば、**no mac address-table learning vlan 223**）または VLAN ID の範囲（たとえば、**no mac address-table learning vlan 1-20, 15**）での MAC アドレス学習をディセーブルにすることができます。

MAC アドレス学習をディセーブルにする前に、ネットワーク トポロジとスイッチ システム設定に詳しいことを確認してください。VLAN で MAC アドレス学習をディセーブルにすると、ネットワークでフラッディングを引き起こす可能性があります。たとえば、Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）を設定済みの VLAN で MAC アドレス学習をディセーブルにした場合、スイッチはレイヤ 2 ドメインにすべての IP パケットをフラッディングします。3 つ以上のポートを含む VLAN で MAC アドレス学習をディセーブルにした場合、スイッチに着信するすべてのパケットは、その VLAN ドメインでフラッディングします。MAC アドレス学習のディセーブル化はポートを 2 つ含む VLAN だけで行い、SVI のある VLAN で MAC アドレス学習をディセーブルにする場合は十分注意してください。

スイッチが内部的に使用する VLAN で MAC アドレス学習はディセーブルにできません。**no mac address-table learning vlan** *vlan-id* コマンドに入力する VLAN ID が内部 VLAN である場合、スイッチはエラーメッセージを生成してコマンドを拒否します。使用している内部 VLAN を表示するには、**show vlan internal usage** 特権 EXEC コマンドを入力します。

プライベート VLAN のプライマリまたはセカンダリ VLAN として設定された VLAN で MAC アドレス学習をディセーブルにする場合、MAC アドレスは、そのプライベート VLAN に属する別の VLAN（プライマリまたはセカンダリ）上で引き続き学習されます。

RSPAN VLAN で MAC アドレス学習はディセーブルにできません。設定すること自体できません。

セキュア ポートを含む VLAN で MAC アドレス学習をディセーブルにする場合、セキュア ポートで MAC アドレス学習はディセーブルになりません。後でインターフェイスのポート セキュリティをディセーブルにすると、ディセーブルになった MAC アドレス学習の状態がイネーブルになります。

すべての VLAN、または指定した VLAN の MAC アドレス学習のステータスを表示するには、**show mac-address-table learning** [**vlan** *vlan-id*] コマンドを入力します。

例

次の例では、VLAN 2003 で MAC アドレス学習をディセーブルにする方法を示します。

```
Switch(config)# no mac address-table learning vlan 2003
```

すべての VLAN、または指定した VLAN の MAC アドレス学習のステータスを表示するには、**show mac-address-table learning** [**vlan** *vlan-id*] コマンドを入力します。

関連コマンド

コマンド	説明
show mac address-table learning	すべての VLAN または指定した VLAN の MAC アドレス学習のステータスを表示します。

mac address-table move update

MAC アドレス テーブル移行更新機能をイネーブルにするには、**mac address-table move update** グローバル コンフィギュレーション 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 move update {**receive** | **transmit**}

no mac address-table move update {**receive** | **transmit**}

構文の説明

receive	スイッチが MAC アドレステーブル移行更新メッセージを処理するよう指定します。
transmit	プライマリ リンクがダウンし、スタンバイ リンクが起動した場合、スイッチが MAC アドレステーブル移行更新メッセージをネットワークの他のスイッチに送信するよう指定します。

コマンド モード

グローバル コンフィギュレーション

デフォルト

デフォルトでは、MAC アドレステーブル移行更新機能はディセーブルです。

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

MAC アドレステーブル移行更新機能により、プライマリ（フォワーディング）リンクがダウンし、スタンバイ リンクがトラフィックのフォワーディングを開始した場合、スイッチは高速双方向コンバージェンスを提供できます。

プライマリ リンクがダウンし、スタンバイ リンクが起動した場合、アクセス スイッチが MAC アドレステーブル移行更新メッセージを送信するように設定できます。アップリンク スイッチが、MAC アドレステーブル移行更新メッセージを受信および処理するように設定できます。

例

次の例では、アクセス スイッチが MAC アドレス テーブル移行更新メッセージを送信するように設定する方法を示します。

```
Switch# configure terminal
Switch(conf)# mac address-table move update transmit
Switch(conf)# end
```

次の例では、アップリンク スイッチが MAC アドレス テーブル移行更新メッセージを取得および処理するように設定する方法を示します。

```
Switch# configure terminal
Switch(conf)# mac address-table move update receive
Switch(conf)# end
```

設定を確認するには、**show mac address-table move update** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
clear mac address-table move update	MAC アドレステーブル移行更新グローバル カウンタをクリアします。
debug matm move update	MAC アドレステーブル移行更新メッセージ処理をデバッグします。
show mac address-table move update	スイッチに MAC アドレス テーブル移行更新情報を表示します。

mac address-table notification

スイッチ スタック上で MAC アドレス通知機能をイネーブルにするには、**mac address-table notification** グローバル コンフィギュレーション 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 notification {**change** [**history-size** *value* | **interval** *value*] | **mac-move** | **threshold** [[**limit** *percentage*] **interval** *time*]}

no mac address-table notification {**change** [**history-size** *value* | **interval** *value*] | **mac-move** | **threshold** [[**limit** *percentage*] **interval** *time*]}

構文の説明

change	スイッチ上で MAC 通知をイネーブルまたはディセーブルにします。
history-size *value*	（任意）MAC 通知履歴テーブルのエントリの最大数を設定します。指定できる範囲は 0 ～ 500 エントリです。デフォルト値は 1 です。
interval *value*	（任意）通知トラップ間隔を設定します。この時間量が過ぎると、スイッチ スタックは通知トラップを送信します。指定できる範囲は 0 ～ 2147483647 秒です。デフォルト値は 1 秒です。
mac-move	MAC 移動通知をイネーブルにします。
threshold	MAC しきい値通知をイネーブルにします。
limit *percentage*	（任意）MAC 利用率しきい値を入力します。指定できる範囲は 1 ～ 100% です。デフォルト値は 50% です。
interval *time*	（任意）MAC しきい値通知の間の時間を入力します。指定できる範囲は 120 ～ 1000000 秒です。デフォルト値は 120 秒です。

デフォルト

デフォルトでは、MAC アドレス通知、MAC 移動、および MAC しきい値モニタリングがディセーブルです。

デフォルトの MAC 変更トラップ間隔は 1 秒です。

履歴テーブルのデフォルトのエントリ数は 1 です。

デフォルトの MAC 利用率しきい値は 50% です。

MAC しきい値通知間のデフォルトの時間は 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(19)EA1	**mac-address-table notification** （ハイフン付き）コマンドが、**mac address-table notification** （ハイフンなし）コマンドに替わりました。
12.2(40)SE	**change**、**mac-move**、および **threshold** [[**limit** *percentage*] **interval** *time*] キーワードが追加されました。

使用上のガイドライン

MAC アドレス通知変更機能は、新しい MAC アドレスが転送テーブルに追加されたり、古いアドレスがそこから削除されたりするたびに、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）トラップを Network Management System（NMS; ネットワーク管理システム）に送信します。MAC 変更通知はダイナミックおよびセキュア MAC アドレスだけに生成され、セルフ アドレス、マルチキャスト アドレス、または他のスタティック アドレスには生成されません。

history-size オプションを設定している場合、既存の MAC アドレス履歴テーブルが削除され、新しいテーブルが作成されます。

mac address-table notification change コマンドを使用すれば、MAC アドレス通知変更機能がイネーブルになります。また、**snmp trap mac-notification change** インターフェイス コンフィギュレーション コマンドでインターフェイス上の MAC アドレス通知トラップをイネーブルにし、**snmp-server enable traps mac-notification change** グローバル コンフィギュレーション コマンドでスイッチが MAC アドレス トラップを NMS に送信するよう設定する必要があります。

また、**mac address-table notification mac-move** コマンドおよび **snmp-server enable traps mac-notification move** グローバル コンフィギュレーション コマンドを入力することにより、MAC アドレスが 1 つのポートから同じ VLAN の別のポートに移動した場合、常にトラップをイネーブルにできます。

MAC アドレス テーブルのしきい値制限に達するかそれを超えた場合に常にトラップを生成するには、**mac address-table notification** *threshold* [**limit** *percentage*] | [**interval** *time*] コマンドおよび **snmp-server enable traps mac-notification threshold** 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。

例

次の例では、MAC アドレス テーブル変更通知機能をイネーブルにし、通知トラップの間隔を 60 秒、履歴テーブルのサイズを 100 エントリに設定する方法を示します。

```
Switch(config)# mac address-table notification change
Switch(config)# mac address-table notification change interval 60
Switch(config)# mac address-table notification change history-size 100
```

show mac address-table notification 特権 EXEC コマンドを入力すれば、設定を確認することができます。

関連コマンド

コマンド	説明
clear mac address-table notification	MAC アドレス通知グローバル カウンタをクリアします。
show mac address-table notification	すべての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対する MAC アドレス通知設定を表示します。
snmp-server enable traps	**mac-notification** キーワードが追加された場合に SNMP MAC 通知トラップを送信します。
snmp trap mac-notification change	特定のインターフェイスの SNMP MAC 通知変更トラップをイネーブルにします。

mac address-table static

MAC アドレス テーブルにスタティック アドレスを追加するには、**mac address-table static** グローバル コンフィギュレーション コマンドを使用します。スタティック エントリをテーブルから削除するには、このコマンドの **no** 形式を使用します。

mac address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

no mac address-table static *mac-addr* **vlan** *vlan-id* [**interface** *interface-id*]

構文の説明

mac-addr	アドレス テーブルに追加する宛先 MAC アドレス（ユニキャストまたはマルチキャスト）。この宛先アドレスを持つパケットが指定した VLAN に着信すると、指定したインターフェイスに転送されます。
vlan *vlan-id*	指定した MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる範囲は 1 ～ 4094 です。
interface *interface-id*	受信されたパケットを転送するインターフェイス。有効なインターフェイスには、物理ポートとポート チャネルが含まれます。

デフォルト

スタティック アドレス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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(19)EA1	**mac-address-table static** コマンド（ハイフンあり）は、**mac address-table static** コマンド（ハイフンなし）に替わりました。

例

次の例では、MAC アドレス テーブルにスタティック アドレス c2f3.220a.12f4 を追加する方法を示します。VLAN 4 でこの MAC アドレスを宛先としてパケットを受信すると、パケットは指定されたインターフェイスに転送されます。

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4
interfacegigabitethernet6/0/1
```

設定を確認するには、**show mac address-table** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show mac address-table static	スタティック MAC アドレス テーブル エントリだけを表示します。

mac address-table static drop

ユニキャスト MAC アドレス フィルタリングをイネーブルにして、特定の送信元または宛先 MAC アドレスのトラフィックをドロップするようにスイッチを設定するには **mac address-table static drop** グローバル コンフィギュレーション 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 static *mac-addr* **vlan** *vlan-id* **drop**

no mac address-table static *mac-addr* **vlan** *vlan-id*

構文の説明

mac-addr	ユニキャスト送信元または宛先 MAC アドレス。この MAC アドレスを持つパケットはドロップされます。
vlan *vlan-id*	指定した MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる VLAN ID の範囲は、1 ～ 4094 です。

デフォルト

ユニキャスト MAC アドレス フィルタリングはディセーブルです。スイッチは、特定の送信元または宛先 MAC アドレスのトラフィックをドロップしません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。

使用上のガイドライン

この機能を使用する場合、次の注意事項に従ってください。

- マルチキャスト MAC アドレス、ブロードキャスト MAC アドレス、およびルータ MAC アドレスはサポートされません。CPU に転送されるパケットもサポートされません。
- ユニキャスト MAC アドレスをスタティック アドレスとして追加し、ユニキャスト MAC アドレス フィルタリングを設定する場合は、最後に入力されたコマンドに応じて、スイッチは MAC アドレスをスタティック アドレスとして追加するか、またはその MAC アドレスを持つパケットをドロップします。2 番目に入力したコマンドは、最初のコマンドを上書きします。

  たとえば、**mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* グローバル コンフィギュレーション コマンドの後に **mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** コマンドを入力した場合は、スイッチは送信元または宛先として指定された MAC アドレスを持つパケットをドロップします。

  mac address-table static *mac-addr* **vlan** *vlan-id* **drop** グローバル コンフィギュレーション コマンドの後に **mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* コマンドを入力した場合は、スイッチがその MAC アドレスをスタティック アドレスとして追加します。

例

次の例では、ユニキャスト MAC アドレス フィルタリングをイネーブルにし、c2f3.220a.12f4 の送信元または宛先アドレスを持つパケットをドロップするようにスイッチを設定する方法を示します。送信元または宛先としてこの MAC アドレスを持つパケットが VLAN4 上で受信された場合、パケットがドロップされます。

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop
```

次の例では、ユニキャスト MAC アドレス フィルタリングをディセーブルにする方法を示します。

```
Switch(config)# no mac address-table static c2f3.220a.12f4 vlan 4
```

show mac address-table static 特権 EXEC コマンドを入力すれば、設定を確認することができます。

関連コマンド

コマンド	説明
show mac address-table static	スタティック MAC アドレス テーブル エントリだけを表示します。

match（アクセス マップ コンフィギュレーション）

VLAN マップを設定して、パケットを 1 つまたは複数のアクセス リストと照合するには、**match** アクセス マップ コンフィギュレーション コマンドを使用します。一致パラメ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。

match {**ip address** {*name* | *number*} [*name* | *number*] [*name* | *number*]...} | {**mac address** {*name*} [*name*] [*name*]...}

no match {**ip address** {*name* | *number*} [*name* | *number*] [*name* | *number*]...} | {**mac address** {*name*} [*name*] [*name*]...}

構文の説明

ip address	パケットを IP アドレス アクセス リストと照合するようにアクセス マップを設定します。
mac address	パケットを MAC アドレス アクセス リストと照合するようにアクセス マップを設定します。
name	パケットを照合するアクセス リストの名前です。
number	パケットを照合するアクセス リストの番号です。このオプションは、MAC アクセス リストに対しては無効です。

デフォルト

デフォルトのアクションでは、一致パラメータは VLAN マップに適用されません。

コマンド モード

アクセス マップ コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

vlan access-map 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、アクセス マップ コンフィギュレーション モードを開始します。

1 つのアクセス リストの名前または番号を入力する必要があります。その他は任意です。パケットは、1 つまたは複数のアクセス リストに対して照合できます。いずれかのリストに一致すると、エントリの一致としてカウントされます。

アクセス マップ コンフィギュレーション モードでは、**match** コマンドを使用して、VLAN に適用される VLAN マップの一致条件を定義できます。**action** コマンドを使用すると、パケットが条件に一致したときに実行するアクションを設定できます。

パケットは、同じプロトコル タイプのアクセス リストに対してだけ照合されます。IP パケットは、IP アクセス リストに対して照合され、その他のパケットはすべて MAC アクセス リストに対して照合されます。

同じマップ エントリに、IP アドレスと MAC アドレスの両方を指定できます。

例

次の例では、VLAN アクセス マップ *vmap4* を定義し VLAN 5 と VLAN 6 に適用する方法を示します。このアクセス マップでは、パケットがアクセス リスト *al2* に定義された条件に一致すると、インターフェイスは IP パケットをドロップします。

```
Switch(config)# vlan access-map vmap4
Switch(config-access-map)# match ip address al2
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vlan filter vmap4 vlan-list 5-6
```

設定を確認するには、**show vlan access-map** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
access-list	番号付き標準 ACL を設定します。
action	パケットが ACL のエントリに一致した場合に、実行されるアクションを指定します。
ip access-list	名前付きアクセス リストを作成します。
mac access-list extended	名前付き MAC アドレス アクセス リストを作成します。
show vlan access-map	スイッチで作成された VLAN アクセス マップを表示します。
vlan access-map	VLAN アクセス マップを作成します。

match（クラスマップ コンフィギュレーション）

トラフィックを分類するための一致条件を定義するには、**match** クラスマップ コンフィギュレーション コマンドを使用します。一致基準を削除するには、このコマンドの **no** 形式を使用します。

match {**access-group** *acl-index-or-name* | **input-interface** *interface-id-list* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list*}

no match {**access-group** *acl-index-or-name* | **input-interface** *interface-id-list* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list*}

構文の説明

access-group *acl-index-or-name*	IP 標準または拡張 Access Control List（ACL; アクセス コントロール リスト）または MAC ACL の番号または名前です。IP 標準 ACL の場合、ACL インデックス範囲は 1 ～ 99 および 1300 ～ 1999 です。IP 拡張 ACL の場合、ACL インデックス範囲は 100 ～ 199 および 2000 ～ 2699 です。
input-interface *interface-id-list*	階層ポリシー マップでインターフェイス レベルのクラス マップを適用する物理ポートを指定します。このコマンドは、子レベルのポリシー マップでだけ使用でき、子レベルのポリシー マップ内での唯一の一致条件である必要があります。ポート（1 エントリとしてカウント）、スペースで区切ったポート（各ポートを 1 エントリとしてカウント）、またはハイフンで区切ったポート範囲（2 エントリとしてカウント）を指定することによって、最大 6 つのエントリを指定することができます。
ip dscp *dscp-list*	着信パケットとの照合を行うための、最大 8 つまでの IP Differentiated Service Code Point（DSCP）値のリストです。各値はスペースで区切ります。指定できる範囲は 0 ～ 63 です。よく使用される値の場合は、ニーモニック名を入力することもできます。
ip precedence *ip-precedence-list*	着信パケットとの照合を行うための、最大 8 つの IP precedence 値のリストです。各値はスペースで区切ります。指定できる範囲は 0 ～ 7 です。よく使用される値の場合は、ニーモニック名を入力することもできます。

デフォルト

一致基準は定義されません。

コマンド モード

クラスマップ コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(25)SE	**input-interface** *interface-id-list* キーワードが追加されました。

使用上のガイドライン

パケットを分類するために着信パケットのどのフィールドを調べるのかを指定する場合は、**match** コマンドを使用します。IP アクセス グループまたは MAC アクセス グループの Ether Type/Len の照合だけがサポートされています。

物理ポート単位でパケット分類を定義するため、クラス マップごとに 1 つずつに限り **match** コマンドがサポートされています。この状況では、**match-all** キーワードと **match-any** キーワードは同じです。

match ip dscp *dscp-list* コマンドまたは **match ip precedence** *ip-precedence-list* コマンドの場合は、よく使用される値のニーモニック名を入力できます。たとえば、**match ip dscp af11** コマンドを入力できます。このコマンドは、**match ip dscp 10** コマンドを入力した場合と同じ結果になります。また、**match ip precedence critical** コマンドを入力できます。このコマンドは、**match ip precedence 5** コマンドを入力した場合と同じ結果になります。サポートされているニーモニックのリストを表示するには、**match ip dscp ?** または **match ip precedence ?** コマンドを入力して、コマンドラインのヘルプ ストリングを表示してください。

階層ポリシー マップ内にインターフェイス レベルのクラス マップを設定するときには、**input-interface** *interface-id-list* キーワードを使用します。*interface-id-list* には、最大 6 つのエントリを指定することができます。

例

次の例では、クラス マップ *class2* を作成する方法を示します。このマップは、DSCP 値 10、11、および 12 を持つすべての着信トラフィックに一致します。

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# exit
```

次の例では、クラス マップ *class3* を作成する方法を示します。このマップは、IP precedence 値 5、6、および 7 を持つすべての着信トラフィックに一致します。

```
Switch(config)# class-map class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# exit
```

次の例では、IP precedence 一致基準を削除し、*acl1* を使用してトラフィックを分類する方法を示します。

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# no match ip precedence
Switch(config-cmap)# match access-group acl1
Switch(config-cmap)# exit
```

次の例では、階層ポリシー マップでインターフェイス レベルのクラス マップが適用する物理ポートのリストの指定方法を示しています。

```
Switch(config)# class-map match-all class4
Switch(config-cmap)# match input-interface gigabitethernet2/0/1 gigabitethernet2/0/2
Switch(config-cmap)# exit
```

次の例では、階層ポリシー マップでインターフェイス レベルのクラス マップが適用する物理ポートの範囲の指定方法を示しています。

```
Switch(config)# class-map match-all class4
Switch(config-cmap)# match input-interface gigabitethernet2/0/1 - gigabitethernet2/0/5
Switch(config-cmap)# exit
```

show class-map 特権 EXEC コマンドを入力すると、設定を確認できます。

関連コマンド

コマンド	説明
class-map	名前を指定したクラスとパケットとの照合に使用されるクラス マップを作成します。
show class-map	Quality of Service（QoS）クラス マップを表示します。

mdix auto

インターフェイス上で Automatic Media-Dependent-Interface Crossover（Auto-MDIX）機能をイネーブルにするには、**mdix auto** 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。Auto MDIX がイネーブルな場合、インターフェイスは自動的に必要なケーブル接続タイプ（ストレートまたはクロス）を検出し、接続を適切に設定します。Auto MDIX 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。

mdix auto

no mdix auto

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

Auto MDIX 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

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。
12.2(18)SE	デフォルト設定が*ディセーブル*から*イネーブル*に変更されました。

使用上のガイドライン

インターフェイスの Auto MDIX をイネーブルにする場合は、機能が正常に動作するように、インターフェイス速度とデュプレックスも **auto** に設定する必要があります。

Auto MDIX が（速度とデュプレックスの自動ネゴシエーションとともに）接続するインターフェイスの一方または両方でイネーブルの場合は、ケーブル タイプ（ストレートまたはクロス）が不正でもリンクがアップします。

Auto-MDIX は、すべての 10/100 および 10/100/1000 Mbps インターフェイス上および 10/100/1000BASE-T/TX Small Form-factor Pluggable（SFP）モジュール インターフェイス上でサポートされます。1000BASE-SX または 1000BASE-LX SFP モジュール インターフェイスではサポートされません。

例

次の例では、ポートの Auto MDIX をイネーブルにする方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

インターフェイスの auto-MDIX の動作ステートを確認するには **show controllers ethernet-controller** *interface-id* **phy** 特権 EXEC コマンドを入力します。

mls qos

スイッチ全体の Quality of Service（QoS）をイネーブルにするには、**mls qos** グローバル コンフィギュレーション コマンドを使用します。**mls qos** コマンドを入力すると、システム内のすべてのポートでデフォルト パラメータが使用されて QoS がイネーブルになります。スイッチ全体のすべての QoS 関連の統計をリセットし、QoS 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 qos

no mls qos

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

QoS はディセーブルです。パケットが変更されない（パケット内の CoS、DSCP、および IP precedence 値は変更されない）ため、信頼できるポートまたは信頼できないポートといった概念は存在しません。トラフィックは Pass-Through モードでスイッチングされます（パケットは書き換えられることなくスイッチングされ、ポリシングなしのベスト エフォートに分類されます）。

mls qos グローバル コンフィギュレーション コマンドによって QoS がイネーブル化され、その他のすべての QoS 設定値がデフォルト値に設定されている場合、トラフィックはポリシングされず、ベスト エフォート（DSCP 値と CoS 値は 0 に設定される）として分類されます。ポリシー マップは設定されません。すべてのポート上のデフォルト ポートの信頼性は、信頼性なし（untrusted）の状態です。デフォルトの入力キューおよび出力キューの設定値が有効となります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

QoS 分類、ポリシング、マークダウンまたはドロップ、キューイング、トラフィック シェーピング機能を使用するには、QoS をグローバルにイネーブルにする必要があります。**mls qos** コマンドを入力する前に、ポリシー マップを作成しそれをポートに適用できます。ただし、**mls qos** コマンドを入力していない場合、QoS 処理はディセーブルになります。

no mls qos コマンドを入力しても、QoS を設定するために使用したポリシー マップとクラスマップは設定から削除されません。ただし、システム リソースを節約するため、ポリシー マップに対応するエントリはスイッチ ハードウェアから削除されます。以前の設定で QoS を再度イネーブルにする場合、**mls qos** コマンドを使用します。

このコマンドでスイッチの QoS 状態を切り替えることで、キューのサイズが修正（再割り当て）されます。キュー サイズの変更時には、ハードウェアを再設定する期間中キューは一時的にシャットダウンされ、スイッチはこのキューに新たに到着したパケットをドロップします。

例

次の例では、スイッチ上で QoS をイネーブルにする方法を示します。

```
Switch(config)# mls qos
```

設定を確認するには、**show mls qos** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show mls qos	QoS 情報を表示します。

mls qos aggregate-policer

ポリサー パラメータを定義するには、**mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。これは、同一のポリシー マップ内の複数のクラスで共有できます。ポリサーは、最大許容伝送速度、最大バースト伝送サイズ、およびいずれかの最大値を超過した場合の対処法を定義します。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 *aggregate-policer-name rate-bps burst-byte* **exceed-action** {**drop** | **policed-dscp-transmit**}

no mls qos aggregate-policer *aggregate-policer-name*

構文の説明

aggregate-policer-name	**police aggregate** ポリシー マップ クラス コンフィギュレーション コマンドが参照する集約ポリサーの名前です。
rate-bps	平均トラフィック伝送速度をビット/秒（b/s）で指定します。指定できる範囲は 8000 ～ 1000000000 です。
burst-byte	通常のバースト サイズ（バイト）を指定します。指定できる範囲は 8000 ～ 1000000 です。
exceed-action drop	指定された伝送速度を超えると、スイッチがパケットをドロップするよう指定します。
exceed-action policed-dscp-transmit	指定された伝送速度を超えると、スイッチがパケットの Differentiated Service Code Point（DSCP）を、ポリシング設定 DSCP マップに指定された値に変更して、パケットを送信するよう指定します。

デフォルト

集約ポリサーは定義されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

ポリサーが複数のクラスによって共有されている場合は、集約ポリサーを定義します。

あるポートのポリサーを別のポートの他のポリサーと共有することはできません。2 つの異なるポートからのトラフィックは、ポリシング目的では集約できません。

2 つ以上の物理ポートを制御するポート ASIC デバイスは、256 個のポリサー（255 個のユーザ設定可能なポリサーと 1 個の内部使用向けに予約されたポリサー）をサポートします。ポートごとにサポートされるユーザ設定可能なポリサーの最大数は 63 です。ポリサーはソフトウェアによってオンデマンドで割り振られ、ハードウェアおよび ASIC の限界によって制約されます。ポートごとにポリサーを予約することはできません（ポートがいずれかのポリサーに割り当てられるとは保証されていません）。

集約ポリサーは同じポリシー マップ内の複数のクラスに適用されます。異なるポリシー マップにまたがって集約ポリサーを使用することはできません。

ポリシー マップ内で使用中の場合、集約ポリサーは削除できません。最初に、**no police aggregate** *aggregate-policer-name* ポリシー マップ クラス コンフィギュレーション コマンドを使用してすべてのポリシー マップから集約ポリサーを削除してから、**no mls qos aggregate-policer** *aggregate-policer-name* コマンドを使用する必要があります。

ポリシングはトークンバケット アルゴリズムを使用します。バケットの深さ（バケットがオーバーフローするまでの許容最大バースト）を設定するには、*police* 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 **burst-byte** オプションまたは **mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。トークンがバケットから削除される速度（平均速度）を設定するには、*police* 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 **rate-bps** オプションまたは **mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、集約ポリサー パラメータを定義する方法と、ポリシー マップ内の複数のクラスにそのポリサーを適用する方法を示します。

```
Switch(config)# mls qos aggregate-policer agg_policer1 1000000 1000000 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate agg_policer2
Switch(config-pmap-c)# exit
```

設定を確認するには、**show mls qos aggregate-policer** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
police aggregate	異なるクラスによって共有されるポリサーを作成します。
show mls qos aggregate-policer	Quality of Service（QoS）集約ポリサー設定を表示します。

mls qos cos

デフォルトのポート Class of Service（CoS）値を定義したり、ポート上のすべての着信パケットにデフォルトの CoS 値を割り当てたりするには、**mls qos cos** 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。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 cos {*default-cos* | **override**}

no mls qos cos {*default-cos* | **override**}

構文の説明

default-cos	デフォルト CoS 値をポートに割り当てます。パケットがタグ付けされていない場合、デフォルトの CoS 値がパケットの CoS 値になります。指定できる CoS 範囲は 0 ～ 7 です。
override	着信パケットの CoS を無効にし、すべての着信パケットにデフォルトのポート CoS 値を適用します。

デフォルト

デフォルトのポート CoS 値は 0 です。

CoS 無効化はディセーブル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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

デフォルト値を使用して、タグなし（着信パケットが CoS 値を持たない場合）で着信したすべてのパケットに CoS 値と Differentiated Service Code Point（DSCP）値を割り当てることができます。また、**override** キーワードを使用すると、デフォルトの CoS 値と DSCP 値をすべての着信パケットに割り当てることができます。

特定のポートに届くすべての着信パケットに、他のポートから着信するパケットより高いプライオリティまたは低いプライオリティを与える場合には、**override** キーワードを使用します。たとえポートがすでに DSCP、CoS、または IP precedence を信頼するように設定されていても、このコマンドは以前に設定済みの信頼状態を無効にし、すべての着信 CoS 値に **mls qos cos** コマンドで設定されたデフォルトの CoS 値が割り当てられます。着信パケットがタグ付きの場合、パケットの CoS 値は、出力ポートで、ポートのデフォルト CoS を使用して変更されます。

例

次の例では、ポートのデフォルト ポート CoS 値を 4 に設定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos cos 4
```

次の例では、ポートで、ポートに着信するすべてのパケットにデフォルトのポート CoS 値 4 を割り当てる方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# mls qos cos 4
Switch(config-if)# mls qos cos override
```

show mls qos interface 特権 EXEC コマンドを入力すると、設定を確認できます。

関連コマンド

コマンド	説明
show mls qos interface	Quality of Service（QoS）情報を表示します。

mls qos dscp-mutation

Differentiated Service Code Point（DSCP）の信頼性のあるポートに対して、DSCP/DSCP 変換マップを適用するには、**mls qos dscp-mutation** 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。マップをデフォルト設定（DSCP 変換なし）に戻すには、このコマンドの **no** 形式を使用します。

mls qos dscp-mutation *dscp-mutation-name*

no mls qos dscp-mutation *dscp-mutation-name*

構文の説明

dscp-mutation-name	DSCP/DSCP 変換マップの名前。このマップは、以前は **mls qos map dscp-mutation** グローバル コンフィギュレーション コマンドで定義されていました。

デフォルト

デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

2 つの Quality of Service（QoS）ドメインが異なる DSCP 定義を持つ場合は、DSCP/DSCP 変換マップを使用して、一方の DSCP 値のセットをもう一方のドメインの定義に適合するように変換します。DSCP/DSCP 変換マップは、QoS 管理ドメインの境界にある受信ポートに適用します（入力変換）。

入力変換では、新しい DSCP 値がパケット内の値を上書きし、QoS はこの新しい値を持つパケットを処理します。スイッチは、新しい DSCP 値とともにそのパケットをポートへ送出します。

入力ポートには複数の DSCP/DSCP 変換マップを設定できます。

マップは、DSCP の信頼性のあるポートにだけ適用します。DSCP 変換マップを信頼できないポート、Class of Service（CoS）または IP precedence の信頼できるポートに適用すると、コマンドはすぐには影響せず、そのポートが DSCP の信頼できるポートになってから効果を発揮します。

例

次の例では、DSCP/DSCP 変換マップ *dscpmutation1* を定義し、そのマップをポートに適用する方法を示します。

```
Switch(config)# mls qos map dscp-mutation dscpmutation1 10 11 12 13 to 30
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation dscpmutation1
```

次の例では、DSCP/DSCP 変換マップ名 *dscpmutation1* をポートから削除し、そのマップをデフォルトにリセットする方法を示します。

```
Switch(config-if)# no mls qos dscp-mutation dscpmutation1
```

設定を確認するには、**show mls qos maps** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos map dscp-mutation	DSCP/DSCP 変換マップを定義します。
mls qos trust	ポートの信頼状態を設定します。
show mls qos maps	QoS のマッピング情報を表示します。

mls qos map

Class of Service（CoS）/Differentiated Service Code Point（DSCP）マップ、DSCP/CoS マップ、DSCP/DSCP 変換マップ、IP precedence/DSCP マップ、およびポリシングされた DSCP のマップを定義するには、**mls qos map** グローバル コンフィギュレーション コマンドを使用します。デフォルトのマップに戻すには、このコマンドの **no** 形式を使用します。

mls qos map {**cos-dscp** *dscp1...dscp8* | **dscp-cos** *dscp-list* **to** *cos* | **dscp-mutation** *dscp-mutation-name in-dscp* **to** *out-dscp* | **ip-prec-dscp** *dscp1...dscp8* | **policed-dscp** *dscp-list* **to** *mark-down-dscp*}

no mls qos map {**cos-dscp** | **dscp-cos** | **dscp-mutation** *dscp-mutation-name* | **ip-prec-dscp** | **policed-dscp**}

構文の説明

cos-dscp *dscp1...dscp8*	CoS/DSCP マップを定義します。 *dscp1...dscp8* には、CoS 値 0 ～ 7 に対応する 8 つの DSCP 値を入力します。各 DSCP 値はスペースで区切ります。指定できる範囲は 0 ～ 63 です。
dscp-cos *dscp-list* **to** *cos*	DSCP/CoS マップを定義します。 *dscp-list* には、各値をスペースで区切って最大 8 つの DSCP 値を入力します。指定できる範囲は 0 ～ 63 です。さらに、**to** キーワードを入力します。 *cos* には、DSCP 値と対応する 1 つの CoS 値を入力します。指定できる範囲は 0 ～ 7 です。
dscp-mutation *dscp-mutation-name in-dscp* **to** *out-dscp*	DSCP/DSCP 変換マップを定義します。 *dscp-mutation-name* には、変換マップ名を入力します。 *in-dscp* には、各値をスペースで区切って最大 8 つの DSCP 値を入力します。さらに、**to** キーワードを入力します。 *out-dscp* には、1 つの DSCP 値を入力します。 指定できる範囲は 0 ～ 63 です。
ip-prec-dscp *dscp1...dscp8*	IP precedence/DSCP マップを定義します。 *dscp1...dscp8* には、IP precedence 値 0 ～ 7 に対応する 8 つの DSCP 値を入力します。各 DSCP 値はスペースで区切ります。指定できる範囲は 0 ～ 63 です。
policed-dscp *dscp-list* **to** *mark-down-dscp*	ポリシング設定 DSCP マップを定義します。 *dscp-list* には、各値をスペースで区切って最大 8 つの DSCP 値を入力します。さらに、**to** キーワードを入力します。 *mark-down-dscp* には、対応するポリシング設定（マークダウンされた）DSCP 値を入力します。 指定できる範囲は 0 ～ 63 です。

デフォルト

表 2-11 に、デフォルトの CoS/DSCP マップを示します。

表 2-11　デフォルトの CoS/DSCP マップ

CoS 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

表 2-12 に、デフォルトの DSCP/CoS マップを示します。

表 2-12　デフォルトの DSCP/CoS マップ

DSCP 値	CoS 値
0 ～ 7	0
8 ～ 15	1
16 ～ 23	2
24 ～ 31	3
32 ～ 39	4
40 ～ 47	5
48 ～ 55	6
56 ～ 63	7

表 2-13 に、デフォルトの IP precedence/DSCP マップを示します。

表 2-13　デフォルトの IP Precedence/DSCP マップ

IP precedence 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。

デフォルトのポリシング設定 DSCP マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌルマップです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

マップはすべてグローバルに定義されています。DSCP/DSCP 変換マップを除くすべてのマップは、すべてのポートに適用されます。DSCP/DSCP 変換マップは、特定のポートに適用されます。

例

次の例では、IP precedence/DSCP マップを定義し、IP precedence 値 0 ～ 7 を DSCP 値 0、10、20、30、40、50、55、および 60 にマッピングする方法を示します。

```
Switch# configure terminal
Switch(config)# mls qos map ip-prec-dscp 0 10 20 30 40 50 55 60
```

次の例では、ポリシング設定 DSCP マップを定義する方法を示します。DSCP 値 1、2、3、4、5、および 6 は DSCP 値 0 にマークダウンされます。明示的に設定されていないマークされた DSCP 値は変更されません。

```
Switch# configure terminal
Switch(config)# mls qos map policed-dscp 1 2 3 4 5 6 to 0
```

次の例では、DSCP/CoS マップを定義する方法を示します。DSCP 値 20、21、22、23、および 24 は、CoS 1 にマッピングされます。DSCP 値 10、11、12、13、14、15、16、および 17 は CoS 0 にマッピングされます。

```
Switch# configure terminal
Switch(config)# mls qos map dscp-cos 20 21 22 23 24 to 1
Switch(config)# mls qos map dscp-cos 10 11 12 13 14 15 16 17 to 0
```

次の例では、CoS/DSCP マップを定義する方法を示します。CoS 値 0 ～ 7 は、DSCP 値 0、5、10、15、20、25、30、および 35 にマッピングされます。

```
Switch# configure terminal
Switch(config)# mls qos map cos-dscp 0 5 10 15 20 25 30 35
```

次の例では、DSCP/DSCP 変換マップを定義する方法を示します。明示的に設定されていないエントリはすべて変更されません（ヌル マップ内の指定のままです）。

```
Switch# configure terminal
Switch(config)# mls qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 10
Switch(config)# mls qos map dscp-mutation mutation1 8 9 10 11 12 13 to 10
Switch(config)# mls qos map dscp-mutation mutation1 20 21 22 to 20
Switch(config)# mls qos map dscp-mutation mutation1 0 31 32 33 34 to 30
```

設定を確認するには、**show mls qos maps** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos dscp-mutation	DSCP/DSCP 変換マップを DSCP の信頼性のあるポートに適用します。
show mls qos maps	Quality of Service（QoS）マッピング情報を表示します。

mls qos queue-set output buffers

キューセット（各ポートの 4 つの出力キュー）にバッファを割り当てるには、**mls qos queue-set output buffers** グローバル コンフィギュレーション 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-set output *qset-id* **buffers** *allocation1 ... allocation4*

no mls qos queue-set output *qset-id* **buffers**

構文の説明

qset-id	キューセットの ID です。各ポートはキューセットに属し、ポート単位で出力キュー 4 つの特性すべてを定義します。指定できる範囲は 1 ～ 2 です。
allocation1 ... allocation4	各キュー（キュー 1 ～ 4 の 4 つのキュー）のバッファ スペース割り当て（%）です。*allocation1*、*allocation3*、*allocation4* の場合、範囲は 0 ～ 99 です。*allocation2* の場合、範囲は 1 ～ 100 です（CPU バッファを含める）。各値はスペースで区切ります。

デフォルト

すべての割り当て値は、4 つのキューに均等にマッピングされます（25、25、25、25）。各キューがバッファ スペースの 1/4 を持ちます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(18)SE	*allocation2* の範囲が 0 ～ 100 から 20 ～ 100 に変更されました。
12.2(20)SE	*allocation1*、*allocation3*、*allocation4* の範囲が 0 ～ 100 から 0 ～ 99 に変更されました。*allocation2* の範囲が 20 ～ 100 から 1 ～ 100 に変更されました。

使用上のガイドライン

4 つの割り当て値を指定します。各値はスペースで区切ります。

トラフィックの重要度に応じてバッファを割り当てます。たとえば、最高プライオリティのトラフィックを持つキューには多くの割合のバッファを与えます。

異なる特性を持つ異なるクラスのトラフィックを設定するには、**mls qos queue-set output** *qset-id* **threshold** グローバル コンフィギュレーション コマンドとともに、このコマンドを使用します。

（注）　出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解した場合に限り、設定を変更します。QoS の詳細については、ソフトウェア コンフィギュレーション ガイドで「*Configuring QoS*」の章を参照してください。

例

次の例では、ポートをキューセット 2 にマッピングする方法を示します。出力キュー 1 にバッファ スペースの 40% を、出力キュー 2、3、および 4 にはそれぞれ 20% ずつ割り当てます。

```
Switch(config)# mls qos queue-set output 2 buffers 40 20 20 20
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# queue-set 2
```

設定を確認するには、**show mls qos interface** [*interface-id*] **buffers** または **show mls qos queue-set** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos queue-set output threshold	Weighted Tail-Drop（WTD）しきい値を設定し、バッファのアベイラビリティを保証し、キューセットに対する最大メモリ割り当てを設定します。
queue-set	ポートをキューセットにマッピングします。
show mls qos interface buffers	Quality of Service（QoS）情報を表示します。
show mls qos queue-set	キューセットの出力キューセット値を表示します。

mls qos queue-set output threshold

Weighted Tail-Drop（WTD）しきい値を設定することで、バッファの可用性を保証し、キューセット（各ポートの 4 つの出力キュー）に対して最大のメモリ割り当てを設定するには、**mls qos queue-set output threshold** グローバル コンフィギュレーション 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-set output *qset-id* **threshold** *queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold*

no mls qos queue-set output *qset-id* **threshold** [*queue-id*]

構文の説明

qset-id	キューセットの ID です。各ポートはキューセットに属し、ポート単位で出力キュー 4 つの特性すべてを定義します。指定できる範囲は 1 ～ 2 です。
queue-id	コマンドが実行されるキューセット内の特定のキューです。指定できる範囲は 1 ～ 4 です。
drop-threshold1 *drop-threshold2*	キューに割り当てられたメモリの割合（%）で表される 2 つの WTD しきい値です。指定できる範囲は 1 ～ 3200% です。
reserved-threshold	キューに対して保証（予約）されるメモリ量です。割り当てられたメモリの割合（%）で表されます。指定できる範囲は 1 ～ 100% です。
maximum-threshold	フル状態のキューが、予約量を超えるバッファを取得できるようにします。これは、キューがパケットをドロップせずに保持できる最大メモリです。指定できる範囲は 1 ～ 3200% です。

デフォルト

Quality of Service（QoS）がイネーブルなときは、WTD もイネーブルです。

表 2-14 は、デフォルトの WTD しきい値の設定値を示しています。

表 2-14　デフォルトの出力キュー WTD しきい値設定値

機能	キュー 1	キュー 2	キュー 3	キュー 4
WTD ドロップしきい値 1	100%	200%	100%	100%
WTD ドロップしきい値 2	100%	200%	100%	100%
予約済みしきい値	50%	100%	50%	50%
最大しきい値	400%	400%	400%	400%

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

mls qos queue-set output *qset-id* **buffers** グローバル コンフィギュレーション コマンドは、キューセット内の 4 つのキューに固定数のバッファを割り当てます。

ドロップしきい値（%）は 100% を超過することができ、最大値まで指定することができます（最大しきい値が 100% を超える場合）。

バッファ範囲により、キューセット内の個々のキューが共通のプールをさらに利用できる場合でも、各キューの最大パケット数は内部で 400%、つまりバッファに割り当てられた数の 4 倍に制限されます。1 つのパケットは 1 つまたは複数のバッファを使用できます。

Cisco IOS Release 12.2(25)SEE1 以降で、*drop-threshold*、*drop-threshold2*、*maximum-threshold* パラメータの範囲が増加しました。

（注）出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

スイッチは、バッファ割り当て方式を使用して、出力キューごとに最小バッファ量を予約し、いずれかのキューまたはポートがすべてのバッファを消費しその他のキューがバッファを使用できなくなるのを防ぎ、バッファ スペースを要求元のキューに許可するかどうかを決定します。スイッチは、ターゲット キューが予約量を超えるバッファを消費していないかどうか（アンダーリミット）、その最大バッファをすべて消費したかどうか（オーバーリミット）、共通のプールが空（空きバッファがない）か空でない（空きバッファ）かを判断します。キューがオーバーリミットでない場合は、スイッチは予約済みプールまたは共通のプール（空でない場合）からバッファ スペースを割り当てることができます。共通のプールに空きバッファがない場合や、キューがオーバーリミットの場合、スイッチはフレームをドロップします。

例

次の例では、ポートをキューセット 2 にマッピングする方法を示します。キュー 2 のドロップしきい値を割り当てられたメモリの 40% と 60% に設定し、割り当てられたメモリの 100% を保証（予約）して、このキューがパケットをドロップせずに保持可能な最大メモリを 200% に設定します。

```
Switch(config)# mls qos queue-set output 2 threshold 2 40 60 100 200
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# queue-set 2
```

設定を確認するには、**show mls qos interface** [*interface-id*] **buffers** または **show mls qos queue-set** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos queue-set output buffers	バッファをキューセットに割り当てます。
queue-set	ポートをキューセットにマッピングします。
show mls qos interface buffers	QoS 情報を表示します。
show mls qos queue-set	キューセットの出力キューセット値を表示します。

mls qos rewrite ip dscp

着信 IP パケットの Differentiated Service Code Point（DSCP）フィールドを変更する（書き換える）ようスイッチを設定するには、**mls qos rewrite ip dscp** グローバル コンフィギュレーション コマンドを使用します。スイッチがパケットの DSCP フィールドを変更（書き換え）しないように設定し、DSCP 透過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。

mls qos rewrite ip dscp

no mls qos rewrite ip dscp

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

DSCP 透過はディセーブルです。スイッチは着信 IP パケットの DSCP フィールドを変更します。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SE	このコマンドが追加されました。

使用上のガイドライン

DSCP 透過は、出力でのパケットの DSCP フィールドにだけ影響を与えます。**no mls qos rewrite ip dscp** コマンドを使用して DSCP 透過がイネーブルになっている場合、スイッチは着信パケットの DSCP フィールドは変更せず、送信パケットの DSCP フィールドも着信パケットのものと同じになります。

（注）　DSCP 透過性をイネーブルにしても、IEEE 802.1Q トンネリング ポート上のポート信頼性の設定には影響しません。

デフォルトでは、DSCP 透過性はディセーブルです。スイッチでは着信パケットの DSCP フィールドが変更され、発信パケットの DSCP フィールドは、ポートの信頼設定、ポリシングとマーキング、DSCP/DSCP 変換マップを含めて Quality of Service（QoS）に基づきます。

DSCP 透過の設定に関係なく、スイッチは、トラフィックのプライオリティを表す Class of Service（CoS）値の生成に使用するパケットの内部 DSCP 値を変更します。また、スイッチは内部 DSCP 値を使用して、出力キューおよびしきい値を選択します。

たとえば、QoS がイネーブルになっていて、着信パケットの DSCP 値が 32 である場合、スイッチは、ポリシー マップ設定に基づいて内部 DSCP 値を 16 に変更します。DSCP 透過がイネーブルになっている場合、送信 DSCP 値は 32（着信の値と同じ）です。DSCP 透過がディセーブルになっている場合、内部 DSCP 値に基づいて、送信 DSCP 値は 16 になります。

例

次の例では、DSCP 透過性をイネーブルにして、スイッチで着信 IP パケットの DSCP 値を変更しないように設定する方法を示しています。

```
Switch(config)# mls qos
Switch(config)# no mls qos rewrite ip dscp
```

次の例では、DSCP 透過性をディセーブルにして、スイッチで着信 IP パケットの DSCP 値を変更するように設定する方法を示しています。

```
Switch(config)# mls qos
Switch(config)# mls qos rewrite ip dscp
```

設定を確認するには、**show running config | include rewrite** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos	QoS をグローバルにイネーブルにします。
show mls qos	QoS 情報を表示します。
show running-config | include rewrite	DSCP 透過性設定を表示します。

mls qos srr-queue input bandwidth

入力キューに Shaped Round Robin（SRR）ウェイトを割り当てるには、**mls qos srr-queue input bandwidth** グローバル コンフィギュレーション コマンドを使用します。重みの比率は、SRR スケジューラがパケットを各キューから送り出す頻度の比率です。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 srr-queue input bandwidth *weight1 weight2*

no mls qos srr-queue input bandwidth

構文の説明

weight1 weight2	*weight1* および *weight2* の比率により、SRR スケジューラがパケットを入力キュー 1 およびキュー 2 から送り出す頻度の比率が決まります。指定できる範囲は 1 ～ 100 です。各値はスペースで区切ります。

デフォルト

weight1 と weight2 は 4 です（帯域幅の 1/2 ずつ 2 つのキューに均等に分配されます）。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

SRR は、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定されたとおり、設定済みの重みに従いプライオリティ キューにサービスを提供します。SRR は、両方の入力キューで残りの帯域幅を共有し、**mls qos srr-queue input bandwidth** *weight1 weight2* グローバル コンフィギュレーション コマンドで設定されたウェイトで指定しているサービスを行います。

どの入力キューがプライオリティ キューであるかを指定するには、**mls qos srr-queue input priority-queue** グローバル コンフィギュレーション コマンドを使用します。

例

次の例では、スタックでキューの入力帯域幅を割り当てる方法を示します。プライオリティ キューイングはディセーブルです。割り当てられる共有帯域幅の比率は、キュー 1 が 25/（25+75）、キュー 2 が 75/（25+75）です。

```
Switch(config)# mls qos srr-queue input priority-queue 2 bandwidth 0
Switch(config)# mls qos srr-queue input bandwidth 25 75
```

この例では、キュー 2 はキュー 1 の 3 倍の帯域幅を持っています。キュー 2 には、キュー 1 の 3 倍の頻度でサービスが提供されます。

次の例では、スタックでキューの入力帯域幅を割り当てる方法を示します。キュー 1 は割り当てられた帯域幅の 10% を持つプライオリティ キューです。キュー 1 とキュー 2 に割り当てられた帯域幅の比率は、4/（4+4）です。SRR は最初、設定された 10% の帯域幅をキュー 1（プライオリティ キュー）にサービスします。その後、SRR は残りの 90% の帯域幅をキュー 1 とキュー 2 にそれぞれ 45% ずつ均等に分配します。

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

設定を確認するには、**show mls qos interface** [*interface-id*] **queueing** または **show mls qos input-queue** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos srr-queue input buffers	入力キュー間のバッファを割り当てます。
mls qos srr-queue input cos-map	Class of Service（CoS）値を入力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue input dscp-map	DSCP 値を入力キューにマッピングするか、DSCP 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue input priority-queue	入力プライオリティ キューを設定し、帯域幅を保証します。
mls qos srr-queue input threshold	Weighted Tail-Drop（WTD）しきい値のパーセンテージを入力キューに割り当てます。
show mls qos input-queue	入力キューの設定を表示します。
show mls qos interface queueing	Quality of Service（QoS）情報を表示します。

mls qos srr-queue input buffers

入力キュー間にバッファを割り当てるには、**mls qos srr-queue input buffers** グローバル コンフィギュレーション 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 srr-queue input buffers *percentage1 percentage2*

no mls qos srr-queue input buffers

構文の説明

percentage1 *percentage2*	入力キュー 1 およびキュー 2 に割り当てられるバッファの割合（%）です。指定できる範囲は 0 ～ 100 です。各値はスペースで区切ります。

デフォルト

バッファの 90% がキュー 1 に、バッファの 10% がキュー 2 に割り当てられます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

キューがバースト性のある着信トラフィックを処理できるようにバッファを割り当てる必要があります。

例

次の例では、入力キュー 1 にバッファ スペースの 60% を、入力キュー 2 にバッファ スペースの 40% を割り当てる方法を示します。

```
Switch(config)# mls qos srr-queue input buffers 60 40
```

設定を確認するには、**show mls qos interface** [*interface-id*] **buffers** または **show mls qos input-queue** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos srr-queue input bandwidth	Shaped Round Robin（SRR）の重みを入力キューに割り当てます。
mls qos srr-queue input cos-map	Class of Service（CoS）値を入力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue input dscp-map	DSCP 値を入力キューにマッピングするか、DSCP 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue input priority-queue	入力プライオリティ キューを設定し、帯域幅を保証します。
mls qos srr-queue input threshold	Weighted Tail-Drop（WTD）しきい値のパーセンテージを入力キューに割り当てます。
show mls qos input-queue	入力キューの設定を表示します。
show mls qos interface buffers	Quality of Service（QoS）情報を表示します。

mls qos srr-queue input cos-map

Class of Service（CoS）値を入力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングするには、**mls qos srr-queue input cos-map** グローバル コンフィギュレーション 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 srr-queue input cos-map queue *queue-id* {*cos1...cos8* | **threshold** *threshold-id cos1...cos8*}

no mls qos srr-queue input cos-map

構文の説明

queue *queue-id*	キュー番号を指定します。 *queue-id* で指定できる範囲は 1 ～ 2 です。
cos1...cos8	CoS 値を入力キューへマッピングします。 *cos1...cos8* には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ～ 7 です。
threshold *threshold-id cos1...cos8*	CoS 値をキューのしきい値 ID にマッピングします。 *threshold-id* で指定できる範囲は 1 ～ 3 です。 *cos1...cos8* には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ～ 7 です。

デフォルト

表 2-15 では、デフォルトの CoS 入力キューしきい値のマッピングを示します。

表 2-15　デフォルトの CoS 入力キューしきい値

CoS 値	キュー ID - しきい値 ID
0 ～ 4	1 - 1
5	2 - 1
6、7	1 - 1

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

入力ポートに割り当てられた CoS によって、入力または出力のキューおよびしきい値が選択されます。

しきい値 3 のドロップしきい値（%）は事前に定義されています。パーセンテージはキューがいっぱいの状態に対して設定されます。**mls qos srr-queue input threshold** グローバル コンフィギュレーション コマンドを使用すると、入力キューに 2 つの Weighted Tail-Drop（WTD）しきい値（%）を割り当てることができます。

各 CoS 値を、異なるキューおよびしきい値の組み合わせに対してマッピングできます。これによりフレームを異なる動作に従わせることができます。

例

次の例では、CoS 値 0 ～ 3 を、入力キュー 1 とドロップしきい値 50% のしきい値 ID 1 にマッピングする方法を示します。CoS 値 4 と 5 は、入力キュー 1 とドロップしきい値 70% のしきい値 ID 2 に割り当てます。

```
Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 2 4 5
Switch(config)# mls qos srr-queue input threshold 1 50 70
```

設定を確認するには、**show mls qos maps** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos srr-queue input bandwidth	Shaped Round Robin（SRR）の重みを入力キューに割り当てます。
mls qos srr-queue input buffers	入力キュー間のバッファを割り当てます。
mls qos srr-queue input dscp-map	DSCP 値を入力キューにマッピングするか、DSCP 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue input priority-queue	入力プライオリティ キューを設定し、帯域幅を保証します。
mls qos srr-queue input threshold	WTD しきい値のパーセンテージを入力キューに割り当てます。
show mls qos maps	QoS のマッピング情報を表示します。

mls qos srr-queue input dscp-map

Differentiated Service Code Point（DSCP）値を入力キューにマッピング、または DSCP 値をキューおよびしきい値 ID にマッピングするには、**mls qos srr-queue input dscp-map** グローバル コンフィギュレーション 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 srr-queue input dscp-map queue *queue-id* {*dscp1...dscp8* | **threshold** *threshold-id dscp1...dscp8*}

no mls qos srr-queue input dscp-map

構文の説明

queue *queue-id*	キュー番号を指定します。 *queue-id* で指定できる範囲は 1 ～ 2 です。
dscp1...dscp8	DSCP 値を入力キューにマッピングします。 *dscp1...dscp8* には、各値をスペースで区切って、最大 8 の値を入力します。指定できる範囲は 0 ～ 63 です。
threshold *threshold-id dscp1...dscp8*	DSCP 値をキューしきい値 ID にマッピングします。 *threshold-id* で指定できる範囲は 1 ～ 3 です。 *dscp1...dscp8* には、各値をスペースで区切って、最大 8 の値を入力します。指定できる範囲は 0 ～ 63 です。

デフォルト

表 2-16 は、デフォルトの DSCP 入力キューしきい値マップを示しています。

表 2-16　デフォルトの DSCP 入力キューしきい値マップ

DSCP 値	キュー ID - しきい値 ID
0 ～ 39	1 - 1
40 ～ 47	2 - 1
48 ～ 63	1 - 1

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

入力ポートに割り当てられた DSCP によって、入力または出力のキューおよびしきい値が選択されます。

しきい値 3 のドロップしきい値（%）は事前に定義されています。パーセンテージはキューがいっぱいの状態に対して設定されます。**mls qos srr-queue input threshold** グローバル コンフィギュレーション コマンドを使用すると、入力キューに 2 つの Weighted Tail-Drop（WTD）しきい値（%）を割り当てることができます。

各 DSCP 値を異なるキューおよびしきい値の組み合わせにマッピングして、フレームが別の方法で処理されるようにすることができます。

コマンドあたり最大 8 個の DSCP 値をマッピングできます。

例

次の例では、DSCP 値 0 ～ 6 を、入力キュー 1 とドロップしきい値 50% のしきい値 1 にマッピングする方法を示します。DSCP 値 20 ～ 26 は、入力キュー 1 とドロップしきい値 70% のしきい値 2 にマッピングします。

```
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 0 1 2 3 4 5 6
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 20 21 22 23 24 25 26
Switch(config)# mls qos srr-queue input threshold 1 50 70
```

設定を確認するには、**show mls qos maps** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos srr-queue input bandwidth	Shaped Round Robin（SRR）の重みを入力キューに割り当てます。
mls qos srr-queue input buffers	入力キュー間のバッファを割り当てます。
mls qos srr-queue input cos-map	Class of Service（CoS）値を入力キューにマッピングするか、CoS 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue input priority-queue	入力プライオリティ キューを設定し、帯域幅を保証します。
mls qos srr-queue input threshold	WTD しきい値のパーセンテージを入力キューに割り当てます。
show mls qos maps	QoS のマッピング情報を表示します。

mls qos srr-queue input priority-queue

リングが輻輳している場合、入力プライオリティ キューを設定して、スタック リング上で帯域幅を保証するには、**mls qos srr-queue input priority-queue** グローバル コンフィギュレーション 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 srr-queue input priority-queue *queue-id* **bandwidth** *weight*

no mls qos srr-queue input priority-queue *queue-id*

構文の説明

queue-id	入力のキュー ID。指定できる範囲は 1 ～ 2 です。
bandwidth *weight*	スタック リングの帯域幅のパーセンテージ。指定できる範囲は 0 ～ 40 です。

デフォルト

プライオリティ キューはキュー 2 で、帯域幅の 10% が割り当てられています。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

プライオリティ キューは、優先して進める必要があるトラフィックに限り使用してください（遅延とジッタを最小限にとどめる必要のある音声トラフィックなど）。

プライオリティ キューはスタック リング上で帯域幅の一部が保証されており、オーバーサブスクライブ型のスタック上でネットワーク トラフィックが多い場合（バックプレーンが送達できる量よりもトラフィックが多い場合、およびキューが満杯でフレームをドロップしている場合）に、遅延とジッタを軽減します。

大きい値はスタック全体に影響を与え、スタック パフォーマンスを低下させるため、保証される帯域幅の合計は制限されます。

Shaped Round Robin（SRR）は、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定されたとおり、設定済みの重みに従いプライオリティ キューにサービスを提供します。SRR は、両方の入力キューで残りの帯域幅を共有し、**mls qos srr-queue input bandwidth** *weight1 weight2* グローバル コンフィギュレーション コマンドで設定されたウェイトで指定しているサービスを行います。

プライオリティ キューイングをディセーブルにするには、帯域幅の重みを 0 に設定します。たとえば、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth 0** と入力します。

例

次の例では、スタックでキューの入力帯域幅を割り当てる方法を示します。キュー 1 は割り当てられた帯域幅の 10% を持つプライオリティ キューです。キュー 1 とキュー 2 に割り当てられた帯域幅の比率は、4/（4+4）です。SRR は最初、設定された 10% の帯域幅をキュー 1（プライオリティ キュー）にサービスします。その後、SRR は残りの 90% の帯域幅をキュー 1 とキュー 2 にそれぞれ 45% ずつ均等に分配します。

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

設定を確認するには、**show mls qos interface** [*interface-id*] **queueing** または **show mls qos input-queue** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos srr-queue input bandwidth	Shaped Round Robin（SRR）の重みを入力キューに割り当てます。
mls qos srr-queue input buffers	入力キュー間のバッファを割り当てます。
mls qos srr-queue input cos-map	Class of Service（CoS）値を入力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue input dscp-map	DSCP 値を入力キューにマッピングするか、DSCP 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue input threshold	Weighted Tail-Drop（WTD）しきい値のパーセンテージを入力キューに割り当てます。
show mls qos input-queue	入力キューの設定を表示します。
show mls qos interface queueing	Quality of Service（QoS）情報を表示します。

mls qos srr-queue input threshold

入力キューに Weighted Tail-Drop（WTD）しきい値のパーセンテージを割り当てるには、**mls qos srr-queue input threshold** グローバル コンフィギュレーション 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 srr-queue input threshold *queue-id threshold-percentage1 threshold-percentage2*

no mls qos srr-queue input threshold *queue-id*

構文の説明

queue-id	入力キューの ID です。指定できる範囲は 1 ～ 2 です。
threshold-percentage1 *threshold-percentage2*	2 つの WTD しきい値（%）です。各しきい値は、キューに割り当てられたキュー記述子の総数に対する割合です。各値はスペースで区切ります。指定できる範囲は 1 ～ 100 です。

デフォルト

Quality of Service（QoS）がイネーブルなときは、WTD もイネーブルです。

2 つの WTD しきい値は、100% に設定されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

QoS は、CoS/ しきい値マップまたは DSCP/ しきい値マップを使用して、どの Class of Service（CoS）値または Differentiated Service Code Point（DSCP）値をしきい値 1 としきい値 2 にマッピングするかを判別します。しきい値 1 を超えた場合は、しきい値を超えなくなるまで、このしきい値に割り当てられた CoS または DSCP を持つパケットがドロップされます。ただし、しきい値 2 に割り当てられたパケットは、2 番目のしきい値を超えることがない限り、引き続きキューに入れられ送信されます。

各キューには、2 つの設定可能な（明示）ドロップしきい値と 1 つの事前設定された（暗黙）ドロップしきい値（フル）があります。

CoS/ しきい値マップを設定するには、**mls qos srr-queue input cos-map** グローバル コンフィギュレーション コマンドを使用します。DSCP/ しきい値マップを設定するには、**mls qos srr-queue input dscp-map** グローバル コンフィギュレーション コマンドを使用します。

例

次の例では、2 つのキューにテールドロップしきい値を設定する方法を示します。キュー 1 のしきい値は 50% と 100%、キュー 2 のしきい値は 70% と 100% です。

```
Switch(config)# mls qos srr-queue input threshold 1 50 100
Switch(config)# mls qos srr-queue input threshold 2 70 100
```

設定を確認するには、**show mls qos interface** [*interface-id*] **buffers** または **show mls qos input-queue** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos srr-queue input bandwidth	Shaped Round Robin（SRR）の重みを入力キューに割り当てます。
mls qos srr-queue input buffers	入力キュー間のバッファを割り当てます。
mls qos srr-queue input cos-map	Class of Service（CoS）値を入力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue input dscp-map	DSCP 値を入力キューにマッピングするか、DSCP 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue input priority-queue	入力プライオリティ キューを設定し、帯域幅を保証します。
show mls qos input-queue	入力キューの設定を表示します。
show mls qos interface buffers	Quality of Service（QoS）情報を表示します。

mls qos srr-queue output cos-map

Class of Service（CoS）値を出力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングするには、**mls qos srr-queue output cos-map** グローバル コンフィギュレーション 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 srr-queue output cos-map queue *queue-id* {*cos1...cos8* | **threshold** *threshold-id cos1...cos8*}

no mls qos srr-queue output cos-map

構文の説明

queue *queue-id*	キュー番号を指定します。 *queue-id* で指定できる範囲は 1 ～ 4 です。
cos1...cos8	CoS 値を出力キューへマッピングします。 *cos1...cos8* には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ～ 7 です。
threshold *threshold-id cos1...cos8*	CoS 値をキューのしきい値 ID にマッピングします。 *threshold-id* で指定できる範囲は 1 ～ 3 です。 *cos1...cos8* には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ～ 7 です。

デフォルト

表 2-17 では、デフォルトの CoS 出力キューしきい値のマッピングを示します。

表 2-17　デフォルトの CoS 出力キューしきい値マップ

CoS 値	キュー ID - しきい値 ID
0、1	2 - 1
2、3	3 - 1
4	4 - 1
5	1 - 1
6、7	4 - 1

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

しきい値 3 のドロップしきい値（%）は事前に定義されています。パーセンテージはキューがいっぱいの状態に対して設定されます。

（注）出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、これらの設定がユーザの Quality of Service（QoS）ソリューションを満たさないと判断した場合に限り、設定を変更することができます。

mls qos queue-set output *qset-id* **threshold** グローバル コンフィギュレーション コマンドを使用すると、出力キューに 2 つの Weighted Tail-Drop（WTD）しきい値（%）を割り当てることができます。

各 CoS 値を、異なるキューおよびしきい値の組み合わせに対してマッピングできます。これによりフレームを異なる動作に従わせることができます。

例

次の例では、ポートをキューセット 1 にマッピングする方法を示します。CoS 値 0 ～ 3 を出力キュー 1 としきい値 ID 1 にマッピングします。キュー 1 のドロップしきい値を割り当てられたメモリの 50% と 70% に設定し、割り当てられたメモリの 100% を保証（予約）して、このキューがパケットをドロップせずに保持できる最大メモリを 200% に設定します。

```
Switch(config)# mls qos srr-queue output cos-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos queue-set output 1 threshold 1 50 70 100 200
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# queue-set 1
```

設定を確認するには、**show mls qos maps**、**show mls qos interface** [*interface-id*] **buffers**、または **show mls qos queue-set** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos srr-queue output dscp-map	Differentiated Service Code Point（DSCP）値を出力キュー、またはキューとしきい値 ID にマッピングします。
mls qos queue-set output threshold	WTD しきい値を設定して、バッファのアベイラビリティを保証し、キューセットへの最大メモリ割り当てを設定します。
queue-set	ポートをキューセットにマッピングします。
show mls qos interface buffers	QoS 情報を表示します。
show mls qos maps	QoS のマッピング情報を表示します。
show mls qos queue-set	キューセットの出力キューセット値を表示します。

mls qos srr-queue output dscp-map

Differentiated Service Code Point（DSCP）値を出力キューにマッピングするか、または DSCP 値をキューおよびしきい値 ID にマッピングするには、**mls qos srr-queue output dscp-map** グローバル コンフィギュレーション 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 srr-queue output dscp-map queue *queue-id* {*dscp1...dscp8* | **threshold** *threshold-id dscp1...dscp8*}

no mls qos srr-queue output dscp-map

構文の説明

queue *queue-id*	キュー番号を指定します。 *queue-id* で指定できる範囲は 1 ～ 4 です。
dscp1...dscp8	DSCP 値を出力キューにマッピングします。 *dscp1...dscp8* には、各値をスペースで区切って、最大 8 の値を入力します。指定できる範囲は 0 ～ 63 です。
threshold *threshold-id dscp1...dscp8*	DSCP 値をキューしきい値 ID にマッピングします。 *threshold-id* で指定できる範囲は 1 ～ 3 です。 *dscp1...dscp8* には、各値をスペースで区切って、最大 8 の値を入力します。指定できる範囲は 0 ～ 63 です。

デフォルト

表 2-18 は、デフォルトの DSCP 出力キューしきい値マップを示しています。

表 2-18　デフォルトの DSCP 出力キューしきい値マップ

DSCP 値	キュー ID - しきい値 ID
0 ～ 15	2 - 1
16 ～ 31	3 - 1
32 ～ 39	4 - 1
40 ～ 47	1 - 1
48 ～ 63	4 - 1

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

しきい値 3 のドロップしきい値（%）は事前に定義されています。パーセンテージはキューがいっぱいの状態に対して設定されます。

（注）出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

mls qos queue-set output *qset-id* **threshold** グローバル コンフィギュレーション コマンドを使用すると、出力キューに 2 つの Weighted Tail-Drop（WTD）しきい値（%）を割り当てることができます。

各 DSCP 値を異なるキューおよびしきい値の組み合わせにマッピングして、フレームが別の方法で処理されるようにすることができます。

コマンドあたり最大 8 個の DSCP 値をマッピングできます。

例

次の例では、ポートをキューセット 1 にマッピングする方法を示します。DSCP 値 0 ～ 3 を出力キュー 1 としきい値 ID 1 にマッピングします。キュー 1 のドロップしきい値を割り当てられたメモリの 50% と 70% に設定し、割り当てられたメモリの 100% を保証（予約）して、このキューがパケットをドロップせずに保持できる最大メモリを 200% に設定します。

```
Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos queue-set output 1 threshold 1 50 70 100 200
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# queue-set 1
```

設定を確認するには、**show mls qos maps**、**show mls qos interface** [*interface-id*] **buffers**、または **show mls qos queue-set** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos srr-queue output cos-map	Class of Service（CoS）値を出力キュー、またはキューとしきい値 ID にマッピングします。
mls qos queue-set output threshold	WTD しきい値を設定して、バッファのアベイラビリティを保証し、キューセットへの最大メモリ割り当てを設定します。
queue-set	ポートをキューセットにマッピングします。
show mls qos interface buffers	Quality of Service（QoS）情報を表示します。
show mls qos maps	QoS のマッピング情報を表示します。
show mls qos queue-set	キューセットの出力キューセット値を表示します。

mls qos trust

ポートの信頼状態を設定するには、**mls qos trust** 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。入力トラフィックを信頼できるようになり、パケットの Differentiated Service Code Point（DSCP）、Class of Service（CoS）、または IP precedence のフィールドを調べることにより分類が実行されます。ポートを信頼できない状態に戻すには、このコマンドの **no** 形式を使用します。

mls qos trust [**cos** | **device cisco-phone** | **dscp** | **ip-precedence**]

no mls qos trust [**cos** | **device** | **dscp** | **ip-precedence**]

構文の説明

cos	（任意）パケットの CoS 値を使用して、入力パケットを分類します。タグのないパケットについては、ポートのデフォルト CoS 値を使用します。
device cisco-phone	（任意）信頼設定に応じて、Cisco IP Phone（信頼される境界）から送信された CoS または DSCP 値を信頼することにより入力パケットを分類します。
dscp	（任意）パケット DSCP 値（8 ビット サービスタイプ フィールドの上位 6 ビット）を使用して、入力パケットを分類します。非 IP パケットでパケットがタグ付きの場合は、パケット CoS が使用されます。タグなしパケットの場合は、デフォルトのポート CoS 値が使用されます。
ip-precedence	（任意）パケットの IP precedence 値（8 ビット サービスタイプ フィールドの上位 3 ビット）を使用して、入力パケットを分類します。非 IP パケットでパケットがタグ付きの場合は、パケット CoS が使用されます。タグのない IP パケットの場合、ポートのデフォルトの CoS 値が使用されます。

デフォルト

ポートは信頼されていません。キーワードを指定せずにコマンドを入力した場合、デフォルトは **dscp** 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**device cisco-phone** キーワードが追加されました。
12.2(20)SE	使用上のガイドラインが改訂されて、Cisco IP Phone がスイッチまたはルーテッド ポートに接続された場合のスイッチの信頼状態の設定方法が説明されています。

使用上のガイドライン

Quality of Service（QoS）ドメインに着信するパケットは、ドメインのエッジで分類されます。パケットがエッジで分類されると、QoS ドメイン内の各スイッチでパケットを分類する必要がないので、QoS ドメイン内のスイッチ ポートはいずれか 1 つの信頼状態に設定できます。ポートが信頼されているかどうか、またどのパケットのフィールドがトラフィックの分類に使用されるのかを指定する場合に、このコマンドを使用します。

ポートに信頼 DSCP または信頼 IP precedence が設定され、着信パケットが非 IP パケットの場合は、CoS/DSCP マップを使用して、CoS 値から対応する DSCP 値が導き出されます。CoS は、トランクポートの場合はパケット CoS、非トランク ポートの場合はデフォルトのポート CoS となります。

DSCP が信頼されている場合、IP パケットの DSCP フィールドは変更されません。ただし、パケットの CoS 値を（DSCP/CoS マップに基づいて）変更することは可能です。

CoS が信頼されている場合、パケットの CoS フィールドは変更されませんが、IP パケットである場合には（CoS/DSCP マップに基づいて）DSCP を変更することはできます。

信頼境界機能は、ユーザがネットワーク化された Cisco IP Phone から PC を切断し、これをスイッチポートに接続して信頼された CoS または DSCP 設定を利用する場合のセキュリティ問題の発生を防止します。スイッチおよび IP Phone に接続されたポートで Cisco Discovery Protocol（CDP）をグローバルにイネーブルにする必要があります。IP Phone が検出されなかった場合、信頼境界機能はスイッチまたはルーテッド ポートの信頼設定をディセーブルにし、高プライオリティ キューが誤って使用されないようにします。

DSCP または IP precedence の信頼設定を行うと、着信パケットの DSCP 値または IP precedence 値が信頼されます。IP Phone に接続するスイッチ ポートで **mls qos cos override** インターフェイス コンフィギュレーション コマンドを設定すると、スイッチは着信音声およびデータパケットの CoS を無効にし、デフォルトの CoS 値をそれらに割り当てます。

QoS ドメイン間境界の場合は、ポートを DSCP 信頼状態に設定し、DSCP 値が QoS ドメイン間で異なる場合は DSCP/DSCP 変換マップを適用することができます。

ポート信頼状態を使用した分類（たとえば、**mls qos trust** [**cos** | **dscp** | **ip-precedence**]）とポリシーマップ（たとえば、**service-policy input** *policy-map-name*）は同時に指定できません。最後に行われた設定により、前の設定が上書きされます。

（注）　Cisco IOS Release 12.2(52)SE 以降では、デュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートを持つ IPv6 ポート ベースのトラストをサポートしています。IPv6 が動作しているスイッチのデュアル IPv4/IPv6 テンプレートを持つスイッチをリロードする必要があります。

例

次の例では、着信パケットの IP precedence フィールドを信頼するようにポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# mls qos trust ip-precedence
```

次の例では、ポートに接続している Cisco IP Phone が信頼できる装置であると指定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# mls qos trust device cisco-phone
```

show mls qos interface 特権 EXEC コマンドを入力すると、設定を確認できます。

関連コマンド

コマンド	説明
mls qos cos	デフォルトのポート CoS 値を定義するか、あるいはポートのすべての着信パケットにデフォルトの CoS 値を割り当てます。
mls qos dscp-mutation	DSCP/DSCP 変換マップを DSCP の信頼できるポートに適用します。

コマンド	説明
mls qos map	CoS/DSCP マップ、DSCP/CoS マップ、DSCP/DSCP 変換マップ、IP precedence/DSCP マップ、およびポリシング設定 DSCP マップを定義します。
show mls qos interface	QoS 情報を表示します。

mls qos vlan-based

物理ポート上で VLAN ベースの Quality of Service（QoS）をイネーブルにするには、**mls qos vlan-based** 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。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。

mls qos vlan-based

no mls qos vlan-based

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

VLAN ベースの QoS 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

コマンド履歴

リリース	変更内容
12.2(25)SE	このコマンドが追加されました。

使用上のガイドライン

階層ポリシー マップを Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）に適用するには、階層ポリシー マップのセカンダリ インターフェイス レベルでポートを指定するときに、物理ポートで **mls qos vlan-based** 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。

階層ポリシングを設定すると、階層ポリシー マップは SVI に適用され、VLAN に属するすべてのトラフィックに反映されます。インターフェイス レベルのトラフィック分類における個々のポリサーは、分類に従って指定された物理ポートだけに反映されます。

階層型ポリシー マップを設定する詳細な手順については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Classifying, Policing, and Marking Traffic by Using Hierarchical Policy Maps」の項を参照してください。

例

次の例では、物理ポート上で VLAN ベースのポリシングをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# mls qos vlan-based
```

show mls qos interface 特権 EXEC コマンドを入力すると、設定を確認できます。

関連コマンド

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

monitor session

新規に Switched Port Analyzer（SPAN）セッションまたは Remote SPAN（RSPAN）の送信元または宛先セッションを開始するには、**monitor session** グローバル コンフィギュレーション コマンドを使用します。これにより、ネットワーク セキュリティ デバイス（Cisco IDS センサー アプライアンスなど）の宛先ポート上にある入力トラフィックをイネーブルにして、既存の SPAN または RSPAN セッションでのインターフェイスまたは VLAN の追加または削除を実行し、SPAN 送信元トラフィックを特定 VLAN に制限（フィルタリング）します。SPAN または RSPAN セッションを削除したり、SPAN または RSPAN セッションから送信元/宛先インターフェイスまたはフィルタを削除したりするには、このコマンドの **no** 形式を使用します。宛先インターフェイスに対してこのコマンドの **no** 形式を使用すると、カプセル化オプションは無視されます。

monitor session *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation replicate**] [**ingress** {**dot1q vlan** *vlan-id* | **isl** | **untagged vlan** *vlan-id* | **vlan** *vlan-id*}]} | {**remote vlan** *vlan-id*}

monitor session *session_number* **filter vlan** *vlan-id* [, | -]

monitor session *session_number* **source** {**interface** *interface-id* [, | -] [**both** | **rx** | **tx**]} | {**vlan** *vlan-id* [, | -] [**both** | **rx** | **tx**]}| {**remote vlan** *vlan-id*}

no monitor session {*session_number* | **all** | **local** | **remote**}

no monitor session *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation replicate**] [**ingress** {**dot1q vlan** *vlan-id* | **isl** | **untagged vlan** *vlan-id* | **vlan** *vlan-id*}]} | {**remote vlan** *vlan-id*}

no monitor session *session_number* **filter vlan** *vlan-id* [, | -]

no monitor session *session_number* **source** {**interface** *interface-id* [, | -] [**both** | **rx** | **tx**]} | {**vlan** *vlan-id* [, | -] [**both** | **rx** | **tx**]} | {**remote vlan** *vlan-id*}

構文の説明

session_number	SPAN または RSPAN セッションで識別されるセッション番号を指定します。指定できる範囲は 1 ～ 66 です。
destination	SPAN または RSPAN の宛先を指定します。宛先は物理ポートである必要があります。
interface *interface-id*	SPAN または RSPAN セッションの宛先または送信元インターフェイスを指定します。有効なインターフェイスは物理ポート（タイプ、スタック メンバ、モジュール、ポート番号を含む）です。送信元インターフェイスの場合は、ポート チャネルも有効なインターフェイス タイプであり、指定できる範囲は 1 ～ 48 です。
encapsulation replicate	（任意）宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 次のキーワードは、ローカル SPAN にだけ有効です。RSPAN、RSPAN VLAN ID は元の VLAN ID を上書きするため、パケットは常にタグなしで送信されます。
ingress	（任意）入力トラフィック転送をイネーブルにします。
dot1q vlan *vlan-id*	デフォルト VLAN として指定された VLAN で IEEE 802.1Q カプセル化を持つ着信パケットを受け入れます。

isl	ISL（スイッチ間リンク）カプセル化を使用して入力トラフィックを転送するように指定します。
untagged vlan *vlan-id*	デフォルト VLAN として指定された VLAN でタグなしカプセル化を持つ着信パケットを受け入れます。
vlan *vlan-id*	**ingress** キーワードだけで使用された場合、入力トラフィックにデフォルトの VLAN を設定します。
remote vlan *vlan-id*	RSPAN 送信元または宛先セッションのリモート VLAN を指定します。指定できる範囲は 2 ～ 1001 または 1006 ～ 4094 です。 RSPAN VLAN は VLAN 1（デフォルトの VLAN）、または VLAN ID 1002 ～ 1005（トークンリングおよび FDDI VLAN に予約済）になることはできません。
,	（任意）一連のインターフェイスまたは VLAN を指定します。または、以前の範囲からインターフェイスまたは VLAN の範囲を分離します。カンマの前後にスペースを入れます。
-	（任意）インターフェイスまたは VLAN の範囲を指定します。ハイフンの前後にスペースを入れます。
filter vlan *vlan-id*	SPAN 送信元トラフィックを特定の VLAN に制限するため、トランクの送信元ポート上のフィルタとして VLAN のリストを指定します。*vlan-id* で指定できる範囲は 1 ～ 4094 です。
source	SPAN または RSPAN の送信元を指定します。物理ポート、ポート チャネル、VLAN が送信元になることができます。
both、**rx**、**tx**	（任意）モニタリングするトラフィックの方向を指定します。トラフィックの方向を指定しない場合、送信元インターフェイスは送受信のトラフィックを送信します。
source vlan *vlan-id*	VLAN ID として SPAN の送信元インターフェイスを指定します。指定できる範囲は 1 ～ 4094 です。
all、**local**、**remote**	すべての SPAN および RSPAN、すべてのローカル SPAN、すべての RSPAN セッションをクリアするため、**no monitor session** コマンドに **all**、**local**、**remote** を指定します。

デフォルト

モニタ セッションは設定されていません。

送信元インターフェイスのデフォルトでは、受信トラフィックと送信トラフィックの両方をモニタリングします。

送信元ポートとして使用されるトランク インターフェイス上では、すべての VLAN がモニタリングされます。

ローカル SPAN の宛先ポートで **encapsulation replicate** が指定されなかった場合、パケットはカプセル化のタグなしのネイティブ形式で送信されます。

入力転送は宛先ポートではディセーブルになっています。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**ingress** {**dot1q vlan** *vlan-id* | **isl** | **untagged vlan** *vlan-id* | **vlan** *vlan-id*} キーワードが追加されました。

使用上のガイドライン

送信元ポートまたは送信元 VLAN を出入りするトラフィックは、SPAN または RSPAN を使用してモニタできます。送信元ポートまたは送信元 VLAN にルーティングされるトラフィックはモニタできません。

2 つのローカル SPAN セッションおよび RSPAN 送信元セッションを組み合わせた最大値を設定することができます。スイッチまたはスイッチ スタック上で、合計 66 の SPAN および RSPAN セッションを保有できます。

スイッチ スタック上で、最大 64 の宛先ポートを保有できます。

SPAN または RSPAN の宛先ポートとして 10 ギガビット イーサネット ポートを設定すると、リンクの回線速度は低下します。

各セッションには複数の入力または出力の送信元ポートまたは VLAN を含めることができますが、1 つのセッション内で送信元ポートと送信元 VLAN を組み合わせることはできません。各セッションは複数の宛先ポートを保有できます。

VLAN-based SPAN（VSPAN）を使用して、VLAN または一連の VLAN 内のネットワーク トラフィックを解析する場合、送信元 VLAN のすべてのアクティブ ポートが SPAN または RSPAN セッションの送信元ポートになります。トランク ポートは VSPAN の送信元ポートとして含まれ、モニタリングされた VLAN ID のパケットだけが宛先ポートに送信されます。

1 つのポート、1 つの VLAN、一連のポート、一連の VLAN、ポート範囲、VLAN 範囲でトラフィックをモニタできます。**[,** | **-]** オプションを使用することにより、一連のインターフェイスまたはインターフェイス範囲、一連の VLAN または VLAN 範囲を指定します。

一連の VLAN またはインターフェイスを指定するときは、カンマ（,）の前後にスペースが必要です。VLAN またはインターフェイスの範囲を指定するときは、ハイフン（-）の前後にスペースが必要です。

EtherChannel ポートは、SPAN または RSPAN 宛先ポートとして設定することはできません。EtherChannel グループのメンバである物理ポートは、宛先ポートとして使用できます。ただし、SPAN の宛先として機能する間は、EtherChannel グループに参加できません。

プライベート VLAN ポートは、SPAN 宛先ポートには設定できません。

個々のポートはそれらが EtherChannel に参加している間もモニタリングすることができます。また、RSPAN 送信元インターフェイスとして **port-channel** 番号を指定することで EtherChannel バンドル全体をモニタリングすることができます。

宛先ポートとして使用しているポートは、SPAN または RSPAN 送信元ポートにすることはできません。また、同時に複数のセッションの宛先ポートにすることはできません。

SPAN または RSPAN 宛先ポートであるポート上で IEEE 802.1x 認証をイネーブルにすることはできますが、ポートが SPAN 宛先として削除されるまで IEEE 802.1x 認証はディセーブルです。IEEE 802.1x 認証がポート上で使用できない場合、スイッチはエラー メッセージを返します。SPAN または RSPAN 送信元ポートでは IEEE 802.1x 認証をイネーブルにすることができます。

VLAN のフィルタリングは、トランクの送信元ポート上で選択された一連の VLAN のネットワーク トラフィック解析を参照します。デフォルトでは、すべての VLAN がトランクの送信元ポートでモニタリングされます。**monitor session** *session_number* **filter vlan** *vlan-id* コマンドを使用すると、トランク送信元ポートの SPAN トラフィックを指定された VLAN だけに限定できます。

VLAN のモニタリングおよび VLAN のフィルタリングは相互に排他的な関係です。VLAN が送信元の場合、VLAN のフィルタリングはイネーブルにできません。VLAN のフィルタリングが設定されている場合、VLAN は送信元になることができません。

入力トラフィック転送がネットワーク セキュリティ デバイスでイネーブルの場合、宛先ポートはレイヤ 2 でトラフィックを転送します。

宛先ポートは次のような動作を設定できます。

- 他のキーワードなしで、**monitor session** *session_number* **destination interface** *interface-id* を入力した場合、出力のカプセル化はタグなしとなり、入力転送はイネーブルになりません。
- **monitor session** *session_number* **destination interface** *interface-id* **ingress** を入力した場合は、出力カプセル化はタグなしで、入力カプセル化はその後に続くキーワードが **dot1q**、**isl**、または **untagged** のいずれであるかによって決まります。
- その他のキーワードを指定せずに、**monitor session** *session_number* **destination interface** *interface-id* **encapsulation replicate** を入力した場合は、出力カプセル化は送信元インターフェイス カプセル化を複製し、入力トラフィック転送はイネーブルにはなりません。（これはローカル SPAN だけに適用します。RSPAN はカプセル化の複製をサポートしていません）。
- **monitor session** *session_number* **destination interface** *interface-id* **encapsulation replicate ingress** を入力した場合は、出力カプセル化は送信元インターフェイスのカプセル化を複製し、入力カプセル化はその後に続くキーワードが、**dot1q**、**isl**、または **untagged** のいずれであるかによって決まります。（これはローカル SPAN だけに適用します。RSPAN はカプセル化の複製をサポートしていません）。

例

次の例では、ローカル SPAN セッション 1 を作成し、スタック メンバ 1 の送信元ポート 1 からスタック メンバ 2 の宛先ポート 2 に送受信するトラフィックをモニタリングする方法を示します。

```
Switch(config)# monitor session 1 source interface gigabitethernet2/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet2/0/2
```

次の例では、宛先ポートを既存のローカル SPAN セッションから削除する方法を示します。

```
Switch(config)# no monitor session 2 destination gigabitethernet2/0/2
```

次の例では、既存のセッションの SPAN トラフィックを指定の VLAN だけに制限する方法を示します。

```
Switch(config)# monitor session 1 filter vlan 100 - 110
```

次の例では、複数の送信元インターフェイスをモニタリングする RSPAN 送信元セッション 1 を設定し、さらに宛先 RSPAN VLAN 900 を設定する方法を示します。

```
Switch(config)# monitor session 1 source interface gigabitethernet2/0/1
Switch(config)# monitor session 1 source interface port-channel 2 tx
Switch(config)# monitor session 1 destination remote vlan 900
Switch(config)# end
```

次の例では、モニタリングされたトラフィックを受信するスイッチに、RSPAN 宛先セッション 10 を設定する方法を示します。

```
Switch(config)# monitor session 10 source remote vlan 900
Switch(config)# monitor session 10 destination interface gigabitethernet2/0/2
```

次の例では、IEEE 802.1Q カプセル化をサポートするセキュリティ装置を使用して、VLAN 5 の入力トラフィックに対応する宛先ポートを設定する方法を示します。出力トラフィックは送信元のカプセル化を複製します。入力トラフィックは IEEE 802.1Q カプセル化を使用します。

```
Switch(config)# monitor session 2 destination interface gigabitethernet2/0/2 encapsulation
replicate ingress dot1q vlan 5
```

次の例では、カプセル化をサポートしないセキュリティ デバイスを使用して、VLAN 5 上の入力トラフィックの宛先ポートを設定する方法を示します。出力トラフィックおよび入力トラフィックはタグなしです。

```
Switch(config)# monitor session 2 destination interface gigabitethernet2/0/2 ingress
untagged vlan 5
```

設定を確認するには、**show monitor** 特権 EXEC コマンドを入力します。**show running-config** 特権 EXEC コマンドを入力すると、スイッチの SPAN および RSPAN 設定を表示することができます。SPAN 情報は出力の最後付近に表示されます。

関連コマンド

コマンド	説明
remote-span	vlan コンフィギュレーション モードで RSPAN VLAN を設定します。
show monitor	SPAN および RSPAN セッション情報を表示します。
show running-config	現在の動作設定を表示します。

mvr（グローバル コンフィギュレーション）

スイッチ上の Multicast VLAN Registration（MVR）機能をイネーブルにするには、キーワードを指定せずに **mvr** グローバル コンフィギュレーション コマンドを使用します。このコマンドをキーワードとともに使用すると、スイッチの MVR モードの設定、MVR IP マルチキャスト アドレスの設定、またはグループ メンバシップからのポートの削除を行う前に、クエリーの返答を待つ最大時間の設定、または MVR マルチキャスト VLAN の指定が行われます。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。

mvr [**group** *ip-address* [*count*] | **mode** [**compatible** | **dynamic**] | **querytime** *value* | **vlan** *vlan-id*]

no mvr [**group** *ip-address* | **mode** [**compatible** | **dynamic**] | **querytime** *value* | **vlan** *vlan-id*]

構文の説明

group *ip-address*	スイッチの MVR グループ IP マルチキャスト アドレスをスタティックに設定します。 スタティックに設定した IP マルチキャスト アドレスまたは連続アドレスを削除したり、IP アドレスが入力されない場合にすべてのスタティックに設定された MVR IP マルチキャスト アドレスを削除したりする場合は、このコマンドの **no** 形式を使用します。
count	（任意）複数の連続 MVR グループ アドレスを設定します。指定できる範囲は 1 ～ 256 です。デフォルト値は 1 です。
mode	（任意）MVR の動作モードを指定します。 デフォルトは compatible モードです。
compatible	MVR モードを設定して、Catalyst 2900 XL および Catalyst 3500 XL スイッチと互換性を持つようにします。このモードでは、送信元ポートでのダイナミック メンバシップ加入は使用できません。
dynamic	MVR モードを設定して、送信元ポートでダイナミック MVR メンバシップを使用できるようにします。
querytime *value*	（任意）レシーバ ポートで IGMP レポート メンバシップを待機する最大時間を設定します。この時間は、レシーバ ポート脱退処理にだけ適用されます。IGMP クエリーがレシーバ ポートから送信された場合、スイッチは、デフォルトまたは設定された MVR クエリー時間が経過するまで IGMP グループ メンバシップ レポートを待ってから、ポートをマルチキャスト グループ メンバシップから削除します。 この値は 10 分の 1 秒単位の応答時間です。指定できる範囲は 1 ～ 100 です。デフォルトは 5/10 秒つまり 1/2 秒です。 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。
vlan *vlan-id*	（任意）MVR マルチキャスト データの受信が予想される VLAN を指定します。これは、すべての送信元ポートが属する VLAN でもあります。指定できる範囲は 1 ～ 4094 です。デフォルト値は VLAN 1 です。

デフォルト

MVR はデフォルトでディセーブルです。

デフォルトの MVR モードは、compatible モードです。

IP マルチキャスト アドレスは、デフォルトではスイッチで設定されます。

デフォルトのグループ IP アドレス カウントは 0 です。

デフォルトのクエリー応答時間は 5/10 秒つまり 1/2 秒です。

デフォルトの MVR 用マルチキャスト VLAN は VLAN 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

最大 256 の MVR マルチキャスト グループを 1 つのスイッチで設定できます。

MVR に属するすべての IP マルチキャスト アドレスをスタティックに設定する場合は、**mvr group** コマンドを使用します。設定したマルチキャスト アドレスに送信されたマルチキャスト データは、スイッチのすべての送信元ポートおよびその IP マルチキャスト アドレスでデータを受信するよう登録されたすべてのレシーバ ポートに送信されます。

MVR はスイッチのエイリアス IP マルチキャスト アドレスをサポートします。ただし、スイッチが Catalyst 3550 または Catalyst 3500 XL スイッチと連携動作している場合は、それらの間でエイリアスとして使用される IP アドレスや予約済みの IP マルチキャスト アドレス（224.0.0.xxx 範囲内）を設定する必要はありません。

mvr querytime コマンドはレシーバ ポートだけに適用されます。

スイッチ MVR が、Catalyst 2900 XL または Catalyst 3500 XL スイッチと相互動作している場合は、マルチキャスト モードを compatible に設定してください。

compatible モードで動作している場合は、MVR は MVR 送信元ポートでの IGMP ダイナミック加入をサポートしません。

MVR はスイッチで IGMP スヌーピングと共存できます。

マルチキャスト ルーティングおよび MVR はスイッチ上で共存できません。MVR がイネーブルになっている状態で、マルチキャスト ルーティングおよびマルチキャスト ルーティング プロトコルをイネーブルにした場合、MVR はディセーブルになり、警告メッセージが表示されます。マルチキャスト ルーティングおよびマルチキャスト ルーティング プロトコルがイネーブルの状態で、MVR をイネーブルにしようとすると、MVR をイネーブルにする操作はキャンセルされ、エラー メッセージが表示されます。

例

次の例では、MVR をイネーブルにする方法を示します。

```
Switch(config)# mvr
```

show mvr 特権 EXEC コマンドを使用すると、最大のマルチキャスト グループの現在の設定を表示できます。

次の例では、228.1.23.4 を IP マルチキャスト アドレスとして設定する方法を示します。

```
Switch(config)# mvr group 228.1.23.4
```

次の例では、228.1.23.1 ～ 228.1.23.10 のマルチキャスト アドレスとともに 10 の連続 IP マルチキャスト グループを設定する方法を示します。

```
Switch(config)# mvr group 228.1.23.1 10
```

スイッチで設定された IP マルチキャスト グループ アドレスを表示する場合は、**show mvr members** 特権 EXEC コマンドを使用します。

次の例では、最大クエリー応答時間を 1 秒（10/10）に設定する方法を示します。

```
Switch(config)# mvr querytime 10
```

次の例では、VLAN 2 をマルチキャスト VLAN として設定する方法を示します。

```
Switch(config)# mvr vlan 2
```

設定を確認するには、**show mvr** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mvr（インターフェイス コンフィギュレーション）	MVR ポートを設定します。
show mvr	MVR グローバル パラメータまたはポート パラメータを表示します。
show mvr interface	設定された MVR インターフェイスをそのタイプ、ステータス、および即時脱退設定とともに表示します。インターフェイスがメンバであるすべての MVR グループを表示します。
show mvr members	MVR マルチキャスト グループのメンバであるすべてのポートを表示します。グループにメンバがいない場合、そのステータスは Inactive として表示されます。

mvr（インターフェイス コンフィギュレーション）

レイヤ 2 のポートを Multicast VLAN Registration（MVR）のレシーバまたは送信元ポートとして設定することで、即時脱退機能を設定し、IP マルチキャスト VLAN と IP アドレスにポートをスタティックに割り当てるには、**mvr** 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。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。

mvr [**immediate** | **type** {**receiver** | **source**} | **vlan** *vlan-id* **group** [*ip-address*]]

no mvr [**immediate** | **type** {**source** | **receiver**}| **vlan** *vlan-id* **group** [*ip-address*]]

構文の説明

immediate	（任意）ポートの MVR の即時脱退機能をイネーブルにします。この機能をディセーブルにするには、**no mvr immediate** コマンドを使用します。
type	（任意）ポートを MVR レシーバ ポートまたは送信元ポートとして設定します。 デフォルト ポート タイプは、MVR 送信元ポートおよびレシーバ ポートのどちらでもありません。**no mvr type** コマンドは、送信元ポートおよびレシーバ ポートのどちらでもないポートとしてポートをリセットします。
receiver	ポートを、マルチキャスト データの受信だけが可能な加入者ポートとして設定します。レシーバ ポートはマルチキャスト VLAN に属することはできません。
source	ポートを、設定済みのマルチキャスト グループとのマルチキャスト データの送受信が可能なアップリンク ポートとして設定します。スイッチの送信元ポートはすべて単一のマルチキャスト VLAN に属します。
vlan *vlan-id* **group**	（任意）ポートを、指定された VLAN ID を持つマルチキャストグループのスタティック メンバとして追加します。 **no mvr vlan** *vlan-id* **group** コマンドは、IP マルチキャスト アドレス グループのメンバシップから VLAN 上のポートを削除します。
ip-address	（任意）指定されたマルチキャスト VLAN ID の指定された MVR IP マルチキャスト グループ アドレスをスタティックに設定します。これは、ポートが加入しているマルチキャスト グループの IP アドレスです。

デフォルト

ポートはレシーバとしても送信元としても設定されません。

即時脱退機能はすべてのポートでディセーブルです。

レシーバ ポートはどの設定済みマルチキャスト グループにも属していません。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

ポートが設定されたマルチキャスト グループ向けマルチキャスト データを送受信できるようにする場合は、ポートを送信元ポートとして設定します。マルチキャスト データは送信元ポートとして設定されているすべてのポートで受信されます。

レシーバ ポートはトランク ポートになることはできません。スイッチのレシーバ ポートは異なる VLAN に属していてもかまいませんが、マルチキャスト VLAN に属することはできません。

MVR に参加していないポートは、MVR レシーバ ポートまたは送信元ポートとして設定しないでください。非 MVR ポートは通常のスイッチ ポートであり、通常のスイッチ動作でマルチキャスト データを送受信することができます。

即時脱退機能がイネーブルの場合、レシーバ ポートはより短時間でマルチキャスト グループから脱退します。即時脱退機能がなく、スイッチがレシーバ ポートのグループから IGMP Leave メッセージを受信した場合、スイッチは、そのポートに IGMP MAC ベースのクエリーを送信し、IGMP グループ メンバシップ レポートを待ちます。設定された時間内にレポートが届かないと、レシーバ ポートがマルチキャスト グループ メンバシップから削除されます。即時脱退機能では、IGMP Leave を受信したレシーバ ポートから IGMP MAC ベースのクエリーは送信されません。Leave メッセージの受信後ただちに、マルチキャスト グループ メンバシップからレシーバ ポートが削除されるので、脱退のための待ち時間が短縮されます。

即時脱退機能をイネーブルにするのは、レシーバ装置が 1 つだけ接続されているレシーバ ポートに限定してください。

mvr vlan group コマンドは、IP マルチキャスト アドレスへ送信されたマルチキャスト トラフィックを受信するようにポートをスタティックに設定します。グループのメンバとしてスタティックに設定されたポートは、スタティックに削除されるまではそのグループのメンバのままです。compatible モードでは、このコマンドはレシーバ ポートだけに適用されます。dynamic モードでは送信元ポートにも適用されます。レシーバ ポートは、IGMP Join メッセージを使用してダイナミックにマルチキャスト グループに加入することもできます。

compatible モードで動作している場合は、MVR は MVR 送信元ポートでの IGMP ダイナミック加入をサポートしません。

MVR ポートはプライベート VLAN ポートにはなれません。

例

次の例では、MVR レシーバ ポートとしてポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# mvr type receiver
```

設定されたレシーバ ポートおよび送信元ポートを表示するには、**show mvr interface** 特権 EXEC コマンドを使用します。

次の例では、ポートの即時脱退機能をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# mvr immediate
```

次の例では、VLAN 1 のポートを IP マルチキャスト グループ 228.1.23.4 のスタティック メンバとして追加する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# mvr vlan1 group 230.1.23.4
```

設定を確認するには、**show mvr members** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mvr（グローバル コンフィギュレーション）	スイッチ上で Multicast VLAN Registration（MVR）をイネーブルにして、設定します。
show mvr	MVR グローバル パラメータまたはポート パラメータを表示します。
show mvr interface	設定済みの MVR インターフェイスを表示するか、またはレシーバ ポートが所属するマルチキャスト グループを表示します。インターフェイスがメンバであるすべての MVR グループを表示します。
show mvr members	MVR マルチキャスト グループのメンバであるすべてのレシーバ ポートを表示します。

network-policy

インターフェイスにネットワークポリシー プロファイルを適用するには、**network-policy** 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。ポリシーを削除する場合は、このコマンドの **no** 形式を使用します。

network-policy *profile number*

no network-policy

構文の説明

profile number	ネットワークポリシー プロファイルの番号を指定します。

デフォルト

ネットワークポリシー プロファイルは適用されません。

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

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

インターフェイスにプロファイルを適用するには、**network-policy** *profile number* 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。

最初にインターフェイス上にネットワークポリシー プロファイルを設定した場合、インターフェイス上に **switchport voice vlan** コマンドを適用できません。**switchport voice vlan** *vlan-id* がすでにインターフェイス上に設定されている場合、ネットワークポリシー プロファイルをインターフェイス上に適用できます。その後、インターフェイスは、インターフェイス上に適用された音声または音声シグナリング VLAN ネットワークポリシー プロファイルを使用します。

例

次の例では、インターフェイスにネットワークポリシー プロファイル 60 を適用する方法を示します。

```
Switch(config)# interface_id
Switch(config-if)# network-policy 60
```

関連コマンド

コマンド	説明
network-policy profile（グローバル コンフィギュレーション）	ネットワークポリシー プロファイルを作成します。
network-policy profile（ネットワークポリシー コンフィギュレーション）	ネットワークポリシー プロファイルの属性を設定します。
show network-policy profile	設定されたネットワークポリシー プロファイルを表示します。

network-policy profile（グローバル コンフィギュレーション）

ネットワークポリシー プロファイルを作成し、ネットワークポリシー コンフィギュレーション モードに入るには、**network-policy profile** グローバル コンフィギュレーション コマンドを使用します。ポリシーを削除し、グローバル コンフィギュレーション モードに戻るには、このコマンドの **no** 形式を使用します。

network-policy profile *profile number*

no network-policy profile *profile number*

構文の説明

profile number	ネットワークポリシー プロファイルの番号を指定します。指定できる範囲は 1 ～ 4294967295 です。

デフォルト

ネットワークポリシー プロファイル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

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

プロファイルを作成し、ネットワークポリシー プロファイル コンフィギュレーション モードに入るには、**network-policy profile** グローバル コンフィギュレーション コマンドを使用します。

ネットワークポリシー プロファイル コンフィギュレーション モードから特権 EXEC モードに戻る場合は、**exit** コマンドを入力します。

ネットワークポリシー プロファイル コンフィギュレーション モードの場合、VLAN、Class of Service（CoS）、Differentiated Service Code Point（DSCP）の値、およびタギング モードを指定することで、音声および音声シグナリング用のプロファイルを作成することができます。

その後、これらのプロファイルの属性は、Link Layer Discovery Protocol for Media Endpoint Devices（LLDP-MED）の **network-policy** Time Length Value（TLV）に含まれます。

例

次の例では、ネットワークポリシー プロファイル 60 を作成する方法を示します。

```
Switch(config)# network-policy profile 60
Switch(config-network-policy)#
```

関連コマンド

コマンド	説明
network-policy	インターフェイスにネットワーク ポリシーを適用します。
network-policy profile（ネットワークポリシー コンフィギュレーション）	ネットワークポリシー プロファイルの属性を設定します。
show network-policy profile	設定されたネットワークポリシー プロファイルを表示します。

network-policy profile（ネットワークポリシー コンフィギュレーション）

network-policy profile 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作成されたネットワーク ポリシー プロファイルを設定するには、**network-policy profile** コンフィギュレーション モード コマンドを使用します。プロファイルを削除する場合は、追加パラメータなしでこのコマンドの **no** 形式を使用します。設定された属性を変更する場合は、パラメータとともにこのコマンドの **no** 形式を使用します。

network-policy profile *profile number* {**voice** | **voice-signaling**} **vlan** [*vlan-id* {**cos** *cvalue* | **dscp** *dvalue*}] | [[**dot1p** {**cos** *cvalue* | **dscp** *dvalue*}] | **none** | **untagged**]

no network-policy profile *profile number* {**voice** | **voice-signaling**} **vlan** [*vlan-id* | {**cos** *cvalue*} | {**dscp** *dvalue*}] | [[**dot1p** {**cos** *cvalue*} | {**dscp** *dvalue*}] | **none** | **untagged**]

構文の説明

voice	音声アプリケーション タイプを指定します。
voice-signaling	音声シグナリング アプリケーション タイプを指定します。
vlan	音声トラフィック用のネイティブ VLAN を指定します。
vlan-id	（任意）音声トラフィック用の VLAN を指定します。指定できる範囲は 1 ～ 4094 です。
cos *cvalue*	（任意）設定された VLAN に対するレイヤ 2 プライオリティ Class of Service（CoS）を指定します。指定できる範囲は 0 ～ 7 です。デフォルト値は 5 です。
dscp *dvalue*	（任意）設定された VLAN に対する Differentiated Service Code Point（DSCP）値を指定します。指定できる範囲は 0 ～ 63 です。デフォルト値は 46 です。
dot1p	（任意）IEEE 802.1p プライオリティ タギングおよび VLAN 0（ネイティブ VLAN）を使用するように電話を設定します。
none	（任意）音声 VLAN に関して IP Phone に指示しません。IP Phone のキー パッドから入力された設定を使用します。
untagged	（任意）IP Phone をタグなしの音声トラフィックを送信するよう設定します。これが IP Phone のデフォルト設定になります。

デフォルト

ネットワーク ポリシーは定義されていません。

コマンド モード

ネットワークポリシー コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

ネットワークポリシー プロファイルの属性を設定するには、**network-policy profile** コマンドを使用します。

voice アプリケーション タイプは IP Phone 専用であり、対話形式の音声サービスをサポートするデバイスに似ています。通常、これらのデバイスは、展開を容易に行えるようにし、データ アプリケーションから隔離してセキュリティを強化するために、別個の VLAN に配置されます。

voice-signaling アプリケーション タイプは、音声メディアと異なる音声シグナリング用のポリシーを必要とするネットワーク トポロジ用です。すべての同じネットワーク ポリシーが **voice policy** TLV にアドバタイズされたポリシーとして適用される場合、このアプリケーション タイプはアドバタイズしないでください。

次の例では、プライオリティ 4 の CoS を持つ VLAN 100 用の音声アプリケーション タイプを設定する方法を示します。

```
Switch(config)# network-policy profile 1
Switch(config-network-policy)# voice vlan 100 cos 4
```

次の例では、DSCP 値 34 を持つ VLAN 100 用の音声アプリケーション タイプを設定する方法を示します。

```
Switch(config)# network-policy profile 1
Switch(config-network-policy)# voice vlan 100 dscp 34
```

次の例では、プライオリティ タギングを持つネイティブ VLAN 用の音声アプリケーション タイプを設定する方法を示します。

```
Switch(config-network-policy)# voice vlan dot1p cos 4
```

関連コマンド

コマンド	説明
network-policy	インターフェイスにネットワーク ポリシーを適用します。
network-policy profile（グローバル コンフィギュレーション）	ネットワークポリシー プロファイルを作成します。
show network-policy profile	設定されたネットワークポリシー プロファイルを表示します。

nmsp

Network Mobility Services Protocol（NMSP）をスイッチ上でイネーブルにするには、**nmsp** グローバル コンフィギュレーション コマンドを使用します。このコマンドは、スイッチで暗号化ソフトウェア イメージが実行されている場合にだけ利用できます。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。

nmsp {**enable** | {**notification interval** {**attachment** | **location**} *interval-seconds*}}

no nmsp {**enable** | {**notification interval** {**attachment** | **location**} *interval-seconds*}}

構文の説明

enable	NMSP 機能をスイッチ上でイネーブルにします。
notification interval	NMSP 通知間隔を指定します。
attachment	アタッチメント通知間隔を指定します。
location	ロケーション通知間隔を指定します。
interval-seconds	スイッチが MSE にロケーションまたはアタッチメントの更新を送信するまでの期間（秒）。指定できる範囲は 1 ～ 30 です。デフォルト値は 30 です。

デフォルト

NMSP 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

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

NMSP ロケーションおよびアタッチメント通知を Cisco Mobility Services Engine（MSE; モビリティ サービス エンジン）に送信するようにスイッチをイネーブルにするには、**nmsp** グローバル コンフィギュレーション コマンドを使用します。

例

次の例では、スイッチ上で NMSP をイネーブルにし、ロケーション通知時間を 10 秒に設定する方法を示します。

```
Switch(config)# vlan enable
Switch(config)# vlan notification interval location 10
```

関連コマンド

コマンド	説明
clear nmsp statistics	NMSP 統計カウンタをクリアします。

コマンド	説明
nmsp attachment suppress	特定のインターフェイスからのアタッチメント情報のレポートを抑制します。
show nmsp	NMSP 情報を表示します。

nmsp attachment suppress

特定のインターフェイスからのアタッチメント情報のレポートを抑制するには、**nmsp attachment suppress** インターフェイス コンフィギュレーション モード コマンドを使用します。このコマンドは、スイッチで暗号化ソフトウェア イメージが実行されている場合にだけ利用できます。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。

nmsp attachment suppress

no nmsp attachment suppress

構文の説明

このコマンドには、引数またはキーワードはありません。

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

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

ロケーションおよびアタッチメント通知を Cisco Mobility Services Engine（MSE; モビリティ サービス エンジン）に送信しないようにインターフェイスを設定するには、**nmsp attachment suppress** 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。

例

次の例では、アタッチメント情報を MSE に送信しないようにインターフェイスを設定する方法を示します。

```
Switch(config)# switch interface interface-id
Switch(config-if)# nmsp attachment suppress
```

関連コマンド

コマンド	説明
nmsp	スイッチ上で Network Mobility Services Protocol（NMSP）をイネーブルにします。
show nmsp	NMSP 情報を表示します。

no authentication logging verbose

認証システム メッセージから詳細な情報をフィルタリングするには、スイッチ スタックまたはスタンドアロン スイッチ上で **no authentication logging verbose** グローバル コンフィギュレーション コマンドを使用します。

no authentication logging verbose

デフォルト

すべての詳細情報はシステム メッセージに表示されます。

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(55)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドにより、認証システム メッセージから、予測される成功などの詳細情報がフィルタリングされます。

例

verbose 認証システム メッセージをフィルタリングするには、次の手順に従います。

```
Switch(config)# no authentication logging verbose
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
no authentication logging verbose	認証システム メッセージから詳細情報をフィルタリングします。
no dot1x logging verbose	802.1x システム メッセージから詳細情報をフィルタリングします。
no mab logging verbose	MAC 認証バイパス（MAB）システム メッセージから詳細情報をフィルタリングします。

no dot1x logging verbose

802.1x システム メッセージから詳細な情報をフィルタリングするには、スイッチ スタックまたはスタンドアロン スイッチ上で **no dot1x logging verbose** グローバル コンフィギュレーション コマンドを使用します。

no dot1x logging verbose

デフォルト

すべての詳細情報はシステム メッセージに表示されます。

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(55)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドにより、802.1x システム メッセージから、予測される成功などの詳細情報がフィルタリングされます。

例

verbose 802.1x システム メッセージをフィルタリングするには、次の手順に従います。

```
Switch(config)# no dot1x logging verbose
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
no authentication logging verbose	認証システム メッセージから詳細情報をフィルタリングします。
no dot1x logging verbose	802.1x システム メッセージから詳細情報をフィルタリングします。
no mab logging verbose	MAC 認証バイパス（MAB）システム メッセージから詳細情報をフィルタリングします。

no mab logging verbose

MAC 認証バイパス（MAB）システム メッセージから詳細な情報をフィルタリングするには、スイッチ スタックまたはスタンドアロン スイッチ上で **no mab logging verbose** グローバル コンフィギュレーション コマンドを使用します。

no mab logging verbose

デフォルト

すべての詳細情報はシステム メッセージに表示されます。

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(55)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドにより、MAC 認証バイパス（MAB）システム メッセージから、予測される成功などの詳細情報がフィルタリングされます。

例

verbose MAB システム メッセージをフィルタリングするには、次の手順に従います。

```
Switch(config)# no mab logging verbose
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
no authentication logging verbose	認証システム メッセージから詳細情報をフィルタリングします。
no dot1x logging verbose	802.1x システム メッセージから詳細情報をフィルタリングします。
no mab logging verbose	MAC 認証バイパス（MAB）システム メッセージから詳細情報をフィルタリングします。

nsf

Open Shortest Path First（OSPF）または Enhanced IGRP（EIGRP）ルーティングの Cisco Nonstop Forwarding（NSF; ノンストップ フォワーディング）をイネーブルにし、設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で、**nsf** ルータ コンフィギュレーション 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**]

no nsf

構文の説明

enforce global	（任意）非 NSF 認識ネイバーが検出された場合、OSPF NSF の再起動をキャンセルします。このキーワードは、OSPF ルータ コンフィギュレーション モードでだけ表示されます。

デフォルト

NSF はディセーブルです。

enforce global オプションはイネーブルです（OSPF 限定）。

コマンド モード

ルータ コンフィギュレーション（OSPF または EIGRP）

コマンド履歴

リリース	変更内容
12.2(35)SE	このコマンドが追加されました。

使用上のガイドライン

nsf コマンドはルータ コンフィギュレーション コマンドで、指定のルーティング プロセスが適用されたすべてのインターフェイスに影響します。スイッチは、OSPF および EIGRP プロトコルに対する Cisco NSF をサポートしています。

NSF がイネーブルで、スタック マスターのスイッチオーバーが検出された場合、NSF 対応ルータは NSF 認識ネイバーまたは NSF 対応ネイバーからのルーティング情報を再構築し、再起動を待機しません。

例

次の例では、OSPF NSF をイネーブルにする方法を示します。

```
Switch(config)# router ospf 100
Switch(config-router)# nsf
```

show ip ospf 特権 EXEC コマンドを使用して、OSPF NSF がイネーブルであることを確認します。

次の例では、EIGRP NSF をイネーブルにする方法を示します。

```
Switch(config)# router eigrp 1
Switch(config-router)# nsf
```

show ip protocols 特権 EXEC コマンドを使用して、EIGRP NSF がイネーブルであることを確認します。

関連コマンド

コマンド	説明
router *protocol-id number*	ルーティング プロセスをイネーブルにします。

pagp learn-method

EtherChannel ポートから受信する着信パケットの送信元アドレスを学習するには、**pagp learn-method** 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。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

構文の説明

aggregation-port	論理ポート チャネルで学習するアドレスを指定します。スイッチは、EtherChannel のいずれかのポートを使用することによって、送信元にパケットを送信します。この設定は、デフォルトです。集約ポート ラーナーの場合、どの物理ポートにパケットが届くかは重要ではありません。
physical-port	EtherChannel 内の物理ポートで学習するアドレスを指定します。スイッチは、送信元アドレスを学習したものと同じ EtherChannel 内のポートを使用して送信元へパケットを送信します。チャネルの一方の終端は、特定の宛先 MAC または IP アドレスのチャネルのポートと同一のポートを使用します。

デフォルト

デフォルトは aggregation-port（論理ポート チャネル）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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

学習方式は、リンクの両端で同一の設定にする必要があります。

（注）Command-Line Interface（CLI; コマンドライン インターフェイス）を経由して **physical-port** キーワードが指定された場合でも、スイッチがサポートするのは、集約ポートでのアドレスの学習だけです。スイッチ ハードウェアでは、**pagp learn-method** および **pagp port-priority** インターフェイス コンフィギュレーション コマンドは無効ですが、Catalyst 1900 スイッチなどの物理ポートによるアドレス学習だけをサポートするデバイスとの PAgP の相互運用にはこれらのコマンドが必要です。

スイッチへのリンク パートナーが物理ラーナーである場合、**pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用してスイッチを物理ポート ラーナーとして設定し、**port-channel load-balance src-mac** 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送信元 MAC アドレスに基づいた負荷分散方式を設定することを推奨します。この状況でだけ、**pagp learn-method** 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。

例

次の例では、学習方式を設定し、EtherChannel 内の物理ポート上のアドレスを学習する方法を示します。

```
Switch(config-if)# pagp learn-method physical-port
```

次の例では、学習方式を設定し、EtherChannel 内のポート チャネル上のアドレスを学習する方法を示します。

```
Switch(config-if)# pagp learn-method aggregation-port
```

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show pagp** *channel-group-number* **internal** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
pagp port-priority	EtherChannel を経由するすべてのトラフィックが送信されるポートを選択します。
show pagp	PAgP チャネル グループ情報を表示します。
show running-config	現在の動作設定を表示します。

pagp port-priority

EtherChannel を経由するすべての Port Aggregation Protocol（PAgP）トラフィックが送信されるポートを選択するには、**pagp port-priority** 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。EtherChannel で使用されていないすべてのポートがホットスタンバイ モードにあり、現在選択されているポートやリンクに障害が発生した場合、これらのポートは稼動状態にできます。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

構文の説明

priority	プライオリティ番号は 0 ～ 255 です。

デフォルト

デフォルト値は 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

同じ EtherChannel 内で動作可能でメンバシップを持つ物理ポートの中で最も高いプライオリティを持つポートが、PAgP 送信用として選択されます。

（注）Command-Line Interface（CLI; コマンドライン インターフェイス）を経由して **physical-port** キーワードが指定された場合でも、スイッチがサポートするのは、集約ポートでのアドレスの学習だけです。スイッチ ハードウェアでは、**pagp learn-method** および **pagp port-priority** インターフェイス コンフィギュレーション コマンドは無効ですが、Catalyst 1900 スイッチなどの物理ポートによるアドレス学習だけをサポートするデバイスとの PAgP の相互運用にはこれらのコマンドが必要です。

スイッチへのリンク パートナーが物理ラーナーである場合、**pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用してスイッチを物理ポート ラーナーとして設定し、**port-channel load-balance src-mac** 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送信元 MAC アドレスに基づいた負荷分散方式を設定することを推奨します。この状況でだけ、**pagp learn-method** 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。

例

次の例では、ポート プライオリティを 200 に設定する方法を示します。

```
Switch(config-if)# pagp port-priority 200
```

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show pagp** *channel-group-number* **internal** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
pagp learn-method	着信パケットの送信元アドレスを学習する機能を提供します。
show pagp	PAgP チャネル グループ情報を表示します。
show running-config	現在の動作設定を表示します。

permit（ARP アクセスリスト コンフィギュレーション）

Dynamic Host Configuration Protocol（DHCP）バインディングとの照合に基づいて Address Resolution Protocol（ARP; アドレス解決プロトコル）パケットを許可するには、**permit** ARP アクセス リスト コンフィギュレーション コマンドを使用します。アクセス コントロール リストから指定された Access Control Entry（ACE）を削除するには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

request	（任意）ARP 要求の照合を要求します。**request** を指定しない場合は、すべての ARP パケットに対して照合が行われます。
ip	送信側 IP アドレスを指定します。
any	すべての IP アドレスまたは MAC アドレスを許可します。
host *sender-ip*	指定された送信側 IP アドレスを許可します。
sender-ip sender-ip-mask	指定された範囲の送信側 IP アドレスを許可します。
mac	送信側 MAC アドレスを指定します。
host *sender-mac*	指定された送信側 MAC アドレスを許可します。
sender-mac sender-mac-mask	指定された範囲の送信側 MAC アドレスを許可します。
response ip	ARP 応答の IP アドレス値を定義します。
host *target-ip*	（任意）指定されたターゲット IP アドレスを許可します。
target-ip target-ip-mask	（任意）指定された範囲のターゲット IP アドレスを許可します。
mac	ARP 応答の MAC アドレス値を指定します。
host *target-mac*	（任意）指定されたターゲット MAC アドレスを許可します。
target-mac target-mac-mask	（任意）指定された範囲のターゲット MAC アドレスを許可します。
log	（任意）ACE と一致するパケットを記録します。**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで **matchlog** キーワードも設定している場合は、一致するパケットはロギングされます。

デフォルト

デフォルト設定はありません。

コマンド モード

ARP アクセス リスト コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

permit 句を追加すると、一部の一致条件に基づいて ARP パケットを転送できます。

例

次の例では、ARP アクセス リストを定義し、IP アドレスが 1.1.1.1 で MAC アドレスが 0000.0000.abcd のホストからの ARP 要求と ARP 応答の両方を許可する方法を示します。

```
Switch(config)# arp access-list static-hosts
Switch(config-arp-nacl)# permit ip host 1.1.1.1 mac host 0000.0000.abcd
Switch(config-arp-nacl)# end
```

設定を確認するには、**show arp access-list** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
arp access-list	ARP ACL を定義します。
deny（ARP アクセスリスト コンフィギュレーション）	DHCP バインディングとの照合に基づいて ARP パケットを拒否します。
ip arp inspection filter vlan	スタティック IP アドレスで設定されたホストからの ARP 要求および応答を許可します。
show arp access-list	ARP アクセス リストに関する詳細を表示します。

permit（IPv6 アクセスリスト コンフィギュレーション）

IPv6 アクセス リストの許可条件を設定するには、**permit** IPv6 アクセス リスト コンフィギュレーション コマンドを使用します。許可条件を削除するには、このコマンドの **no** 形式を使用します。

permit {*protocol*} {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**fragments**] [**log**] [**log-input**] [**sequence** *value*] [**time-range** *name*]

no permit {*protocol*} {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**fragments**] [**log**] [**log-input**] [**sequence** *value*] [**time-range** *name*]

（注）　**flow-label**、**reflect**、および **routing** キーワードはコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

Internet Control Message Protocol（ICMP）

permit icmp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*] | *icmp-message*] [**dscp** *value*] [**log**] [**log-input**] [**sequence** *value*] [**time-range** *name*]

Transmission Control Protocol（TCP; 伝送制御プロトコル）

permit tcp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**ack**] [**dscp** *value*] [**established**] [**fin**] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**psh**] [**range** {*port* | *protocol*}] [**rst**] [**sequence** *value*] [**syn**] [**time-range** *name*] [**urg**]

User Datagram Protocol（UDP）

permit udp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**range** {*port* | *protocol*}] [**sequence** *value*] [**time-range** *name*]

（注）　**flow-label**、**reflect**、および **routing** キーワードはコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

構文の説明

protocol	インターネット プロトコルの名前または番号。**ahp**、**esp**、**icmp**、**ipv6**、**pcp**、**sctp**、**tcp**、または **udp** キーワードの 1 つ、あるいは IPv6 プロトコル番号を示す 0 ～ 255 の範囲の整数にすることができます。
source-ipv6-prefix/prefix-length	許可条件を設定する送信元 IPv6 ネットワークまたはネットワークのクラス。 この引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。 **（注）** CLI ヘルプでは /0 ～ /128 のプレフィクス長が表示されますが、スイッチは集約可能なグローバル ユニキャストおよびリンク ローカル ホスト アドレスの /0 ～ /64 のプレフィクス、および Extended Universal Identifier（EUI）ベースの /128 プレフィクスに対してだけ IPv6 アドレス照合をサポートします。
any	IPv6 プレフィクス ::/0 の省略形。
host *source-ipv6-address*	許可条件の設定先である送信元 IPv6 ホスト アドレス。 この *source-ipv6-address* 引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。
operator [*port-number*]	（任意）指定のプロトコルの送信元または宛先ポートを比較する演算子を指定します。演算子は、**lt**（less than：未満）、**gt**（greater than：より大きい）、**eq**（equal：一致）、**neq**（not equal：不一致）、**range**（inclusive range：包含範囲）です。 *source-ipv6-prefix/prefix-length* 引数の後ろに演算子が置かれた場合、送信元ポートと一致する必要があります。 *destination-ipv6-prefix/prefix-length* 引数の後ろに演算子が置かれた場合、宛先ポートと一致する必要があります。 **range** 演算子には 2 つのポート番号が必要です。他のすべての演算子は 1 つのポート番号が必要です。 任意の *port-number* 引数は 10 進数、または TCP あるいは UDP ポートの名前です。ポート番号の範囲は 0 ～ 65535 です。TCP ポート名は TCP をフィルタリングする場合に限り使用できます。UDP ポート名は UDP をフィルタリングする場合に限り使用できます。
destination-ipv6-prefix/ prefix-length	許可条件を設定する宛先 IPv6 ネットワーク、またはネットワークのクラス。 この引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。 **（注）** CLI ヘルプでは /0 ～ /128 のプレフィクス長が表示されますが、スイッチは集約可能なグローバル ユニキャストおよびリンク ローカル ホスト アドレスの /0 ～ /64 のプレフィクス、および EUI ベースの /128 プレフィクスに対してだけ IPv6 アドレス照合をサポートします。
host *destination-ipv6-address*	許可条件の設定先である宛先 IPv6 ホスト アドレス。 この *destination-ipv6-address* 引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。
dscp *value*	（任意）各 IPv6 パケット ヘッダーのトラフィック クラス フィールドのトラフィック クラス値と Differentiated Service Code Point（DSCP）値を照合します。指定できる範囲は 0 ～ 63 です。

fragments	（任意）フラグメント拡張ヘッダーに 0 以外のフラグメント オフセットが含まれる場合、初期状態でないフラグメント パケットを照合します。**fragments** キーワードは、プロトコルが **ipv6** で *operator* [*port-number*] 引数が指定されていない場合に限り、指定できるオプションです。
log	（任意）エントリと一致するパケットに関する情報ロギング メッセージをコンソールに送信します （コンソールに記憶されるメッセージのレベルは **logging console** コマンドで制御します）。 メッセージには、アクセス リスト名、シーケンス番号、パケットが許可されたかどうか、プロトコル（TCP、UDP、ICMP または番号のいずれか）、適正な場合には送信元 / 宛先アドレス、送信元 / 宛先ポート番号が含まれます。メッセージは、一致した最初のパケットに対して生成され、その後、5 分間隔で許可されたパケット数を含めて生成されます。
log-input	（任意）**log** キーワードと同じ機能を提供します（ただし、ロギング メッセージには受信インターフェイスも表示されます）。
timeout *value*	（任意）再帰 IPv6 アクセス リストがタイムアウトになる前のアイドル時間の間隔（秒単位）。指定できる範囲は 1 ～ 4294967295 です。デフォルト値は 180 秒です。
sequence *value*	（任意）アクセス リスト ステートメントのシーケンス番号を指定します。指定できる範囲は 1 ～ 4294967295 です。
time-range *name*	（任意）許可ステートメントに適用する時間範囲を指定します。時間範囲の名前と制限事項は、**time-range** コマンドと、**absolute** または **periodic** コマンドによってそれぞれ指定します。
icmp-type	（任意）ICMP パケットのフィルタリングに ICMP メッセージ タイプを指定します。ICMP パケットは ICMP メッセージ タイプによってフィルタリングできます。メッセージ タイプの番号は 0 ～ 255 です。
icmp-code	（任意）ICMP パケットのフィルタリングに ICMP メッセージ コードを指定します。ICMP メッセージ タイプによってフィルタリングされる ICMP パケットは、ICMP メッセージ コードによってフィルタリングできます。メッセージ コードの番号は 0 ～ 255 です。
icmp-message	（任意）ICMP パケットのフィルタリングに ICMP メッセージ名を指定します。ICMP パケットは、ICMP メッセージ名、または ICMP メッセージ タイプおよびコードによってフィルタリングできます。使用可能な名前については、「使用上のガイドライン」の項を参照してください。
ack	（任意）TCP プロトコルの場合の ACK ビット設定
established	（任意）TCP プロトコルの場合に限り、接続が確立済みであることを意味します。TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われます。接続するための初期 TCP データグラムの場合は照合しません。
fin	（任意）TCP プロトコルの場合に限り、FIN ビットを設定します。送信元からのデータはこれ以上ありません。
neq {*port* | *protocol*}	（任意）指定のポート番号上にないパケットだけを照合します。
psh	（任意）TCP プロトコルの場合に限り、PSH ビットを設定します。
range {*port* | *protocol*}	（任意）ポート番号範囲のパケットだけを照合します。
rst	（任意）TCP プロトコルの場合に限り RST ビットを設定します。
syn	（任意）TCP プロトコルの場合に限り SYN ビットを設定します。
urg	（任意）TCP プロトコルの場合に限り URG ビットを設定します。

デフォルト

IPv6 アクセス リストは定義されていません。

コマンド モード

IPv6 アクセス リスト コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

permit（IPv6 アクセス リスト コンフィギュレーション モード）コマンドは、IPv6 専用である点を除き **permit**（IPv4 アクセス リスト コンフィギュレーション モード）コマンドと類似しています。

IPv6 アクセス リスト コンフィギュレーション モードを開始し、パケットがアクセス リストを通過する条件を定義するには、**ipv6 access-list** コマンドの後ろに **permit**（IPv6）コマンドを使用します。

protocol 引数に IPv6 を指定すると、パケットの IPv6 ヘッダーに対して照合を行います。

デフォルトでは、アクセス リストの最初のステートメントは 10 で、その次のステートメントからは 10 ずつ増加します。

リスト全体を再入力しないで、**permit**、**deny**、または **remark** ステートメントを既存のアクセス リストに追加できます。リストの最後以外の場所に新しいステートメントを追加するには、挿入する場所を示す、既存の 2 つのエントリ番号の間にある適切なエントリ番号を持った新しいステートメントを作成します。

IPv6 ACL の定義の詳細については、**ipv6 access-list** コマンドを参照してください。

（注）すべての IPv6 ACL には最後の一致条件として、暗黙の **permit icmp any any nd-na**、**permit icmp any any nd-ns**、および **deny ipv6 any any** ステートメントがあります。このうち 2 つの **permit** 条件は、ICMPv6 近隣探索を許可します。ICMPv6 近隣探索を許可しないで **icmp any any nd-na** または **icmp any any nd-ns** を拒否するには、明示的な拒否エントリが ACL 内にある必要があります。暗黙的な **deny ipv6 any any** ステートメントを有効にするには、IPv6 ACL に 1 つ以上のエントリを含める必要があります。

IPv6 近隣探索プロセスでは、IPv6 ネットワーク レイヤ サービスを使用します。したがって、デフォルトでは IPv6 ACL により、IPv6 近隣探索パケットのインターフェイス上での送受信が暗黙的に許可されます。IPv4 では、IPv6 近隣探索プロセスと同等の Address Resolution Protocol（ARP; アドレス解決プロトコル）は、別のデータリンク レイヤ プロトコルを使用します。したがってデフォルトでは、IPv4 ACL により、ARP パケットのインターフェイス上での送受信が暗黙的に許可されます。

source-ipv6-prefix/prefix-length と *destination-ipv6-prefix/prefix-length* の両方の引数をトラフィックのフィルタリングに使用します（送信元プレフィクスはトラフィックの送信元に基づいて、宛先プレフィクスはトラフィックの宛先に基づいてトラフィックをフィルタリングします）。

スイッチは集約可能なグローバル ユニキャストおよびリンク ローカル ホスト アドレスの /0 ～ /64 のプレフィクスと EUI ベースの /128 プレフィクスだけをサポートします。

fragments キーワードは、*operator* [*port-number*] 引数が指定されていない場合に限り指定できるオプションです。

次に、ICMP メッセージ名を表示します。

beyond-scope	destination-unreachable
echo-reply	echo-request
header	hop-limit
mld-query	mld-reduction
mld-report	nd-na
nd-ns	next-header
no-admin	no-route
packet-too-big	parameter-option
parameter-problem	port-unreachable
reassembly-timeout	renum-command
renum-result	renum-seq-number
router-advertisement	router-renumbering
router-solicitation	time-exceeded
unreachable	

例

次の例では、OUTBOUND および INBOUND という名の IPv6 アクセス リスト 2 つを設定し、そのアクセス リストをレイヤ 3 インターフェイス上の発信および着信トラフィックに適用する方法を示します。OUTBOUND リストの最初と 2 番目の許可エントリは、ネットワーク 2001:ODB8:0300:0201::/64 からの TCP および UDP パケットすべてがインターフェイスで送信されるのを許可します。OUTBOUND リストの拒否エントリは、ネットワーク FE80:0:0:0201::/64 でのすべてのパケット（送信元 IPv6 アドレスの最初の 64 ビットとして、リンクローカル プレフィクス FE80:0:0:0201 のあるパケット）がインターフェイスで送信されるのを防ぎます。OUTBOUND リストの 3 番目の許可エントリは、すべての ICMP パケットがインターフェイスで送信されるのを許可します。

INBOUND リストの許可エントリは、すべての ICMP パケットをインターフェイスで受信するのを許可します。

```
Switch(config)#ipv6 access-list OUTBOUND
Switch(config-ipv6-acl)# permit tcp 2001:0DB8:0300:0201::/64 any
Switch(config-ipv6-acl)# permit udp 2001:0DB8:0300:0201::/64 any
Switch(config-ipv6-acl)# deny FE80:0:0:0201::/64 any
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# exit
Switch(config)#ipv6 access-list INBOUND
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# exit
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter OUTBOUND out
Switch(config-if)# ipv6 traffic-filter INBOUND in
```

（注） **permit any any** ステートメントが OUTBOUND または INBOUND アクセス リストの最後のエントリとして含まれていない場合、TCP、UDP、および ICMP パケットだけがインターフェイスの双方向（着信および発信）で許可されます（アクセス リストの末尾にある、暗黙の条件によりインターフェイス上のその他のパケット タイプはすべて拒否されます）。

関連コマンド

コマンド	説明
ipv6 access-list	IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ipv6 traffic-filter	インターフェイス上の着信または発信 IPv6 トラフィックをフィルタリングします。
deny（IPv6 アクセスリスト コンフィギュレーション）	IPv6 アクセス リストに拒否条件を設定します。
show ipv6 access-list	現在の IPv6 アクセス リストすべての内容を表示します。

permit（MAC アクセスリスト コンフィギュレーション）

条件が一致した場合に転送される非 IP トラフィックを許可するには、**permit** MAC アクセス リスト コンフィギュレーション コマンドを使用します。許可条件を拡張 MAC アクセス リストから削除するには、このコマンドの **no** 形式を使用します。

{**permit** | **deny**} {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **cos** *cos* | **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**]

no {**permit** | **deny**} {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **cos** *cos* | **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** |**vines-ip** | **xns-idp**]

（注）　**appletalk** は、コマンドラインのヘルプ ストリングには表示されますが、一致条件としてはサポートされていません。

構文の説明

any	あらゆる送信元または宛先 MAC アドレスを拒否するために指定するキーワードです。
host *src-MAC-addr* | *src-MAC-addr mask*	ホスト MAC アドレスと任意のサブネット マスクを定義します。パケットの送信元アドレスが定義されたアドレスに一致する場合、そのアドレスからの非 IP トラフィックは拒否されます。
host *dst-MAC-addr* | *dst-MAC-addr mask*	宛先 MAC アドレスと任意のサブネット マスクを定義します。パケットの宛先アドレスが定義されたアドレスに一致する場合、そのアドレスへの非 IP トラフィックは拒否されます。
type mask	（任意）パケットの Ethertype 番号と、Ethernet II または Subnetwork Access Protocol（SNAP）カプセル化を使用して、パケットのプロトコルを識別します。 • *type* には、0 ～ 65535 の 16 進数を指定できます。 • *mask* は、照合を行う前に Ethertype に適用される *don’t care* ビットのマスクです。
aarp	（任意）データリンク アドレスをネットワーク アドレスにマッピングする Ethertype AppleTalk Address Resolution Protocol を選択します。
amber	（任意）EtherType DEC-Amber を選択します。
cos *cos*	（任意）プライオリティを設定するため、0 ～ 7 までの任意の Class of Service（CoS）値を選択します。CoS に基づくフィルタリングは、ハードウェアでだけ実行可能です。**cos** オプションが設定されているかどうかを確認する警告メッセージが表示されます。
dec-spanning	（任意）EtherType Digital Equipment Corporation（DEC）スパニング ツリーを選択します。
decnet-iv	（任意）EtherType DECnet Phase IV プロトコルを選択します。
diagnostic	（任意）EtherType DEC-Diagnostic を選択します。
dsm	（任意）EtherType DEC-DSM を選択します。

etype-6000	（任意）EtherType 0x6000 を選択します。
etype-8042	（任意）EtherType 0x8042 を選択します。
lat	（任意）EtherType DEC-LAT を選択します。
lavc-sca	（任意）EtherType DEC-LAVC-SCA を選択します。
lsap *lsap-number mask*	（任意）パケットの LSAP 番号（0 ～ 65535）と 802.2 カプセル化を使用して、パケットのプロトコルを識別します。 *mask* は、照合を行う前に LSAP 番号に適用される *don’t care* ビットのマスクです。
mop-console	（任意）EtherType DEC-MOP Remote Console を選択します。
mop-dump	（任意）EtherType DEC-MOP Dump を選択します。
msdos	（任意）EtherType DEC-MSDOS を選択します。
mumps	（任意）EtherType DEC-MUMPS を選択します。
netbios	（任意）EtherType DEC-Network Basic Input/Output System（NETBIOS）を選択します。
vines-echo	（任意）Banyan Systems による EtherType Virtual Integrated Network Service（VINES）を選択します。
vines-ip	（任意）EtherType VINES IP を選択します。
xns-idp	（任意）EtherType Xerox Network Systems（XNS）プロトコル スイートを選択します。

IPX トラフィックをフィルタリングするには、使用されている IPX カプセル化のタイプに応じて、*type mask* または **lsap** *lsap mask* キーワードを使用します。表 2-19 に、Novell 用語と Cisco IOS 用語での IPX カプセル化タイプに対応するフィルタ条件を一覧表示します。

表 2-19　IPX フィルタ基準

IPX カプセル化タイプ		
Cisco IOS 名	**Novell 名**	**フィルタ基準**
arpa	Ethernet II	Ethertype 0x8137
snap	Ethernet-snap	Ethertype 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

デフォルト

このコマンドには、デフォルトはありません。ただし、名前付き MAC ACL のデフォルト アクションは拒否です。

コマンド モード

MAC アクセス リスト コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

mac access-list extended 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、MAC アクセス リスト コンフィギュレーション モードを開始します。

host キーワードを使用した場合、アドレス マスクは入力できません。**any** キーワードまたは **host** キーワードを使用しない場合は、アドレス マスクを入力する必要があります。

Access Control Entry（ACE）が ACL に追加された場合、リストの最後には暗黙の **deny-any-any** 条件が存在します。つまり、一致がない場合にはパケットは拒否されます。ただし、最初の ACE が追加される前に、リストはすべてのパケットを許可します。

名前付き MAC 拡張アクセス リストの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、あらゆる送信元から MAC アドレス 00c0.00a0.03fa への NETBIOS トラフィックを許可する名前付き MAC 拡張アクセス リストを定義する方法を示します。このリストに一致するトラフィックは許可されます。

```
Switch(config-ext-macl)# permit any host 00c0.00a0.03fa netbios
```

次の例では、名前付き MAC 拡張アクセス リストから許可条件を削除する方法を示します。

```
Switch(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
```

次の例では、Ethertype 0x4321 のすべてのパケットを許可します。

```
Switch(config-ext-macl)# permit any any 0x4321 0
```

設定を確認するには、**show access-lists** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
deny（MAC アクセスリスト コンフィギュレーション）	条件が一致した場合に非 IP トラフィックが転送されるのを拒否します。
mac access-list extended	非 IP トラフィック用に MAC アドレス ベースのアクセス リストを作成します。
show access-lists	スイッチに設定された ACL を表示します。

police

分類されたトラフィックのポリサーを定義するには、**police** ポリシー マップ クラス コンフィギュレーション コマンドを使用します。ポリサーは、最大許容伝送速度、最大バースト伝送サイズ、およびいずれかの最大値を超過した場合の対処法を定義します。既存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 *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}]

no police *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}]

構文の説明

rate-bps	平均トラフィック伝送速度をビット/秒（b/s）で指定します。指定できる範囲は 8000 ～ 1000000000 です。
burst-byte	通常のバーストサイズ（バイト）を指定します。指定できる範囲は 8000 ～ 1000000 です。
exceed-action drop	（任意）指定された伝送速度を超えた場合は、スイッチがパケットをドロップするように指定します。
exceed-action policed-dscp-transmit	（任意）指定された伝送速度を超えた場合、スイッチがパケットの Differentiated Service Code Point（DSCP）をポリシング設定 DSCP マップに指定された値に変え、パケットを送信するように指定します。

デフォルト

ポリサーは定義されません。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

階層ポリシー マップを設定する場合、セカンダリ インターフェイス レベルのポリシー マップで使用できるのは **police** ポリシー マップ コマンドだけです。

2 つ以上の物理ポートを制御するポート ASIC デバイスは、256 個のポリサー（255 個のユーザ設定可能なポリサーと 1 個の内部使用向けに予約されたポリサー）をサポートします。ポートごとにサポートされるユーザ設定可能なポリサーの最大数は 63 です。ポリサーはソフトウェアによってオンデマンドで割り振られ、ハードウェアおよび ASIC の限界によって制約されます。ポートごとにポリサーを予約することはできません。ポートがいずれかのポリサーに割り当てるという保証はありません。

ポリシー マップ コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

ポリシングはトークンバケット アルゴリズムを使用します。バケットの深さ（バケットがオーバーフローするまでの許容最大バースト）を設定するには、**police** 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 *burst-byte* オプションまたは **mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。トークンがバケットから削除される速度（平均速度）を設定する

には、**police** 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 *rate-bps* オプションまたは **mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

ポリシー マップの **police aggregate** コマンドを 10 ギガビット イーサネット インターフェイスで使用すると、エラーになります。

例

次の例では、トラフィックがバースト サイズ 20 KB で平均伝送速度 1 Mb/s を超えた場合に、ポリサーがパケットをドロップするように設定する方法を示します。着信パケットの DSCP が信頼され、パケットは変更されません。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 20000 exceed-action drop
Switch(config-pmap-c)# exit
```

次の例では、DSCP 値をポリシング設定 DSCP マップに定義された値でマークダウンしてパケットを送信するポリサーを設定する方法を示します。

```
Switch(config)# policy-map policy2
Switch(config-pmap)# class class2
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
```

設定を確認するには、**show policy-map** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
class	指定されたクラスマップ名のトラフィック分類一致条件（**police**、**set**、および **trust** ポリシー マップ クラス コンフィギュレーション コマンドによる）を定義します。
mls qos map policed-dscp	ポリシング設定 DSCP マップを DSCP の信頼できるポートに適用します。
policy-map	複数のポートに接続可能なポリシー マップを作成または変更して、サービス ポリシーを指定します。
set	パケットに DSCP 値または IP precedence 値を設定することによって、IP トラフィックを分類します。
show policy-map	Quality of Service（QoS）ポリシー マップを表示します。
trust	**class** ポリシー マップ コンフィギュレーション コマンドまたは **class-map** 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分類されたトラフィックの信頼状態を定義します。

police aggregate

同一のポリシー マップにある複数のクラスに集約ポリサーを適用するには、**police aggregate** ポリシー マップ クラス コンフィギュレーション コマンドを使用します。ポリサーは、最大許容伝送速度、最大バースト伝送サイズ、およびいずれかの最大値を超過した場合の対処法を定義します。指定された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 aggregate *aggregate-policer-name*

no police aggregate *aggregate-policer-name*

構文の説明

aggregate-policer-name	集約ポリサーの名前です。

デフォルト

集約ポリサーは定義されません。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

2 つ以上の物理ポートを制御するポート ASIC デバイスは、256 個のポリサー（255 個のユーザ設定可能なポリサーと 1 個の内部使用向けに予約されたポリサー）をサポートします。ポートごとにサポートされるユーザ設定可能なポリサーの最大数は 63 です。ポリサーはソフトウェアによってオンデマンドで割り振られ、ハードウェアおよび ASIC の限界によって制約されます。ポートごとにポリサーを予約することはできません。ポートがいずれかのポリサーに割り当てるという保証はありません。

集約ポリサー パラメータを設定するには、**mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。集約ポリサーは同じポリシー マップ内の複数のクラスに適用されます。異なるポリシー マップにまたがって集約ポリサーを使用することはできません。

ポリシー マップ コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

police aggregate コマンドを使用するポリシー マップを 10 ギガビット イーサネット インターフェイスに適用すると、エラーになります。

階層ポリシー マップで集約ポリサーを設定することはできません。

例

次の例では、集約ポリサー パラメータを定義する方法と、ポリシー マップ内の複数のクラスにそのポリサーを適用する方法を示します。

```
Switch(config)# mls qos aggregate-policer agg_policer1 10000 1000000 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate agg_policer2
Switch(config-pmap-c)# exit
```

設定を確認するには、**show mls qos aggregate-policer** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos aggregate-policer	ポリシー マップ内の複数のクラスが共有できるポリサー パラメータを定義します。
show mls qos aggregate-policer	Quality of Service（QoS）集約ポリサー設定を表示します。

policy-map

複数の物理ポートまたは Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）に適用可能なポリシー マップを作成または変更し、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、**policy-map** グローバル コンフィギュレーション コマンドを使用します。既存のポリシー マップを削除し、グローバル コンフィギュレーション モードに戻るには、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*

構文の説明

policy-map-name	ポリシー マップ名です。

デフォルト

ポリシー マップは定義されません。

デフォルトの動作は、パケットが IP パケットの場合には Differentiated Service Code Point（DSCP）を 0 に設定し、パケットがタグ付きの場合には Class of Service（CoS）を 0 に設定します。ポリシングは実行されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(25)SE	SVI のポリシー マップ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 コマンドを入力すると、ポリシー マップ コンフィギュレーション モードに入り、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。

- **class**：指定したクラス マップの分類一致基準を定義します。詳細については、「class」（P.2-81）を参照してください。
- **description**：ポリシー マップを説明します（最大 200 文字）。
- **exit**：ポリシー マップ クラス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
- **no**：以前定義したポリシー マップを削除します。
- **rename**：現在のポリシー マップの名前を変更します。

グローバル コンフィギュレーション モードに戻る場合は、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

一致基準がクラス マップに定義されているクラスのポリシーを設定する前に、**policy-map** コマンドを使用して作成、追加または変更するポリシー マップの名前を指定します。**policy-map** コマンドを入力した場合も、ポリシー マップ コンフィギュレーション モードがイネーブルになり、このモードでポリシー マップのクラス ポリシーを設定または変更することができます。

クラス ポリシーをポリシー マップ内で設定できるのは、クラスに一致基準が定義されている場合だけです。クラスの一致基準を設定するには、**class-map** グローバル コンフィギュレーション コマンドおよび **match** クラス マップ コンフィギュレーション コマンドを使用します。物理ポート単位でパケット分類を定義します。

1 つの入力ポートまたは SVI では、1 つのポリシー マップだけがサポートされています。同じポリシー マップを複数の物理ポートまたは SVI に適用できます。

物理ポートまたは SVI に非階層ポリシー マップを適用できます。ただし、階層ポリシー マップを適用できるのは SVI だけです。

階層ポリシー マップには 2 つのレベルがあります。1 つは VLAN レベルで、SVI のトラフィック フローに対して実行するアクションを指定します。もう 1 つはインターフェイス レベルで、インターフェイス レベルのポリシー マップに指定されていて、SVI に属する物理ポートのトラフィックに対して実行するアクションを指定します。

プライマリ VLAN レベル ポリシー マップでは、信頼状態の設定、あるいはパケットでの新しい DSCP または IP precedence 値の設定だけが可能です。セカンダリ インターフェイス レベル ポリシー マップでは、SVI に属する物理ポートの個々のポリサーの設定だけが可能です。

階層ポリシー マップを SVI に適用すると、インターフェイス レベル ポリシー マップを変更したり、階層ポリシー マップから削除したりすることはできません。階層ポリシー マップに、新しいインターフェイス レベル ポリシー マップを追加することもできません。このような変更を行いたい場合は、まず階層ポリシー マップを SVI から削除する必要があります。

階層ポリシー マップの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドで「Configuring QoS」の章の「Policing on SVIs」の項を参照してください。

例

次の例では、*policy1* という名前のポリシー マップを作成する方法を示します。入力ポートに適用した場合、*class1* で定義されたすべての着信トラフィックの照合を行い、IP DSCP を 10 に設定し、平均伝送速度 1 Mb/s、バースト 20 KB のトラフィックをポリシングします。プロファイルを超えるトラフィックは、ポリシング設定 DSCP マップから取得した DSCP 値がマークされてから送信されます。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
```

次の例では、ポリシー マップ *policymap2* に複数のクラスを設定する方法を示します。

```
Switch(config)# policy-map policymap2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police 100000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 100000 20000 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# set dscp 0 (no policer)
Switch(config-pmap-c)# exit
```

次の例は、階層ポリシー マップを作成し、SVI に適用する方法を示しています。

```
Switch(config)# class-map cm-non-int
Switch(config-cmap)# match access-group 101
Switch(config-cmap)# exit
Switch(config)# class-map cm-non-int-2
Switch(config-cmap)# match access-group 102
Switch(config-cmap)# exit
Switch(config)# class-map cm-test-int
Switch(config-cmap)# match input-interface gigabitethernet2/0/2 - gigabitethernet2/0/3
Switch(config-cmap)# exit
Switch(config)# policy-map pm-test-int
Switch(config-pmap)# class cm-test-int
Switch(config-pmap-c)# police 18000000 8000 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map pm-test-pm-2
Switch(config-pmap)# class cm-non-int
Switch(config-pmap-c)# set dscp 7
Switch(config-pmap-c)# service-policy pm-test-int
Switch(config-pmap)# class cm-non-int-2
Switch(config-pmap-c)# set dscp 15
Switch(config-pmap-c)# service-policy pm-test-int
Switch(config-pmap-c)# end
Switch(config-cmap)# exit
Switch(config)# interface vlan 10
Switch(config-if)# service-policy input pm-test-pm-2
```

次の例では、*policymap2* を削除する方法を示します。

```
Switch(config)# no policy-map policymap2
```

設定を確認するには、**show policy-map** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
class	指定のクラスマップ名のトラフィック分類の一致基準を定義します（**police**、**set**、および **trust** ポリシー マップ クラス コンフィギュレーション コマンドを使用）。
class-map	名前を指定したクラスとパケットとの照合に使用されるクラス マップを作成します。
service-policy	ポートにポリシー マップを適用します。
show mls qos vlan	SVI に適用されている Quality of Service（QoS）ポリシー マップを表示します。
show policy-map	QoS ポリシー マップを表示します。

port-channel load-balance

EtherChannel のポート間で負荷分散方式を設定するには、**port-channel load-balance** グローバル コンフィギュレーション 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 {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}

no port-channel load-balance

構文の説明

dst-ip	宛先ホストの IP アドレスに基づいた負荷分散。
dst-mac	宛先ホストの MAC アドレスに基づいた負荷分散。同一の宛先に対するパケットは同一のポートに送信され、異なる宛先のパケットはチャネルの異なるポートに送信されます。
src-dst-ip	送信元および宛先ホストの IP アドレスに基づいた負荷分散。
src-dst-mac	送信元および宛先ホストの MAC アドレスに基づいた負荷分散。
src-ip	送信元ホストの IP アドレスに基づいた負荷分散。
src-mac	送信元 MAC アドレスに基づいた負荷分散。異なるホストからのパケットは、チャネルで異なるポートを使用し、同一のホストからのパケットは同一のポートを使用します。

デフォルト

デフォルトは、**src-mac** 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

これらの転送方式をどのような場合に使用するかについての詳細は、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring EtherChannels」の章を参照してください。

例

次の例では、負荷分散方式を **dst-mac** に設定する方法を示します。

```
Switch(config)# port-channel load-balance dst-mac
```

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show etherchannel load-balance** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
interface port-channel	ポート チャネルへのアクセスや、ポート チャネルの作成を行います。
show etherchannel	チャネルの EtherChannel 情報を表示します。
show running-config	現在の動作設定を表示します。

power inline

Power over Ethernet（PoE）ポート上で電力管理モードを設定にするには、**power inline** 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。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。

power inline {**auto** [**max** *max-wattage*] | **never** | **police [action log]** | **static** [**max** *max-wattage*]}

no power inline {**auto** | **never** | **police** | **static**}

構文の説明

auto	受電装置の検出をイネーブルにします。十分な電力がある場合は、装置の検出後に PoE ポートに電力を自動的に割り当てます。
max *max-wattage*	（任意）ポートに供給される電力を制限します。指定できる範囲は 4000 ～ 15400 ミリワットです。値を指定しない場合は、最大電力が供給されます。
never	装置の検出とポートへの電力供給をディセーブルにします。
static	受電装置の検出をイネーブルにします。スイッチが受電装置を検出する前に、ポートへの電力を事前に割り当てます（確保します）。

デフォルト

デフォルトの設定は **auto**（イネーブル）です。

最大ワット数は、15400 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

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。
12.2(25)SE	**static** および **max** *max-wattage* オプションが追加されました。

使用上のガイドライン

このコマンドは、PoE 対応ポートだけでサポートされています。PoE がサポートされていないポートでこの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。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# power inline auto
                  ^
% Invalid input detected at '^' marker.
```

スイッチ スタックでは、このコマンドは PoE をサポートしているスタックの全ポートでサポートされます。

すべての PoE 対応スイッチ ポートは、IEEE 802.3 af に準拠しています。

max *max-wattage* オプションを使用して、受電装置の電力が制限を超えないようにします。この設定によって、受電装置が最大ワット数より多い電力を要求する Cisco Discovery Protocol（CDP）メッセージを送信すると、スイッチはポートへ電力を供給しません。受電装置の IEEE クラスの最大値が最大ワット数を超えると、スイッチは装置に電力を供給しません。電力は、グローバル パワー バジェットに送られます。

（注）　**power inline max** *max-wattage* コマンドが 15.4 W 未満に設定されている場合、スイッチは Class 0 または Class 3 装置に電力を供給しません。

スイッチが受電装置への電力供給を拒否する場合（受電装置が CDP メッセージを通じて制限を超えた電力を要求する場合、または IEEE クラスの最大値が最大ワット数を超えている場合）、PoE ポートは power-deny ステートになります。スイッチはシステム メッセージを生成し、**show power inline** ユーザ EXEC コマンド出力の Oper カラムに *power-deny* が表示されます。

ポートに高いプライオリティを与えるには、**power inline static max** *max-wattage* コマンドを使用します。スイッチは、auto モードに設定されたポートに電力を割り当てる前に、static モードに設定されたポートに PoE を割り当てます。スイッチは、装置検出より優先的に設定されている場合に、スタティック ポートの電力を確保します。接続された装置がない場合は、ポートがシャットダウン状態か否かに関係なく、スタティック ポートの電力が確保されます。スイッチは、設定された最大ワット数をポートに割り当てます。その値は、IEEE クラスまたは受電装置からの CDP メッセージによって調節されることはありません。電力が事前割り当てされているので、最大ワット数以下の電力を使用する受電装置は、スタティック ポートに接続されていれば電力が保証されます。ただし、受電装置の IEEE クラスが最大ワット数を超えると、スイッチは装置に電力を供給しません。CDP メッセージを通じて受電装置が最大ワット数を超えた量を要求していることをスイッチが認識すると、受電装置がシャットダウンします。

ポートが static モードの場合にスイッチが電力を事前割り当てできない場合（たとえば、パワー バジェット全体がすでに別の自動ポートまたはスタティック ポートに割り当てられているなど）、次のメッセージが表示されます。`Command rejected: power inline static: pwr not available`。ポートの設定は、そのまま変更されません。

power inline auto または **power inline static** インターフェイス コンフィギュレーション コマンドを使用してポートを設定すると、ポートは設定された速度とデュプレックス設定を使用して自動ネゴシエーションします。これは、受電装置であるかどうかに関係なく、接続された装置の電力要件を判別するのに必要です。電力要件が判別された後、スイッチはインターフェイスをリセットすることなく、設定された速度とデュプレックス設定を使用してインターフェイスをハードコードします。

power inline never コマンドを使用してポートを設定する場合、ポートは設定された速度とデュプレックス設定に戻ります。

ポートにシスコ製の受電装置が接続されている場合は、**power inline never** コマンドでポートを設定しないでください。ポートで不正なリンクアップが生じ、errdisable ステートになる可能性があります。

例

次の例では、受電装置の検出をイネーブルにし、PoE ポートに自動的に電力を供給する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/2 Switch(config-if)# power inline auto
```

次の例では、Class 1 または Class 2 の受電装置を受け入れるように PoE ポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# power inline auto max 7000
```

次の例では、受電装置の検出をディセーブルにし、PoE ポートへの電力供給を停止する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# power inline never
```

設定を確認するには、**show power inline** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
logging event power-inline-status	PoE イベントのロギングをイネーブルにします。
show controllers power inline	指定した PoE コントローラのレジスタ値を表示します。
show power inline	指定した PoE ポートまたはすべての PoE ポートの PoE ステータスを表示します。

power inline consumption

各受電装置が使用するワット数を指定することにより、デバイスの IEEE 分類によって指定された電力量を無効にするには、**power inline consumption** 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 コマンドを使用します。デフォルトの電力設定に戻すには、このコマンドの **no** 形式を使用します。

power inline consumption default *wattage*

no power inline consumption default

（注）　**default** キーワードは、グローバル コンフィギュレーション コマンドでだけ表示されます。

構文の説明

wattage	スイッチがポート用に確保する電力を指定します。指定できる範囲は 4000 ～ 15400 ミリワットです。

デフォルト

Power over Ethernet（PoE）ポートのデフォルトの電力は 15400 ミリワットです。

コマンド モード

グローバル コンフィギュレーション

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SEC	このコマンドが追加されました。

使用上のガイドライン

シスコの受電装置が PoE ポートに接続されている場合、スイッチは Cisco Discovery Protocol（CDP）を使用して*実際に*装置が消費する電力量を決定して、それに応じてパワー バジェットを調整します。この機能は、IEEE サードパーティの受電装置には適用されません。この装置の場合、スイッチが電力要求を許可したときに、受電装置の IEEE 分類に応じてパワー バジェットを調整します。受電装置が Class 0（クラス ステータスは不明）または Class 3 である場合、実際に必要な電力量に関係なく、スイッチは装置用に 15400 ミリワットの電力を確保します。受電装置が実際の電力消費量よりも高いクラスであるか、または電力分類（デフォルトで Class 0）をサポートしない場合、スイッチは IEEE クラス情報を使用してグローバル パワー バジェットを追跡するので、少しの装置にしか電力を供給しません。

power inline consumption *wattage* コンフィギュレーション コマンドを使用することで、IEEE 分類で指定されたデフォルトの電力要件を無効にできます。IEEE 分類で指定された電力と実際に装置が必要とする電力の差は、追加の装置が使用するためグローバル パワー バジェットに入れられます。したがって、スイッチのパワー バジェットを拡張してもっと効率的に使用できます。

たとえば、スイッチが各 PoE ポートで 15400 ミリワットの電力を確保した場合、Class0 の受電装置を 24 台だけしか接続できません。Class0 の装置の電力要件が実際には 5000 ミリワットである場合、消費ワット数を 5000 ミリワットに設定すると、最大 48 台の装置を接続できます。24 ポートまたは 48 ポート スイッチで利用できる PoE 総出力電力は 370,000 ミリワットです。

注意　慎重にスイッチのパワー バジェットを計画し、電源装置がオーバーサブスクライブ状態にならないようにしてください。

power inline consumption default *wattage* または **no power inline consumption default** グローバル コンフィギュレーション コマンドを入力するか、**power inline consumption** *wattage* または **no power inline consumption** インターフェイス コンフィギュレーション コマンドを入力すると、次の注意メッセージが表示されます。

```
%CAUTION: Interface interface-id: Misconfiguring the 'power inline consumption/allocation'
command may cause damage to the switch and void your warranty.Take precaution not to
oversubscribe the power supply.Refer to documentation.
```

（注）　手動でパワー バジェットを設定する場合、スイッチと受電装置の間のケーブルでの電力消失を考慮する必要があります。

IEEE 分類に関する詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring Interface Characteristics」の章を参照してください。

このコマンドは、PoE 対応ポートだけでサポートされています。PoE をサポートしていないスイッチまたはポートでこのコマンドを入力すると、エラー メッセージが表示されます。

スイッチ スタックでは、このコマンドは PoE をサポートしているスタックの全スイッチまたはポートでサポートされます。

例

次の例では、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、各 PoE ポートに 5000 ミリワットの電力を確保するようスイッチを設定する方法を示します。

```
Switch(config)# power inline consumption default 5000
%CAUTION: Interface Gi1/0/1: Misconfiguring the 'power inline consumption/allocation'
command may cause damage to the switch and void your warranty.Take precaution not to
oversubscribe the power supply.Refer to documentation.
```

次の例では、インターフェイス コンフィギュレーション コマンドを使用して、特定の PoE ポートに接続された受電装置に 12000 ミリワットの電力を確保するようスイッチを設定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# power inline consumption 12000
%CAUTION: Interface Gi1/0/2: Misconfiguring the 'power inline consumption/allocation'
command may cause damage to the switch and void your warranty.Take precaution not to
oversubscribe the power supply.Refer to documentation.
```

設定を確認するには、**show power inline consumption** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
power inline	PoE ポート上で電力管理モードを設定します。
show power inline	指定した PoE ポートまたはすべての PoE ポートの PoE ステータスを表示します。

power rps

スイッチ スタックまたはスタンドアロン スイッチに接続された Cisco Redundant Power System 2300（RPS 2300 とも呼ばれる）を設定して管理するには、スイッチ スタックまたはスタンドアロン スイッチ上で **power rps** ユーザ EXEC コマンドを使用します。

power rps *switch-number* {**name** {*string* | **serialnumber**} | **port** *rps-port-id* {**mode** {**active** | **standby**} {**priority** *priority*}

（注）　**power rps** コマンドは、Catalyst 3750v2 スイッチ上だけでサポートされています。

構文の説明

switch-number	RPS 2300 が接続されているスタック メンバを指定します。指定できる範囲は 1 ～ 9 です（スタックのスイッチ メンバ番号に対応）。 このパラメータは、Catalyst 3750v2 スイッチ上でだけ使用できます。
name {*string* | **serialnumber**}	RPS 名を設定します。 • *port1* または「*port 1*」などの名前を指定する*文字列*を入力します。名前の前後に引用符を使用することは任意ですが、ポート名にスペースを含める場合、引用符を使用する必要があります。名前には最大 16 文字を含めることができます。 • スイッチが RPS のシリアル番号を名前として使用するように設定するには、**serialnumber** キーワードを入力します。
port *rps-port-id*	RPS ポートを指定します。指定できる範囲は 1 ～ 6 です。
mode {**active** | **standby**}	RPS ポート モードを設定します。 • **active**：スイッチ内部電源が電力を提供できない場合、RPS がスイッチに電力を提供できます。 • **standby**：RPS はスイッチに電力を提供していません。
priority *priority*	RPS ポートのプライオリティを設定します。指定できる範囲は 1 ～ 6 です。 • 1 の値は、ポートおよびその接続装置に最も高いプライオリティを割り当てます。 • 6 の値は、ポートおよびその接続装置に最も低いプライオリティを割り当てます。

デフォルト

RPS 名は設定されていません。

RPS ポートは **active** モードです。

RPS ポートのプライオリティは 6 です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(50)SE1	このコマンドが追加されました。

使用上のガイドライン

power rps コマンドは、Catalyst 3750v2 スタンドアロン スイッチまたはスイッチ スタックに接続された RPS 2300 だけに適用されます。

スタック メンバに接続された RPS 2300 を設定する場合、RPS の名前またはシリアル番号を入力する前に、メンバを指定する必要があります。

スタンドアロン スイッチでは、名前は接続された冗長電源システムに適用されます。スイッチ スタックでは、名前は指定されたスイッチに接続された冗長電源システムのポートに適用されます。たとえば、9 つのスイッチのスタックが 3 つの冗長電源システムに接続されていて、**power rps 1 name "abc"** コマンドを入力する場合、スイッチ 1 に接続された冗長電源システムの名前は *abc* で、その他の冗長電源システムの名前は変わりません。

RPS から指定された RPS ポートに接続されたスイッチに電力を提供しないが、スイッチと冗長電源システム間の RPS ケーブルを接続解除しない場合、**power rps** *switch-number* **port** *rps-port-id* **mode standby** コマンドを使用します。

RPS 2300 ポートのプライオリティを 1 ～ 6 の範囲で設定できます。1 の値は、ポートおよびその接続装置に最も高いプライオリティを割り当てます。6 の値は、ポートおよびその接続装置に最も低いプライオリティを割り当てます。

RPS 2300 に接続された複数のスイッチで電力が必要な場合、RPS 2300 はプライオリティが最も高いスイッチに電力を提供します。プライオリティが低いスイッチには、使用可能な他の電力を適用します。

no power rps ユーザ EXEC コマンドはサポートされません。

- デフォルトの名前設定（名前が設定されていない）に戻るには、引用符の間にスペースを入れずに、**power rps** *switch-number* **port** *rps-port-id* **name** グローバル コンフィギュレーション コマンドを使用します。
- デフォルトの RPS ポート モードに戻るには、**power rps** *switch-number* **port** *rps-port-id* **active** コマンドを使用します。
- デフォルトの RPS ポート プライオリティに戻るには、**power rps** *switch-number* **port** *rps-port-id* **priority** コマンドを使用します。

例

次の例では、スイッチ スタックに接続された RPS 2300 の名前を*文字列*として設定する方法を示します。

```
Switch> power rps 2 name RPS_Accounting
```

次の例では、スイッチに接続された RPS 2300 の名前をシリアル番号として設定する方法を示します。

```
Switch> power rps name serialnumber
```

次の例では、RPS ポート 1 のモードをスイッチ上のスタンバイとして設定する方法を示します。

```
Switch> power rps port 1 mode standby
```

次の例では、スイッチ上で 4 のプライオリティ値を持つ RPS ポート 3 のプライオリティを設定する方法を示します。

```
Switch> power rps 1 port 3 priority 4
```

設定を確認するには、**show env power** または **show env rps** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show env power	スイッチまたはスイッチ スタックの電源のステータスを表示します。
show env rps	スイッチまたはスイッチ スタックに接続された冗長電源システムのステータスを表示します。

priority-queue

ポート上で出力緊急キューをイネーブルにするには、**priority-queue** 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。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。

priority-queue out

no priority-queue out

構文の説明

out	出力緊急キューをイネーブルにします。

デフォルト

出力緊急キューは、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

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。

使用上のガイドライン

priority-queue out コマンドを設定する場合、Shaped Round Robin（SRR）に参加するキューが 1 つ少ないため、SRR の重み比が影響を受けます。これは、**srr-queue bandwidth shape** 内の *weight1* または **srr-queue bandwidth shape** インターフェイス コンフィギュレーション コマンドが無視されることを意味します（比率計算に使用されません）。緊急キューはプライオリティ キューであり、他のキューのサービスが提供される前に空になるまでサービスを提供します。

緊急キューがイネーブルにされているとき、または SRR の重みに基づいて出力キューのサービスが提供されるときには、次の注意事項に従ってください。

- 出力緊急キューがイネーブルにされている場合は、キュー 1 に対して SRR のシェーピングおよび共有された重みが無効にされます。
- 出力緊急キューがディセーブルにされており、SRR のシェーピングおよび共有された重みが設定されている場合は、キュー 1 に対して shaped モードは shared モードを無効にし、SRR はこのキューに shaped モードでサービスを提供します。
- 出力緊急キューがディセーブルにされており、SRR のシェーピングされた重みが設定されていない場合は、SRR はキューに対して shared モードでサービスを提供します。

例

次の例では、SRR の重みが設定されている場合、出力緊急キューをイネーブルにする方法を示します。出力緊急キューは、設定された SRR ウェイトを上書きします。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# priority-queue out
```

次の例では、SRR のシェーピングおよび共有された重みが設定された後、出力緊急キューをディセーブルにする方法を示します。シェーピング モードは、共有モードを無効にします。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# no priority-queue out
```

show mls qos interface *interface-id* **queueing** または **show running-config** 特権 EXEC コマンドを入力すれば、設定を確認することができます。

関連コマンド

コマンド	説明
show mls qos interface queueing	キューイング方法（SRR、プライオリティ キューイング）、キューに相応する重み、および Class of Service（CoS）から出力キューへのマップを表示します。
srr-queue bandwidth shape	シェーピングされた重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅シェーピングをイネーブルにします。
srr-queue bandwidth share	共有する重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅の共有をイネーブルにします。

private-vlan

プライベート VLAN を設定して、プライベート VLAN のプライマリおよびセカンダリ VLAN 間のアソシエーションを設定するには、**private-vlan** VLAN コンフィギュレーション コマンドを使用します。通常の VLAN 設定に VLAN を戻すには、このコマンドの **no** 形式を使用します。

private-vlan {association [**add** | **remove**] *secondary-vlan-list* | **community** | **isolated** | **primary}**

no private-vlan {association | **community** | **isolated** | **primary}**

構文の説明

association	プライマリ VLAN とセカンダリ VLAN とのアソシエーションを作成します。
secondary-vlan-list	プライベート VLAN 内のプライマリ VLAN に関連付ける 1 つまたは複数のセカンダリ VLAN を指定します。
add	セカンダリ VLAN をプライマリ VLAN に関連付けます。
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。
community	VLAN をコミュニティ VLAN として指定します。
isolated	VLAN をコミュニティ VLAN として指定します。
primary	VLAN をコミュニティ VLAN として指定します。

デフォルト

デフォルトでは、プライベート VLAN が設定されていません。

コマンド モード

VLAN コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

プライベート VLAN を設定する前に、VLAN Trunking Protocol（VTP）をディセーブル（VTP 透過モード）にする必要があります。プライベート VLAN を設定した後で、VTP モードをクライアントまたはサーバに変更できません。

VTP は、プライベート VLAN の設定を伝播しません。レイヤ 2 ネットワーク内のすべてのスイッチにプライベート VLAN を手動で設定して、レイヤ 2 データベースを結合し、プライベート VLAN トラフィックのフラッディングを防ぐ必要があります。

プライベート VLAN には、VLAN 1 または VLAN 1002 ～ 1005 を設定できません。拡張 VLAN（VLAN ID 1006 ～ 4094）はプライベート VLAN に設定できます。

セカンダリ（隔離またはコミュニティ）VLAN を 1 つのプライマリ VLAN だけに関連付けることができます。プライマリ VLAN には、1 つの隔離 VLAN および複数のコミュニティ VLAN を関連付けることができます。

- セカンダリ VLAN をプライマリ VLAN として設定できません。

- *secondary_vlan_list* パラメータには、スペースを含めないでください。複数のカンマ区切りの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、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。リストには、1 つの隔離 VLAN と複数のコミュニティ VLAN を含めることができます。
- プライマリまたはセカンダリ VLAN のいずれかを削除すると、VLAN に関連付けられたポートが非アクティブになります。

コミュニティ VLAN は、コミュニティ ポート間、およびコミュニティ ポートから対応するプライマリ VLAN の混合ポートにトラフィックを伝送します。

隔離 VLAN は、混合ポートと通信を行うために隔離ポートによって使用されます。同一のプライマリ VLAN ドメインで他のコミュニティ ポートまたは隔離ポートにトラフィックを伝送しません。

プライマリ VLAN は、ゲートウェイからプライベート ポートのカスタマー エンド ステーションにトラフィックを伝送する VLAN です。

レイヤ 3 VLAN インターフェイス（SVI）はプライマリ VLAN にだけ設定してください。セカンダリ VLAN には、レイヤ 3 VLAN インターフェイスを設定できません。VLAN がセカンダリ VLAN として設定されている間、セカンダリ VLAN の SVI は非アクティブになります。

VLAN コンフィギュレーション モードを終了するまで、**private-vlan** コマンドは作用しません。

プライベート VLAN ポートを EtherChannel として設定しないでください。ポートがプライベート VLAN 設定に含まれていると、ポートの EtherChannel 設定が非アクティブになります。

プライベート VLAN を Remote Switched Port Analyzer（RSPAN）VLAN として設定しないでください。

プライベート VLAN を音声 VLAN として設定しないでください。

プライベート VLAN が設定されたスイッチにフォールバック ブリッジングを設定しないでください。

プライベート VLAN には複数の VLAN が含まれますが、プライベート VLAN 全体で実行されるのは 1 つの STP インスタンスだけです。セカンダリ VLAN がプライマリ VLAN に関連付けられている場合、プライマリ VLAN の STP パラメータがセカンダリ VLAN に伝播されます。

ホスト ポートおよび混合ポートの設定に関する情報については、**switchport mode private-vlan** コマンドを参照してください。

プライベート VLAN の他の機能との相互作用に関する詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、VLAN 20 をプライマリ VLAN に、VLAN 501 を隔離 VLAN に、VLAN 502 および 503 をコミュニティ VLAN に設定し、プライベート VLAN に関連付ける方法を示します。

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 501
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 502
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 503
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan association 501-503
Switch(config-vlan)# end
```

設定を確認するには、**show vlan private-vlan** または **show interfaces status** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces status	所属する VLAN を含むインターフェイスのステータスを表示します。
show vlan private-vlan	スイッチ スタックで設定されたプライベート VLAN および VLAN アソシエーションを表示します。
switchport mode private-vlan	ホスト ポートまたは混合ポートとしてプライベート VLAN ポートを設定します。

private-vlan mapping

プライベート VLAN のプライマリ VLAN とセカンダリ VLAN 間でマッピングを作成して、両方の VLAN で同じプライマリ VLAN Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）を共有できるようにするには、**private-vlan mapping** 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。SVI からプライベート VLAN 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。

private-vlan mapping {[**add** | **remove**] *secondary-vlan-list*}

no private-vlan mapping

構文の説明

secondary-vlan-list	プライマリ VLAN SVI にマッピングされる 1 つまたは複数のセカンダリ VLAN を指定します。
add	（任意）セカンダリ VLAN をプライマリ VLAN SVI 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 SVI 間のマッピングを削除します。

デフォルト

デフォルトでは、プライベート VLAN SVI の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

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

プライベート VLAN を設定する場合は、スイッチが VTP 透過モードになっている必要があります。

プライマリ VLAN の SVI は、レイヤ 3 で作成されます。

レイヤ 3 VLAN インターフェイス（SVI）はプライマリ VLAN にだけ設定してください。セカンダリ VLAN には、レイヤ 3 VLAN インターフェイスを設定できません。VLAN がセカンダリ VLAN として設定されている間、セカンダリ VLAN の SVI は非アクティブになります。

secondary_vlan_list パラメータには、スペースを含めないでください。複数のカンマ区切りの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、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。リストには、1 つの隔離 VLAN と複数のコミュニティ VLAN を含めることができます。

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。

セカンダリ VLAN は、1 つのプライマリ SVI だけにマッピングできます。プライマリ VLAN がセカンダリ VLAN として設定されると、このコマンドで指定されたすべての SVI はダウンします。

有効なレイヤ 2 プライベート VLAN のアソシエーションがない 2 つの VLAN 間のマッピングを設定する場合、マッピングの設定は作用しません。

例

次の例では、VLAN 20 のインターフェイスを VLAN 18 の SVI にマッピングする方法を示します。

```
Switch# configure terminal
Switch# interface vlan 18
Switch(config-if)# private-vlan mapping 20
Switch(config-vlan)# end
```

次の例では、セカンダリ VLAN 303 ～ 305、および 307 からのセカンダリ VLAN トラフィックのルーティングを VLAN 20 SVI を介して許可する方法を示します。

```
Switch# configure terminal
Switch# interface vlan 20
Switch(config-if)# private-vlan mapping 303-305, 307
Switch(config-vlan)# end
```

設定を確認するには、**show interfaces private-vlan mapping** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces private-vlan mapping	VLAN SVI に対するプライベート VLAN のマッピング情報を表示します。

queue-set

キューセットに対してポートをマッピングするには、**queue-set** 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。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。

queue-set *qset-id*

no queue-set *qset-id*

構文の説明

qset-id	キューセットの ID です。各ポートはキューセットに属し、ポート単位で出力キュー 4 つの特性すべてを定義します。指定できる範囲は 1 ～ 2 です。

デフォルト

キューセット ID 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

auto qos voip コマンドによるキューセット ID の自動生成の詳細については、**auto qos voip** コマンドの「Usage Guidelines」を参照してください。

例

次の例では、ポートをキューセット 2 にマッピングする方法を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# queue-set 2
```

設定を確認するには、**show mls qos interface** [*interface-id*] **buffers** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos queue-set output buffers	バッファをキューセットに割り当てます。
mls qos queue-set output threshold	Weighted Tail-Drop（WTD）しきい値を設定し、バッファのアベイラビリティを保証し、キューセットに対する最大メモリ割り当てを設定します。
show mls qos interface buffers	Quality of Service（QoS）情報を表示します。

radius-server dead-criteria

RADIUS サーバが使用不可または *デッド*状態であると考えられる場合に決定する条件を設定するには、**radius-server dead-criteria** グローバル コンフィギュレーション 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。

radius-server dead-criteria [**time** *seconds* [**tries** *number*] | **tries** *number*]

no radius-server dead-criteria [**time** *seconds* [**tries** *number*] | **tries** *number*]

構文の説明

time *seconds*	（任意）RADIUS サーバからの有効な応答をスイッチが取得するのに必要としない時間（秒）を設定します。指定できる範囲は 1 ～ 120 秒です。
tries *number*	（任意）サーバが使用不可と見なされる前に RADIUS サーバから有効な応答をスイッチが取得するのに必要としない回数を指定します。指定できる範囲は 1 ～ 100 です。

デフォルト

スイッチは、10 ～ 60 秒の *seconds* 値を動的に決定します。

スイッチは、10 ～ 100 の *tries* 値を動的に決定します。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

次の *seconds* および *number* パラメータを設定することを推奨します。

- IEEE 802.1x 認証が期限切れになる前に RADIUS サーバへの応答を待機する時間（秒）を指定するには、**radius-server timeout** *seconds* グローバル コンフィギュレーション コマンドを使用します。スイッチは、10 ～ 60 秒のデフォルトの *seconds* 値を動的に決定します。
- RADIUS サーバが使用不能と見なされる前に RADIUS サーバへの送信を試行する時間（秒）を指定するには、**radius-server retransmit** *retries* グローバル コンフィギュレーション コマンドを使用します。スイッチは、10 ～ 100 のデフォルトの *tries* 値を動的に決定します。
- *seconds* パラメータは、IEEE 802.1x 認証が期限切れになる前に再送信を試行する秒数以下か、または同じです。
- *tries* パラメータは、再送信試行回数と同じである必要があります。

例

次の例では、RADIUS サーバが使用不可と見なされた場合に決定する条件として、**時間**に 60 を設定し、**試行**回数に 10 を設定する方法を示します。

```
Switch(config)# radius-server dead-criteria time 60 tries 10
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x critical（グローバル コンフィギュレーション）	アクセス不能な認証バイパス機能のパラメータを設定します。
dot1x critical（インターフェイス コンフィギュレーション）	アクセス不能な認証バイパス機能をインターフェイス上でイネーブルにし、ポートが critical-authentication ステートに置かれた場合にスイッチがクリティカルなポートに割り当てるアクセス VLAN を設定します。
radius-server retransmit *retries*	RADIUS サーバが使用不可と見なされる前にスイッチが RADIUS サーバに送信を試行する回数を指定します。
radius-server timeout *seconds*	IEEE 802.1x 認証が期限切れになる前にスイッチが RADIUS サーバへの応答を待機する時間（秒）を指定します。
show running-config	スイッチの実行コンフィギュレーションを表示します。

radius-server host

RADIUS アカウンティングおよび RADIUS 認証を含む RADIUS サーバのパラメータを設定するには、**radius-server host** グローバル コンフィギュレーション 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。

radius-server host *ip-address* [**acct-port** *udp-port*] [**auth-port** *udp-port*] [**test username** *name* [**idle-time** *time*] [**ignore-acct-port**] [**ignore-auth-port**]] [**key** *string*]

no radius-server host *ip-address*

構文の説明

ip-address	RADIUS サーバの IP アドレスを指定します。
acct-port *udp-port*	（任意）RADIUS アカウンティング サーバの UDP ポートを指定します。指定できる範囲は 0 ～ 65536 です。
auth-port *udp-port*	（任意）RADIUS 認証サーバの UDP ポートを指定します。指定できる範囲は 0 ～ 65536 です。
test *username* *name*	（任意）RADIUS サーバ ステータスの自動サーバ テストをイネーブルにし、使用されるユーザ名を指定します。
idle-time *time*	（任意）スイッチがテスト パケットをサーバに送信した後の間隔（分）を設定します。指定できる範囲は 1 ～ 35791 分です。
ignore-acct-port	（任意）RADIUS サーバ アカウンティング ポートのテストをディセーブルにします。
ignore-auth-port	（任意）RADIUS サーバ認証ポートのテストをディセーブルにします。
key *string*	（任意）スイッチおよび RADIUS デーモン間のすべての RADIUS コミュニケーションの認証鍵および暗号鍵を指定します。key は文字列であり、RADIUS サーバで使用されている暗号化キーと一致する必要があります。必ずこのコマンドの最終項目として key を設定してください。先頭のスペースは無視されますが、key の中間および末尾のスペースは使用されます。key にスペースが含まれる場合は、引用符が key の一部でない限り、key を引用符で囲まないでください。

デフォルト

RADIUS アカウンティング サーバの UDP ポートは 1646 です。

RADIUS 認証サーバの UDP ポートは 1645 です。

自動サーバ テストはディセーブルです。

アイドル時間は 60 分（1 時間）です。

自動テストがイネーブルの場合、UDP ポートのアカウンティングおよび認証時にテストが実行されます。

認証鍵および暗号鍵（*string*）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

コマンド履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

RADIUS アカウンティング サーバおよび RADIUS 認証サーバの UDP ポートをデフォルト以外の値に設定することを推奨します。

RADIUS サーバ ステータスの自動サーバ テストをイネーブルにし、使用されるユーザ名を指定するには、**test username** *name* キーワードを使用します。

radius-server host *ip-address* **key** *string* または **radius-server key** {**0** *string* | **7** *string* | *string*} 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認証鍵および暗号鍵を設定できます。必ずこのコマンドの最終項目として key を設定してください。

例

次の例では、アカウンティング サーバの UDP ポートを 1500、認証サーバの UDP ポートを 1510 に設定する例を示します。

```
Switch(config)# radius-server host 1.1.1.1 acct-port 1500 auth-port 1510
```

次の例では、アカウンティング サーバおよび認証サーバの UDP ポートを設定し、RADIUS サーバ ステータスの自動テストをイネーブルにし、使用されるユーザ名を指定し、キー ストリングを設定する例を示します。

```
Switch(config)# radius-server host 1.1.1.2 acct-port 800 auth-port 900 test username
aaafail idle-time 75 key abc123
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x critical（グローバル コンフィギュレーション）	アクセス不能な認証バイパス機能のパラメータを設定します。
dot1x critical（インターフェイス コンフィギュレーション）	アクセス不能な認証バイパス機能をインターフェイス上でイネーブルにし、ポートが critical-authentication ステートに置かれた場合にスイッチがクリティカルなポートに割り当てるアクセス VLAN を設定します。
radius-server key {**0** *string* | **7** *string* | *string*}	ルータおよび RADIUS デーモン間のすべての RADIUS コミュニケーションの認証鍵および暗号鍵を指定します。
show running-config	スイッチの実行コンフィギュレーションを表示します。

rcommand

Telnet セッションを開始し、クラスタ コマンド スイッチまたはスイッチ スタックからクラスタ メンバ スイッチのコマンドを実行するには、スイッチ スタックまたはクラスタ コマンド スイッチ上で **rcommand** ユーザ EXEC コマンドを使用します。セッションを終了するには、**exit** コマンドを入力します。

rcommand {*n* | **commander** | **mac-address** *hw-addr*}

構文の説明

n	クラスタ メンバを識別する番号を提供します。指定できる範囲は 0 ～ 15 です。
commander	クラスタ メンバ スイッチからクラスタ コマンド スイッチへアクセスできるようにします。
mac-address *hw-addr*	クラスタ メンバ スイッチの MAC アドレス

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドが利用できるのは、クラスタ コマンド スイッチ スタックまたはクラスタ コマンド スイッチに限られます。

スイッチがクラスタ コマンド スイッチで、クラスタ メンバ スイッチ *n* が存在していない場合、エラー メッセージが表示されます。スイッチ番号を得るには、クラスタ コマンド スイッチで **show cluster members** 特権 EXEC コマンドを入力します。

このコマンドを使用してクラスタ コマンド スイッチ プロンプトからクラスタ メンバ スイッチにアクセスしたり、メンバ スイッチ プロンプトからクラスタ コマンド スイッチにアクセスしたりすることができます。

Catalyst 2900 XL、Catalyst 3500 XL、Catalyst 2950、Catalyst 2960、Catalyst 2970、Catalyst 3550、Catalyst 3560、および Catalyst 3750 スイッチの場合、Telnet セッションは、クラスタ コマンド スイッチと同じ権限レベルでメンバ スイッチ Command-Line Interface（CLI; コマンドライン インターフェイス）にアクセスします。たとえば、このコマンドをクラスタ コマンド スイッチからユーザ レベルで入力した場合、メンバ スイッチはユーザ レベルでアクセスされます。このコマンドをクラスタ コマンド スイッチからイネーブル レベルで使用した場合、コマンドはイネーブル レベルでリモート デバイスにアクセスします。*権限レベル*よりも低い中間イネーブル レベルを使用した場合、クラスタ メンバ スイッチはユーザ レベルとなります。

Standard Edition ソフトウェアが稼動している Catalyst 1900 および Catalyst 2820 スイッチの場合、クラスタ コマンド スイッチの権限レベルが 15 であれば、Telnet セッションはメニュー コンソール（メニュー方式インターフェイス）にアクセスします。クラスタ コマンド スイッチの権限レベルが 1 であ

れば、パスワードの入力を要求するプロンプトが表示され、入力後にメニュー コンソールにアクセスできます。クラスタ コマンド スイッチの権限レベルは、Standard Edition ソフトウェアが稼動しているクラスタ メンバ スイッチに次のようにマッピングします。

- クラスタ コマンド スイッチの権限レベルが 1 ～ 14 である場合、クラスタ メンバ スイッチへのアクセスは権限レベル 1 で行われます。
- クラスタ コマンド スイッチの権限レベルが 15 である場合、クラスタ メンバ スイッチへのアクセスは権限レベル 15 で行われます。

Catalyst 1900 および Catalyst 2820 の CLI が利用できるのは、スイッチで Enterprise Edition ソフトウェアが稼動している場合に限られます。

クラスタ コマンド スイッチの vty ラインにアクセス クラス コンフィギュレーションがある場合、このコマンドは機能しません。

クラスタ メンバ スイッチはクラスタ コマンド スイッチのパスワードを継承するため、クラスタ メンバ スイッチがクラスタに加入してもパスワードを要求するプロンプトは表示されません。

例

次の例では、メンバ 3 でセッションを開始する方法を示します。**exit** コマンドを入力するか、あるいはセッションを閉じるまで、このコマンドに続くすべてのコマンドは、メンバ 3 へ向けられます。

```
Switch# rcommand 3
Switch-3# show version
Cisco Internet Operating System Software ...
...
Switch-3# exit
Switch#
```

関連コマンド

コマンド	説明
show cluster members	クラスタ メンバに関する情報を表示します。

reload

スタック メンバをリロードし、設定の変更を有効にするには、**reload** 特権 EXEC コマンドを使用します。

reload [*LINE* | **at** | **cancel** | **in** | **slot** *stack-member-number* | **standby-cpu**]

構文の説明

LINE	リロードする理由を指定します。
at	リロードを実行する時間（hh:mm）を指定します。
cancel	中断しているリロードをキャンセルします。
in	リロードを実行する時間間隔（mmm または hhh:mm）を指定します。
slot *stack-member-number*	指定のスタック メンバ上で変更を保存し、再起動します。
standby-cpu	スタンバイ Route Processor（RP; ルート プロセッサ）をリロードします。

デフォルト

スタック メンバをただちにリロードし、設定の変更を有効にします。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

スイッチ スタックに複数のスイッチがある場合に **reload slot** *stack-member-number* コマンドを入力すると、設定の保存を要求するプロンプトが表示されません。

例

次の例では、スイッチ スタックをリロードする方法を示します。

```
Switch(config)# reload
System configuration has been modified.Save?[yes/no]: y
Proceed to reload the whole Stack?[confirm] y
```

次の例では、特定のスタック メンバをリロードする方法を示します。

```
Switch(config)# reload slot 6
Proceed with reload?[confirm]y
```

次の例では、単一スイッチのスイッチ スタック（メンバ スイッチが 1 つだけ）をリロードする方法を示します。

```
Switch(config)# reload slot 3
System configuration has been modified.Save?[yes/no]: y
Proceed to reload the whole Stack?[confirm] y
```

関連コマンド

コマンド	説明
rcommand	特定のスタック メンバにアクセスします。
switch	スタック メンバのプライオリティ値を変更します。
switch renumber	スタック メンバ番号を変更します。
show switch	スイッチ スタックおよびスタック メンバの情報を表示します。

remote command

すべてのまたは指定のスタック メンバをモニタリングするには、**remote command** 特権 EXEC コマンドを使用します。

remote command {**all** | *stack-member-number*} *LINE*

構文の説明

all	すべてのスタック メンバに適用します。
stack-member-number	スタック メンバを指定します。指定できる範囲は 1 ～ 9 です。
LINE	実行するコマンドを指定します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

ストリングを実行する LINE コマンドで使用するコマンド（**debug**、**show**、または **clear** など）は、指定のスタック メンバまたはスイッチ スタックに適用されます。

例

次の例では、スイッチ スタックで **undebug** コマンドを実行する方法を示します。

```
Switch(config)# remote command all undebug all
Switch :1 :
------------
All possible debugging has been turned off
Switch :5 :
------------
All possible debugging has been turned off
Switch :9 :
------------
All possible debugging has been turned off
```

次の例では、スタック メンバ 5 で **debug udld event** コマンドを実行する方法を示します。

```
Switch(config)# remote command 5 undebug all
Switch :5 :
------------
UDLD events debugging is on
```

関連コマンド

コマンド	説明
reload	特定のスタック メンバにアクセスします。
switch	スタック メンバのプライオリティ値を変更します。
switch renumber	スタック メンバ番号を変更します。
show switch	スイッチ スタックおよびスタック メンバの情報を表示します。

remote-span

VLAN を Remote Switched Port Analyzer（RSPAN）VLAN として設定するには、**remote-span** VLAN コンフィギュレーション コマンドを使用します。RSPAN 指定を VLAN から削除するには、このコマンドの **no** 形式を使用します。

remote-span

no remote-span

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

RSPAN VLAN は定義されません。

コマンド モード

VLAN コンフィギュレーション（config-VLAN）

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

RSPAN VLAN を設定できるのは config-VLAN モードの場合だけです（このモードは、**vlan** グローバル コンフィギュレーション コマンドで開始します）。**vlan database** 特権 EXEC コマンドを使用して開始された VLAN コンフィギュレーション モードでは設定できません。

VLAN Trunking Protocol（VTP）がイネーブルで、VLAN ID が 1005 未満の場合は、RSPAN 機能は VTP によって伝達されます。RSPAN VLAN ID が拡張範囲内の場合は、手動で中間スイッチを設定する必要があります（送信元スイッチと宛先スイッチの間の RSPAN VLAN 内に設定）。

RSPAN **remote-span** コマンドを設定する前に、**vlan**（グローバル コンフィギュレーション）コマンドで VLAN を作成してください。

RSPAN VLAN には、次の特性があります。

- MAC アドレス ラーニングは実行されません。
- トランク ポートでは RSPAN VLAN トラフィックだけが流れます。
- Spanning-Tree Protocol（STP）は RSPAN VLAN 内では稼動できますが、RSPAN 宛先ポートでは稼動しません。

既存の VLAN が RSPAN VLAN として設定されている場合は、その VLAN が最初に削除され、RSPAN VLAN として再作成されます。アクセス ポートは、RSPAN 機能がディセーブルになるまでは非アクティブです。

例

次の例では、RSPAN VLAN として VLAN を設定する方法を示します。

```
Switch(config)# vlan 901
Switch(config-vlan)# remote-span
```

次の例では、VLAN から RSPAN 機能を削除する方法を示します。

```
Switch(config)# vlan 901
Switch(config-vlan)# no remote-span
```

show vlan remote-span ユーザ EXEC コマンドを入力すると、設定を確認することができます。

関連コマンド

コマンド	説明
monitor session	ポートで Switched Port Analyzer（SPAN）および RSPAN モニタリングをイネーブルにし、ポートを送信元ポートまたは宛先ポートとして設定します。
usb-inactivity-timeout	VLAN 1 ～ 4094 を設定できる config-vlan モードに変更します。

renew ip dhcp snooping database

Dynamic Host Configuration Protocol（DHCP）スヌーピング バインディング データベースを更新するには、**renew ip dhcp snooping database** 特権 EXEC コマンドを使用します。

renew ip dhcp snooping database [{**flash**[*number*]*:/filename* | **ftp:***//user:password@host/filename* | **nvram:***/filename* | **rcp:***//user@host/filename* | **tftp:***//host/filename*}] [**validation none**]

構文の説明

flash[*number*]**:**/*filename*	（任意）データベース エージェントまたはバインディング ファイルがフラッシュ メモリにあることを指定します。スタック マスターのスタック メンバ番号を指定するには、*number* パラメータを使用します。*number に指定できる範囲は* 1 ～ 9 です。 **（注）**
ftp://*user*:*password@host*/*filename*	（任意）データベース エージェントまたはバインディング ファイルが FTP（ファイル転送プロトコル）サーバにあることを指定します。
nvram:/*filename*	（任意）データベース エージェントまたはバインディング ファイルが NVRAM（不揮発性 RAM）にあることを指定します。
rcp://*user@host*/*filename*	（任意）データベース エージェントまたはバインディング ファイルが Remote Control Protocol（RCP）サーバにあることを指定します。
tftp://*host*/*filename*	（任意）データベース エージェントまたはバインディング ファイルが TFTP（簡易ファイル転送プロトコル）サーバにあることを指定します。
validation none	（任意）URL によって指定されたバインディング ファイルのエントリに対して、Cyclic Redundancy Check（CRC; 巡回冗長検査）を検証しないようにスイッチに指定します。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

URL を指定しない場合は、スイッチは設定された URL からファイルを読み込もうとします。

例

次の例では、ファイル内の CRC 値のチェックを省略して、DHCP スヌーピング バインディング データベースを更新する方法を示します。

```
Switch# renew ip dhcp snooping database validation none
```

設定を確認するには、**show ip dhcp snooping database** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip dhcp snooping	VLAN 上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping binding	DHCP スヌーピング バインディング データベースを設定します。
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。

reserved-only

Dynamic Host Configuration Protocol（DHCP）アドレス プールに予約済みのアドレスだけ割り当てるには、**reserved-only** DHCP プール コンフィギュレーション モード 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。

reserved-only

no reserved-only

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトでは、プール アドレスは制限されません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

reserved-only コマンドを入力すると、DHCP プールから事前設定された予約への割り当てが制限されます。ネットワークまたはプール上の範囲の一部である予約されていないアドレスがクライアントには提供されず、他のクライアントはプールによるサービスを受けられません。

このコマンドの入力により、ユーザは、共通の IP サブネットを共有し、他のスイッチのクライアントからの要求を無視する DHCP プールを持つスイッチのグループを設定できます。

DHCP プール コンフィギュレーション モードにアクセスするには、**ip dhcp pool** *name* 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。

例

次の例では、予約済みのアドレスだけを割り当てるように DHCP プールを設定する方法を示します。

```
Switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip dhcp pool test1
Switch(dhcp-config)# reserved-only
```

設定を確認するには、**show ip dhcp pool** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ip dhcp pool	DHCP アドレス プールを表示します。

rmon collection stats

イーサネット グループの統計（ブロードキャストおよびマルチキャスト パケットに関する使用率の統計、Cyclic Redundancy Check（CRC; 巡回冗長検査）整合性エラーおよび衝突に関するエラー統計も含む）を収集するには、**rmon collection stats** 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。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。

rmon collection stats *index* [**owner** *name*]

no rmon collection stats *index* [**owner** *name*]

構文の説明

index	Remote Network Monitoring（RMON）収集制御インデックス。指定できる範囲は 1 ～ 65535 です。
owner *name*	（任意）RMON 収集の所有者

デフォルト

RMON 統計情報収集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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

RMON 統計情報収集コマンドはハードウェア カウンタに基づいています。

例

次の例では、所有者 *root* の RMON 統計情報を収集する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# rmon collection stats 2 owner root
```

設定を確認するには、**show rmon statistics** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show rmon statistics	RMON 統計情報を表示します。

sdm prefer

Switch Database Management（SDM）リソース割り当てで使用するテンプレートを設定するには、**sdm prefer** グローバル コンフィギュレーション コマンドを使用します。テンプレートを使用してシステム リソースを割り当てることで、アプリケーションで使用される機能を最大限にサポートできます。テンプレートを使用することにより、ユニキャスト ルーティングまたは VLAN 設定でシステム利用率を最大限にしたり、アグリゲータ テンプレート（Catalyst 3750-12S だけ）をデスクトップ テンプレートに変更したり、デュアル IPv4/IPv6 テンプレートを選択して IPv6 フォワーディングをサポートしたりできます。デフォルトのテンプレートに戻すには、このコマンドの **no** 形式を使用します。

sdm prefer {access | default | dual-ipv4-and-ipv6 {default | routing | vlan} | routing | vlan} [desktop]

no sdm prefer

構文の説明

access	Access Control Lists（ACL; アクセス コントロール リスト）のシステム使用率を最大限にします。ACL が多数ある場合、このテンプレートを使用します。
default	スイッチでデフォルトのテンプレートを使用するように設定します。Catalyst 3750-12S スイッチでは、デフォルトのデスクトップ テンプレートに設定するには、**desktop** キーワードを使用します （デスクトップ スイッチでデフォルトのデスクトップ テンプレートに設定するか、またはアグリゲータ スイッチでデフォルトのアグリゲータ テンプレートに設定するには、**no sdm prefer** コマンドを使用します）。
dual-ipv4-and-ipv6 {default | routing | vlan}	IPv4 と IPv6 両方のルーティングをサポートするテンプレートを選択します。 • **default** : IPv4 と IPv6 のレイヤ 2 とレイヤ 3 の機能を均等に動作させます。 • **routing** : IPv4 ポリシーベース ルーティングを含む IPv4 および IPv6 ルーティングのシステム使用率を最大限にします。 • **vlan** : IPv4 と IPv6 の VLAN のシステム使用率を最大限にします。
routing	ユニキャスト ルーティングのシステム使用率を最大限にします。通常、このテンプレートをネットワークの中心にあるルータまたはアグリゲータで使用します。
vlan	VLAN のシステム使用率を最大限にします。このテンプレートは、ルーティングしないレイヤ 2 スイッチの使用に対してシステム リソースを最大にします。
desktop	Catalyst 3750-12S スイッチ（アグリゲータ テンプレートがデフォルト）上だけで使用し、desktop **default**、**routing**、**vlan** のテンプレートを選択します。

デフォルト

デフォルトのテンプレートはすべての機能を均等に動作させます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	アグリゲータ テンプレートが追加されました。

リリース	変更内容
12.2(25)SEA	デュアル IPv4/IPv6 テンプレートが追加されました。
12.2(25)SED	アクセス テンプレートが追加されました。
12.2(25)SEE	**デュアル IPv4/IPv6 ルーティング** テンプレートが追加されました。

使用上のガイドライン

この設定を有効にするには、スイッチをリロードする必要があります。**reload** 特権 EXEC コマンドを入力する前に、**show sdm prefer** コマンドを入力すると、**show sdm prefer** コマンドにより、現在使用しているテンプレートおよびリロード後にアクティブになるテンプレートが表示されます。

デスクトップ スイッチは、デスクトップ テンプレートだけをサポートします。アグリゲータ スイッチ（Catalyst 3750-12S）はデスクトップおよびアグリゲータ テンプレートの両方をサポートします。アグリゲータ スイッチ上で、デスクトップ キーワードを入力しない場合、アグリゲータ テンプレートが選択されます。

すべてのスタック メンバは同一の SDM デスクトップまたはアグリゲータ テンプレート（スタック マスター上に保存）を使用します。新しいスイッチ メンバがスタックに追加された場合、マスター上に保存されている SDM の設定は、スイッチ コンフィギュレーション ファイルおよび VLAN データベース ファイルと同様に、個々のスイッチで設定されたテンプレートを上書きします。

スイッチ スタックで IPv6 パケットをルーティングするには、スタック内のすべてのスイッチで IP サービス イメージを実行している必要があります。例外（IPv6Options）を持つパケット以外、IPv6 パケットはスタック上のハードウェアでルーティングされるため、スイッチがハードウェア リソースを使い果たすことはありません。

メンバがマスター スイッチ上で実行されているテンプレートをサポートできない場合、スイッチは SDM ミスマッチ モードに入り、マスター スイッチが SDM テンプレートを変更しないようにします。その場合、スイッチはスタックのメンバとして機能できません。

- マスター スイッチが Catalyst 3750-12S で、アグリゲータ テンプレートからデスクトップ テンプレートに変更し、スイッチをリロードした場合、スタック全体がデスクトップ テンプレートを選択した状態で動作します。このため、Ternary CAM（TCAM）エントリの数がデスクトップ テンプレートのサイズを超えた場合、設定が失われる可能性があります。
- Catalyst 3750-12S マスター上のテンプレートをデスクトップ テンプレートからアグリゲータ テンプレートに変更し、スイッチをリロードした場合、スタックのメンバであったすべてのデスクトップ スイッチは SDM ミスマッチ モードに入ります。
- アグリゲータ テンプレートを実行している Catalyst 3750-12S スイッチを、マスターがデスクトップ スイッチのスタックに追加する場合、スタックは、マスター上で選択されているデスクトップ テンプレートで動作します。そのため、TCAM エントリの数がデスクトップ テンプレートのサイズを超えた場合、Catalyst 3750-12S メンバ上にある設定は失われる可能性があります。

スタックに関する詳細情報は、ソフトウェア コンフィギュレーション ガイドの「Managing Switch Stacks」の章を参照してください。

アクセス テンプレートは、多数のアクセス コントロール リスト（ACL）に対応できるように ACL のシステム リソースを最大限にします。

デフォルトのテンプレートは、システム リソースを均等に使用します。

sdm prefer vlan [**desktop**] グローバル コンフィギュレーション コマンドは、ルーティングしないレイヤ 2 スイッチングを目的としたスイッチ上だけで使用します。VLAN テンプレートを使用する場合、システム リソースはルーティング エントリに予約されません。ルーティングはソフトウェアで実行されます。この場合、CPU に負荷がかかり、ルーティングのパフォーマンスが大幅に低下します。

スイッチ上でルーティングがイネーブルになっていない場合、ルーティング テンプレートを使用しないでください。**sdm prefer routing** [**desktop**] グローバル コンフィギュレーション コマンドを入力することで、ルーティング テンプレートのユニキャスト ルーティングに割り当てたメモリを他の機能に使用させないようにします。

スイッチで IPv6 ルーティングをイネーブルにしない場合は、IPv4/IPv6 テンプレートを使用しないでください。**sdm prefer ipv4-and-ipv6** {**default** | **routing** | **vlan**} [**desktop**] グローバル コンフィギュレーション コマンドを入力すると、リソースが IPv4 と IPv6 に振り分けられて、IPv4 フォワーディングに割り当てられたリソースが制限されます。

表 2-20 に、デスクトップまたはアグリゲータ スイッチの IPv4 限定テンプレートそれぞれでサポートされる各リソースの概算を示します。テンプレート内の値は、8 つのルーティング対象のインターフェイスと約 1000 の VLAN に基づいており、テンプレートが選択された場合のハードウェア境界セットの概略を示しています。ハードウェア リソースのセクションが満杯の場合、処理できないものはすべて CPU に送信されるため、スイッチのパフォーマンスに著しく影響します。

表 2-20　IPv4 テンプレートによって許容される機能リソースの概算

	デスクトップ テンプレート				アグリゲータ テンプレート			
リソース	アクセス	デフォルト	ルーティング	VLAN	アクセス	デフォルト	ルーティング	VLAN
ユニキャスト MAC アドレス	4 K	6 K	3 K	12 K	6 K	6 K	6 K	12 K
Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）グループおよびマルチキャスト ルート	1 K	1 K	1 K	1 K	1 K	1 K	1 K	1 K
ユニキャスト ルート	6 K	8 K	11 K	0	12 K	12 K	20 K	0
• ホストに直接接続	4 K	6 K	3 K	0	6 K	6 K	6 K	0
• 間接ルート	2 K	2 K	8 K	0	6 K	6 K	14 K	0
ポリシーベース ルーティング アクセス コントロール エントリ（ACE）	512	0	512	0	512	0	512	0
Quality of Service（QoS）分類の ACE	512	512	512	512	896	896	512	896
セキュリティの ACE	2 K	1 K	1 K	1 K	4 K	1 K	1 K	1 K
レイヤ 2 VLAN	1 K	1 K	1 K	1 K	1 K	1 K	1 K	1 K

表 2-21 に、デスクトップまたはアグリゲータ スイッチのデュアル IPv4/IPv6 テンプレートそれぞれでサポートされる各リソースの概算を示します。

表 2-21　デュアル IPv4/IPv6 テンプレートによって許容される機能リソースの概算

	デスクトップ IPv4/IPv6 テンプレート			アグリゲータ IPv4/IPv6 テンプレート		
リソース	デフォルト	ルーティング	VLAN	デフォルト	ルーティング	VLAN
ユニキャスト MAC アドレス	2 K	1536	8 K	2 K	2 K	8 K
IPv4 IGMP グループおよびマルチキャスト ルート	1 K	1 K	1 K	1 K	1 K	0
IPv4 ユニキャスト ルートの合計：	3 K	2816	0	3 K	8 K	0
• IPv4 ホストに直接接続	2 K	1536	0	2 K	2 K	0
• 間接 IPv4 ルート	1 K	1280	0	1 K	6 K	1 K

表 2-21　デュアル IPv4/IPv6 テンプレートによって許容される機能リソースの概算 （続き）

リソース	デスクトップ IPv4/IPv6 テンプレート			アグリゲータ IPv4/IPv6 テンプレート		
	デフォルト	ルーティング	VLAN	デフォルト	ルーティング	VLAN
IPv6 マルチキャスト グループ	1 K	1152	1 K	1 K	2176	1 K
IPv6 ユニキャスト ルートの合計：	3 K	2816	0	3 K	8 K	0
• 直接接続された IPv6 アドレス	2 K	1536	0	2 K	2 K	0
• 間接 IPv6 ユニキャスト ルート	1 K	1280	0	1 K	6 K	0
IPv4 ポリシー ベース ルーティング ACE	0	256	0	0	512	0
IPv4 または MAC QoS ACE（合計）	512	512	512	876	896	876
IPv4 または MAC セキュリティの ACE（合計）	1 K	512	1 K	512	1 K	1 K
IPv6 ポリシー ベース ルーティング ACE[1]	0	255	0	0	510	0
IPv6 QoS ACE	510	510	510	876	510	876
IPv6 セキュリティの ACE	510	510	510	876	510	876

1. このリリースでは、IPv6 ポリシー ベース ルーティングはサポートされていません。

例

次の例では、デスクトップ スイッチ上でアクセス テンプレートを設定する方法を示します。

```
Switch(config)# sdm prefer access
Switch(config)# exit
Switch# reload
```

次の例では、デスクトップ スイッチ上でルーティング テンプレートを設定する方法を示します。

```
Switch(config)# sdm prefer routing
Switch(config)# exit
Switch# reload
```

次の例では、アグリゲータ スイッチ上でデスクトップ ルーティング テンプレートを設定する方法を示します。

```
Switch(config)# sdm prefer routing desktop
Switch(config)# exit
Switch# reload
```

次の例では、デスクトップ スイッチ上でデフォルトのデュアル IPv4/IPv6 テンプレートを設定する方法を示します。

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# exit
Switch# reload
```

次の例では、スイッチのテンプレートをデフォルトのテンプレートに変更する方法を示します。アグリゲータ スイッチ上では、これはデフォルトのアグリゲータ テンプレートで、デスクトップ スイッチ上では、これはデフォルトのデスクトップ テンプレートです。

```
Switch(config)# no sdm prefer
Switch#(config)# exit
Switch# reload
```

次の例では、アグリゲータ スイッチ上でデスクトップ デフォルト テンプレートを設定する方法を示します。

```
Switch(config)# sdm prefer default desktop
Switch(config)# exit
Switch# reload
```

設定を確認するには、**show sdm prefer** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show sdm prefer	現在使用されている SDM テンプレート、または機能ごとのリソース割り当ての概算による使用可能なテンプレートを表示します。

service password-recovery

パスワードの回復メカニズムをイネーブル（デフォルト）にするには、**service password-recovery** グローバル コンフィギュレーション コマンドを使用します。このメカニズムでは、スイッチに物理的にアクセスするエンド ユーザは、スイッチの電源投入時に Mode ボタンを押して起動プロセスを中断し、新しいパスワードを割り当てることができます。パスワード回復機能の一部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。パスワード回復メカニズムがディセーブルになると、ユーザがシステムをデフォルト設定に戻すことに同意した場合だけ、ブート プロセスを中断できます。

service password-recovery

no service password-recovery

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

パスワード回復メカニズムはイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

システム管理者は **no service password-recovery** コマンドを使用して、パスワード回復機能の一部をディセーブルにできます。これによりエンド ユーザは、システムをデフォルト設定に戻すことに同意した場合だけ、パスワードをリセットできます。

パスワード回復手順を使用するには、スイッチに物理的にアクセスするユーザは、装置の電源投入時、およびポート 1X の上にある LED が消灯してから 1 ～ 2 秒の間に Mode ボタンを押します。ボタンを放すと、システムは初期化を続けます。

パスワード回復メカニズムがディセーブルの場合、次のメッセージが表示されます。

```
The password-recovery mechanism has been triggered, but
is currently disabled.Access to the boot loader prompt
through the password-recovery mechanism is disallowed at
this point.However, if you agree to let the system be
reset back to the default system configuration, access
to the boot loader prompt can still be allowed.

Would you like to reset the system back to the default configuration (y/n)?
```

（注）ユーザがシステムをデフォルト設定にリセットしない場合、Mode ボタンを押さないときと同じように通常の起動プロセスが続行します。ユーザがシステムをデフォルト設定にリセットすることを選択した場合、フラッシュ メモリのコンフィギュレーション ファイルが削除され、VLAN データベース ファイル、および *flash:vlan.dat* がある場合にはこのファイルも削除されます。**no service password-recovery** コマンドを使用して、エンド ユーザのパスワード アクセスを制御する場合、エンド ユーザがパスワード回復手順を使用してシステムをデフォルト値に戻す状況を考慮し、スイッチとは別の場所に config ファイルのコピーを保存しておくよう推奨します。スイッチ上に config ファイルのバックアップを保存しないでください。

スイッチが VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）透過モードで動作している場合、vlan.dat ファイルもスイッチとは別の場所にコピーを保存しておくことを推奨します。

service password-recovery または **no service password-recovery** コマンドをスタック マスター上で入力した場合、コマンドはスタック全体に伝播され、スタック内のすべてのスイッチに適用されます。

パスワードの回復がイネーブルかディセーブルかを確認するには、**show version** 特権 EXEC コマンドを入力します。

例

次の例では、スイッチ上またはスイッチ スタック上でパスワード回復をディセーブルにする方法を示します。ユーザはデフォルト設定に戻すことに同意した場合だけ、パスワードをリセットできます。

```
Switch(config)# no service-password recovery
Switch(config)# exit
```

関連コマンド

コマンド	説明
show version	ハードウェアおよびファームウェアのバージョン情報を表示します。

service-policy

policy-map コマンドで定義されたポリシー マップを、物理ポートまたは Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）の入力に適用するには、**service-policy** 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。ポリシー マップとポートの対応付けを削除するには、このコマンドの **no** 形式を使用します。

service-policy input *policy-map-name*

no service-policy input *policy-map-name*

構文の説明

input *policy-map-name*	物理ポートまたは SVI の入力に、指定したポリシー マップを適用します。

（注）

history キーワードは、コマンドラインのヘルプ ストリングには表示されますが、サポートされていません。このキーワードが収集した統計情報は無視します。**output** キーワードもサポートされていません。

デフォルト

ポートにポリシー マップは適用されていません。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(25)SE	ポリシー マップを物理ポートまたは SVI に適用できます。
12.2(25)SED	階層ポリシー マップを SVI に適用できます。

使用上のガイドライン

サポートされるポリシー マップは、入力ポートに 1 つだけです。

ポリシー マップは物理ポートまたは SVI で設定できます。物理ポートに **no mls qos vlan-based** インターフェイス コンフィギュレーション コマンドを使用して VLAN ベース Quality of Service（QoS）をディセーブルにすると、ポートにポート ベースのポリシー マップを設定できます。**no mls qos vlan-based** インターフェイス コンフィギュレーション コマンドを使用して物理ポートで VLAN ベース QoS をイネーブルにすると、すでに設定済みのポート ベース ポリシー マップが削除されます。階層ポリシー マップを設定して SVI に適用すると、インターフェイス レベル ポリシー マップがインターフェイスに反映されます。

ポリシー マップは、物理ポートまたは SVI 上の着信トラフィックに適用できます。VLAN レベルのポリシー マップで定義された各クラスに対して、異なるインターフェイス レベル ポリシー マップを設定できます。階層ポリシー マップについては、このリリースに対応するソフトウェア コンフィギュレーション ガイドで「Configuring QoS」の章を参照してください。

ポート信頼状態を使用した分類（たとえば、**mls qos trust** [**cos** | **dscp** | **ip-precedence**]）とポリシーマップ（たとえば、**service-policy input** *policy-map-name*）は同時に指定できません。最後に行われた設定により、前の設定が上書きされます。

police aggregate コマンドを使用するポリシー マップを 10 ギガビット イーサネット インターフェイスに適用すると、エラーになります。

例

次の例では、物理入力ポートに *plcmap1* を適用する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# service-policy input plcmap1
```

次の例では、物理ポートから *plcmap2* を削除する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# no service-policy input plcmap2
```

次の例では、VLAN ベース QoS がイネーブルの場合に、入力 SVI に *plcmap1* を適用する方法を示します。

```
Switch(config)# interface vlan 10
Switch(config-if)# service-policy input plcmap1
```

次の例は、階層ポリシー マップを作成し、SVI に適用する方法を示しています。

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# access-list 101 permit ip any any
Switch(config)# class-map cm-1
Switch(config-cmap)# match access 101
Switch(config-cmap)# exit
Switch(config)# exit
Switch#
Switch#
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# class-map cm-interface-1
Switch(config-cmap)# match input gigabitethernet3/0/1 - gigabitethernet3/0/2
Switch(config-cmap)# exit
Switch(config)# policy-map port-plcmap
Switch(config-pmap)# class-map cm-interface-1
Switch(config-pmap-c)# police 900000 9000 exc policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)#exit
Switch(config)# policy-map vlan-plcmap
Switch(config-pmap)# class-map cm-1
Switch(config-pmap-c)# set dscp 7
Switch(config-pmap-c)# service-policy port-plcmap-1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class-map cm-2
Switch(config-pmap-c)# match ip dscp 2
Switch(config-pmap-c)# service-policy port-plcmap-1
Switch(config-pmap)# exit
Switch(config-pmap)# class-map cm-3
Switch(config-pmap-c)# match ip dscp 3
Switch(config-pmap-c)# service-policy port-plcmap-2
Switch(config-pmap)# exit
Switch(config-pmap)# class-map cm-4
Switch(config-pmap-c)# trust dscp
Switch(config-pmap)# exit
Switch(config)# interface vlan 10
```

```
Switch(config-if)#
Switch(config-if)# ser input vlan-plcmap
Switch(config-if)# exit
Switch(config)# exit
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
policy-map	複数のポートに接続可能なポリシー マップを作成または変更して、サービス ポリシーを指定します。
show policy-map	QoS ポリシー マップを表示します。
show running-config	スイッチの実行コンフィギュレーションを表示します。

session

特定のスタック メンバにアクセスするか、Catalyst 3750G Integrated Wireless LAN Controller スイッチのコントローラにアクセスするには、スタック マスター上で **session** 特権 EXEC コマンドを使用します。

session *stack-member-number* [**processor 1**]

構文の説明

stack-member-number	メンバ番号を指定します。指定できる範囲は 1 ～ 9 です。
processor 1	（任意）セッションの宛先プロセッサ（Catalyst 3750G Integrated Wireless LAN Controller スイッチの組み込みコントローラ）を指定します。このキーワードを入力すると、コントローラ CLI を使用できます。 **（注）** このキーワードは、ワイヤレス LAN コントローラ スイッチだけに適用されます。

デフォルト

デフォルト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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(25)FZ	Catalyst 3750G Integrated Wireless LAN Controller スイッチの **processor** キーワードが追加されました。

使用上のガイドライン

メンバにアクセスすると、メンバの番号がシステム プロンプトに追加されます。

メンバ スイッチにアクセスするには、マスターから **session** コマンドを使用します。

内部コントローラにアクセスするには、マスターまたはスタンドアロン スイッチから、**processor 1** を指定して **session** コマンドを使用します。スタンドアロン スイッチは常にメンバ 1 です。

コントローラのコマンドライン インターフェイスに変更するには、**processor 1** キーワードを使用します。コントローラの設定情報については、『*Cisco Wireless LAN Controller Configuration Guide Release 4.0*』を参照してください。

例

次の例では、メンバ 6 にアクセスする方法を示します。

```
Switch(config)# session 6
Switch-6#
```

次の例では、Catalyst 3750G Wireless LAN Controller スイッチ（スタンドアロンまたはスタック マスター）であるメンバ 2 のコントローラにアクセスする方法を示します。

```
Switch# session 2 processor 1
```

```
(Cisco Controller)
User:
```

関連コマンド

コマンド	説明
reload	メンバをリロードし、設定の変更を有効にします。
switch	メンバのプライオリティ値を変更します。
switch renumber	メンバ番号を変更します。
show switch	スタックおよびそのメンバに関する情報を表示します。

set

パケットの Differentiated Services Code Point（DSCP; DiffServ コード ポイント）または IP precedence 値を設定して IP トラフィックを分類するには、**set** ポリシー マップ クラス コンフィギュレーション コマンドを使用します。トラフィックの分類を削除するには、このコマンドの **no** 形式を使用します。

set {**dscp** *new-dscp* | [**ip**] **precedence** *new-precedence*}

no set {**dscp** *new-dscp* | [**ip**] **precedence** *new-precedence*}

構文の説明

dscp *new-dscp*	分類されたトラフィックに割り当てられる新しい DSCP 値です。指定できる範囲は 0 ～ 63 です。一般的に使用する値に対してはニーモニック名を入力することもできます。
[**ip**] **precedence** *new-precedence*	分類されたトラフィックに割り当てられる新しい IP precedence 値です。指定できる範囲は 0 ～ 7 です。一般的に使用する値に対してはニーモニック名を入力することもできます。

デフォルト

トラフィックの分類は定義されていません。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(25)SE	**ip dscp** *new-dscp* キーワードは、**dscp** *new-dscp* に変更されました。 **set dscp** *new-dscp* コマンドは **set ip dscp** *new-dscp* コマンドに変更されました。
12.2(25)SEC	**ip** キーワードは任意です。

使用上のガイドライン

set ip dscp ポリシー マップ クラス コンフィギュレーション コマンドを使用した場合は、スイッチによってこのコマンドはスイッチ コンフィギュレーションの **set dscp** に変更されます。**set ip dscp** ポリシー マップ クラス コンフィギュレーション コマンドを入力すると、スイッチ コンフィギュレーションではこの設定は **set dscp** として表示されます。

set ip precedence ポリシー マップ クラス コンフィギュレーション コマンドまたは **set precedence** ポリシー マップ クラス コンフィギュレーション コマンドを使用できます。スイッチ コンフィギュレーションではこの設定は **set ip precedence** として表示されます。

同じポリシー マップ内では、**set** コマンドと **trust** ポリシー マップ クラス コンフィギュレーション コマンドを同時に指定できません。

set dscp *new-dscp* コマンドまたは **set ip precedence** *new-precedence* コマンドについては、一般的な値にニーモニック名を入力できます。たとえば、**set dscp af11** コマンドを入力できます。これは **set dscp 10** コマンドの入力と同じです。**set ip precedence critical** コマンドを入力できます。これは **set ip**

precedence 5 コマンドの入力と同じです。サポートされるニーモニックのリストについては、**set dscp ?** または **set ip precedence ?** コマンドを入力して、コマンドラインのヘルプ ストリングを表示してください。

ポリシー マップ コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

例

次の例では、ポリサーが設定されていないすべての FTP トラフィックに DSCP 値 10 を割り当てる方法を示します。

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap)# exit
```

設定を確認するには、**show policy-map** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
class	指定されたクラスマップ名のトラフィック分類一致条件（**police**、**set**、および **trust** ポリシー マップ クラス コンフィギュレーション コマンドによる）を定義します。
police	分類したトラフィックにポリサーを定義します。
policy-map	複数のポートに接続可能なポリシー マップを作成または変更して、サービス ポリシーを指定します。
show policy-map	QoS ポリシー マップを表示します。
trust	**class** ポリシー マップ コンフィギュレーション コマンドまたは **class-map** 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分類されたトラフィックの信頼状態を定義します。

setup

スイッチを初期設定に設定するには、**setup** 特権 EXEC コマンドを使用します。

setup

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

setup コマンドを使用する場合、次の情報が必要になります。

- IP アドレスおよびネットワーク マスク
- 使用環境に対するパスワードの方針
- スイッチがクラスタ コマンド スイッチおよびクラスタ名として使用されるかどうか

setup コマンドを入力すると、System Configuration Dialog という対話形式のダイアログが表示されます。コンフィギュレーション プロセスが開始され、情報を求めるプロンプトが表示されます。各プロンプトの隣に表示されるカッコで囲まれた値は、**setup** コマンド機能または **configure** 特権 EXEC コマンドのいずれかを使用して設定された最後のデフォルト値です。

各プロンプトでヘルプ テキストが提供されます。ヘルプ テキストにアクセスするには、プロンプトで疑問符（**?**）のキーを入力します。

変更を中断し、System Configuration Dialog を最後まで実行せずに特権 EXEC プロンプトに戻るには、**Ctrl+C** を押します。

変更が完了すると、セットアップ プログラムにより、セットアップ セッション中に作成されたコンフィギュレーション コマンド スクリプトが表示されます。設定を NVRAM に保存するか、あるいは設定を保存せずにセットアップ プログラムまたはコマンドライン プロンプトに戻ることができます。

例

次の例では、**setup** コマンドの出力を示します。

```
Switch# setup
--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system.
```

```
Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:
Enter host name [Switch]:host-name

  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: enable-secret-password

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: enable-password

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: terminal-password

  Configure SNMP Network Management? [no]: yes
  Community string [public]:

Current interface summary
Any interface listed with OK? value "NO" does not have a valid configuration

Interface                  IP-Address      OK? Method Status                Protocol
Vlan1                      172.20.135.202  YES NVRAM  up                    up

GigabitEthernet6/0/1 unassigned      YES unset  up                    up

GigabitEthernet6/0/2 unassigned      YES unset  up                    down

<output truncated>

Port-channel1              unassigned      YES unset  up                    down

Enter interface name used to connect to the
management network from the above interface summary: vlan1

Configuring interface vlan1:
Configure IP on this interface? [yes]: yes
IP address for this interface: ip_address
Subnet mask for this interface [255.0.0.0]: subnet_mask

Would you like to enable as a cluster command switch? [yes/no]: yes

Enter cluster name: cluster-name

The following configuration command script was created:

hostname host-name
enable secret 5 $1$LiBw$0Xc1wyT.PXPkuhFwqyhVi0
enable password enable-password
line vty 0 15
password terminal-password
snmp-server community public
!
no ip routing
!
interface GigabitEthernet6/0/1
no ip address
!
interface GigabitEthernet6/0/2
no ip address
!
```

```
cluster enable cluster-name
!
end
Use this configuration? [yes/no]: yes
!
[0] Go to the IOS command prompt without saving this config.

[1] Return back to the setup without saving this config.

[2] Save this configuration to nvram and exit.

Enter your selection [2]:
```

関連コマンド

コマンド	説明
show running-config	スイッチの実行コンフィギュレーションを表示します。
show version	ハードウェアおよびファームウェアのバージョン情報を表示します。

setup express

Express Setup モードをイネーブルにするには、**setup express** グローバル コンフィギュレーション コマンドを使用します。Express Setup モードをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

setup express

no setup express

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

Express Setup 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

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

新しいスイッチ（未設定）上で Express Setup をイネーブルにする場合、Mode ボタンを 2 秒間押すことで Express Setup を開始できます。IP アドレス 10.0.0.1 を使用するとイーサネット ポート経由でスイッチにアクセスできます。その後、スイッチを Web ベースの Express Setup プログラム、または Command-Line Interface（CLI; コマンドライン インターフェイス）ベースのセットアップ プログラムで設定できます。

設定したスイッチで Mode ボタンを 2 秒間押すと、Mode ボタンの上にある LED が点滅し始めます。Mode ボタンを合計 10 秒間押し続けると、スイッチの設定は削除され、スイッチが再起動されます。その場合、スイッチは、Web ベースの Express Setup プログラムまたは CLI ベースのセットアップ プログラムのいずれかで、新しいスイッチのように設定し直すことができます。

（注）設定の変更（CLI ベースのセットアップ プログラムの始めで *no* を入力することを含む）を行うとすぐに、Express Setup による設定を利用できなくなります。Mode ボタンを 10 秒間押し続けると、再度 Express Setup だけを実行できます。これにより、設定は削除され、スイッチが再起動します。

スイッチ上で Express Setup がアクティブな場合に、**write memory** または **copy running-configuration startup-configuration** 特権 EXEC コマンドを入力すると、Express Setup は非アクティブ化されます。スイッチの IP アドレス 10.0.0.1 は有効ではなくなり、この IP アドレスを使用している接続も終了します。

no setup express コマンドの主な目的は、Mode ボタンを 10 秒間押すことによってスイッチの設定が削除されるのを防ぐことです。

例

次の例では、Express Setup モードをイネーブルにする方法を示します。

```
Switch(config)# setup express
```

Mode ボタンを押すと、Express Setup モードがイネーブルであることを確認できます。

- 未設定のスイッチでは、Mode ボタンの上にある LED は 3 秒後にグリーンになります。
- 設定されたスイッチ上では、Mode の LED が 2 秒後に点滅し、10 秒後にグリーンになります。

注意　Mode ボタンを合計 10 秒間*押し続ける*と、設定は削除され、スイッチが再起動されます。

次の例では、Express Setup モードをディセーブルにする方法を示します。

```
Switch(config)# no setup express
```

Mode ボタンを押すと、Express Setup モードがディセーブルであることを確認できます。Express Setup モードがスイッチでイネーブルでない場合、Mode LED はグリーンに点灯しない、*または*グリーンに点滅し始めます。

関連コマンド

コマンド	説明
show setup express	Express Setup モードがアクティブかどうか表示します。

show access-lists

スイッチで設定されたアクセス コントロール リスト（ACL）を表示するには、**show access-lists** 特権 EXEC コマンドを使用します。

show access-lists [*name* | *number* | **hardware counters** | **ipc**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

name	（任意）ACL の名前です。
number	（任意）ACL の番号です。指定できる範囲は 1 ～ 2699 です。
hardware counters	（任意）切り替えられ、ルーティングされたパケットのグローバル ハードウェア ACL 統計情報を表示します。
ipc	（任意）プロセス間通信（IPC）プロトコル アクセス リスト コンフィギュレーションのダウンロード情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

（注）　**rate-limit** キーワードは、コマンドラインのヘルプ ストリングには表示されていますが、サポートされていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**ipc** キーワードが追加されました。

使用上のガイドライン

スイッチは IP 標準および拡張アクセス リストだけをサポートします。したがって、許可される数値は、1 ～ 199 と 1300 ～ 2699 だけです。

このコマンドでは、設定された MAC ACL も表示します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show access-lists** コマンドの出力を示します。

```
Switch# show access-lists
Standard IP access list 1
    10 permit 1.1.1.1
    20 permit 2.2.2.2
    30 permit any
    40 permit 0.255.255.255, wildcard bits 12.0.0.0
```

```
Standard IP access list videowizard_1-1-1-1
    10 permit 1.1.1.1
Standard IP access list videowizard_10-10-10-10
    10 permit 10.10.10.10
Extended IP access list 121
    10 permit ahp host 10.10.10.10 host 20.20.10.10 precedence routine
Extended IP access list CMP-NAT-ACL
    Dynamic Cluster-HSRP deny   ip any any
    10 deny ip any host 19.19.11.11
    20 deny ip any host 10.11.12.13
    Dynamic Cluster-NAT permit ip any any
    10 permit ip host 10.99.100.128 any
    20 permit ip host 10.46.22.128 any
    30 permit ip host 10.45.101.64 any
    40 permit ip host 10.45.20.64 any
    50 permit ip host 10.213.43.128 any
    60 permit ip host 10.91.28.64 any
    70 permit ip host 10.99.75.128 any
    80 permit ip host 10.38.49.0 any
```

次の例では、**show access-lists hardware counters** コマンドの出力を示します。

```
Switch# show access-lists hardware counters
L2 ACL INPUT Statistics
     Drop:                All frame count: 855
     Drop:                All bytes count: 94143
     Drop And Log:        All frame count: 0
     Drop And Log:        All bytes count: 0
     Bridge Only:         All frame count: 0
     Bridge Only:         All bytes count: 0
     Bridge Only And Log: All frame count: 0
     Bridge Only And Log: All bytes count: 0
     Forwarding To CPU:   All frame count: 0
     Forwarding To CPU:   All bytes count: 0
     Forwarded:           All frame count: 2121
     Forwarded:           All bytes count: 180762
     Forwarded And Log:   All frame count: 0
     Forwarded And Log:   All bytes count: 0

 L3 ACL INPUT Statistics
     Drop:                All frame count: 0
     Drop:                All bytes count: 0
     Drop And Log:        All frame count: 0
     Drop And Log:        All bytes count: 0
     Bridge Only:         All frame count: 0
     Bridge Only:         All bytes count: 0
     Bridge Only And Log: All frame count: 0
     Bridge Only And Log: All bytes count: 0
     Forwarding To CPU:   All frame count: 0
     Forwarding To CPU:   All bytes count: 0
     Forwarded:           All frame count: 13586
     Forwarded:           All bytes count: 1236182
     Forwarded And Log:   All frame count: 0
     Forwarded And Log:   All bytes count: 0

 L2 ACL OUTPUT Statistics
     Drop:                All frame count: 0
     Drop:                All bytes count: 0
     Drop And Log:        All frame count: 0
     Drop And Log:        All bytes count: 0
     Bridge Only:         All frame count: 0
     Bridge Only:         All bytes count: 0
     Bridge Only And Log: All frame count: 0
     Bridge Only And Log: All bytes count: 0
```

```
    Forwarding To CPU:   All frame count: 0
    Forwarding To CPU:   All bytes count: 0
    Forwarded:           All frame count: 232983
    Forwarded:           All bytes count: 16825661
    Forwarded And Log:   All frame count: 0
    Forwarded And Log:   All bytes count: 0

L3 ACL OUTPUT Statistics
    Drop:                All frame count: 0
    Drop:                All bytes count: 0
    Drop And Log:        All frame count: 0
    Drop And Log:        All bytes count: 0
    Bridge Only:         All frame count: 0
    Bridge Only:         All bytes count: 0
    Bridge Only And Log: All frame count: 0
    Bridge Only And Log: All bytes count: 0
    Forwarding To CPU:   All frame count: 0
    Forwarding To CPU:   All bytes count: 0
    Forwarded:           All frame count: 514434
    Forwarded:           All bytes count: 39048748
    Forwarded And Log:   All frame count: 0
    Forwarded And Log:   All bytes count: 0
```

関連コマンド

コマンド	説明
access-list	スイッチに標準または拡張番号アクセス リストを設定します。
ip access-list	スイッチに指定された IP アクセス リストを設定します。
mac access-list extended	スイッチに、指定されたまたは番号の付いた MAC アクセス リストを設定します。

show archive status

HTTP または TFTP プロトコルでスイッチにダウンロードされた新しいイメージのステータスを表示するには、**show archive status** 特権 EXEC コマンドを使用します。

show archive status [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

archive download-sw 特権 EXEC コマンドを使用してイメージを TFTP サーバにダウンロードする場合、**archive download-sw** コマンドの出力では、ダウンロードのステータスが表示されます。

TFTP サーバがない場合、HTTP を使用してイメージをダウンロードするには、Network Assistant または組み込みデバイス マネージャを使用します。**show archive status** コマンドでは、ダウンロードの進捗状況が表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show archive status** コマンドの出力を示します。

```
Switch# show archive status
IDLE: No upgrade in progress

Switch# show archive status
LOADING: Upgrade in progress

Switch# show archive status
EXTRACT: Extracting the image

Switch# show archive status
VERIFY: Verifying software

Switch# show archive status
RELOAD: Upgrade completed. Reload pending
```

関連コマンド

コマンド	説明
archive download-sw	TFTP サーバからスイッチに新しいイメージをダウンロードします。

show arp access-list

Address Resolution Protocol（ARP; アドレス解決プロトコル）アクセス コントロール（リスト）に関する詳細情報を表示するには、**show arp access-list** ユーザ EXEC コマンドを使用します。

show arp access-list [*acl-name*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

acl-name	（任意）ACL の名前です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show arp access-list** コマンドの出力を示します。

```
Switch> show arp access-list
ARP access list rose
    permit ip 10.101.1.1 0.0.0.255 mac any
    permit ip 20.3.1.0 0.0.0.255 mac any
```

関連コマンド

コマンド	説明
arp access-list	ARP ACL を定義します。
deny（ARP アクセスリスト コンフィギュレーション）	Dynamic Host Configuration Protocol（DHCP）バインディングとの一致に基づいて ARP パケットを拒否します。
ip arp inspection filter vlan	スタティック IP アドレスで設定されたホストからの ARP 要求および応答を許可します。
permit（ARP アクセスリスト コンフィギュレーション）	DHCP バインディングとの一致に基づいて ARP パケットを許可します。

show authentication

スイッチで認証マネージャ イベントに関する情報を表示するには、**show authentication** コマンドを（ユーザ EXEC または特権 EXEC モードのいずれかで）使用します。

show authentication {interface *interface-id* **| registrations | sessions [session-id** *session-id***] [handle** *handle***] [interface** *interface-id***] [mac** ***mac***] **[method** ***method***]**}**

構文の説明

interface *interface-id*	（任意）指定したインターフェイスに関する認証マネージャの詳細をすべて表示します。
method *method*	（任意）指定した認証方式（**dot1x**、**mab**、または **webauth**）によって許可されたクライアントをすべて表示します。
registrations	（任意）認証マネージャ レジストレーションを表示します。
sessions	（任意）現在の認証マネージャのセッション（たとえば、クライアント装置）の詳細を表示します。オプションの指定子を入力しないと、現在アクティブなセッションがすべて表示されます。特定のセッション（またはセッションのグループ）を表示するには、指定子を単独で、または組み合わせて入力できます。
session-id *session-id*	（任意）認証マネージャのセッションを指定します。
handle *handle*	（任意）1 ～ 4294967295 の範囲を指定します。
mac *mac*	（任意）指定した MAC アドレスの認証マネージャ情報を表示します。

コマンド デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

特権 EXEC およびユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

表 2-22 で、**show authentication** コマンドの出力に表示される重要なフィールドについて説明します。

（注）　セッションのステータスに使用できる値を次に示します。終了ステートのセッションでは、結果を出した方式がない場合は、*Authz Success* または *Authz Failed* が *No methods* とともに表示されます。

表 2-22　show authentication コマンドの出力

フィールド	説明
Idle	セッションが初期化されました。方式はまだ実行されていません。
Running	このセッションの方式が実行中です。
No methods	このセッションの結果を出した方式はありません。

表 2-22　show authentication コマンドの出力 （続き）

フィールド	説明
Authc Success	方式によって、このセッションの認証が成功しました。
Authc Failed	方式によって、このセッションの認証は失敗しました。
Authz Success	このセッションでは、すべての機能が正常に適用されました。
Authz Failed	このセッションで、機能の適用に失敗しました。

表 2-23 に、方式のステートに使用できる値をリストします。終了ステートのセッションでは、*Authc Success*、*Authc Failed*、または *Failed over* が表示されます。*Failed over* は、認証方式が実行され、次の方式にフェールオーバーし、結果は提供されなかったことを意味します。*Not run* は、スタンバイで同期化したセッションの場合に表示されます。

表 2-23　ステート方式の値

方式のステート	ステート レベル	説明
Not run	終了	このセッションの方式は実行されていません。
Running	中間	このセッションの方式が実行中です。
Failed over	終了	この方式は失敗しました。次の方式が結果を出すことが予期されています。
Authc Success	終了	この方式は、セッションの成功した認証結果を提供しました。
Authc Failed	終了	この方式は、セッションの失敗した認証結果を提供しました。

例

次の例では、**show authentication registrations** コマンドを示します。

```
Switch# show authentication registrations
Auth Methods registered with the Auth Manager:
Handle Priority Name
3 0 dot1x
2 1 mab
1 2 webauth
```

次の例では、**show authentication interface** *interface-id* コマンドを示します。

```
Switch# show authentication interface gigabitethernet1/0/23
Client list:
MAC Address Domain Status Handle Interface
000e.84af.59bd DATA Authz Success 0xE0000000 GigabitEthernet1/0/23
Available methods list:
Handle Priority Name
3 0 dot1x
Runnable methods list:
Handle Priority Name
3 0 dot1x
```

次の例では、**show authentication sessions** コマンドを示します。

```
Switch# show authentication sessions
Interface  MAC Address     Method   Domain   Status         Session ID
Gi3/45     (unknown)       N/A      DATA     Authz Failed   09081404000000007003651EC
Gi3/46     (unknown)       N/A      DATA     Authz Success  09081404000000080057C274
```

次の例では、指定されたインターフェイスの **show authentication sessions** コマンドを示します。

```
Switch# show authentication sessions int gigabitethernet 3/0/46
            Interface:  GigabitEthernet3/0/46
          MAC Address:  Unknown
           IP Address:  Unknown
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  multi-host
     Oper control dir:  both
        Authorized By:  Guest Vlan
          Vlan Policy:  4094
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  09081404000000080057C274
      Acct Session ID:  0x0000000A
               Handle:  0xCC000008
Runnable methods list:
       Method   State
       dot1x    Failed over
```

次の例では、指定された MAC アドレスの **show authentication sessions** コマンドを示します。

```
Switch# show authentication sessions mac 000e.84af.59bd
Interface: GigabitEthernet3/0/46
MAC Address: 000e.84af.59bd
Status: Authz Success
Domain: DATA
Oper host mode: single-host
Authorized By: Authentication Server
Vlan Policy: 10
Handle: 0xE0000000
Runnable methods list:
Method State
dot1x Authc Success
```

次の例では、指定された方式の **show authentication session method** コマンドを示します。

```
Switch# show authentication sessions method mab
No Auth Manager contexts match supplied criteria
Switch# show authentication sessions method dot1x
MAC Address Domain Status Handle Interface
000e.84af.59bd DATA Authz Success 0xE0000000 GigabitEthernet1/23
```

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。

コマンド	説明
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータと再認証パラメータを設定します。

show auto qos

Automatic QoS（auto-QoS）がイネーブルのインターフェイスで入力された Quality of Service（QoS）コマンドを表示するには、**show auto qos** ユーザ EXEC コマンドを使用します。

show auto qos [**interface** [*interface-id*]]

構文の説明

interface [*interface-id*]	（任意）指定されたポートまたはすべてのポートの auto-QoS 情報を表示します。有効なインターフェイスには、物理ポートが含まれます。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。
12.2(20)SE	コマンド出力の情報が変更され、ユーザの注意事項が更新されました。
12.2(40)SE	コマンド出力の情報が変更されました。

使用上のガイドライン

show auto qos コマンド出力には、各インターフェイスに入力された auto-QoS コマンドだけが表示されます。**show auto qos interface** *interface-id* コマンド出力は、特定のインターフェイスに入力された auto-QoS コマンドを表示します。

auto-QoS 設定およびユーザ変更を表示する場合は、**show running-config** 特権 EXEC コマンドを使用します。

show auto qos コマンド出力には、Cisco IP Phone のサービス ポリシー情報も表示されます。

auto-QoS の影響を受ける可能性のある現在の QoS の設定情報を表示するには、次のいずれかのコマンドを使用します。

- **show mls qos**
- **show mls qos maps cos-dscp**
- **show mls qos interface** [*interface-id*] [**buffers** | **queueing**]
- **show mls qos maps** [**cos-dscp** | **cos-input-q** | **cos-output-q** | **dscp-cos** | **dscp-input-q** | **dscp-output-q**]
- **show mls qos input-queue**
- **show running-config**

例

次の例では、**auto qos voip cisco-phone** および **auto qos voip cisco-softphone** インターフェイス コンフィギュレーション コマンドを入力した場合の **show auto qos** コマンドの出力を示します。

```
Switch> show auto qos
GigabitEthernet2/0/4
auto qos voip cisco-softphone

GigabitEthernet2/0/5
auto qos voip cisco-phone

GigabitEthernet2/0/6
auto qos voip cisco-phone
```

次の例では、**auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドを入力した場合の **show auto qos interface** *interface-id* コマンドの出力を示します。

```
Switch> show auto qos interface gigabitethernet 2/0/5
GigabitEthernet2/0/5
auto qos voip cisco-phone
```

次の例では、**auto qos voip cisco-phone** および **auto qos voip cisco-softphone** インターフェイス コンフィギュレーション コマンドを入力した場合の **show running-config** 特権 EXEC コマンドの出力を示します。

```
Switch# show running-config
Building configuration...
...
mls qos map policed-dscp  24 26 46 to 0
mls qos map cos-dscp 0 8 16 26 32 46 48 56
mls qos srr-queue input bandwidth 90 10
mls qos srr-queue input threshold 1 8 16
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 67 33
mls qos srr-queue input cos-map queue 1 threshold 2  1
mls qos srr-queue input cos-map queue 1 threshold 3  0
mls qos srr-queue input cos-map queue 2 threshold 1  2
mls qos srr-queue input cos-map queue 2 threshold 2  4 6 7
mls qos srr-queue input cos-map queue 2 threshold 3  3 5
mls qos srr-queue input dscp-map queue 1 threshold 2  9 10 11 12 13 14 15
mls qos srr-queue input dscp-map queue 1 threshold 3  0 1 2 3 4 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3  32
mls qos srr-queue input dscp-map queue 2 threshold 1  16 17 18 19 20 21 22 23
mls qos srr-queue input dscp-map queue 2 threshold 2  33 34 35 36 37 38 39 48
mls qos srr-queue input dscp-map queue 2 threshold 2  49 50 51 52 53 54 55 56
mls qos srr-queue input dscp-map queue 2 threshold 2  57 58 59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3  24 25 26 27 28 29 30 31
mls qos srr-queue input dscp-map queue 2 threshold 3  40 41 42 43 44 45 46 47
mls qos srr-queue output cos-map queue 1 threshold 3  5
mls qos srr-queue output cos-map queue 2 threshold 3  3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3  2 4
mls qos srr-queue output cos-map queue 4 threshold 2  1
mls qos srr-queue output cos-map queue 4 threshold 3  0
mls qos srr-queue output dscp-map queue 1 threshold 3  40 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3  24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 2 threshold 3  48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3  56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3  16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3  32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1  8
mls qos srr-queue output dscp-map queue 4 threshold 2  9 10 11 12 13 14 15
mls qos srr-queue output dscp-map queue 4 threshold 3  0 1 2 3 4 5 6 7
mls qos queue-set output 1 threshold 1 100 100 100 100
```

```
mls qos queue-set output 1 threshold 2 75 75 75 250
mls qos queue-set output 1 threshold 3 75 150 100 300
mls qos queue-set output 1 threshold 4 50 100 75 400
mls qos queue-set output 2 threshold 1 100 100 100 100
mls qos queue-set output 2 threshold 2 35 35 35 35
mls qos queue-set output 2 threshold 3 55 82 100 182
mls qos queue-set output 2 threshold 4 90 250 100 400
mls qos queue-set output 1 buffers 15 20 20 45
mls qos queue-set output 2 buffers 24 20 26 30
mls qos
...
!
class-map match-all AutoQoS-VoIP-RTP-Trust
  match ip dscp ef
class-map match-all AutoQoS-VoIP-Control-Trust
  match ip dscp cs3  af31
!
policy-map AutoQoS-Police-SoftPhone
  class AutoQoS-VoIP-RTP-Trust
   set dscp ef
    police 320000 8000 exceed-action policed-dscp-transmit
  class AutoQoS-VoIP-Control-Trust
   set dscp cs3
    police 32000 8000 exceed-action policed-dscp-transmit
!
policy-map AutoQoS-Police-CiscoPhone
  class AutoQoS-VoIP-RTP-Trust
   set dscp ef
    police 320000 8000 exceed-action policed-dscp-transmit
  class AutoQoS-VoIP-Control-Trust
   set dscp cs3
    police 32000 8000 exceed-action policed-dscp-transmit
...
!
interface GigabitEthernet2/0/4
switchport mode access
 switchport port-security maximum 400
 service-policy input AutoQoS-Police-SoftPhone
 speed 100
 duplex half
 srr-queue bandwidth share 10 10 60 20
 priority-queue out
 auto qos voip cisco-softphone
!
interface GigabitEthernet2/0/5
 switchport mode access
 switchport port-security maximum 1999
 speed 100
 duplex full
 srr-queue bandwidth share 10 10 60 20
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
!
interface GigabitEthernet2/0/6
switchport trunk encapsulation dot1q
 switchport trunk native vlan 2
 switchport mode access
 speed 10
 srr-queue bandwidth share 10 10 60 20
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
```

```
 auto qos voip cisco-phone
!
interface GigabitEthernet4/0/1
srr-queue bandwidth share 10 10 60 20
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 mls qos trust device cisco-phone
service-policy input AutoQoS-Police-CiscoPhone

<output truncated>
```

次の例では、**auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドを入力した場合の **show auto qos interface** *interface-id* コマンドの出力を示します。

```
Switch> show auto qos interface fastethernet1/0/2
FastEthernet1/0/2
auto qos voip cisco-softphone
```

次の例では、Auto-QoS がスイッチでディセーブルの場合の **show auto qos** コマンドの出力を示します。

```
Switch> show auto qos
AutoQoS not enabled on any interface
```

次の例では、Auto-QoS がインターフェイスでディセーブルの場合の **show auto qos interface** *interface-id* コマンドの出力を示します。

```
Switch> show auto qos interface gigabitethernet3/0/1
AutoQoS is disabled
```

関連コマンド

コマンド	説明
auto qos voip	QoS ドメイン内の Voice over IP（VoIP）に QoS を自動設定します。
debug auto qos	auto-QoS 機能のデバッグをイネーブルにします。

show boot

BOOT 環境変数の設定を表示するには、**show boot** 特権 EXEC コマンドを使用します。

show boot [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show boot** コマンドの出力を示します。表 2-24 に、表示される各フィールドの説明を示します。

```
Switch# show boot
BOOT path-list      :flash:/image
Config file         :flash:/config.text
Private Config file :flash:/private-config.text
Enable Break        :no
Manual Boot         :yes
HELPER path-list    :
Auto upgrade        :yes
-------------------
```

スイッチ スタックでは、情報はスタック内の各スイッチに対して表示されます。

表 2-24　show boot のフィールドの説明

フィールド	説明
BOOT path-list	自動起動時にロードおよび実行しようとする実行可能ファイルのセミコロン区切りリストを表示します。 BOOT 環境変数が設定されていない場合、システムは、フラッシュ ファイル システム全体に再帰的な縦型検索を行って、最初に検出された実行可能イメージをロードして実行を試みます。ディレクトリの縦型検索では、検出した各サブディレクトリを完全に検索してから元のディレクトリでの検索を続けます。 BOOT 環境変数が設定されていても指定されたイメージをロードできない場合は、システムはフラッシュ ファイル システムで最初に見つかったブート ファイルを起動しようとします。
Config file	Cisco IOS がシステム コンフィギュレーションの不揮発性コピーの読み書きに使用するファイル名を表示します。
Private Config file	Cisco IOS がシステム コンフィギュレーションの不揮発性コピーの読み書きに使用するファイル名を表示します。
Enable Break	起動中のブレークがイネーブルか、またはディセーブルかを表示します。yes、on、または 1 に設定されている場合は、フラッシュ ファイル システムの初期化後にコンソール上で Break キーを押すと、自動起動プロセスを中断できます。
Manual Boot	スイッチが自動で起動するか、または手動で起動するかを表示します。no または 0 に設定されている場合、ブート ローダーはシステムを自動的に起動しようとします。それ以外に設定されている場合は、ブート ローダー モードから手動でスイッチを起動する必要があります。
Helper path-list	ブート ローダーの初期化中に動的にロードされるロード可能ファイルのセミコロン区切りリストを表示します。ヘルパー ファイルは、ブート ローダーの機能を拡張したり、パッチを当てたりします。
Auto upgrade	スイッチ スタックが、互換性のないスイッチがスタックに加入できるよう、ソフトウェア バージョンの自動コピーが設定されているかどうかを表示します。 Version-Mismatch モードにあるスイッチは、スタックとは異なるバージョンのスタック プロトコルが適用されています。Version-Mismatch モードのスイッチはスタックに加入できません。スタックが Version-Mismatch モードのスイッチにコピーできるイメージを保有し、**boot auto-copy-sw** 機能がイネーブルの場合、他のスタック メンバからのイメージを Version-Mismatch モードのスイッチに自動的にコピーします。その場合、スイッチは Version-Mismatch モードを終了し、再起動後にスタックに加入します。

関連コマンド

コマンド	説明
boot auto-copy-sw	Version-Mismatch モードのスイッチを自動的にアップグレードするには、自動アップグレード（auto-upgrade）プロセスをイネーブルにします。
boot config-file	Cisco IOS がシステム設定の不揮発性コピーの読み書きに使用するファイル名を指定します。
boot enable-break	自動起動プロセスを中断できます。
boot manual	次の起動サイクル時の手動スイッチ起動をイネーブルにします。
boot private-config-file	Cisco IOS がプライベート設定の不揮発性コピーの読み書きに使用するファイル名を指定します。
boot system	次の起動サイクル中にロードする Cisco IOS イメージを指定します。

show cable-diagnostics tdr

Time Domain Reflector（TDR; タイム ドメイン反射率計）結果を表示するには、**show cable-diagnostics tdr** 特権 EXEC コマンドを使用します。

show cable-diagnostics tdr interface *interface-id* [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface-id	TDR が実行されているインターフェイスを指定します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。

使用上のガイドライン

TDR は、銅線のイーサネット 10/100/100 ポートだけでサポートされます。10/100 ポート、10 ギガビット モジュール ポート、または SFP モジュール ポートではサポートされません。TDR の詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、Catalyst 3750G-24PS または 3750G-48PS スイッチ以外のスイッチでの **show cable-diagnostics tdr interface** *interface-id* コマンドの出力を示します。

```
Switch# show cable-diagnostics tdr interface gigabitethernet1/01/0/2
TDR test last run on: March 01 20:15:40
Interface Speed Local pair Pair length        Remote pair Pair status
--------- ----- ---------- ------------------ ----------- --------------------
Gi/2     auto  Pair A     0    +/- 2  meters N/A         Open

               Pair B     0    +/- 2  meters N/A         Open
               Pair C     0    +/- 2  meters N/A         Open
               Pair D     0    +/- 2  meters N/A         Open
```

次の例では、Catalyst 3750G-24PS または 3750G-48PS スイッチでの **show cable-diagnostics tdr interface** *interface-id* コマンドの出力を示します。

```
Switch# show cable-diagnostics tdr interface gigabitethernet1/0/2
TDR test last run on: March 01 20:15:40
Interface Speed Local pair Pair length        Remote pair Pair status
--------- ----- ---------- ------------------ ----------- --------------------
Gi1/0/2   auto  Pair A     0    +/- 4 meters  N/A         Open

                Pair B     0    +/- 4 meters  N/A         Open
                Pair C     0    +/- 4 meters  N/A         Open
                Pair D     0    +/- 4 meters  N/A         Open
```

表 2-25 に、**show cable-diagnostics tdr** コマンドで出力されるフィールドの説明を示します。

表 2-25　show cable-diagnostics tdr コマンドで出力されるフィールドの説明

フィールド	説明
Interface	TDR が実行されたインターフェイス
Speed	接続速度
Local pair	ローカル インターフェイスで TDR がテストを実行するワイヤ ペア名
Pair length	使用するスイッチについて、問題が発生したケーブルの場所。次のいずれかの場合に限り、TDR は場所を特定できます。 • ケーブルが正しく接続され、リンクがアップ状態で、インターフェイス速度が 1000 Mb/s である場合 • ケーブルが断線している場合 • ケーブルがショートしている場合
Remote pair	ローカル ペアが接続されたワイヤ ペア名。ケーブルが正しく接続されリンクがアップ状態である場合だけ、TDR はリモート ペアについて確認します。
Pair status	TDR が実行されているワイヤ ペアのステータス • Normal：ワイヤ ペアが正しく接続されています。 • Not completed：テストは実行中で、完了していません。 • Not supported：インターフェイスは TDR をサポートしません。 • Open：ワイヤ ペアが断線しています。 • Shorted：ワイヤ ペアがショートしています。 • ImpedanceMis：インピーダンスが一致しません。 • Short/Impedance Mismatched：インピーダンスが一致しないかケーブルがショートしています。 • InProgress：診断テストが進行中です。

次の例では、TDR が実行されているときの **show interfaces** *interface-id* コマンドの出力を示します。

```
Switch# show interfaces gigabitethernet1/01/2
gigabitethernet1/0/2 is up, line protocol is up (connected: TDR in Progress)
```

次の例では、TDR が実行されていないときの **show cable-diagnostics tdr interface** *interface-id* コマンドの出力を示します。

```
Switch# show cable-diagnostics tdr interface gigabitethernet1/01/2
% TDR test was never issued on Gi1/0/2
```

インターフェイスで TDR がサポートされない場合、次のメッセージが表示されます。

```
% TDR test is not supported on switch 1
```

関連コマンド

コマンド	説明
test cable-diagnostics tdr	インターフェイスで TDR をイネーブルにし、実行します。

show cdp forward

CDP フォワーディング テーブルを表示するには、**show cdp forward** ユーザ EXEC コマンドを使用します。

show cdp forward [**entry** | **forward** | **interface** *interface-id* | **neighbor** | **traffic**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

entry	（任意）特定のネイバー エントリに関する情報を表示します。
forward	（任意）CDP フォワーディング情報を表示します。
interface *interface-id*	（任意）CDP インターフェイスのステータスと設定を表示します。
neighbor	（任意）CDP ネイバー エントリを表示します。
traffic	（任意）CDP の統計情報を表示します。
begin	（任意）expression と一致する行から表示を開始します。
exclude	（任意）expression と一致する行を表示から除外します。
include	（任意）指定された expression と一致する行を表示に含めます。
expression	（任意）参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(53)SE	このコマンドが追加されました。

使用上のガイドライン

show cdp forward コマンド出力は、入力ポートと出力ポートの各マッピングで転送される CDP パケットの数、および転送されてドロップされたパケットの統計情報を表示します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

```
Switch# show cdp forward
Ingress         Egress          # packets         # packets
Port            Port            forwarded         dropped
-------------------------------------------------------------
 Gi2/0/2        Gi2/0/13            0                 0
```

関連コマンド

コマンド	説明
cdp forward	CDP トラフィックの入力および出力スイッチ ポートを設定します。

show cisp

指定されたインターフェイスの CISP 情報を表示するには、**show cisp** 特権 EXEC コマンドを使用します。

show cisp {[**interface** *interface-id*] | **clients** | **summary**} | {[**begin** | **exclude** | **include**} *expression*]}

構文の説明

clients	（任意）CISP クライアントの詳細を表示します。
interface *interface-id*	（任意）指定されたインターフェイスの CISP 情報を表示します。有効なインターフェイスには、物理ポートとポート チャネルが含まれます。
summary	（任意）表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

例

次の例では、**show cisp interface** コマンドの出力を示します。

```
WS-C3750E-48TD#show cisp interface fast 0
CISP not enabled on specified interface
```

次の例では、**show cisp summary** コマンドの出力を示します。

```
CISP is not running on any interface
```

関連コマンド

コマンド	説明
dot1x credentials *profile*	サプリカント スイッチでプロファイルを設定します。
cisp enable	Client Information Signalling Protocol（CISP）をイネーブルにします。

show class-map

トラフィックを分類するための一致基準を定義する Quality of Service（QoS）クラス マップを表示するには、**show class-map** ユーザ EXEC コマンドを使用します。

show class-map [*class-map-name*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

class-map-name	（任意）指定されたクラス マップの内容を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show class-map** コマンドの出力を示します。

```
Switch> show class-map
Class Map match-all videowizard_10-10-10-10 (id 2)
   Match access-group name videowizard_10-10-10-10

 Class Map match-any class-default (id 0)
   Match any
 Class Map match-all dscp5 (id 3)
   Match ip dscp 5
```

関連コマンド

コマンド	説明
class-map	名前を指定したクラスとパケットとの照合に使用されるクラス マップを作成します。
match（クラスマップ コンフィギュレーション）	トラフィックを分類するための一致条件を定義します。

show cluster

スイッチが属するクラスタのステータスおよびサマリーを表示するには、**show cluster** ユーザ EXEC コマンドを使用します。このコマンドは、クラスタ コマンド スイッチとクラスタ メンバ スイッチで入力できます。

show cluster [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

クラスタのメンバでないスイッチ上でこのコマンドを入力すると、エラー メッセージ「`Not a management cluster member`」が表示されます。

クラスタ メンバ スイッチ上でこのコマンドを入力すると、クラスタ コマンド スイッチの ID、そのスイッチ メンバの番号、およびクラスタ コマンド スイッチとの接続状態が表示されます。

クラスタ コマンド スイッチのスタックまたはクラスタ コマンド スイッチ上でこのコマンドを入力すると、クラスタ名およびメンバの総数が表示されます。また、ステータス変更後のクラスタのステータスおよび時間も表示されます。冗長構成がイネーブルの場合は、プライマリおよびセカンダリ コマンド スイッチの情報が表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、アクティブなクラスタ コマンド スイッチ上で **show cluster** コマンドを入力した場合の出力を示します。

```
Switch> show cluster
Command switch for cluster "Ajang"
        Total number of members:        7
        Status:                         1 members are unreachable
        Time since last status change:  0 days, 0 hours, 2 minutes
        Redundancy:                     Enabled
                Standby command switch: Member 1
                Standby Group:          Ajang_standby
                Standby Group Number:   110
        Heartbeat interval:             8
        Heartbeat hold-time:            80
        Extended discovery hop count:   3
```

次の例では、クラスタ メンバ スイッチ上で **show cluster** コマンドを入力した場合の出力を示します。

```
Switch1> show cluster
Member switch for cluster "hapuna"
        Member number:                  3
        Management IP address:          192.192.192.192
        Command switch mac address:     0000.0c07.ac14
        Heartbeat interval:             8
        Heartbeat hold-time:            80
```

次の例では、スタンバイ クラスタ コマンド スイッチとして設定されたクラスタ メンバ スイッチ上で **show cluster** コマンドを入力した場合の出力を示します。

```
Switch> show cluster
Member switch for cluster "hapuna"
        Member number:                  3 (Standby command switch)
        Management IP address:          192.192.192.192
        Command switch mac address:     0000.0c07.ac14
        Heartbeat interval:             8
        Heartbeat hold-time:            80
```

次の例では、メンバ 1 との接続が切断されたクラスタ コマンド スイッチ上で **show cluster** コマンドを入力した場合の出力を示します。

```
Switch> show cluster
Command switch for cluster "Ajang"
        Total number of members:        7
        Status:                         1 members are unreachable
        Time since last status change:  0 days, 0 hours, 5 minutes
        Redundancy:                     Disabled
        Heartbeat interval:             8
        Heartbeat hold-time:            80
        Extended discovery hop count:   3
```

次の例では、クラスタ コマンド スイッチとの接続が切断されたクラスタ メンバ スイッチ上で **show cluster** コマンドを入力した場合の出力を示します。

```
Switch> show cluster
Member switch for cluster "hapuna"
        Member number:                  <UNKNOWN>
        Management IP address:          192.192.192.192
        Command switch mac address:     0000.0c07.ac14
        Heartbeat interval:             8
        Heartbeat hold-time:            80
```

関連コマンド

コマンド	説明
cluster enable	コマンド対応スイッチをクラスタ コマンド スイッチとしてイネーブルにし、クラスタ名、およびオプションとしてメンバ番号を割り当てます。
show cluster candidates	候補スイッチのリストを表示します。
show cluster members	クラスタ メンバに関する情報を表示します。

show cluster candidates

候補スイッチのリストを表示するには、**show cluster candidates** 特権 EXEC コマンドを使用します。

show cluster candidates [**detail** | **mac-address** *H.H.H.*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

detail	（任意）すべての候補に関する詳細を表示します。
mac-address *H.H.H.*	（任意）クラスタ候補の MAC アドレスです。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドが利用できるのは、クラスタ コマンド スイッチ スタックまたはクラスタ コマンド スイッチに限られます。

スイッチがクラスタ コマンド スイッチでない場合は、プロンプトに空行が表示されます。

出力内の SN は、*スイッチ メンバ番号*を意味します。SN 列の値に E が表示された場合、スイッチは拡張検出によって検出されています。SN 列の値が E でない場合、*スイッチ メンバ番号*のスイッチは、候補スイッチのアップストリーム側ネイバーです。ホップ数は、クラスタ コマンド スイッチから候補スイッチまでのデバイス数です。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show cluster candidates** コマンドの出力を示します。

```
Switch> show cluster candidates
                                                          |---Upstream---|
        MAC Address    Name         Device Type      PortIf  FEC Hops SN PortIf  FEC
        00d0.7961.c4c0 StLouis-2    WS-C3750-12T     Gi6/0/1        2   1  Fa0/11
        00d0.bbf5.e900 ldf-dist-128 WS-C3524-XL      Fa0/7        1   0  Fa0/24
        00e0.1e7e.be80 1900_Switch  1900             3        0   1   0  Fa0/11
        00e0.1e9f.7a00 Surfers-24   WS-C2924-XL      Fa0/5        1   0  Fa0/3
        00e0.1e9f.8c00 Surfers-12-2 WS-C2912-XL      Fa0/4        1   0  Fa0/7
        00e0.1e9f.8c40 Surfers-12-1 WS-C2912-XL      Fa0/1        1   0  Fa0/9
```

次の例では、クラスタ コマンド スイッチに直接接続された、クラスタ メンバ スイッチの MAC アドレスを使用した場合の **show cluster candidates** コマンドの出力を示します。

```
Switch> show cluster candidates mac-address 00d0.7961.c4c0
```

```
Device 'Tahiti-12' with mac address number 00d0.7961.c4c0
        Device type:            cisco WS-C3750-12T
        Upstream MAC address:   00d0.796d.2f00 (Cluster Member 0)
        Local port:             Gi6/0/1   FEC number:
        Upstream port:          GI6/0/11  FEC Number:
Hops from cluster edge: 1
        Hops from command device: 1
```

次の例では、クラスタ エッジからのホップ数が 3 である、クラスタ メンバ スイッチの MAC アドレスを使用した場合の **show cluster candidates** コマンドの出力を示します。

```
Switch> show cluster candidates mac-address 0010.7bb6.1cc0
Device 'Ventura' with mac address number 0010.7bb6.1cc0
        Device type:            cisco WS-C2912MF-XL
        Upstream MAC address:   0010.7bb6.1cd4
        Local port:             Fa2/1   FEC number:
        Upstream port:          Fa0/24  FEC Number:
        Hops from cluster edge: 3
        Hops from command device: -
```

次の例では、**show cluster candidates detail** コマンドの出力を示します。

```
Switch> show cluster candidates detail
Device 'Tahiti-12' with mac address number 00d0.7961.c4c0
        Device type:            cisco WS-C3512-XL
        Upstream MAC address:   00d0.796d.2f00 (Cluster Member 1)
        Local port:             Fa0/3   FEC number:
        Upstream port:          Fa0/13  FEC Number:
        Hops from cluster edge: 1
        Hops from command device: 2
Device '1900_Switch' with mac address number 00e0.1e7e.be80
        Device type:            cisco 1900
        Upstream MAC address:   00d0.796d.2f00 (Cluster Member 2)
        Local port:             3       FEC number: 0
        Upstream port:          Fa0/11  FEC Number:
        Hops from cluster edge: 1
        Hops from command device: 2
Device 'Surfers-24' with mac address number 00e0.1e9f.7a00
        Device type:            cisco WS-C2924-XL
        Upstream MAC address:   00d0.796d.2f00 (Cluster Member 3)
        Local port:             Fa0/5   FEC number:
        Upstream port:          Fa0/3   FEC Number:
        Hops from cluster edge: 1
        Hops from command device: 2
```

関連コマンド

コマンド	説明
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。
show cluster members	クラスタ メンバに関する情報を表示します。

show cluster members

クラスタ メンバの情報を表示するには、**show cluster members** 特権 EXEC コマンドを使用します。

show cluster members [*n* | **detail**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

n	（任意）クラスタ メンバを識別する番号。指定できる範囲は 0 ～ 15 です。
detail	（任意）すべてのクラスタ メンバに関する詳細を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドが利用できるのは、クラスタ コマンド スイッチ スタックまたはクラスタ コマンド スイッチに限られます。

クラスタ内にメンバがない場合は、プロンプトに空行が表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show cluster members** コマンドの出力を示します。出力内の SN は、*スイッチ番号*を意味します。

```
Switch# show cluster members
                                                |---Upstream---|
SN MAC Address    Name         PortIf FEC Hops   SN PortIf  FEC  State
0  0002.4b29.2e00 StLouis1                 0                    Up   (Cmdr)
1  0030.946c.d740 tal-switch-1 Fa0/13      1     0  Gi0/1       Up
2  0002.b922.7180 nms-2820     10      0   2     1  Fa0/18      Up
3  0002.4b29.4400 SanJuan2     Gi0/1       2     1  Fa0/11      Up
4  0002.4b28.c480 GenieTest    Gi0/2       2     1  Fa0/9       Up
```

次の例では、クラスタ メンバ 3 に対する **show cluster members** の出力を示します。

```
Switch# show cluster members 3
Device 'SanJuan2' with member number 3
        Device type:            cisco WS-C3750
        MAC address:            0002.4b29.4400
        Upstream MAC address:   0030.946c.d740 (Cluster member 1)
        Local port:             Gi6/0/1   FEC number:
        Upstream port:          GI6/0/11  FEC Number:
        Hops from command device: 2
```

次の例では、**show cluster members detail** コマンドの出力を示します。

```
Switch# show cluster members detail
Device 'StLouis1' with member number 0 (Command Switch)
        Device type:            cisco WS-C3750
        MAC address:            0002.4b29.2e00
        Upstream MAC address:
        Local port:                     FEC number:
        Upstream port:                  FEC Number:
        Hops from command device: 0
Device 'tal-switch-14' with member number 1
        Device type:            cisco WS-C3548-XL
        MAC address:            0030.946c.d740
        Upstream MAC address:   0002.4b29.2e00 (Cluster member 0)
        Local port:             Fa0/13  FEC number:
        Upstream port:          Gi0/1   FEC Number:
        Hops from command device: 1
Device 'nms-2820' with member number 2
        Device type:            cisco 2820
        MAC address:            0002.b922.7180
        Upstream MAC address:   0030.946c.d740 (Cluster member 1)
        Local port:             10      FEC number: 0
        Upstream port:          Fa0/18  FEC Number:
        Hops from command device: 2
Device 'SanJuan2' with member number 3
        Device type:            cisco WS-C3750
        MAC address:            0002.4b29.4400
        Upstream MAC address:   0030.946c.d740 (Cluster member 1)
        Local port:             Gi6/0/1   FEC number:
        Upstream port:          Fa6/0/11  FEC Number:
        Hops from command device: 2
Device 'GenieTest' with member number 4
        Device type:            cisco SeaHorse
        MAC address:            0002.4b28.c480
        Upstream MAC address:   0030.946c.d740 (Cluster member 1)
        Local port:             Gi0/2   FEC number:
        Upstream port:          Fa0/9   FEC Number:
        Hops from command device: 2
Device 'Palpatine' with member number 5
        Device type:            cisco WS-C2924M-XL
        MAC address:            00b0.6404.f8c0
        Upstream MAC address:   0002.4b29.2e00 (Cluster member 0)
        Local port:             Gi2/1   FEC number:
        Upstream port:          Gi0/7   FEC Number:
        Hops from command device: 1
```

関連コマンド

コマンド	説明
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。
show cluster candidates	候補スイッチのリストを表示します。

show controllers cpu-interface

CPU ネットワーク インターフェイス ASIC（特定用途向け集積回路）のステートを表示し、CPU に達するパケットに関する統計情報を送受信するには、**show controllers cpu-interface** 特権 EXEC コマンドを使用します。

show controllers cpu-interface [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用することで、シスコのテクニカル サポート担当がスイッチのトラブルシューティングを行うのに役立つ情報が表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show controllers cpu-interface** コマンドの出力を示します。

```
Switch# show controllers cpu-interface
cpu-queue-frames  retrieved  dropped    invalid    hol-block
----------------- ---------- ---------- ---------- ----------
rpc               4523063    0          0          0
stp               1545035    0          0          0
ipc               1903047    0          0          0
routing protocol  96145      0          0          0
L2 protocol       79596      0          0          0
remote console    0          0          0          0
sw forwarding     5756       0          0          0
host              225646     0          0          0
broadcast         46472      0          0          0
cbt-to-spt        0          0          0          0
igmp snooping     68411      0          0          0
icmp              0          0          0          0
logging           0          0          0          0
rpf-fail          0          0          0          0
queue14           0          0          0          0
cpu heartbeat     1710501    0          0          0
```

```
Supervisor ASIC receive-queue parameters
----------------------------------------
 queue 0 maxrecevsize 5EE pakhead 1419A20 paktail 13EAED4
 queue 1 maxrecevsize 5EE pakhead 15828E0 paktail 157FBFC
 queue 2 maxrecevsize 5EE pakhead 1470D40 paktail 1470FE4
 queue 3 maxrecevsize 5EE pakhead 19CDDD0 paktail 19D02C8

<output truncated>

Supervisor ASIC Mic Registers
-----------------------------
MicDirectPollInfo               80000800
MicIndicationsReceived          00000000
MicInterruptsReceived           00000000
MicPcsInfo                      0001001F
MicPlbMasterConfiguration       00000000
MicRxFifosAvailable             00000000
MicRxFifosReady                 0000BFFF
MicTimeOutPeriod:       FrameTOPeriod: 00000EA6 DirectTOPeriod: 00004000

<output truncated>

MicTransmitFifoInfo:
Fifo0:   StartPtrs:     038C2800        ReadPtr:        038C2C38
        WritePtrs:      038C2C38        Fifo_Flag:      8A800800
        Weights:        001E001E
Fifo1:  StartPtr:       03A9BC00        ReadPtr:        03A9BC60
        WritePtrs:      03A9BC60        Fifo_Flag:      89800400
        writeHeaderPtr: 03A9BC60
Fifo2:  StartPtr:       038C8800        ReadPtr:        038C88E0
        WritePtrs:      038C88E0        Fifo_Flag:      88800200
        writeHeaderPtr: 038C88E0
Fifo3:  StartPtr:       03C30400        ReadPtr:        03C30638
        WritePtrs:      03C30638        Fifo_Flag:      89800400
        writeHeaderPtr: 03C30638
Fifo4:  StartPtr:       03AD5000        ReadPtr:        03AD50A0
        WritePtrs:      03AD50A0        Fifo_Flag:      89800400
        writeHeaderPtr: 03AD50A0
Fifo5:  StartPtr:       03A7A600        ReadPtr:        03A7A600
        WritePtrs:      03A7A600        Fifo_Flag:      88800200
        writeHeaderPtr: 03A7A600
Fifo6:  StartPtr:       03BF8400        ReadPtr:        03BF87F0
        WritePtrs:      03BF87F0        Fifo_Flag:      89800400

<output truncated>
```

関連コマンド

コマンド	説明
show controllers ethernet-controller	ハードウェアまたはインターフェイスの内部レジスタから読み込まれる、各インターフェイスの送受信の統計情報を表示します。
show interfaces	すべてのインターフェイスまたは指定されたインターフェイスの管理ステータスおよび動作ステータスを表示します。

show controllers ethernet-controller

ハードウェアから読み込んだ送受信に関するインターフェイス単位の統計情報をキーワードなしで表示するには、**show controllers ethernet-controller** 特権 EXEC コマンドを使用します。**phy** キーワードを指定して使用すると、インターフェイス内部レジスタが表示され、**port-asic** キーワードを指定すると、ポート ASIC に関する情報が表示されます。

show controllers ethernet-controller [*interface-id*] [**phy** [**detail**]] [**port-asic** {**configuration** | **statistics**}] [**fastethernet 0**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface-id	物理インターフェイス（タイプ、スタック メンバ、モジュール、ポート番号を含む）
phy	（任意）デバイス、またはインターフェイスのスイッチの物理層（PHY）デバイスの内部レジスタ ステータスを表示します。インターフェイスの Automatic Medium-Dependent Interface Crossover（Auto-MDIX）機能の動作ステートを表示に含めます。
detail	（任意）PHY 内部レジスタの詳細情報を表示します。
port-asic	（任意）ポートの ASIC 内部レジスタの情報を表示します。
configuration	ポートの ASIC 内部レジスタの設定を表示します。
statistics	ポートの ASIC 統計情報（Rx/Sup キューおよびその他の統計情報を含む）を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC（ユーザ EXEC モードの *interface-id* キーワードを指定した場合だけサポート）

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(20)SE	XENPAK モジュール シリアル EEPROM の内容が表示されるようになりました。

使用上のガイドライン

すべてのインターフェイスまたは指定されたインターフェイスの基本的な RMON 統計情報を含むトラフィック統計情報をキーワードなしで表示します。

phy または **port-asic** キーワードを入力した場合は、主にシスコのテクニカル サポート担当によるスイッチのトラブルシューティングに役立つ情報が表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、あるインターフェイスに対する **show controllers ethernet-controller phy** コマンドの出力を示します。表 2-26 に *Transmit* フィールドを一覧表示し、表 2-27 に *Receive* フィールドを一覧表示します。

```
Switch# show controllers ethernet-controller gigabitethernet6/0/1
Transmit GigabitEthernet6/0/1              Receive
         0 Bytes                              0 Bytes
         0 Unicast frames                     0 Unicast frames
         0 Multicast frames                   0 Multicast frames
         0 Broadcast frames                   0 Broadcast frames
         0 Too old frames                     0 Unicast bytes
         0 Deferred frames                    0 Multicast bytes
         0 MTU exceeded frames                0 Broadcast bytes
         0 1 collision frames                 0 Alignment errors
         0 2 collision frames                 0 FCS errors
         0 3 collision frames                 0 Oversize frames
         0 4 collision frames                 0 Undersize frames
         0 5 collision frames                 0 Collision fragments
         0 6 collision frames
         0 7 collision frames                 0 Minimum size frames
         0 8 collision frames                 0 65 to 127 byte frames
         0 9 collision frames                 0 128 to 255 byte frames
         0 10 collision frames                0 256 to 511 byte frames
         0 11 collision frames                0 512 to 1023 byte frames
         0 12 collision frames                0 1024 to 1518 byte frames
         0 13 collision frames                0 Overrun frames
         0 14 collision frames                0 Pause frames
         0 15 collision frames                0 Symbol error frames
         0 Excessive collisions
         0 Late collisions                    0 Invalid frames, too large
         0 VLAN discard frames                0 Valid frames, too large
         0 Excess defer frames                0 Invalid frames, too small
         0 64 byte frames                     0 Valid frames, too small
         0 127 byte frames
         0 255 byte frames                    0 Too old frames
         0 511 byte frames                    0 Valid oversize frames
         0 1023 byte frames                   0 System FCS error frames
         0 1518 byte frames                   0 RxPortFifoFull drop frame
         0 Too large frames
         0 Good (1 coll) frames
```

表 2-26　Transmit のフィールドの説明

フィールド	説明
Bytes	インターフェイス上で送信されたバイトの総数。
Unicast Frames	ユニキャスト アドレスに送信されたフレームの総数。
Multicast frames	マルチキャスト アドレスに送信されたフレームの総数。
Broadcast frames	ブロードキャスト アドレスに送信されたフレームの総数。
Too old frames	パケットが有効期限切れのため出力ポートでドロップされたフレームの数。
Deferred frames	時間が 2* 最大パケット時間を超えた後で送信されなかったフレームの数。
MTU exceeded frames	最大許可フレーム サイズを超えたフレームの数。
1 collision frames	1 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
2 collision frames	2 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
3 collision frames	3 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
4 collision frames	4 回の衝突後、インターフェイス上で正常に送信されたフレームの数。

表 2-26　Transmit のフィールドの説明 （続き）

フィールド	説明
5 collision frames	5 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
6 collision frames	6 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
7 collision frames	7 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
8 collision frames	8 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
9 collision frames	9 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
10 collision frames	10 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
11 collision frames	11 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
12 collision frames	12 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
13 collision frames	13 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
14 collision frames	14 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
15 collision frames	15 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
Excessive collisions	16 回の衝突後、インターフェイス上で送信できなかったフレームの数。
Late collisions	フレームが送信された後で、フレームの送信時に検出されたレイト コリジョンのためにドロップされたフレームの数。
VLAN discard frames	CFI[1] ビットが設定されたことによりインターフェイス上でドロップされたフレームの数。
Excess defer frames	時間が最大パケット時間を超えた後で送信されなかったフレームの数。
64 byte frames	インターフェイス上で送信された 64 バイトのフレームの総数。
127 byte frames	インターフェイス上で送信された 65 ～ 127 バイトのフレームの総数。
255 byte frames	インターフェイス上で送信された 128 ～ 255 バイトのフレームの総数。
511 byte frames	インターフェイス上で送信された 256 ～ 511 バイトのフレームの総数。
1023 byte frames	インターフェイス上で送信された 512 ～ 1023 バイトのフレームの総数。
1518 byte frames	インターフェイス上で送信された 1024 ～ 1518 バイトのフレームの総数。
Too large frames	インターフェイス上で送信された最大許可フレーム サイズを超えたフレームの数。
Good (1 coll) frames	1 回の衝突後、インターフェイス上で正常に送信されたフレームの数。この値には 1 回の衝突後、インターフェイス上で正常に送信されなかったフレームの数は含まれません。

1. CFI = Canonical Format Indicator（フォーマット形式表示）

表 2-27　Receive のフィールドの説明

フィールド	説明
Bytes	インターフェイス上で受信されたフレームによって使用されたメモリ（バイト）の総量。FCS[1] 値および正常形式でないフレームも含まれます。この値には、フレーム ヘッダー ビットが含まれません。
Unicast frames	インターフェイス上で正常に受信されたユニキャスト アドレスに向けられたフレームの総数。
Multicast frames	インターフェイス上で正常に受信されたマルチキャスト アドレスに向けられたフレームの総数。
Broadcast frames	インターフェイス上で正常に受信されたブロードキャスト アドレスに向けられたフレームの総数。
Unicast bytes	インターフェイス上で受信されたユニキャスト フレームによって使用されたメモリ（バイト）の総量。FCS 値および正常形式でないフレームも含まれます。この値には、フレーム ヘッダー ビットが含まれません。

表 2-27　Receive のフィールドの説明 （続き）

フィールド	説明
Multicast bytes	インターフェイス上で受信されたマルチキャスト フレームによって使用されたメモリ（バイト）の総量。FCS 値および正常形式でないフレームも含まれます。この値には、フレーム ヘッダー ビットが含まれません。
Broadcast bytes	インターフェイス上で受信されたブロードキャスト フレームによって使用されたメモリ（バイト）の総量。FCS 値および正常形式でないフレームも含まれます。この値には、フレーム ヘッダー ビットが含まれません。
Alignment errors	インターフェイス上で受信されたアライメント エラーを持つフレームの総数。
FCS errors	インターフェイス上で受信された有効な長さ（バイト）を持ち、正常な FCS 値を持たないフレームの総数。
Oversize frames	インターフェイス上で受信された最大許可フレーム サイズを超えたフレームの数。
Undersize frames	インターフェイス上で受信された 64 バイト未満のフレームの数。
Collision fragments	インターフェイス上で受信されたコリジョン フラグメントの数。
Minimum size frames	最小フレーム サイズのフレームの総数。
65 to 127 byte frames	65 ～ 127 バイトのフレームの総数。
128 to 255 byte frames	128 ～ 255 バイトのフレームの総数。
256 to 511 byte frames	256 ～ 511 バイトのフレームの総数。
512 to 1023 byte frames	512 ～ 1023 バイトのフレームの総数。
1024 to 1518 byte frames	1024 ～ 1518 バイトのフレームの総数。
Overrun frames	インターフェイス上で受信されたオーバーラン フレームの総数。
Pause frames	インターフェイス上で受信されたポーズ フレームの数。
Symbol error frames	インターフェイス上で受信されたシンボル エラーを持つフレームの数。
Invalid frames, too large	最大許可 MTU[2] サイズ（FCS ビットを含み、フレーム ヘッダーを含まない）を超え、FCS エラーまたはアライメント エラーのいずれかを持つ、受信済みフレームの数。
Valid frames, too large	インターフェイス上で受信された最大許可フレーム サイズを超えたフレームの数。
Invalid frames, too small	64 バイト（FCS ビットを含み、フレーム ヘッダーを含まない）未満で、FCS エラーまたはアライメント エラーのいずれかを持つ、受信済みフレームの数。
Valid frames, too small	64 バイト（または VLAN タグ付きフレームでは 68 バイト）未満で、有効な FCS 値を持つインターフェイスで受信されたフレームの数。フレーム サイズには、FCS ビットが含まれ、フレーム ヘッダー ビットは含まれません。
Too old frames	パケットが有効期限切れのため入力ポートでドロップされたフレームの数。
Valid oversize frames	インターフェイス上で受信された最大許可フレーム サイズを超え、有効な FCS 値を持つフレームの数。フレーム サイズには、FCS 値が含まれ、VLAN タグは含まれません。
System FCS error frames	インターフェイス上で受信された有効な長さ（バイト）を持ち、正常な FCS 値を持たないフレームの総数。
RxPortFifoFull drop frames	入力キューが満杯であるためドロップされた、インターフェイス上で受信されたフレームの総数。

1. FCS = frame check sequence（フレーム チェック シーケンス）
2. MTU = Maximum Transmission Unit（最大伝送ユニット）

次の例では、特定のインターフェイスに対する **show controllers ethernet-controller phy** コマンドの出力を示します。

```
Switch# show controllers ethernet-controller gigabitethernet1/0/2 phy
```

```
 Control Register                      :  0001 0001 0100 0000
 Control STATUS                        :  0111 1001 0100 1001
 Phy ID 1                              :  0000 0001 0100 0001
 Phy ID 2                              :  0000 1100 0010 0100
 Auto-Negotiation Advertisement        :  0000 0011 1110 0001
 Auto-Negotiation Link Partner         :  0000 0000 0000 0000
 Auto-Negotiation Expansion Reg        :  0000 0000 0000 0100
 Next Page Transmit Register           :  0010 0000 0000 0001
 Link Partner Next page Registe        :  0000 0000 0000 0000
 1000BASE-T Control Register           :  0000 1111 0000 0000
 1000BASE-T Status Register            :  0100 0000 0000 0000
 Extended Status Register              :  0011 0000 0000 0000
 PHY Specific Control Register         :  0000 0000 0111 1000
 PHY Specific Status Register          :  1000 0001 0100 0000
 Interrupt Enable                      :  0000 0000 0000 0000
 Interrupt Status                      :  0000 0000 0100 0000
 Extended PHY Specific Control         :  0000 1100 0110 1000
 Receive Error Counter                 :  0000 0000 0000 0000
 Reserved Register 1                   :  0000 0000 0000 0000
 Global Status                         :  0000 0000 0000 0000
 LED Control                           :  0100 0001 0000 0000
 Manual LED Override                   :  0000 1000 0010 1010
 Extended PHY Specific Control         :  0000 0000 0001 1010
 Disable Receiver 1                    :  0000 0000 0000 1011
 Disable Receiver 2                    :  1000 0000 0000 0100
 Extended PHY Specific Status          :  1000 0100 1000 0000
 Auto-MDIX                             :  On   [AdminState=1   Flags=0x00052248]
```

次の例では、10 ギガビット イーサネット インターフェイスの **show controllers ethernet-controller tengigabitethernet1/0/1 phy** コマンドの出力を示します。XENPAK モジュール シリアル EEPROM の内容が表示されます。

EEPROM マップおよび出力のフィールド説明の詳細については、次のサイトの XENPAK Multisource Agreement（MSA）を参照してください。

http://www.xenpak.org/MSA/XENPAK_MSA_R2.1.pdf

http://www.xenpak.org/MSA/XENPAK_MSA_R3.0.pdf

どのバージョンの XENPAK マニュアルを読むべきかを判断するには、出力の *XENPAK MSA Version supported* フィールドを確認してください。バージョン 2.1 は 15（16 進数）で、バージョン 3.0 は 1E（16 進数）です。

```
Switch# show controllers ethernet-controller tengigabitethernet1/0/1 phy

TenGigabitEthernet1/0/1 (gpn:472, port-number:1)
------------------------------------------------------------

XENPAK Serial EEPROM Contents:
Non-Volatile Register (NVR) Fields
 XENPAK MSA Version supported         :0x15
 NVR Size in bytes                    :0x100
 Number of bytes used                 :0xD0
 Basic Field Address                  :0xB
 Customer Field Address               :0x77
 Vendor Field Address                 :0xA7
 Extended Vendor Field Address        :0x100
 Reserved                             :0x0
 Transceiver type                     :0x1 =XENPAK
 Optical connector type               :0x1 =SC
 Bit encoding                         :0x1 =NRZ
 Normal BitRate in multiple of 1M b/s :0x2848
 Protocol Type                        :0x1 =10GgE
```

```
Standards Compliance Codes :
10GbE Code Byte 0                    :0x2 =10GBASE-LR
 10GbE Code Byte 1                    :0x0
 SONET/SDH Code Byte 0                :0x0
 SONET/SDH Code Byte 1                :0x0
 SONET/SDH Code Byte 2                :0x0
 SONET/SDH Code Byte 3                :0x0
 10GFC Code Byte 0                    :0x0
 10GFC Code Byte 1                    :0x0
 10GFC Code Byte 2                    :0x0
 10GFC Code Byte 3                    :0x0
 Transmission range in 10m            :0x3E8
Fibre Type :
Fibre Type Byte 0                    :0x40 =NDSF only
 Fibre Type Byte 1                    :0x0 =Unspecified

 Centre Optical Wavelength in 0.01nm steps - Channel 0 :0x1 0xFF 0xB8
 Centre Optical Wavelength in 0.01nm steps - Channel 1 :0x0 0x0 0x0
 Centre Optical Wavelength in 0.01nm steps - Channel 2 :0x0 0x0 0x0
 Centre Optical Wavelength in 0.01nm steps - Channel 3 :0x0 0x0 0x0
 Package Identifier OUI  :0x41F420
 Transceiver Vendor OUI  :0x3400871
 Transceiver vendor name :CISCO-OPNEXT,INC
 Part number provided by transceiver vendor       :800-24558-01
 Revision level of part number provided by vendor :01
 Vendor serial number           :ONJ0735003U
 Vendor manufacturing date code :2003082700

 Reserved1 :00 00 00 00 00 00 00
 Basic Field Checksum :0x6C

 Customer Writable Area :
0x00:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x20:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

 Vendor Specific :
0x00:41 00 20 F4 88 84 28 94 C0 00 30 14 06 39 00 D9
  0x10:03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x20:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x30:00 00 00 00 11 5E 19 E9 BF 1B AD 98 03 9B DF 87
  0x40:CC F6 45 FF 99 00 00 00 00 00 00 00 00 00 C0 48
  0x50:46 D2 00 00 00 00 00 00 00
```

次の例では、**show controllers ethernet-controller port-asic configuration** コマンドの出力を示します。

```
Switch# show controllers ethernet-controller port-asic configuration
========================================================================
Switch 1, PortASIC 0 Registers
------------------------------------------------------------------------
DeviceType                        : 000101BC
Reset                             : 00000000
PmadMicConfig                     : 00000001
PmadMicDiag                       : 00000003
SupervisorReceiveFifoSramInfo     : 000007D0 000007D0 40000000
SupervisorTransmitFifoSramInfo    : 000001D0 000001D0 40000000
GlobalStatus                      : 00000800
IndicationStatus                  : 00000000
IndicationStatusMask              : FFFFFFFF
InterruptStatus                   : 00000000
InterruptStatusMask               : 01FFE800
SupervisorDiag                    : 00000000
SupervisorFrameSizeLimit          : 000007C8
```

```
SupervisorBroadcast                : 000A0F01
GeneralIO                          : 000003F9 00000000 00000004
StackPcsInfo                       : FFFF1000 860329BD 5555FFFF FFFFFFFF
                                     FF0FFF00 86020000 5555FFFF 00000000
StackRacInfo                       : 73001630 00000003 7F001644 00000003
                                     24140003 FD632B00 18E418E0 FFFFFFFF
StackControlStatus                 : 18E418E0
stackControlStatusMask             : FFFFFFFF
TransmitBufferFreeListInfo         : 00000854 00000800 00000FF8 00000000
                                     0000088A 0000085D 00000FF8 00000000
TransmitRingFifoInfo               : 00000016 00000016 40000000 00000000
                                     0000000C 0000000C 40000000 00000000
TransmitBufferInfo                 : 00012000 00000FFF 00000000 00000030
TransmitBufferCommonCount          : 00000F7A
TransmitBufferCommonCountPeak      : 0000001E
TransmitBufferCommonCommonEmpty    : 000000FF
NetworkActivity                    : 00000000 00000000 00000000 02400000
DroppedStatistics                  : 00000000
FrameLengthDeltaSelect             : 00000001
SneakPortFifoInfo                  : 00000000
MacInfo                            : 0EC0801C 00000001 0EC0801B 00000001
                                     00C0001D 00000001 00C0001E 00000001

<output truncated>
```

次の例では、**show controllers ethernet-controller port-asic statistics** コマンドの出力を示します。

```
Switch# show controllers ethernet-controller port-asic statistics
==============================================================================
 Switch 1, PortASIC 0 Statistics
------------------------------------------------------------------------------
         0 RxQ-0, wt-0 enqueue frames            0 RxQ-0, wt-0 drop frames
   4118966 RxQ-0, wt-1 enqueue frames            0 RxQ-0, wt-1 drop frames
         0 RxQ-0, wt-2 enqueue frames            0 RxQ-0, wt-2 drop frames

         0 RxQ-1, wt-0 enqueue frames            0 RxQ-1, wt-0 drop frames
       296 RxQ-1, wt-1 enqueue frames            0 RxQ-1, wt-1 drop frames
   2836036 RxQ-1, wt-2 enqueue frames            0 RxQ-1, wt-2 drop frames

         0 RxQ-2, wt-0 enqueue frames            0 RxQ-2, wt-0 drop frames
         0 RxQ-2, wt-1 enqueue frames            0 RxQ-2, wt-1 drop frames
    158377 RxQ-2, wt-2 enqueue frames            0 RxQ-2, wt-2 drop frames

         0 RxQ-3, wt-0 enqueue frames            0 RxQ-3, wt-0 drop frames
         0 RxQ-3, wt-1 enqueue frames            0 RxQ-3, wt-1 drop frames
         0 RxQ-3, wt-2 enqueue frames            0 RxQ-3, wt-2 drop frames


        15 TxBufferFull Drop Count               0 Rx Fcs Error Frames
         0 TxBufferFrameDesc BadCrc16            0 Rx Invalid Oversize Frames
         0 TxBuffer Bandwidth Drop Cou           0 Rx Invalid Too Large Frames
         0 TxQueue Bandwidth Drop Coun           0 Rx Invalid Too Large Frames
         0 TxQueue Missed Drop Statist           0 Rx Invalid Too Small Frames
        74 RxBuffer Drop DestIndex Cou           0 Rx Too Old Frames
         0 SneakQueue Drop Count                 0 Tx Too Old Frames
         0 Learning Queue Overflow Fra           0 System Fcs Error Frames
         0 Learning Cam Skip Count

        15 Sup Queue 0 Drop Frames               0 Sup Queue 8 Drop Frames
         0 Sup Queue 1 Drop Frames               0 Sup Queue 9 Drop Frames
         0 Sup Queue 2 Drop Frames               0 Sup Queue 10 Drop Frames
         0 Sup Queue 3 Drop Frames               0 Sup Queue 11 Drop Frames
         0 Sup Queue 4 Drop Frames               0 Sup Queue 12 Drop Frames
         0 Sup Queue 5 Drop Frames               0 Sup Queue 13 Drop Frames
```

```
         0 Sup Queue 6 Drop Frames               0 Sup Queue 14 Drop Frames
         0 Sup Queue 7 Drop Frames               0 Sup Queue 15 Drop Frames
==========================================================================
 Switch 1, PortASIC 1 Statistics
--------------------------------------------------------------------------
         0 RxQ-0, wt-0 enqueue frames            0 RxQ-0, wt-0 drop frames
        52 RxQ-0, wt-1 enqueue frames            0 RxQ-0, wt-1 drop frames
         0 RxQ-0, wt-2 enqueue frames            0 RxQ-0, wt-2 drop frames

<output truncated>
```

関連コマンド

コマンド	説明
show controllers cpu-interface	CPU ネットワーク ASIC の状態、および CPU に届くパケットの送受信の統計情報を表示します。
show controllers tcam	システム内のすべての Ternary CAM（TCAM）と CAM コントローラである TCAM インターフェイス ASIC のレジスタ ステートを表示します。
show idprom	指定したインターフェイスの IDPROM 情報を表示します。

show controllers power inline

指定した Power over Ethernet（PoE）コントローラのレジスタの値を表示するには、**show controllers power inline** ユーザ EXEC コマンドを使用します。

show controllers power inline [*instance] [module switch-number*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

instance	（任意）電源コントローラのインスタンス。各インスタンスは 4 つのポートに対応します。詳細については、「使用上のガイドライン」の項を参照してください。インスタンスを指定しない場合は、すべてのインスタンスが表示されます。
module *switch number*	**（注）**（任意）指定されたスタック メンバのポートだけを表示します。スイッチ番号は 1 ～ 9 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。

使用上のガイドライン

Catalyst 3750-48PS スイッチでは、指定できる *instance* 範囲は 0 ～ 11 です。

Catalyst 3750-24PS スイッチでは、指定できる *instance* 範囲は 0 ～ 5 です。

Catalyst 3750G-48PS スイッチでは、指定できる *instance* 範囲は 0 ～ 2 です。0 ～ 2 以外の instance では、スイッチは出力を提供しません。

Catalyst 3750G-24PS スイッチでは、指定できる *instance* 範囲は 0 ～ 1 です。0 ～ 1 以外の instance では、スイッチは出力を提供しません。

このコマンドは、すべてのスイッチで表示されますが、PoE スイッチだけで有効です。PoE をサポートしないスイッチの情報は提供されません。

このコマンドを使用すると、シスコのテクニカル サポート担当がスイッチのトラブルシューティングを行うのに役立つ情報が表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、Catalyst 3750G-48PS または 3750G-24PS スイッチ以外のスイッチでの **show controllers power inline** コマンドの出力を示します。

```
Switch> show controllers power inline
Module 1, Controller Instance 0, Address 0x40
  Interrupt           Reg 0x0  = 0x0
```

```
  Intr Mask           Reg 0x1  = 0xF6
  Power Event         Reg 0x2  = 0x0
  Detect Event        Reg 0x4  = 0x0
  Fault Event         Reg 0x6  = 0x0
  T-Start Event       Reg 0x8  = 0x0
  Supply Event        Reg 0xA  = 0x0
  Port 1 Status       Reg 0xC  = 0x24
  Port 2 Status       Reg 0xD  = 0x24
  Port 3 Status       Reg 0xE  = 0x3
  Port 4 Status       Reg 0xF  = 0x3
  Power Status        Reg 0x10 = 0xFF
  Pin Status          Reg 0x11 = 0x0
  Operating Mode      Reg 0x12 = 0xAA
  Disconnect Enable   Reg 0x13 = 0xA0
  Detect/Class Enable Reg 0x14 = 0xFF
  Reserved            Reg 0x15 = 0x0
  Timing Config       Reg 0x16 = 0x2
  Misc Config         Reg 0x17 = 0xA0
  ID Revision         Reg 0x1A = 0x64

Module 1, Controller Instance 1, Address 0x42
<output truncated>
```

次の例では、Catalyst 3750G-24PS スイッチでの **show controllers power inline** コマンドの出力を示します。

```
Switch> show controllers power inline
Alchemy instance 0, address 0
 Pending event flag    :N N N N N N N N N N N N
 Current State         :00 05 10 51 61 11
 Current Event         :00 01 00 10 40 00
 Timers                :00 C5 57 03 12 20 04 B2 05 06 07 07
 Error State           :00 00 00 00 10 00
 Error Code            :00 00 00 00 00 00 00 00 00 00 00 00
 Power Status          :N Y N N Y N N N N N N N
 Auto Config           :N Y Y N Y Y Y Y Y Y Y Y
 Disconnect            :N N N N N N N N N N N N
 Detection Status      :00 00 00 30 00 00
 Current Class         :00 00 00 30 00 00
 Tweetie debug         :00 00 00 00
 POE Commands pending at sub:
     Command 0 on each port :00 00 00 00 00 00
     Command 1 on each port :00 00 00 00 00 00
     Command 2 on each port :00 00 00 00 00 00
     Command 3 on each port :00 00 00 00 00 00
```

関連コマンド

コマンド	説明
logging event power-inline-status	PoE イベントのロギングをイネーブルにします。
power inline	指定した PoE ポートまたはすべての PoE ポートの電力管理モードを設定します。
show power inline	指定した PoE ポートまたはすべての PoE ポートの PoE ステータスを表示します。

show controllers tcam

システムのすべての Ternary CAM（TCAM）、および CAM コントローラであるすべての TCAM インターフェイス ASIC のレジスタのステートを表示するには、**show controllers tcam** 特権 EXEC コマンドを使用します。

show controllers tcam [**asic** [**number**]] [**detail**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

asic	（任意）ポートの ASIC TCAM 情報を表示します。
number	（任意）指定されたポート ASIC 番号の情報を表示します。指定できる範囲は 0 ～ 15 です。
detail	（任意）TCAM レジスタの詳細情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**asic** [**number**] キーワードが追加されました。

使用上のガイドライン

このコマンドを使用することで、シスコのテクニカル サポート担当がスイッチのトラブルシューティングを行うのに役立つ情報が表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show controllers tcam** コマンドの出力を示します。

```
Switch# show controllers tcam
---------------------------------------------------------------------------
TCAM-0 Registers
---------------------------------------------------------------------------
  REV:    00B30103
  SIZE:   00080040
  ID:     00000000
  CCR:    00000000_F0000020

  RPID0:  00000000_00000000
  RPID1:  00000000_00000000
  RPID2:  00000000_00000000
  RPID3:  00000000_00000000

  HRR0:   00000000_E000CAFC
  HRR1:   00000000_00000000
```

```
  HRR2:   00000000_00000000
  HRR3:   00000000_00000000
  HRR4:   00000000_00000000
  HRR5:   00000000_00000000
  HRR6:   00000000_00000000
  HRR7:   00000000_00000000
<output truncated>

  GMR31:  FF_FFFFFFFF_FFFFFFFF
  GMR32:  FF_FFFFFFFF_FFFFFFFF
  GMR33:  FF_FFFFFFFF_FFFFFFFF

==============================================================================
 TCAM related PortASIC 1 registers
==============================================================================
LookupType:                   89A1C67D_24E35F00
LastCamIndex:                 0000FFE0
LocalNoMatch:                 000069E0
ForwardingRamBaseAddress:
                              00022A00 0002FE00 00040600 0002FE00 0000D400
                              00000000 003FBA00 00009000 00009000 00040600
                              00000000 00012800 00012900
```

関連コマンド

コマンド	説明
show controllers cpu-interface	CPU ネットワーク ASIC の状態、および CPU に届くパケットの送受信の統計情報を表示します。
show controllers ethernet-controller	ハードウェアまたはインターフェイスの内部レジスタから読み込まれる、各インターフェイスの送受信の統計情報を表示します。

show controllers utilization

スイッチまたは特定のポートの帯域利用率を表示するには、**show controllers utilization** ユーザ EXEC コマンドを使用します。

show controllers [*interface-id*] **utilization** [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface-id	（任意）スイッチ インターフェイスの ID です。
| begin	（任意）指定された *expression* と一致する行から表示を開始します。
| exclude	（任意）指定された *expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)SE	このコマンドが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例は、**show controllers utilization** コマンドの出力を示しています。

```
Switch> show controllers utilization
Port       Receive Utilization  Transmit Utilization
Fa1/0/1            0                    0
Fa1/0/2            0                    0
Fa1/0/3            0
Fa1/0/4            0                    0
Fa1/0/5            0                    0
Fa1/0/6            0                    0
Fa1/0/7            0                    0
<output truncated>

<output truncated>

Switch Receive Bandwidth Percentage Utilization  : 0
Switch Transmit Bandwidth Percentage Utilization : 0

Switch Fabric Percentage Utilization : 0
```

次の例では、特定のポートでの **show controllers utilization** コマンドの出力を示します。

```
Switch> show controllers gigabitethernet1/0/1 utilization
Receive Bandwidth Percentage Utilization   : 0
Transmit Bandwidth Percentage Utilization  : 0
```

表 2-28　show controllers utilization のフィールドの説明

フィールド	説明
Receive Bandwidth Percentage Utilization	スイッチの受信帯域利用率を表示します。これは、すべてのポートの受信トラフィックの合計をスイッチの受信容量で割ったものです。
Transmit Bandwidth Percentage Utilization	スイッチの送信帯域利用率を表示します。これは、すべてのポートの送信トラフィックの合計をスイッチの送信容量で割ったものです。
Fabric Percentage Utilization	スイッチの送信と受信の両方の帯域利用率の平均を表示します。

関連コマンド

コマンド	説明
show controllers ethernet-controller	インターフェイスの内部レジスタを表示します。

show diagnostic

オンライン診断テストの結果を表示して、サポートされるテスト スイートをリストするには、**show diagnostic** ユーザ EXEC コマンドを使用します。

show diagnostic content switch [*num* | **all**] [| {**begin** | **exclude** | **include**} *expression*]

show diagnostic post [{**begin** | **exclude** | **include**} *expression*]

show diagnostic result switch [*num* | **all**] [**detail** | **test** {*test-id* | *test-id-range* | **all**} [**detail**]] [| {**begin** | **exclude** | **include**} *expression*]

show diagnostic schedule switch [*num* | **all**] [| {**begin** | **exclude** | **include**} *expression*]

show diagnostic status [| {**begin** | **exclude** | **include**} *expression*]

show diagnostic switch [*num* | **all**] [**detail**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

content	各テストおよびすべてのモジュールに関して、テスト ID、テスト属性、およびサポートされるカバレッジ テスト レベルを含むテスト情報を表示します。
switch *num*	スイッチ番号を指定します。指定できる範囲は 1 ～ 9 です。
switch all	スイッチ スタックのすべてのスイッチを指定します。
post	Power-on Self-Test（POST; 電源投入時セルフテスト）の結果を表示します。コマンドの出力は **show post** コマンドと同じです。
result	テスト結果を表示します。
detail	（任意）すべてのテスト統計を表示します。
test	テストを指定します。
test-id	テストの識別番号。その他の情報については、「使用上のガイドライン」の項を参照してください。
test-id-range	テストの識別番号の範囲。その他の情報については、「使用上のガイドライン」の項を参照してください。
all	すべてのテスト
schedule	現在スケジュールされている診断タスクを表示します。
status	テスト ステータスを表示します。
|**begin**	（任意）expression と一致する行から表示を開始します。
|**exclude**	（任意）expression と一致する行を表示から除外します。
|**include**	（任意）指定された expression と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

switch *num* を入力しない場合、すべてのスイッチの情報が表示されます。

コマンド出力では、表示されるテスト結果は次のとおりです。

- Passed（.）
- Failed（F）
- Unknown（U）

例

次の例では、スイッチに設定されているオンライン診断を表示する方法を示します。

```
Switch# show diagnostic content switch 3

Switch 3:
Diagnostics test suite attributes:
    B/* - Basic ondemand test / NA
  P/V/* - Per port test / Per device test / NA
  D/N/* - Disruptive test / Non-disruptive test / NA
    S/* - Only applicable to standby unit / NA
    X/* - Not a health monitoring test / NA
    F/* - Fixed monitoring interval test / NA
    E/* - Always enabled monitoring test / NA
    A/I - Monitoring is active / Monitoring is inactive
    R/* - Switch will reload after test list completion / NA
    P/* - will partition stack / NA
                                                   Test Interval   Thre-
ID    Test Name                            attributes  day hh:mm:ss.ms shold
==== ================================== ============ =============== =====
 1)    TestPortAsicStackPortLoopback     B*N****A**   000 00:01:00.00  n/a
 2)    TestPortAsicLoopback              B*D*X**IR*   not configured  n/a
 3)    TestPortAsicCam                   B*D*X**IR*   not configured  n/a
 4)    TestPortAsicRingLoopback          B*D*X**IR*   not configured  n/a
 5)    TestMicRingLoopback               B*D*X**IR*   not configured  n/a
 6)    TestPortAsicMem                   B*D*X**IR*   not configured  n/a
```

次の例では、スイッチのオンライン診断結果を表示する方法を示します。

```
Switch# show diagnostic result switch 1
Switch 1: SerialNo :
Overall diagnostic result: PASS
Test results: (.= Pass, F = Fail, U = Untested)
1) TestPortAsicStackPortLoopback ---> .
2) TestPortAsicLoopback ------------> .
3) TestPortAsicCam -----------------> .
4) TestPortAsicRingLoopback --------> .
5) TestMicRingLoopback -------------> .
6) TestPortAsicMem -----------------> .
```

次の例では、オンライン診断テストのステータスを表示する方法を示します。

```
Switch# show diagnostic status
<BU> - Bootup Diagnostics, <HM> - Health Monitoring Diagnostics,
<OD> - OnDemand Diagnostics, <SCH> - Scheduled Diagnostics
====== ================================= ============================== ======
Card   Description                       Current Running Test             Run by
------ --------------------------------- ---------------------            ------
```

```
1                                          N/A                              N/A
2                                          TestPortAsicStackPortLoopback    <OD>
                                           TestPortAsicLoopback             <OD>
                                           TestPortAsicCam                  <OD>
                                           TestPortAsicRingLoopback         <OD>
                                           TestMicRingLoopback              <OD>
                                           TestPortAsicMem                  <OD>
3                                          N/A                              N/A
4                                          N/A                              N/A
====== ================================= ================================ ======
Switch#
```

次の例では、スイッチのオンライン診断のテスト スケジュールを表示する方法を示します。

```
Switch# show diagnostic schedule switch 1
Current Time = 14:39:49 PST Tue Jul 5 2005
Diagnostic for Switch 1:
Schedule #1:
To be run daily 12:00
Test ID(s) to be executed: 1.
```

関連コマンド

コマンド	説明
clear arp inspection log	ヘルス モニタリング診断テストを設定します。
diagnostic schedule	テストベースのオンライン診断テストのスケジューリングを設定します。
diagnostic start	オンライン診断テストを開始します。

show dot1q-tunnel

IEEE 802.1Q トンネル ポートに関する情報を表示するには、**show dot1q-tunnel** ユーザ EXEC コマンドを使用します。

show dot1q-tunnel [**interface** *interface-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface *interface-id*	（任意）IEEE 802.1Q トンネリング情報を表示するインターフェイスを指定します。有効なインターフェイスには、物理ポートとポート チャネルが含まれます。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)EA1	このコマンドが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show dot1q-tunnel** コマンドの出力を示します。

```
Switch> show dot1q-tunnel
dot1q-tunnel mode LAN Port(s)
-----------------------------
Gi1/0/1
Gi1/0/2
Gi1/0/3
Gi1/0/6
Po2

Switch> show dot1q-tunnel interface gigabitethernet1/0/1
dot1q-tunnel mode LAN Port(s)
-----------------------------
Gi1/0/1
```

関連コマンド

コマンド	説明
show vlan dot1q tag native	IEEE 802.1Q ネイティブ VLAN タギング ステータスを表示します。
switchport mode dot1q-tunnel	インターフェイスを IEEE 802.1Q トンネル ポートとして設定します。

show dot1x

スイッチまたは指定されたポートの IEEE 802.1x 統計情報、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 dot1x** ユーザ EXEC コマンドを使用します。

show dot1x [{**all** [**summary**] | **interface** *interface-id*} [**details** | **statistics**]] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

all [**summary**]	（任意）すべてのポートの IEEE 802.1x ステータスを表示します。
interface *interface-id*	**（注）**（任意）指定されたポート（タイプ、スタック メンバ、モジュール、ポート番号を含む）の IEEE 802.1x のステータスを表示します。
details	（任意）IEEE 802.1x インターフェイスの詳細を表示します。
statistics	指定されたポートの IEEE 802.1x 統計情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**all** キーワードが追加されました。
12.2(25)SED	認証ステートのマシン ステートおよびポート ステータス フィールドに **auth-fail-vlan** が含まれるように表示が拡張されました。
12.2(25)SEE	コマンド構文が変更され、コマンド出力が修正されました。
12.2(35)SE	表示が、ホストと IP Phone（Cisco IP Phone またはシスコ以外のメーカーの電話機）の両方として設定されたポートのステータスを含むよう拡張されました。

使用上のガイドライン

ポートを指定しない場合は、グローバル パラメータおよびサマリーが表示されます。ポートを指定する場合、ポートの詳細が表示されます。

単一方向または双方向の制御としてポート制御が設定され、この設定がスイッチの設定と対立する場合、**show dot1x** {**all** | **interface** *interface-id*} 特権 EXEC コマンド出力にその情報が表示されます。

```
ControlDirection          = In (Inactive)
```

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show dot1x** ユーザ EXEC コマンドの出力を示します。

```
Switch> show dot1x
Sysauthcontrol              Enabled
```

```
Dot1x Protocol Version            2
Critical Recovery Delay         100
Critical EAPOL             Disabled
```

次の例では、**show dot1x all** ユーザ EXEC コマンドの出力を示します。

```
Switch> show dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version            2
Critical Recovery Delay         100
Critical EAPOL             Disabled

Dot1x Info for GigabitEthernet1/0/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
Violation Mode            = PROTECT
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0

<output truncated>
```

次の例では、**show dot1x all summary** ユーザ EXEC コマンドの出力を示します。

```
Interface       PAE     Client          Status
---------------------------------------------------------
Gi2/0/1         AUTH    none            UNAUTHORIZED
Gi2/0/2         AUTH    00a0.c9b8.0072  AUTHORIZED
Gi2/0/3 AUTH    none            UNAUTHORIZED
```

次の例では、**show dot1x interface** *interface-id* ユーザ EXEC コマンドの出力を示します。

```
Switch> show dot1x interface gigabitethernet1/0/2
Dot1x Info for GigabitEthernet1/0/2
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = In
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0
```

次の例では、**show dot1x interface** *interface-id* **details** ユーザ EXEC コマンドの出力を示します。

```
Switch# show dot1x interface gigabitethernet1/0/2 details
Dot1x Info for GigabitEthernet1/0/2
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
```

```
ControlDirection          = Both
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0

Dot1x Authenticator Client List Empty
```

次の例では、ポートがゲスト VLAN に割り当てられ、ホスト モードが multiple-hosts モードに変更された場合の **show dot1x interface** *interface-id* **details** コマンドの出力を示します。

```
Switch# show dot1x interface gigabitethernet1/0/1 details
Dot1x Info for GigabitEthernet1/0/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
ReAuthentication          = Enabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0
Guest-Vlan                = 182

Dot1x Authenticator Client List Empty

Port Status               = AUTHORIZED
Authorized By             = Guest-Vlan
Operational HostMode      = MULTI_HOST
Vlan Policy               = 182
```

次の例では、ポートがホストと IP Phone（Cisco IP Phone またはシスコ以外のメーカーの電話機）の両方として設定された場合の **show dot1x interface** *interface-id* **details** コマンドの出力を示します。HostMode フィールドは `MULTI-DOMAIN` を示します。

```
LOTR# show dot1x interface gigabitEthernet 2/0/3 details

Dot1x Info for GigabitEthernet2/0/3
-----------------------------------
PAE = AUTHENTICATOR
PortControl = AUTO
ControlDirection = Both
HostMode = MULTI_DOMAIN
ReAuthentication = Disabled
QuietPeriod = 60
ServerTimeout = 30
SuppTimeout = 30
ReAuthPeriod = 3600 (Locally configured)
ReAuthMax = 2
MaxReq = 2
TxPeriod = 1
RateLimitPeriod = 0
Mac-Auth-Bypass = Enabled
```

```
Critical-Auth = Enabled
Critical Recovery Action = Reinitialize
Critical-Auth VLAN = 10
Guest-Vlan = 15

Dot1x Authenticator Client List

-------------------------------
Domain = DATA
Supplicant = 0000.aaaa.bbbb
Auth SM State = AUTHENTICATED
Auth BEND SM Stat = IDLE
Port Status = AUTHORIZED
Authentication Method = MAB
Vlan Policy = 20
```

次の例では、**show dot1x interface** *interface-id* **statistics** コマンドの出力を示します。表 2-29 に、この出力で表示されるフィールドの説明を示します。

```
Switch> show dot1x interface gigabitethernet1/0/2 statistics
Dot1x Authenticator Port Statistics for GigabitEthernet1/0/2
---------------------------------------------
RxStart = 0      RxLogoff = 0     RxResp = 1       RxRespID = 1
RxInvalid = 0    RxLenErr = 0     RxTotal = 2

TxReq = 2        TxReqID = 132    TxTotal = 134

RxVersion = 2    LastRxSrcMAC = 00a0.c9b8.0072
```

表 2-29　show dot1x statistics のフィールドの説明

フィールド	説明
RxStart	受信された有効な Extensible Authentication Protocol over LAN（EAPOL）-Start フレームの数
RxLogoff	受信された EAPOL-Logoff フレームの数
RxResp	受信された有効な Extensible Authentication Protocol（EAP）-Response フレーム（Response/Identity フレーム以外）の数
RxRespID	受信された EAP-Response/Identity フレームの数
RxInvalid	受信された EAPOL フレームのうち、フレーム タイプを認識できないフレームの数
RxLenError	受信された EAPOL フレームのうち、パケット本体の長さを示すフィールドが無効なフレームの数
RxTotal	受信されたすべてのタイプの有効な EAPOL フレームの数
TxReq	送信された EAP-Request フレーム（Request/Identity フレーム以外）の数
TxReqId	送信された Extensible Authentication Protocol（EAP）-Request/Identity フレームの数
TxTotal	送信されたすべてのタイプの Extensible Authentication Protocol over LAN（EAPOL）フレームの数
RxVersion	IEEE 802.1x バージョン 1 形式で受信されたパケットの数
LastRxSrcMac	最後に受信した EAPOL フレームで伝送された送信元 MAC アドレス

関連コマンド

コマンド	説明
dot1x default	IEEE 802.1x パラメータをデフォルト値に戻します。

show dtp

スイッチまたは指定されたインターフェイスの Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）情報を表示するには、**show dtp** 特権 EXEC コマンドを使用します。

show dtp [**interface** *interface-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface *interface-id*	（注）	（任意）指定されたインターフェイスのポート セキュリティ設定を表示します。有効なインターフェイスには、物理ポート（タイプ、スタック メンバ、モジュール、ポート番号を含む）が含まれます。
| begin	（任意）	*expression* と一致する行から表示を開始します。
| exclude	（任意）	*expression* と一致する行を表示から除外します。
| include	（任意）	指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。	

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show dtp** コマンドの出力を示します。

```
Switch# show dtp
Global DTP information
        Sending DTP Hello packets every 30 seconds
        Dynamic Trunk timeout is 300 seconds
        21 interfaces using DTP
```

次の例では、**show dtp interface** コマンドの出力を示します。

```
Switch# show dtp interface gigabitethernet1/0/1
DTP information for GigabitEthernet1/0/1:
  TOS/TAS/TNS:                              ACCESS/AUTO/ACCESS
  TOT/TAT/TNT:                              NATIVE/NEGOTIATE/NATIVE
  Neighbor address 1:                       000943A7D081
  Neighbor address 2:                       000000000000
  Hello timer expiration (sec/state):       1/RUNNING
  Access timer expiration (sec/state):      never/STOPPED
  Negotiation timer expiration (sec/state): never/STOPPED
  Multidrop timer expiration (sec/state):   never/STOPPED
  FSM state:                                S2:ACCESS
  # times multi & trunk                     0
  Enabled:                                  yes
  In STP:                                   no
```

```
Statistics
----------
3160 packets received (3160 good)
0 packets dropped
    0 nonegotiate, 0 bad version, 0 domain mismatches, 0 bad TLVs, 0 other
6320 packets output (6320 good)
    3160 native, 3160 software encap isl, 0 isl hardware native
0 output errors
0 trunk timeouts
1 link ups, last link up on Mon Mar 01 1993, 01:02:29
0 link downs
```

関連コマンド

コマンド	説明
show interfaces trunk	インターフェイス トランク情報を表示します。

show eap

スイッチまたは指定されたポートの Extensible Authentication Protocol（EAP）レジストレーション情報およびセッション情報を表示するには、**show eap** 特権 EXEC コマンドを使用します。

show eap {{**registrations** [**method** [*name*] | **transport** [*name*]]} | {**sessions** [**credentials** *name* [**interface** *interface-id*] | **interface** *interface-id* | **method** *name* | **transport** *name*]}} [**credentials** *name* | **interface** *interface-id* | **transport** *name*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

registrations	EAP レジストレーション情報を表示します。
method *name*	（任意）EAP 方式のレジストレーション情報を表示します。
transport *name*	（任意）EAP トランスポートのレジストレーション情報を表示します。
sessions	EAP セッション情報を表示します。
credentials *name*	（任意）EAP 方式のレジストレーション情報を表示します。
interface *interface-id*	**（注）**　（任意）指定されたポート（タイプ、スタック メンバ、モジュール、ポート番号を含む）の EAP 情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

次のキーワードとともに **show eap registrations** 特権 EXEC コマンドを使用する場合、コマンド出力には次の情報が表示されます。

- None：EAP および登録された EAP 方式で使用されるすべての下位レベル
- **method** *name* キーワード：登録された指定の方式
- **transport** *name* キーワード：登録された特定の下位レベル

次のキーワードを含む **show eap sessions** 特権 EXEC コマンドを使用する場合、コマンド出力には次の情報が表示されます。

- None：すべてのアクティブな EAP セッション
- **credentials** *name* キーワード：指定された資格情報プロファイル
- **interface** *interface-id* キーワード：指定されたインターフェイスのパラメータ
- **method** *name* キーワード：指定された EAP 方式
- **transport** *name* キーワード：指定された下位レイヤ

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show eap registrations** 特権 EXEC コマンドの出力を示します。

```
Switch> show eap registrations
Registered EAP Methods:
  Method  Type            Name
    4     Peer            MD5

Registered EAP Lower Layers:
  Handle  Type            Name
    2     Authenticator   Dot1x-Authenticator
    1     Authenticator   MAB
```

次の例では、**show eap registrations transport** 特権ユーザ EXEC コマンドの出力を示します。

```
Switch> show eap registrations transport all
Registered EAP Lower Layers:
  Handle  Type            Name
    2     Authenticator   Dot1x-Authenticator
    1     Authenticator   MAB
```

次の例では、**show eap sessions** 特権 EXEC コマンドの出力を示します。

```
Switch> show eap sessions
Role:                    Authenticator   Decision:                Fail
Lower layer:             Dot1x-AuthenticaInterface:               Gi1/0/1
Current method:          None            Method state:            Uninitialised
Retransmission count:    0  (max: 2)     Timer:                   Authenticator
ReqId Retransmit (timeout: 30s, remaining: 2s)
EAP handle:              0x5200000A      Credentials profile:     None
Lower layer context ID:  0x93000004      Eap profile name:        None
Method context ID:       0x00000000      Peer Identity:           None
Start timeout (s):       1               Retransmit timeout (s):  30 (30)
Current ID:              2               Available local methods: None

Role:                    Authenticator   Decision:                Fail
Lower layer:             Dot1x-AuthenticaInterface:               Gi1/0/2
Current method:          None            Method state:            Uninitialised
Retransmission count:    0  (max: 2)     Timer:                   Authenticator
ReqId Retransmit (timeout: 30s, remaining: 2s)
EAP handle:              0xA800000B      Credentials profile:     None
Lower layer context ID:  0x0D000005      Eap profile name:        None
Method context ID:       0x00000000      Peer Identity:           None
Start timeout (s):       1               Retransmit timeout (s):  30 (30)
Current ID:              2               Available local methods: None

<Output truncated>
```

次の例では、**show eap sessions interface** *interface-id* 特権 EXEC コマンドの出力を示します。

```
Switch# show eap sessions gigabitethernet1/0/1
Role:                    Authenticator   Decision:                Fail
Lower layer:             Dot1x-AuthenticaInterface:               Gi1/0/1
Current method:          None            Method state:            Uninitialised
Retransmission count:    1  (max: 2)     Timer:                   Authenticator
ReqId Retransmit (timeout: 30s, remaining: 13s)
EAP handle:              0x5200000A      Credentials profile:     None
Lower layer context ID:  0x93000004      Eap profile name:        None
Method context ID:       0x00000000      Peer Identity:           None
Start timeout (s):       1               Retransmit timeout (s):  30 (30)
```

```
Current ID:              2              Available local methods: None
```

関連コマンド

コマンド	説明
clear eap sessions	スイッチまたは指定されたポートの EAP のセッション情報をクリアします。

show env

スタンドアロン スイッチ、スタック マスター、スタック メンバのようなスイッチのファン、温度、Redundant Power System（RPS; 冗長電源システム）の可用性、および電源情報を表示するには、**show env** ユーザ EXEC コマンドを使用します。**stack** キーワードを指定して使用すると、スタックまたはスタック内で指定されたスイッチに関するすべての情報が表示されます。

show env {**all** | **fan** | **power** | **rps** [**all** | **detail** | **switch** [*switch-number*]] | **stack** [*switch-number*] | **temperature** [**status**]} [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

all	ファンと温度環境の両方の状態を表示します。
fan	スイッチ ファンの状態を表示します。
power	スイッチの電源の状態を表示します。
rps	RPS 300 Redundant Power System（RPS 300）、Cisco RPS675 Redundant Power System（RPS 675）、または Cisco Redundant Power System 2300（RPS 2300）がスイッチに接続されているかどうか表示します。
rps all	（任意）スタンドアロン スイッチまたはスイッチ スタックに接続されたすべての冗長電源システムを表示します。 次のキーワードは、Catalyst 3750v2 スイッチ上でだけ使用できます。
rps detail	（任意）スイッチまたはスイッチ スタックに接続された冗長電源システムの詳細情報を表示します。 次のキーワードは、Catalyst 3750v2 スイッチ上でだけ使用できます。
rps switch [*switch-number*]	（任意）スタック内の各スイッチまたは指定されたスイッチに接続された冗長電源システムを表示します。*switch-number* に指定できる範囲は 1 ～ 9 です（スタックのスイッチ メンバ番号に対応）。 次のキーワードは、Catalyst 3750v2 スイッチ上でだけ使用できます。
stack [*switch-number*]	**（注）** スタックの各スイッチまたは指定されたスイッチのすべての環境ステータスを表示します。指定できる範囲は 1 ～ 9 です（スタックのスイッチ メンバ番号に対応）。
temperature	スイッチの温度ステータスを表示します。
status	（任意）スイッチの内部温度（外部温度ではなく）およびしきい値を表示します。このキーワードは、Catalyst 3750G-48TS、3750G-48PS、3750G-24TS-1U、および 3750G-24PS スイッチだけで使用できます。
| **begin**	（任意）*expression* と一致する行から表示を開始します。
| **exclude**	（任意）*expression* と一致する行を表示から除外します。
| **include**	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

リリース	変更内容
12.2(20)SE3	**temperature status** キーワードが追加されました。
12.2(50)SE1	**rps** [**all** | **detail** | **switch** [*switch-number*]] キーワードが追加されました。

使用上のガイドライン

マスター以外の特定のスイッチから情報にアクセスするには、**session** 特権 EXEC コマンドを使用します。

任意のスイッチ メンバからスタック内のスイッチに関する情報を表示するには、**show env stack** [*switch-number*] コマンドを使用します。

show env temperature status コマンドはすべてのスイッチ上で表示されますが、Catalyst 3750G-48TS、3750G-48PS、3750G-24TS-1U、および 3750G-24PS スイッチだけで有効です。これらのスイッチにこのコマンドを入力すると、スイッチの温度ステートとしきい値レベルがコマンド出力に表示されます。これらの 4 つのスイッチ以外のスイッチにコマンドを入力すると、出力フィールドに `Not Applicable` が表示されます。

また、Catalyst 3750G-48PS または 3750G-24PS スイッチでは、**show env temperature** コマンドを使用してスイッチの温度ステータスも表示できます。コマンド出力では、GREEN および YELLOW ステートを *OK* と表示し、RED ステートを *FAULTY* と表示します。このスイッチに **show env all** コマンドを入力する場合、コマンド出力は **show env temperature status** コマンド出力と同じです。

しきい値レベルに関する詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、マスター スイッチまたはスタンドアロン スイッチから入力した **show env all** コマンドの出力を示します。

```
Switch> show env all
FAN is OK
TEMPERATURE is OK
Temperature Value: 33 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 56 Degree Celsius
Red Threshold    : 66 Degree Celsius
SW  PID                 Serial#     Status           Sys Pwr  PoE Pwr  Watts
--  ------------------  ----------  ---------------  -------  -------  -----
 1  Built-in                                         Good

SW  Status          RPS Name          RPS Serial#  RPS Port#
--  -------------   ----------------  -----------  ---------
```

次の例では、**show env fan** コマンドの出力を示します。

```
Switch> show env fan
FAN is OK
```

次の例では、スタック マスターでの **show env rps** コマンドの出力を示します。

```
Switch> show env rps
SW  Status          RPS Name          RPS Serial#  RPS Port#
--  -------------   ----------------  -----------  ---------
3   Active          CiscoRPS          CAT1050VGF3  3

RPS Name: CiscoRPS
  State: Active
```

```
  PID: PWR-RPS2300
  Serial#: CAT1050VGF3
  Fan: Good
  Temperature: Green

  RPS Power Supply A: Present
    PID             : C3K-PWR-750WAC
    Serial#         : DTH1050M04S
    System Power    : Good
    PoE Power       : Good
    Watts           : 300/420 (System/PoE)

  RPS Power Supply B: Present
    PID             : C3K-PWR-750WAC
    Serial#         : DTH1050M03H
    System Power    : Good
    PoE Power       : Good
    Watts           : 300/420 (System/PoE)

DCOut  State   Connected  Priority  BackingUp  WillBackup  Portname        SW#
-----  ------- ---------  --------  ---------  ----------  --------------- ---
    1  Active  Yes               6  Yes        Yes         <>                -
    2  Active  Yes               6  Yes        Yes         <>                -
    3  Active  Yes               3  No         Yes         Switch            3
    4  Active  No                1  No         Yes         <>                -
    5  Active  No                6  No         No          <>                -
    6  Active  No                6  No         No          <>                -
```

次の例では、スタック マスターでの **show env rps all** コマンドの出力を示します。

```
Switch> show env rps all
SWITCH 1:
RPS:
    RPS is active
    Fan:           Good
    Temperature:   Green

DC port legends:
Y   = Yes                      :  N   = No
Act = Active                   :  Sby = Standby
OK  = Power Supply is good     :  NP  = Power Supply is not present or bad
BU  = RPS actively backing up  :  NB  = RPS not actively backing up
12v/PoE  12v/PoE   RPS
Port  State  Prio   Status   Backup   Avail  PortName         Switch Name
----  -----  ----   ------   ------   -----  ---------------  ---------------
 1     Act     1    OK/OK    NB/NB      Y    <>               <remote>
 2     Act     4    OK/NP    NB/NB      Y    <>               <remote>
 3     Act     1    OK/OK    NB/NB      Y    <>               Switch
 4     Act     1    OK/OK    NB/NB      Y    Switch           <remote>
 5     Act     2    OK/OK    NB/NB      Y    <>               <remote>
 6     Act     6    OK/OK    NB/NB      Y    <>               <remote>

<output truncated>
```

次の例では、**show env stack** コマンドの出力を示します。

```
Switch> show env stack
SWITCH: 1
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
SWITCH: 2
FAN is OK
```

```
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
SWITCH: 3
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
```

次の例では、マスター スイッチからスタック メンバ 3 に関する情報を表示する方法を示します。

```
Switch> show env stack 3
SWITCH: 3
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
```

次の例では、温度値、ステート、およびしきい値を表示する方法を示します。表 2-30 に、コマンド出力の温度ステートの説明を示します。

```
Switch> show env temperature status
Temperature Value:28 Degree Celsius
Temperature State:GREEN
Yellow Threshold :70 Degree Celsius
Red Threshold    :75 Degree Celsius
```

表 2-30　show env temperature status コマンド出力のステート

ステート	説明
Green	スイッチの温度が*正常な*動作範囲にあります。
Yellow	温度が*警告*範囲にあります。スイッチの外の周辺温度を確認する必要があります。
Red	温度が*クリティカル*範囲にあります。温度がこの範囲にある場合、スイッチが正常に実行されない可能性があります。

show errdisable detect

errdisable の検出状態を表示するには、**show errdisable detect** ユーザ EXEC コマンドを使用します。

show errdisable detect [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(37)SE	**show errdisable detect** の出力に Mode 列が追加されました。

使用上のガイドライン

表示された `gbic-invalid` エラーの理由は、無効な Small Form-Factor Pluggable（SFP）モジュールを意味します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

コマンド出力内の errdisable の理由がアルファベット順に表示されます。Mode 列は、errdisable が機能ごとにどのように設定されているかを示します。

errdisable 検出は次のモードで設定できます。

- ポート モード：違反が発生した場合、物理ポート全体が errdisable になります。
- VLAN モード：違反が発生した場合、VLAN が errdisable になります。
- ポート /VLAN モード：一部のポートでは物理ポート全体が errdisable になり、その他のポートでは VLAN ごとに errdisable になります。

例

次の例では、**show errdisable detect** コマンドの出力を示します。

```
Switch> show errdisable detect
ErrDisable Reason    Detection    Mode
-----------------    ---------    ----
arp-inspection       Enabled      port
bpduguard            Enabled      vlan
channel-misconfig    Enabled      port
community-limit      Enabled      port
dhcp-rate-limit      Enabled      port
dtp-flap             Enabled      port
gbic-invalid         Enabled      port
inline-power         Enabled      port
invalid-policy       Enabled      port
l2ptguard            Enabled      port
```

```
link-flap            Enabled      port
loopback             Enabled      port
lsgroup              Enabled      port
pagp-flap            Enabled      port
psecure-violation    Enabled      port/vlan
security-violatio    Enabled      port
sfp-config-mismat    Enabled      port
storm-control        Enabled      port
udld                 Enabled      port
vmps                 Enabled      port
```

関連コマンド

コマンド	説明
errdisable detect cause	特定の原因、またはすべての原因に対して errdisable 検出をイネーブルにします。
show errdisable flap-values	認識されている状態のエラー情報を表示します。
show errdisable recovery	errdisable 回復タイマーの情報を表示します。
show interfaces status	インターフェイスのステータスまたは errdisable ステートにあるインターフェイスのリストを表示します。

show errdisable flap-values

ある原因をエラーとして認識させる条件を表示するには、**show errdisable flap-values** ユーザ EXEC コマンドを使用します。

show errdisable flap-values [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

Flaps 列には、指定された時間間隔内にステートへの変更を何回行うと、エラーが検出されてポートがディセーブルになるのかが表示されます。たとえば、3 つの Dynamic Trunking Protocol（DTP）ステート（ポート モード アクセス/トランク）、またはポート集約プロトコル（PAgP）フラップが 30 秒間隔で変更された場合、または 5 つのリンク ステート（リンク アップ/ダウン）が 10 秒間隔で変更された場合は、エラーと見なされてポートがシャットダウンすることが示されます。

```
ErrDisable Reason    Flaps    Time (sec)
-----------------    ------   ----------
pagp-flap              3       30
dtp-flap               3       30
link-flap              5       10
```

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show errdisable flap-values** コマンドの出力を示します。

```
Switch> show errdisable flap-values
ErrDisable Reason    Flaps    Time (sec)
-----------------    ------   ----------
pagp-flap              3       30
dtp-flap               3       30
link-flap              5       10
```

関連コマンド

コマンド	説明
errdisable detect cause	特定の原因、またはすべての原因に対して errdisable 検出をイネーブルにします。
show errdisable detect	errdisable 検出ステータスを表示します。
show errdisable recovery	errdisable 回復タイマーの情報を表示します。
show interfaces status	インターフェイスのステータスまたは errdisable ステートにあるインターフェイスのリストを表示します。

show errdisable recovery

errdisable 回復タイマー情報を表示するには、**show errdisable recovery** ユーザ EXEC コマンドを使用します。

show errdisable recovery [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

gbic-invalid error-disable の理由は、無効な Small Form-factor Pluggable（SFP; 着脱可能小型フォームファクタ）インターフェイスを意味します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show errdisable recovery** コマンドの出力を示します。

```
Switch> show errdisable recovery
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Disabled
security-violatio    Disabled
channel-misconfig    Disabled
vmps                 Disabled
pagp-flap            Disabled
dtp-flap             Disabled
link-flap            Enabled
l2ptguard            Disabled
psecure-violation    Disabled
gbic-invalid         Disabled
dhcp-rate-limit      Disabled
unicast-flood        Disabled
storm-control        Disabled
arp-inspection       Disabled
loopback             Disabled

Timer interval:300 seconds
```

```
Interfaces that will be enabled at the next timeout:

Interface    Errdisable reason    Time left(sec)
---------    -----------------    --------------
Gi1/0/2      link-flap             279
```

（注）unicast-flood フィールドは、出力に表示はされますが無効です。

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 errdisable detect	errdisable 検出ステータスを表示します。
show errdisable flap-values	認識されている状態のエラー情報を表示します。
show interfaces status	インターフェイスのステータスまたは errdisable ステートにあるインターフェイスのリストを表示します。

show etherchannel

チャネルの EtherChannel 情報を表示するには、**show etherchannel** ユーザ EXEC コマンドを使用します。

show etherchannel [*channel-group-number* {**detail** | **port** | **port-channel** | **protocol** | **summary**}] {**detail** | **load-balance** | **port** | **port-channel** | **protocol** | **summary**} [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

channel-group-number	（任意）チャネル グループの番号です。指定できる範囲は 1 ～ 48 です。
detail	EtherChannel の詳細を表示します。
load-balance	ポート チャネル内のポート間の負荷分散方式、またはフレーム配布方式を表示します。
port	EtherChannel ポート情報を表示します。
port-channel	ポートチャネル情報を表示します。
protocol	EtherChannel で使用されるプロトコルを表示します。
summary	各チャネル グループのサマリーを 1 行で表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**protocol** キーワードが追加されました。
12.2(25)SE	*channel-group-number* 範囲が 1 ～ 12 から 1 ～ 48 に変更されました。

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。

出力では、ポート リストの Passive フィールドはレイヤ 3 のポート チャネルだけで表示されます。このフィールドは、まだ起動していない物理ポートがチャネル グループ内で設定されていること（および間接的にチャネル グループ内で唯一のポート チャネルであること）を意味します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show etherchannel 1 detail** コマンドの出力を示します。

```
Switch> show etherchannel 1 detail
Group state = L2
Ports: 2   Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:   LACP
```

```
                Ports in the group:
                -------------------
Port: Gi1/0/1
------------

Port state    = Up Mstr In-Bndl
Channel group = 1           Mode = Active      Gcchange = -
Port-channel  = Po1         GC   =   -         Pseudo port-channel = Po1
Port index    = 0           Load = 0x00        Protocol =   LACP

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDU
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port     Port
Port      Flags   State     Priority      Key       Key     Number   State
Gi1/0/1   SA      bndl      32768         0x1       0x1     0x101    0x3D
Gi1/0/2   SA      bndl      32768         0x0       0x1     0x0      0x3D

Age of the port in the current state: 01d:20h:06m:04s

                Port-channels in the group:
                ----------------------

Port-channel: Po1    (Primary Aggregator)
------------

Age of the Port-channel   = 01d:20h:20m:26s
Logical slot/port   = 10/1          Number of ports = 2
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gi1/0/1  Active          0
  0     00     Gi1/0/2  Active          0

Time since last port bundled:    01d:20h:20m:20s    Gi1/0/2
```

次の例では、**show etherchannel 1 summary** コマンドの出力を示します。

```
Switch> show etherchannel 1 summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        u - unsuitable for bundling
        U - in use      f - failed to allocate aggregator
        d - default port

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
1      Po1(SU)         LACP      Gi1/0/1(P)  Gi1/0/2(P)
```

次の例では、**show etherchannel 1 port-channel** コマンドの出力を示します。

```
Switch> show etherchannel 1 port-channel
                Port-channels in the group:
                ----------------------
Port-channel: Po1    (Primary Aggregator)

------------

Age of the Port-channel   = 01d:20h:24m:50s
Logical slot/port   = 10/1          Number of ports = 2
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gi1/0/1  Active          0
  0     00     Gi1/0/2  Active          0

Time since last port bundled:    01d:20h:24m:44s    Gi1/0/2
```

次の例では、**show etherchannel protocol** コマンドの出力を示します。

```
Switch# show etherchannel protocol
                Channel-group listing:
                -----------------------
Group: 1
----------
Protocol:  LACP

Group: 2
----------
Protocol:  PAgP
```

関連コマンド

コマンド	説明
channel-group	EtherChannel グループにイーサネット ポートを割り当てます。
channel-protocol	チャネリングを管理するため、ポート上で使用されるプロトコルを制限します。
interface port-channel	ポート チャネルへのアクセスや、ポート チャネルの作成を行います。

show fallback profile

スイッチで設定されたフォールバック プロファイルを表示するには、**show fallback profile** 特権 EXEC コマンドを使用します。

show fallback profile [append | begin | exclude | include | { [redirect | tee] *url*} *expression*]

構文の説明

| append	（任意）指定 URL にリダイレクト出力を付加します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
| redirect	（任意）指定 URL に出力をコピーします。
| tee	（任意）指定 URL に出力をコピーします。
expression	参照ポイントとして使用する出力内の文字列です。
url	出力を誘導する URL です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(35)SE	このコマンドが追加されました。

使用上のガイドライン

スイッチで設定されたプロファイルを表示するには、**show fallback profile** 特権 EXEC コマンドを使用します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show fallback profile** コマンドの出力を示します。

```
switch# show fallback profile
Profile Name: dot1x-www
-------------------------------------
Description       : NONE
IP Admission Rule : webauth-fallback
IP Access-Group IN: default-policy
Profile Name: dot1x-www-lpip
-------------------------------------
Description       : NONE
IP Admission Rule : web-lpip
IP Access-Group IN: default-policy
Profile Name: profile1
-------------------------------------
Description       : NONE
IP Admission Rule : NONE
IP Access-Group IN: NONE
```

関連コマンド

コマンド	説明
dot1x fallback profile	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
fallback profile profile	Web 認証のフォールバック プロファイルを作成します。
ip admission rule	スイッチ ポートで Web 認証をイネーブルにします。
ip admission name proxy http	スイッチで Web 認証をグローバルにイネーブルにします。
show dot1x [**interface** *interface-id*]	指定されたポートの IEEE 802.1x の状態を表示します。

show flowcontrol

フロー制御ステータスおよび統計情報を表示するには、**show flowcontrol** ユーザ EXEC コマンドを使用します。

show flowcontrol [**interface** *interface-id* | **module** *number*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface *interface-id*	（任意）特定のインターフェイスのフロー制御ステータスおよび統計情報を表示します。
module *number*	（任意）指定されたスタック メンバ スイッチのすべてのインターフェイスのフロー制御ステータスと統計情報を表示します。指定できる範囲は 1 ～ 9 です。このオプションは、特定のインターフェイス ID を入力したときは利用できません。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

スイッチまたは特定のインターフェイスのフロー制御ステータスおよび統計情報を表示するには、このコマンドを使用します。

スイッチ インターフェイス情報をすべて表示するには、**show flowcontrol** コマンドを使用します。スタンドアロン スイッチでは、**show flowcontrol** コマンドの出力結果は、**show flowcontrol module** *number* コマンドの出力結果と同じになります。

特定のインターフェイスの情報を表示するには、**show flowcontrol interface** *interface-id* コマンドを使用します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show flowcontrol** コマンドの出力を示します。

```
Switch> show flowcontrol
Port       Send FlowControl  Receive FlowControl  RxPause TxPause
           admin    oper     admin    oper
---------  -------- -------- -------- --------    ------- -------
Gi2/0/1    Unsupp.  Unsupp.  off      off         0       0
Gi2/0/2    desired  off      off      off         0       0
Gi2/0/3    desired  off      off      off         0       0
<output truncated>
```

次の例では、**show flowcontrol interface** *interface-id* コマンドの出力を示します。

```
Switch> show flowcontrol gigabitethernet2/0/2
Port       Send FlowControl  Receive FlowControl  RxPause TxPause
           admin    oper     admin    oper
---------  -------- -------- -------- --------    ------- -------
Gi2/0/2    desired  off      off      off         0       0
```

関連コマンド

コマンド	説明
flowcontrol	インターフェイスの受信フロー制御ステートを設定します。

show idprom

指定されたインターフェイスの IDPROM 情報を表示するには、**show idprom** ユーザ EXEC コマンドを使用します。

show idprom {**interface** *interface-id*} [**detail**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface *interface-id*	指定された 10 ギガビット イーサネット インターフェイスの IDPROM 情報を表示します。
detail	（任意）IDPROM の詳細情報（16 進数）を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(20)SE1	このコマンドが追加されました。

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 インターフェイスにだけ適用されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、10 ギガビット イーサネット インターフェイスの **show idprom interface tengigabitethernet1/0/1** コマンドの出力を示します。XENPAK モジュール シリアル EEPROM の内容が表示されます。

EEPROM マップおよび出力のフィールド説明の詳細については、次のサイトの XENPAK Multisource Agreement（MSA）を参照してください。

http://www.xenpak.org/MSA/XENPAK_MSA_R2.1.pdf

http://www.xenpak.org/MSA/XENPAK_MSA_R3.0.pdf

どのバージョンの XENPAK マニュアルを読むべきかを判断するには、出力の *XENPAK MSA Version supported* フィールドを確認してください。バージョン 2.1 は 15（16 進数）で、バージョン 3.0 は 1E（16 進数）です（例示なし）。

```
Switch# show idprom interface tengigabitethernet1/0/1
TenGigabitEthernet1/0/1 (gpn:472, port-number:1)
------------------------------------------------------------
XENPAK Serial EEPROM Contents:
Non-Volatile Register (NVR) Fields
 XENPAK MSA Version supported         :0x15
 NVR Size in bytes                    :0x100
 Number of bytes used                 :0xD0
 Basic Field Address                  :0xB
```

```
 Customer Field Address                :0x77
 Vendor Field Address                  :0xA7
 Extended Vendor Field Address         :0x100
 Reserved                              :0x0
 Transceiver type                      :0x1 =XENPAK
 Optical connector type                :0x1 =SC
 Bit encoding                          :0x1 =NRZ
 Normal BitRate in multiple of 1M b/s :0x2848
 Protocol Type                         :0x1 =10GgE

Standards Compliance Codes :
10GbE Code Byte 0                     :0x2 =10GBASE-LR
 10GbE Code Byte 1                     :0x0
 SONET/SDH Code Byte 0                 :0x0
 SONET/SDH Code Byte 1                 :0x0
 SONET/SDH Code Byte 2                 :0x0
 SONET/SDH Code Byte 3                 :0x0
 10GFC Code Byte 0                     :0x0
 10GFC Code Byte 1                     :0x0
 10GFC Code Byte 2                     :0x0
 10GFC Code Byte 3                     :0x0
 Transmission range in 10m             :0x3E8
Fibre Type :
Fibre Type Byte 0                     :0x40 =NDSF only
 Fibre Type Byte 1                     :0x0 =Unspecified

 Centre Optical Wavelength in 0.01nm steps - Channel 0 :0x1 0xFF 0xB8
 Centre Optical Wavelength in 0.01nm steps - Channel 1 :0x0 0x0 0x0
 Centre Optical Wavelength in 0.01nm steps - Channel 2 :0x0 0x0 0x0
 Centre Optical Wavelength in 0.01nm steps - Channel 3 :0x0 0x0 0x0
 Package Identifier OUI  :0x41F420
 Transceiver Vendor OUI  :0x3400871
 Transceiver vendor name :CISCO-OPNEXT,INC
 Part number provided by transceiver vendor       :800-24558-01
 Revision level of part number provided by vendor :01
 Vendor serial number           :ONJ0735003U
 Vendor manufacturing date code :2003082700

 Reserved1 :00 00 00 00 00 00 00
 Basic Field Checksum :0x6C

 Customer Writable Area :
0x00:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x20:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

 Vendor Specific :
0x00:41 00 20 F4 88 84 28 94 C0 00 30 14 06 39 00 D9
  0x10:03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x20:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x30:00 00 00 00 11 5E 19 E9 BF 1B AD 98 03 9B DF 87
  0x40:CC F6 45 FF 99 00 00 00 00 00 00 00 00 00 C0 48
  0x50:46 D2 00 00 00 00 00 00 00
```

関連コマンド

コマンド	説明
show controllers ethernet-controller	ハードウェア、インターフェイス内部レジスタ、またはポート ASIC（特定用途向け集積回路）情報から読み込まれる、各インターフェイスの送受信の統計情報を表示します。

show interfaces

すべてのインターフェイスまたは指定されたインターフェイス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** 特権 EXEC コマンドを使用します。

show interfaces [*interface-id* | **vlan** *vlan-id*] [**accounting** | **capabilities** [**module** *number*] | **counters** | **description** | **etherchannel** | **flowcontrol** | **private-vlan mapping** | **pruning** | **stats** | **status** [**err-disabled**] | **switchport** [**backup** | **module** *number*] | **transceiver** {**tengigabitethernet** *interface-id*} | **properties** | **detail** [**module** *number*] | **trunk**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface-id	（任意）有効なインターフェイスには、物理ポート（タイプ、スタック メンバ、モジュール、およびポート番号を含む）やポート チャネルが含まれます。ポート チャネル範囲は 1 ～ 48 です。
vlan *vlan-id*	（任意）VLAN ID です。指定できる範囲は 1 ～ 4094 です。
accounting	（任意）インターフェイスのアカウント情報（アクティブ プロトコル、入出力のパケット、オクテットを含む）を表示します。 **（注）** ソフトウェアで処理されたパケットだけが表示されます。ハードウェアでスイッチングされるパケットは表示されません。
capabilities	（任意）すべてのインターフェイスまたは指定されたインターフェイスの性能（機能、インターフェイス上で設定可能なオプションを含む）を表示します。このオプションはコマンドラインのヘルプに表示されますが、VLAN ID に使用できません。
module *number*	**（注）** （任意）指定されたスタック メンバのすべてのインターフェイスの**機能**、**スイッチポート** コンフィギュレーション、または**トランシーバ**の特性（上記のキーワードに対応）を表示します。指定できる範囲は 1 ～ 9 です。このオプションは、特定のインターフェイス ID を入力するときは利用できません。
counters	（任意）**show interfaces counters** コマンドを参照してください。
description	（任意）特定のインターフェイスに設定された管理ステータスおよび説明を表示します。
etherchannel	（任意）インターフェイス EtherChannel 情報を表示します。
flowcontrol	（任意）インターフェイスのフロー制御情報を表示します。
private-vlan mapping	（任意）VLAN Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）のプライベート VLAN のマッピング情報を表示します。このキーワードは、スイッチが IP サービス イメージ（従来の Enhanced Multilayer Image（EMI））を実行している場合だけ利用できます。
pruning	（任意）インターフェイス トランク VTP プルーニング情報を表示します。
stats	（任意）インターフェイスのスイッチング パスによる入出力パケットを表示します。
status	（任意）インターフェイスのステータスを表示します。Type フィールドの *unsupported* のステータスは、他社製の Small Form-Factor Pluggable（SFP）モジュールがモジュール スロットに装着されていることを示しています。
err-disabled	（任意）errdisable ステートのインターフェイスを表示します。
switchport	（任意）ポート ブロッキング、ポート保護設定など、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。

backup	（任意）スタック上の指定したインターフェイスまたはすべてのインターフェイスの、Flex Link バックアップ インターフェイス コンフィギュレーションおよびステータスを表示します。
tengigabitethernet	接続している 10 ギガビット モジュールのステータスを表示します。
transceiver [**detail** | **properties**]	（任意）CWDM[1] または DWDM[2] Small Form-Factor（SFP）モジュール インターフェイスの物理プロパティを表示します。キーワードの意味は次のとおりです。 • **detail**：（任意）高低の番号、アラーム情報を含む較正プロパティを表示します。 • **properties**：（任意）インターフェイスの速度、デュプレックス、およびインライン パワー設定を表示します。
trunk	インターフェイス トランク情報を表示します。インターフェイスを指定しない場合は、アクティブなトランキング ポートの情報だけが表示されます。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

1. 低密度波長分割多重
2. 高密度波長分割多重

（注）　**crb**、**fair-queue**、**irb**、**mac-accounting**、**precedence**、**random-detect**、**rate-limit**、および **shape** キーワードは、コマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**capabilities** キーワードのサポートが追加されました。
12.2(20)SE	**private-vlan mapping**、**backup**、**transceiver calibration**、**detail**、および **properties** キーワードが追加されました。
12.2(25)SEA	**calibration** キーワードが削除されました。
12.2(25)SEE	**backup**、**counters**、**detail**、および **trunk** キーワードが追加されました。
12.2(44)SE	**tengigabitethernet** *interface-id* **transceiver detail** キーワードが追加されました。

使用上のガイドライン

show interfaces capabilities コマンドに異なるキーワードを指定することで、次のような結果になります。

- **show interfaces capabilities module** *number* コマンドを使用して、スタックのスイッチ上のすべてのインターフェイスの性能を表示します。スタック内に該当するモジュール番号を持つスイッチがない場合、出力はありません。
- 指定されたインターフェイスの機能を表示するには、**show interfaces** *interface-id* **capabilities** を使用します。

- スタック内のすべてのインターフェイスの機能を表示するには、**show interfaces capabilities** を使用します（モジュール番号またはインターフェイス ID の指定なし）。

show interfaces switchport module *number* コマンドを使用して、スタックのスイッチ上のすべてのインターフェイスのスイッチ ポートの特性を表示します。スタック内に該当するモジュール番号を持つスイッチがない場合、出力の表現では大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、スタック メンバ 3 のインターフェイスに対する **show interfaces** コマンドの出力を示します。

```
Switch# show interfaces gigabitethernet3/0/2
GigabitEthernet3/0/2 is down, line protocol is down
  Hardware is Gigabit Ethernet, address is 0009.43a7.d085 (bia 0009.43a7.d085)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00 Last input never, output never, output hang never
  Last clearing of "show interfaces" 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
     2 packets input, 1040 bytes, 0 no buffer
     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 pause input
     0 input packets with dribble condition detected
     4 packets output, 1040 bytes, 0 underruns
     0 output errors, 0 collisions, 3 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
```

次の例では、**show interfaces accounting** コマンドの出力を示します。

```
Switch# show interfaces accounting
Vlan1
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                      IP    1094395  131900022     559555   84077157
           Spanning Tree     283896   17033760         42       2520
                     ARP      63738    3825680        231      13860
Interface Vlan2 is disabled
Vlan7
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
Vlan31
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.

GigabitEthernet1/0/1
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
GigabitEthernet1/0/2
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
```

```
<output truncated>
```

次の例では、インターフェイスの **show interfaces capabilities** コマンドの出力を示します。

```
Switch# show interfaces gigabitethernet1/0/2 capabilities
GigabitEthernet1/0/2
  Model:                 WS-C3750G-24TS
Type:                  10/100/1000BaseTX
  Speed:                 10,100,1000,auto
  Duplex:                full,auto
  Trunk encap.type:     802.1Q,ISL
  Trunk mode:            on,off,desirable,nonegotiate
  Channel:               yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:           rx-(off,on,desired),tx-(none)
  Fast Start:            yes
  QoS scheduling:        rx-(not configurable on per port basis),tx-(4q2t)
  CoS rewrite:           yes
  ToS rewrite:           yes
  UDLD:                  yes
  Inline power:          no
  SPAN:                  source/destination
  PortSecure:            yes
  Dot1x:                 yes
  Multiple Media Types:  rj45, sfp, auto-select
```

次の例では、**description** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスを *Connects to Marketing* として指定した場合の **show interfaces** *interface-id* **description** コマンドの出力を示します。

```
Switch# show interfaces gigabitethernet1/0/2 description
Interface Status         Protocol Description
Gi1/0/2     up             down     Connects to Marketing
```

次の例では、スイッチにポート チャネルが設定されている場合の **show interfaces etherchannel** コマンドの出力を示します。

```
Switch# show interfaces etherchannel
----
Port-channel1:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port   = 10/1          Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse

Port-channel2:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port   = 10/2          Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse

Port-channel3:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port   = 10/3          Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse
```

次の例では、プライベート VLAN のプライマリ VLAN が VLAN 10 で、セカンダリ VLAN が VLAN 501 と 502 の場合の **show interfaces private-vlan mapping** コマンドの出力を示します。

```
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan10    501            isolated
```

```
vlan10    502            community
```

次の例では、VTP ドメイン内でプルーニングがイネーブルの場合の **show interfaces** *interface-id* **pruning** コマンドの出力を示します。

```
Switch# show interfaces gigibitethernet1/0/2 pruning
Port    Vlans pruned for lack of request by neighbor
Gi1/0/2   3,4

Port    Vlans traffic requested of neighbor
Gi1/0/2   1-3
```

次の例では、指定した VLAN インターフェイスの **show interfaces stats** コマンドの出力を示します。

```
Switch# show interfaces vlan 1 stats
Switching path    Pkts In   Chars In   Pkts Out  Chars Out
        Processor    1165354  136205310     570800   91731594
      Route cache          0          0          0          0
            Total    1165354  136205310     570800   91731594
```

次の例では、**show interfaces status** コマンドの出力の一部を示します。すべてのインターフェイスのステータスが表示されます。

```
Switch# show interfaces status
1/0/1                     connected    routed     a-half  a-100 10/100BaseTX
Fa1/0/2                     notconnect   121,40       auto   auto 10/100BaseTX
Fa1/0/3                     notconnect   1            auto   auto 10/100BaseTX
Fa1/0/4                     notconnect   18           auto   auto Not Present
Fa1/0/5                     connected    121        a-full a-1000 10/100BaseTX
Fa1/0/6                     connected    122,11     a-full a-1000 10/100BaseTX

<output truncated>
Gi1/0/1                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/2                     notconnect   1            auto   auto unsupported
```

次の例では、プライベート VLAN が設定されている場合の特定のインターフェイスの **show interfaces status** コマンドの出力を示します。ポート 2 をプライベート VLAN ホスト ポートとして設定しています。ポート 22 は、プライマリ VLAN 20 とセカンダリ VLAN 25 に関連付けられます。

```
Switch# show interfaces fastethernet1/0/2 status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa1/0/2                     connected    20,25      a-full  a-100 10/100BaseTX
```

次の例では、ポート 3 がプライベート VLAN 混合ポートとして設定されています。この出力は、プライマリ VLAN 20 だけを表示します。

```
Switch# show interfaces fastethernet1/0/3 status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa1/0/3                     connected    20         a-full  a-100 10/100BaseTX
```

次の例では、**show interfaces status err-disabled** コマンドの出力を示します。errdisable ステートのインターフェイスのステータスを表示します。

```
Switch# show interfaces status err-disabled
Port      Name               Status       Reason
Gi2/0/26                     err-disabled gbic-invalid
```

次の例では、ポートの **show interfaces switchport** コマンドの出力を示します。表 2-31 に、この出力で表示されるフィールドの説明を示します。

（注） プライベート VLAN トランクはこのリリースではサポートされないため、フィールドは適用されません。

```
Switch# show interfaces gigabitethernet1/0/1 switchport
Name: Gi1/0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association:10 (VLAN0010) 502 (VLAN0502)
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled

Voice VLAN: none (Inactive)
Appliance trust: none
```

表 2-31　show interfaces switchport のフィールドの説明

フィールド	説明
Name	ポートの名前を表示します。
Switchport	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。この出力の場合、ポートはスイッチポート モードです。
Administrative Mode Operational Mode	管理モードおよび動作モードを表示します。
Administrative Trunking Encapsulation Operational Trunking Encapsulation Negotiation of Trunking	管理上および運用上のカプセル化方式、およびトランキングネゴシエーションがイネーブルかどうかを表示します。
Access Mode VLAN	ポートを設定する VLAN ID を表示します。
Trunking Native Mode VLAN Trunking VLANs Enabled Trunking VLANs Active	ネイティブ モードのトランクの VLAN ID を一覧表示します。トランク上の許可 VLAN を一覧表示します。トランク上のアクティブ VLAN を一覧表示します。
Pruning VLANs Enabled	プルーニングに適格な VLAN を一覧表示します。
Protected	インターフェイス上で保護ポートがイネーブル（True）であるかまたはディセーブル（False）であるかを表示します。
Unknown unicast blocked Unknown multicast blocked	不明なマルチキャストおよび不明なユニキャスト トラフィックがインターフェイス上でブロックされているかどうかを表示します。
Voice VLAN	音声 VLAN がイネーブルである VLAN ID を表示します。

表 2-31　show interfaces switchport のフィールドの説明 （続き）

フィールド	説明
Administrative private-vlan host-association	プライベート VLAN ホスト ポートの管理 VLAN のアソシエーションを表示します。
Administrative private-vlan mapping	プライベート VLAN 混合ポートの管理 VLAN のマッピングを表示します。
Operational private-vlan	プライベート VLAN の動作ステータスを表示します。
Appliance trust	IP Phone のデータ パケットのサービス クラス（CoS）設定を表示します。

次の例では、プライベート VLAN 混合ポートとして設定されたポートの **show interfaces switchport** コマンドの出力を示します。プライマリ VLAN 20 は、セカンダリ VLAN 25、30、35 にマッピングされます。

```
Switch# show interfaces gigabitethernet1/0/2 switchport
Name: Gi1/01/2
Switchport: Enabled
Administrative Mode: private-vlan promiscuous
Operational Mode: private-vlan promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: 20 (VLAN0020) 25 (VLAN0025) 30 (VLAN0030) 35
(VLAN0035)
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan:
20 (VLAN0020) 25 (VLAN0025)
30 (VLAN0030)
35 (VLAN0035)

<output truncated>
```

次の例では、**show interfaces switchport backup** コマンドの出力を示します。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
     Active Interface    Backup Interface    State
     ------------------------------------------------------------
     Fa1/0/1               Fa1/0/2             Active Up/Backup Standby
     Fa3/0/3               Fa4/0/5             Active Down/Backup Up
     Po1                       Po2                 Active Standby/Backup Up
```

次の例では、**show interfaces switchport backup** コマンドの出力を示します。この例では、スイッチで VLAN 1 ～ 50、60、100 ～ 120 が設定されています。

```
Switch(config)#interface gigabitEthernet 2/0/6
Switch(config-if)#switchport backup interface gigabitEthernet 2/0/8 prefer vlan 60,100-120
```

両方のインターフェイスが起動している場合、Gi2/0/8 が VLAN 60、100 ～ 120 のトラフィックを転送し、Gi2/0/6 が VLAN 1 ～ 50 のトラフィックを転送します。

```
Switch#show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet2/0/6 GigabitEthernet2/0/8 Active Down/Backup Up

Vlans on Interface Gi 2/0/6: 1-50
Vlans on Interface Gi 2/0/8: 60, 100-120
```

Flex Link インターフェイスがダウンすると（LINK_DOWN）、このインターフェイスで優先される VLAN は、Flex Link ペアのピア インターフェイスに移動します。この例では、インターフェイス Gi2/0/6 がダウンして、Gi2/0/8 が Flex Link ペアのすべての VLAN を引き継ぎます。

```
Switch#show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet2/0/6 GigabitEthernet2/0/8 Active Down/Backup Up

Vlans on Interface Gi 2/0/6:
Vlans on Interface Gi 2/0/8: 1-50, 60, 100-120
```

Flex Link インターフェイスがアップになると、このインターフェイスで優先される VLAN はピア インターフェイスでブロックされ、アップしたインターフェイスでフォワーディング ステートになります。この例では、インターフェイス Gi2/0/6 がアップになると、このインターフェイスで優先される VLAN はピア インターフェイス Gi2/0/8 でブロックされ、Gi2/0/6 で転送されます。

```
Switch#show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet2/0/6 GigabitEthernet2/0/8 Active Down/Backup Up

Vlans on Interface Gi 2/0/6: 1-50
Vlans on Interface Gi 2/0/8: 60, 100-120
```

次の例では、**show interfaces** *interface-id* **pruning** コマンドの出力を示します。

```
Switch# show interfaces gigibitethernet1/0/2 pruning
Port    Vlans pruned for lack of request by neighbor
```

次の例では、**show interfaces** *interface-id* **trunk** コマンドの出力を示します。ポートのトランキング情報が表示されます。

```
Switch# show interfaces gigabitethernet1/0/2 trunk
Port          Mode         Encapsulation  Status        Native vlan
Gi1/0/1      auto         negotiate      trunking      1

Port          Vlans allowed on trunk
Gi1/0/1      1-4094

Port          Vlans allowed and active in management domain
Gi1/0/1      1-4

Port          Vlans in spanning tree forwarding state and not pruned
Gi1/0/1       1-4
```

次の例では、**show interfaces** *interface-id* **transceiver properties** コマンドの出力を示します。

```
Switch# show interfaces gigabitethernet1/0/2 transceiver properties
Name : Gi1/0/2
```

```
Administrative Speed: auto
Operational Speed: auto
Administrative Duplex: auto
Administrative Power Inline: enable
Operational Duplex: auto
Administrative Auto-MDIX: off
Operational Auto-MDIX: off
```

次の例では、**show interfaces** *interface-id* **transceiver detail** コマンドの出力を示します。

```
Switch# show interfaces gigabitethernet2/0/3 transceiver detail
ITU Channel not available (Wavelength not available),
Transceiver is externally calibrated.
mA:milliamperes, dBm:decibels (milliwatts), 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 uncalibrated.

                           High Alarm  High Warn  Low Warn   Low Alarm
        Temperature        Threshold   Threshold  Threshold  Threshold
Port     (Celsius)         (Celsius)   (Celsius)  (Celsius)  (Celsius)
------- ------------------ ----------  ---------  ---------  ---------
Gi2/0/3 41.5               110.0       103.0      -8.0       -12.0

                           High Alarm  High Warn  Low Warn   Low Alarm
         Voltage           Threshold   Threshold  Threshold  Threshold
Port     (Volts)           (Volts)     (Volts)    (Volts)    (Volts)
-------  ---------------   ----------  ---------  ---------  ---------
Gi2/0/3  3.20              4.00        3.70       3.00       2.95

                           High Alarm  High Warn  Low Warn   Low Alarm
         Current           Threshold   Threshold  Threshold  Threshold
Port     (milliamperes)    (mA)        (mA)       (mA)       (mA)
-------  -----------------  ----------  ---------  ---------  ---------
Gi2/0/3  31.0              84.0        70.0       4.0        2.0

         Optical           High Alarm  High Warn  Low Warn   Low Alarm
         Transmit Power    Threshold   Threshold  Threshold  Threshold
Port     (dBm)             (dBm)       (dBm)      (dBm)      (dBm)
-------  -----------------  ----------  ---------  ---------  ---------
Gi2/0/3  -0.0 ( -0.0)      -0.0        -0.0       -0.0       -0.0

         Optical           High Alarm  High Warn  Low Warn   Low Alarm
         Receive Power     Threshold   Threshold  Threshold  Threshold
Port     (dBm)             (dBm)       (dBm)      (dBm)      (dBm)
-------  -----------------  ----------  ---------  ---------  ---------
Gi2/0/3  N/A  ( -0.0) --   -0.0        -0.0       -0.0       -0.0
```

次の例では、**show interfaces** tengigabitethernet *interface-id* **transceiver detail** コマンドの出力を示します。

```
Switch# show interfaces tengigabitethernet1/0/1 transceiver detail
Transceiver monitoring is disabled for all interfaces.

ITU Channel not available (Wavelength not available),
Transceiver is internally calibrated.
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.
High Alarm High Warn Low Warn Low Alarm
Temperature Threshold Threshold Threshold Threshold
Port (Celsius) (Celsius) (Celsius) (Celsius) (Celsius)
--------- ------------------ ---------- --------- --------- ---------
```

```
Te1/0/1 26.8 70.0 60.0 5.0 0.0
High Alarm High Warn Low Warn Low Alarm
Voltage Threshold Threshold Threshold Threshold
Port (Volts) (Volts) (Volts) (Volts) (Volts)
--------- --------------- ---------- --------- --------- ---------
Te1/0/1 3.15 3.63 3.63 2.97 2.97
High Alarm High Warn Low Warn Low Alarm
Current Threshold Threshold Threshold Threshold
Port (milliamperes) (mA) (mA) (mA) (mA)
--------- ----------------- ---------- --------- --------- ---------
Te1/0/1 5.0 16.3 15.3 3.9 3.2
Optical High Alarm High Warn Low Warn Low Alarm
Transmit Power Threshold Threshold Threshold Threshold
Port (dBm) (dBm) (dBm) (dBm) (dBm)
--------- ----------------- ---------- --------- --------- ---------
Te1/0/1 -1.9 1.0 0.5 -8.2 -8.5
Optical High Alarm High Warn Low Warn Low Alarm
Receive Power Threshold Threshold Threshold Threshold
Port (dBm) (dBm) (dBm) (dBm) (dBm)
------- ----------------- ---------- --------- --------- ---------
Te1/0/1 -1.4 1.0 0.5 -14.1 -15.0
```

次の例では、**show interfaces tengigabitethernet** *interface-id* **transceiver properties** コマンドの出力を示します。

```
Switch# show interfaces tengigabitethernet1/0/1 transceiver properties
Transceiver monitoring is disabled for all interfaces.

ITU Channel not available (Wavelength not available),
Transceiver is internally calibrated.
Name : Te1/0/1
Administrative Speed: 10000
Administrative Duplex: full
Administrative Auto-MDIX: on
Administrative Power Inline: N/A
Operational Speed: 10000
Operational Duplex: full
Operational Auto-MDIX: off
Media Type: 10GBase-LR
```

関連コマンド

コマンド	説明
switchport access	ポートをスタティック アクセス ポートまたはダイナミック アクセス ポートとして設定します。
switchport block	インターフェイス上で不明なユニキャストまたはマルチキャスト トラフィックをブロックします。
switchport backup interface	相互バックアップを提供するレイヤ 2 インターフェイスのペアである Flex Link を設定します。
switchport mode	ポートの VLAN メンバシップ モードを設定します。
switchport mode private-vlan	ポートをプライベート VLAN のホスト ポートまたは混合ポートとして設定します。
switchport private-vlan	ホスト ポートのプライベート VLAN のアソシエーション、または混合ポートのプライベート VLAN のマッピングを定義します。
switchport protected	同じスイッチの他の保護されたポートからレイヤ 2 のユニキャスト、マルチキャスト、およびブロードキャスト トラフィックを分離します。
switchport trunk pruning	トランキング モードのポートの VLAN プルーニング適格リストを設定します。

show interfaces counters

スイッチまたは特定のインターフェイスの各種カウンタを表示するには、**show interfaces counters** 特権 EXEC コマンドを使用します。

show interfaces [*interface-id* | **vlan** *vlan-id*] **counters** [**errors** | **etherchannel** | **module** *switch- number* | **protocol status** | **trunk**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface-id	（任意）物理インターフェイスの ID です。
errors	（任意）エラー カウンタを表示します。
etherchannel	（任意）送受信されたオクテット、ブロードキャスト パケット、マルチキャスト パケット、およびユニキャスト パケットなど、EtherChannel カウンタを表示します。
module *switch- number*	（任意）指定されたスタック メンバのカウンタを表示します。指定できる範囲は 1 ～ 9 です（スタックのスイッチ番号に対応）。 **（注）** このコマンドでは、**module** キーワードはスタック メンバ番号（1 ～ 9）を参照しています。インターフェイス ID に含まれるモジュール番号は、常に 0 です。
protocol status	（任意）インターフェイスでイネーブルになっているプロトコルのステータスを表示します。
trunk	（任意）トランク カウンタを表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

（注） **vlan** *vlan-id* キーワードは、コマンドラインのヘルプ ストリングには表示されますが、サポートされていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(25)SE	**etherchannel** キーワードおよび **protocol status** キーワードが追加されました。**broadcast**、**multicast**、および **unicast** キーワードが削除されました。

使用上のガイドライン

キーワードを入力しない場合は、すべてのインターフェイスのすべてのカウンタが表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show interfaces counters** コマンドの出力の一部を示します。スイッチのすべてのカウンタが表示されます。

```
Switch# show interfaces counters
Port            InOctets   InUcastPkts   InMcastPkts   InBcastPkts
Gi1/0/1                0             0             0             0
Gi1/0/2                0             0             0             0

<output truncated>
```

次の例では、スタック メンバ 2 の **show interfaces counters module** コマンドの出力の一部を示します。スタック内で指定されたスイッチのすべてのカウンタが表示されます。

```
Switch# show interfaces counters module 2
Port            InOctets   InUcastPkts   InMcastPkts   InBcastPkts
Fa2/0/1              520             2             0             0
Fa2/0/2              520             2             0             0
Fa2/0/3              520             2             0             0
Fa2/0/4              520             2             0             0
Fa2/0/5              520             2             0             0
Fa2/0/6              520             2             0             0
Fa2/0/7              520             2             0             0
Fa2/0/8              520             2             0             0

<output truncated>
```

次の例では、すべてのインターフェイスに対する **show interfaces counters protocol status** コマンドの出力の一部を示します。

```
Switch# show interfaces counters protocol status
Protocols allocated:
 Vlan1: Other, IP
 Vlan20: Other, IP, ARP
 Vlan30: Other, IP, ARP
 Vlan40: Other, IP, ARP
 Vlan50: Other, IP, ARP
 Vlan60: Other, IP, ARP
 Vlan70: Other, IP, ARP
 Vlan80: Other, IP, ARP
 Vlan90: Other, IP, ARP
 Vlan900: Other, IP, ARP
 Vlan3000: Other, IP
 Vlan3500: Other, IP
 FastEthernet1/0/1: Other, IP, ARP, CDP
 FastEthernet1/0/2: Other, IP
 FastEthernet1/0/3: Other, IP
 FastEthernet1/0/4: Other, IP
 FastEthernet1/0/5: Other, IP
 FastEthernet1/0/6: Other, IP
 FastEthernet1/0/7: Other, IP
 FastEthernet1/0/8: Other, IP
 FastEthernet1/0/9: Other, IP
 FastEthernet1/0/10: Other, IP, CDP

<output truncated>
```

次の例では、**show interfaces counters trunk** コマンドの出力を示します。すべてのインターフェイスのトランク カウンタが表示されます。

```
Switch# show interfaces counters trunk
Port        TrunkFramesTx  TrunkFramesRx  WrongEncap
Gi1/0/1                 0              0           0
Gi1/0/2                 0              0           0
Gi1/0/3             80678           4155           0
```

```
Gi1/0/4              82320            126           0
Gi1/0/5                  0              0           0

<output truncated>
```

関連コマンド

コマンド	説明
show interfaces	追加のインターフェイスの特性を表示します。

show inventory

ハードウェアの Product Identification（PID）情報を表示するには、**show inventory** ユーザ EXEC コマンドを使用します。

show inventory [*entity-name* | **raw**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

entity-name	（任意）指定されたエンティティを表示します。たとえば、Small Form-Factor Pluggable（SFP）モジュールのインストール先となるインターフェイス（gigabitethernet1/0/1 など）を入力します。
raw	（任意）デバイスのすべてのエンティティを表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)SEC	このコマンドが追加されました。

使用上のガイドライン

コマンドでは大文字と小文字が区別されます。引数がない場合、**show inventory** コマンドは製品識別情報を持つすべての識別可能なエンティティのコンパクト ダンプを生成します。コンパクト ダンプには、エンティティの場所（スロット ID）、エンティティの説明、およびそのエンティティの Unique Device Indicator（UDI）（PID、VID、および SN）が表示されます。

（注）　PID がない場合は、**show inventory** コマンドを入力しても出力は表示されません。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show inventory** コマンドの出力を示します。

```
Switch> show inventory
NAME: "5", DESCR: "WS-C3750G-12S"
PID: WS-C3750G-12S-S   , VID: E0 , SN: CAT0749R204
```

show ip arp inspection

ダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査の設定および動作ステート、あるいはすべての VLAN または指定されたインターフェイスや VLAN に対するこの機能のステータスを表示するには、**show ip arp inspection** 特権 EXEC コマンドを使用します。

show ip arp inspection [**interfaces** [*interface-id*] | **log** | **statistics** [**vlan** *vlan-range*] | **vlan** *vlan-range*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interfaces [*interface-id*]	（任意）指定されたインターフェイスまたはすべての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。有効なインターフェイスには、物理ポートとポート チャネルが含まれます。
log	（任意）ダイナミック ARP 検査ログ バッファの設定と内容を表示します。
statistics [**vlan** *vlan-range*]	（任意）指定された VLAN の転送済みパケット、ドロップ済みパケット、MAC 検証に失敗したパケット、IP 検証に失敗したパケット、アクセス コントロール リスト（ACL）によって許可および拒否されたパケット、DHCP によって許可および拒否されたパケットの統計情報を表示します。VLAN が指定されていない場合、または範囲が指定されている場合は、ダイナミック ARP 検査がイネーブルにされた（アクティブ）VLAN だけの情報を表示します。 VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。
vlan *vlan-range*	（任意）指定された VLAN のダイナミック ARP 検査の設定および動作ステートを表示します。VLAN が指定されていない場合、または範囲が指定されている場合は、ダイナミック ARP 検査がイネーブルにされた（アクティブ）VLAN だけの情報を表示します。 VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。
12.2(37)SE	出力にプローブ ロギング情報が含まれるように変更されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show ip arp inspection** コマンドの出力を示します。

```
Switch# show ip arp inspection

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Enabled

  Vlan     Configuration    Operation   ACL Match          Static ACL
  ----     -------------    ---------   ---------          ----------
     1     Enabled          Active      deny-all           No

  Vlan     ACL Logging      DHCP Logging      Probe Logging
  ----     -----------      ------------      -------------
     1     Acl-Match        All               Permit

  Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
  ----      ---------        -------     ----------      ---------
     1              0              0              0              0

  Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
  ----   ------------    -----------  -------------   -------------------
     1              0              0              0                     0

  Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
  ----   -----------------   ----------------------   ---------------------
     1                  0                        0                       0
```

次の例では、**show ip arp inspection interfaces** コマンドの出力を示します。

```
Switch# show ip arp inspection interfaces
 Interface        Trust State     Rate (pps)    Burst Interval
 ---------------  -----------     ----------    --------------
 Gi1/0/1            Untrusted               15                 1
 Gi1/0/2            Untrusted               15                 1
 Gi1/0/3            Untrusted               15                 1
```

次の例では、**show ip arp inspection interfaces** *interface-id* コマンドの出力を示します。

```
Switch# show ip arp inspection interfaces gigabitethernet1/0/1
 Interface        Trust State     Rate (pps)    Burst Interval
 ---------------  -----------     ----------    --------------
 Gi1/0/1            Untrusted               15                 1
```

次の例では、**show ip arp inspection log** コマンドの出力を示します。バッファがクリアされる前のログ バッファの内容を表示します。

```
Switch# show ip arp inspection log
Total Log Buffer Size : 32
Syslog rate : 10 entries per 300 seconds.

Interface   Vlan  Sender MAC      Sender IP        Num Pkts   Reason       Time
----------  ----  --------------  ---------------  ---------  -----------  ----
Gi1/0/1       5     0003.0000.d673  192.2.10.4               5  DHCP Deny    19:39:01 UTC
Mon Mar 1 1993
Gi1/0/1       5     0001.0000.d774  128.1.9.25               6  DHCP Deny    19:39:02 UTC
Mon Mar 1 1993
Gi1/0/1       5     0001.c940.1111  10.10.10.1               7  DHCP Deny    19:39:03 UTC
Mon Mar 1 1993
Gi1/0/1       5     0001.c940.1112  10.10.10.2               8  DHCP Deny    19:39:04 UTC
Mon Mar 1 1993
Gi1/0/1       5     0001.c940.1114  173.1.1.1               10  DHCP Deny    19:39:06 UTC
Mon Mar 1 1993
```

```
Gi1/0/1       5     0001.c940.1115  173.1.1.2               11  DHCP Deny    19:39:07 UTC
Mon Mar 1 1993
Gi1/0/1       5     0001.c940.1116  173.1.1.3               12  DHCP Deny    19:39:08 UTC
Mon Mar 1 1993
```

ログ バッファがオーバーフローする場合は、ログ イベントがログ バッファに収まらないことを意味しており、**show ip arp inspection log** 特権 EXEC コマンドの出力が影響を受けます。パケット数および時間以外のすべてのデータの代わりに -- が表示されます。このエントリには、これ以外の統計情報が提供されません。出力にこのエントリが表示される場合は、ログ バッファのエントリ数を増やすか、**ip arp inspection log-buffer** グローバル コンフィギュレーション コマンドでロギング レートを増やします。

次の例では、**show ip arp inspection statistics** コマンドの出力を示します。ダイナミック ARP 検査によって処理されたすべてのアクティブ VLAN のパケットの統計情報を表示します。

```
Switch# show ip arp inspection statistics
Vlan       Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
    5              3           4618           4605              4
 2000              0              0              0              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    5              0             12                     0
 2000              0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    5                  0                        9
 2000                  0                        0
```

show ip arp inspection statistics コマンドでは、スイッチは信頼されたダイナミック ARP 検査ポート上の各 ARP 要求および応答パケットの転送済みパケット数を増加させます。スイッチは、送信元 MAC、宛先 MAC、または IP 検証チェックによって拒否された各パケットの ACL または DHCP 許可済みパケット数を増加させ、適切な失敗数を増加させます。

次の例では、**show ip arp inspection statistics vlan 5** コマンドの出力を示します。ダイナミック ARP 検査によって処理された VLAN 5 のパケットの統計情報を表示します。

```
Switch# show ip arp inspection statistics vlan 5
Vlan       Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
    5              3           4618           4605              4

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    5              0             12                     0

 Vlan   Dest MAC Failures   IP Validation Failures      Invalid Protocol Data
 ----   -----------------   ----------------------      ---------------------
    5                  0                        9                          3
```

次の例では、**show ip arp inspection vlan 5** コマンドの出力を示します。VLAN 5 のダイナミック ARP 検査の設定および動作ステートを表示します。

```
Switch# show ip arp inspection vlan 5
Source Mac Validation      :Enabled
Destination Mac Validation :Enabled
IP Address Validation      :Enabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    5     Enabled          Active      second             No
```

```
Vlan      ACL Logging       DHCP Logging
----      -----------       ------------
   5      Acl-Match         All
```

関連コマンド

コマンド	説明
arp access-list	ARP ACL を定義します。
clear ip arp inspection log	ダイナミック ARP 検査ログ バッファをクリアします。
clear ip arp inspection statistics	ダイナミック ARP 検査の統計情報をクリアします。
ip arp inspection log-buffer	ダイナミック ARP 検査ロギング バッファを設定します。
ip arp inspection vlan logging	VLAN 単位で記録するパケットのタイプを制御します。
show arp access-list	ARP アクセス リストに関する詳細を表示します。

show ip dhcp snooping

Dynamic Host Configuration Protocol（DHCP）スヌーピング設定を表示するには、**show ip dhcp snooping** ユーザ EXEC コマンドを使用します。

show ip dhcp snooping [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。
12.2(25)SEE	グローバル サブオプション設定を表示するため、コマンド出力が更新されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

このコマンドは、グローバル コンフィギュレーションの結果だけを表示します。したがって、この例では、ストリングがサーキット ID 用に設定されていた場合も、サーキット ID サブオプションは **vlan-mod-port** のデフォルト形式で表示されます。

例

次の例では、**show ip dhcp snooping** コマンドの出力を示します。

```
Switch> show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
40-42
Insertion of option 82 is enabled
    circuit-id format: vlan-mod-port
    remote-id format: string
Option 82 on untrusted port is allowed
Verification of hwaddr field is enabled
Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
GigabitEthernet1/0/1             yes         unlimited
GigabitEthernet1/0/2             yes         unlimited
GigabitEthernet2/0/3             no          2000
GigabitEthernet2/0/4             yes         unlimited
```

関連コマンド

コマンド	説明
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

show ip dhcp snooping binding

スイッチ上にある全インターフェイスの DHCP スヌーピング バインディング データベースおよび設定情報を表示するには、**show ip dhcp snooping binding** ユーザ EXEC コマンドを使用します。

show ip dhcp snooping binding [*ip-address*] [*mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

ip-address	（任意）バインディング エントリ IP アドレスを指定します。
mac-address	（任意）バインディング エントリ MAC アドレスを指定します。
interface *interface-id*	（任意）バインディング入力インターフェイスを指定します。
vlan *vlan-id*	（任意）バインディング エントリ VLAN を指定します。
| begin	*expression* と一致する行から表示を開始します。
| exclude	*expression* と一致する行を表示から除外します。
| include	指定した *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。
12.2(18)SE	**dynamic** および **static** キーワードが削除されました。

使用上のガイドライン

show ip dhcp snooping binding コマンドの出力は、ダイナミックに設定されたバインディングだけを表示します。DHCP スヌーピング バインディング データベース内のダイナミックおよびスタティックに設定されたバインディングを表示するには、**show ip source binding** 特権 EXEC コマンドを使用します。

DHCP スヌーピングがイネーブルでインターフェイスがダウン ステートに変更された場合、静的に設定されたバインディングは削除されません。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、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方法を示します。

```
Switch> show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
01:02:03:04:05:06   10.1.2.150       9837        dhcp-snooping  20    GigabitEthernet2/0/1
00:D0:B7:1B:35:DE   10.1.2.151       237         dhcp-snooping  20    GigabitEthernet2/0/2
Total number of bindings: 2
```

次の例では、特定の IP アドレスの DHCP スヌーピング バインディング エントリを表示する方法を示します。

```
Switch> show ip dhcp snooping binding 10.1.2.150
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
01:02:03:04:05:06   10.1.2.150       9810        dhcp-snooping  20    GigabitEthernet2/0/1
Total number of bindings: 1
```

次の例では、特定の MAC アドレスの DHCP スヌーピング バインディング エントリを表示する方法を示します。

```
Switch> show ip dhcp snooping binding 0102.0304.0506
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
01:02:03:04:05:06   10.1.2.150       9788        dhcp-snooping  20    GigabitEthernet2/0/2
Total number of bindings: 1
```

次の例では、ポートの DHCP スヌーピング バインディング エントリを表示する方法を示します。

```
Switch> show ip dhcp snooping binding interface gigabitethernet2/0/2
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:30:94:C2:EF:35   10.1.2.151       290         dhcp-snooping  20    GigabitEthernet2/0/2
Total number of bindings: 1
```

次の例では、VLAN 20 の DHCP スヌーピング バインディング エントリを表示する方法を示します。

```
Switch> show ip dhcp snooping binding vlan 20
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
01:02:03:04:05:06   10.1.2.150       9747        dhcp-snooping  20    GigabitEthernet2/0/1
00:00:00:00:00:02   10.1.2.151       65          dhcp-snooping  20    GigabitEthernet2/0/2
Total number of bindings: 2
```

表 2-32 に、**show ip dhcp snooping binding** コマンド出力のフィールドの説明を示します。

表 2-32　show ip dhcp snooping binding コマンド出力

フィールド	説明
MacAddress	クライアント ハードウェアの MAC アドレス
IpAddress	DHCP サーバに割り当てられたクライアント IP アドレス
Lease(sec)	IP アドレスに対する残りのリース時間
Type	バインディング タイプ
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
Total number of bindings	スイッチに設定される合計バインディング数 **（注）** コマンド出力では、合計バインディング数が表示されないこともあります。たとえば、200 バインディングがスイッチに設定されてすべてのバインディングが表示される前に表示を停止させた場合、合計数は変更されません。

関連コマンド

コマンド	説明
ip dhcp snooping binding	DHCP スヌーピング バインディング データベースを設定します。
show ip dhcp snooping	DHCP スヌーピング設定を表示します。

show ip dhcp snooping database

DHCP スヌーピング バインディング 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** ユーザ EXEC コマンドを使用します。

show ip dhcp snooping database [**detail**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

detail	（任意）詳細なステータスと統計情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

例

次の例では、**show ip dhcp snooping database** コマンドの出力を示します。

```
Switch> 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 Succeded 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
```

次の例では、**show ip dhcp snooping database detail** コマンドの出力を示します。

```
Switch# 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 Succeded Time : None
```

```
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
```

関連コマンド

コマンド	説明
ip dhcp snooping	VLAN 上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping database	DHCP スヌーピング バインディング データベース エージェントまたはバインディング ファイルを設定します。
show ip dhcp snooping	DHCP スヌーピング情報を表示します。

show ip dhcp snooping statistics

DHCP スヌーピング統計情報をサマリー形式または詳細形式で表示するには、**show ip dhcp snooping statistics** ユーザ EXEC コマンドを使用します。

show ip dhcp snooping statistics [**detail**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

detail	（任意）詳細な統計情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(37)SE	このコマンドが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

スイッチ スタックでは、すべての統計情報がスタック マスターで生成されます。新しいスタック マスターが選出された場合、統計カウンタはリセットされます。

例

次の例では、**show ip dhcp snooping statistics** コマンドの出力を示します。

```
Switch> show ip dhcp snooping statistics
 Packets Forwarded                                    = 0
 Packets Dropped                                      = 0
 Packets Dropped From untrusted ports                 = 0
```

次の例では、**show ip dhcp snooping statistics detail** コマンドの出力を示します。

```
Switch> show ip dhcp snooping statistics detail
 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
   Binding mismatch                                   = 0
   Insertion of opt82 fail                            = 0
   Interface Down                                     = 0
   Unknown output interface                           = 0
   Reply output port equal to input port              = 0
   Packet denied by platform                          = 0
```

表 2-33 に、DHCP スヌーピング統計情報およびその説明を示します。

表 2-33　DHCP スヌーピング統計情報

DHCP スヌーピング統計情報	説明
Packets Processed by DHCP Snooping	転送されたパケットおよびドロップされたパケットも含めて、DHCP スヌーピングによって処理されたパケットの合計数。
Packets Dropped Because IDB not known	パケットの入力インターフェイスを判断できないエラーの数。
Queue full	パケットの処理に使用される内部キューが満杯であるエラーの数。非常に高いレートで DHCP パケットを受信し、入力ポートでレート制限がイネーブルになっていない場合、このエラーが発生することがあります。
Interface is in errdisabled	errdisable としてマークされたポートでパケットを受信した回数。これが発生する可能性があるのは、ポートが errdisable ステートである場合にパケットが処理キューに入り、そのパケットが後で処理される場合です。
Rate limit exceeded	ポートで設定されているレート制限を超えて、インターフェイスが errdisable ステートになった回数。
Received on untrusted ports	信頼できないポートで DHCP サーバ パケット（OFFER、ACK、NAK、LEASEQUERY のいずれか）を受信してドロップした回数。
Nonzero giaddr	信頼できないポートで受信した DHCP パケットのリレー エージェント アドレス フィールド（giaddr）がゼロ以外だった回数。または **no ip dhcp snooping information option allow-untrusted** グローバル コンフィギュレーション コマンドを設定しておらず、信頼できないポートで受信したパケットにオプション 82 データが含まれていた回数。
Source mac not equal to chaddr	DHCP パケットのクライアント MAC アドレス フィールド（chaddr）がパケットの送信元 MAC アドレスと一致せず、**ip dhcp snooping verify mac-address** グローバル コンフィギュレーション コマンドが設定されている回数。
Binding mismatch	MAC アドレスと VLAN のペアのバインディングになっているポートとは異なるポートで、RELEASE パケットまたは DECLINE パケットを受信した回数。これは、誰かが本来のクライアントをスプーフィングしようとしている可能性があることを示しますが、クライアントがスイッチの別のポートに移動して RELEASE または DECLINE を実行したことを表すこともあります。MAC アドレスは、イーサネット ヘッダーの送信元 MAC アドレスではなく、DHCP パケットの chaddr フィールドから採用されます。
Insertion of opt82 fail	パケットへのオプション 82 挿入がエラーになった回数。オプション 82 データを含むパケットがインターネットの単一物理パケットのサイズを超えた場合、挿入はエラーになることがあります。
Interface Down	パケットが DHCP リレー エージェントへの応答であるが、リレー エージェントの SVI インターフェイスがダウンしている回数。DHCP サーバへのクライアント要求の送信と応答の受信の間で SVI がダウンした場合に発生するエラーですが、めったに発生しません。
Unknown output interface	オプション 82 データまたは MAC アドレス テーブルのルックアップのいずれかで、DHCP 応答パケットの出力インターフェイスを判断できなかった回数。パケットはドロップされます。オプション 82 が使用されておらず、クライアント MAC アドレスが期限切れになった場合に発生することがあります。ポートセキュリティ オプションで IPSG がイネーブルであり、オプション 82 がイネーブルでない場合、クライアントの MAC アドレスは学習されず、応答パケットはドロップされます。

表 2-33　DHCP スヌーピング統計情報 （続き）

DHCP スヌーピング統計情報	説明
Reply output port equal to input port	DHCP 応答パケットの出力ポートが入力ポートと同じであり、ループの可能性の原因となった回数。ネットワークの設定の誤り、またはポートの信頼設定の誤用の可能性を示します。
Packet denied by platform	プラットフォーム固有のレジストリによってパケットが拒否された回数。

関連コマンド

コマンド	説明
clear ip dhcp snooping	DHCP スヌーピング バインディング データベース カウンタ、DHCP スヌーピング バインディング データベース エージェント統計情報カウンタ、DHCP スヌーピング統計情報カウンタをクリアします。

show ip igmp profile

設定されたすべてのインターネット グループ管理プロトコル（IGMP）プロファイル、または指定された IGMP プロファイルを表示するには、**show ip igmp profile** 特権 EXEC コマンドを使用します。

show ip igmp profile [*profile number*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

profile number	（任意）表示する IGMP プロファイル番号。指定できる範囲は 1 ～ 4294967295 です。プロファイル番号が入力されていない場合、すべての IGMP プロファイルが表示されます。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、プロファイル番号を指定した場合と指定しない場合の **show ip igmp profile** 特権 EXEC コマンドの出力を示します。プロファイル番号が入力されていない場合、表示にはスイッチ上で設定されたすべてのプロファイルが含まれます。

```
Switch# show ip igmp profile 40
IGMP Profile 40
    permit
    range 233.1.1.1 233.255.255.255

Switch# show ip igmp profile
IGMP Profile 3
    range 230.9.9.0 230.9.9.0
IGMP Profile 4
    permit
    range 229.9.9.0 229.255.255.255
```

関連コマンド

コマンド	説明
ip igmp profile	指定された IGMP プロファイル番号を設定します。

show ip igmp snooping

スイッチまたは VLAN のインターネット グループ管理プロトコル（IGMP）スヌーピング設定を表示するには、**show ip igmp snooping** ユーザ EXEC コマンドを使用します。

show ip igmp snooping [**groups** | **mrouter** | **querier**] [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

groups	（任意）**show ip igmp snooping groups** コマンドを参照してください。
mrouter	（任意）**show ip igmp snooping mrouter** コマンドを参照してください。
querier	（任意）**show ip igmp snooping querier** コマンドを参照してください。
vlan *vlan-id*	（任意）VLAN を指定します。範囲は 1 ～ 1001 および 1006 ～ 4094 です（特権 EXEC モードの場合だけ使用可能）。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(19)EA1	**querier** キーワードが追加されました。
12.2(18)SE	**groups** キーワードが追加されました。**show ip igmp snooping multicast** コマンドから **show ip igmp snooping groups** コマンドに替わりました。

使用上のガイドライン

スイッチまたは特定の VLAN のスヌーピングの設定を表示するのにこのコマンドを使用します。

VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show ip igmp snooping vlan 1** コマンドの出力を示します。ここでは、特定の VLAN のスヌーピング特性を表示します。

```
Switch# show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
------------------------------------
IGMP snooping              :Enabled
IGMPv3 snooping (minimal)  :Enabled
Report suppression         :Enabled
TCN solicit query          :Disabled
TCN flood query count      :2
Last member query interval : 100
```

```
Vlan 1:
--------
IGMP snooping                        :Enabled
Immediate leave                      :Disabled
Multicast router learning mode       :pim-dvmrp
Source only learning age timer       :10
CGMP interoperability mode           :IGMP_ONLY
Last member query interval : 100
```

次の例では、**show ip igmp snooping** コマンドの出力を示します。ここでは、スイッチ上の VLAN すべてのスヌーピング特性を表示します。

```
Switch> show ip igmp snooping
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping              : Enabled
IGMPv3 snooping (minimal)  : Enabled
Report suppression         : Enabled
TCN solicit query          : Disabled
TCN flood query count      : 2
Last member query interval : 100

Vlan 1:
--------
IGMP snooping                        :Enabled
Immediate leave                      :Disabled
Multicast router learning mode       :pim-dvmrp
Source only learning age timer       :10
CGMP interoperability mode           :IGMP_ONLY
Last member query interval           : 100

Vlan 2:
--------
IGMP snooping                        :Enabled
Immediate leave                      :Disabled
Multicast router learning mode       :pim-dvmrp
Source only learning age timer       :10
CGMP interoperability mode           :IGMP_ONLY
Last member query interval           : 333

<output truncated>
```

関連コマンド

コマンド	説明
ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピングをイネーブルにします。
ip igmp snooping last-member-query-interval	IGMP スヌーピングの設定可能な Leave タイマーをイネーブルにします。
ip igmp snooping querier	レイヤ 2 ネットワークの IGMP クエリア機能をイネーブルにします。
ip igmp snooping report-suppression	IGMP レポート抑制をイネーブルにします。
ip igmp snooping tcn	IGMP トポロジ変更通知動作を設定します。
ip igmp snooping tcn flood	IGMP トポロジ変更通知動作としてマルチキャスト フラッディングを指定します。
ip igmp snooping vlan immediate-leave	VLAN の IGMP スヌーピング即時脱退処理をイネーブルにします。

コマンド	説明
ip igmp snooping vlan mrouter	マルチキャスト ルータ ポートを追加、またはマルチキャストの学習方式を設定します。
ip igmp snooping vlan static	レイヤ 2 ポートをマルチキャスト グループのメンバとして静的に追加します。
show ip igmp snooping groups	スイッチの IGMP スヌーピング マルチキャスト テーブルを表示します。
show ip igmp snooping mrouter	スイッチまたは指定されたマルチキャスト VLAN の IGMP スヌーピング マルチキャスト ルータ ポートを表示します。
show ip igmp snooping querier	スイッチ上に設定された IGMP クエリアの設定および動作情報を表示します。

show ip igmp snooping groups

スイッチのインターネット グループ管理プロトコル（IGMP）スヌーピング マルチキャスト テーブル、またはマルチキャスト情報を表示するには、**show ip igmp snooping groups** 特権 EXEC コマンドを使用します。指定されたマルチキャスト VLAN のマルチキャスト テーブル、または特定のマルチキャスト情報を表示するには、**vlan** キーワードを指定して使用します。

show ip igmp snooping groups [**count** | **dynamic** [**count**] | **user** [**count**]] [| {**begin** | **exclude** | **include**} *expression*]

show ip igmp snooping groups vlan *vlan-id* [*ip_address* | **count** | **dynamic** [**count**] | **user** [**count**]] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

count	（任意）実エントリの代わりに、指定されたコマンド オプションのエントリ総数を表示します。
dynamic	（任意）IGMP スヌーピングにより学習したエントリを表示します。
user	（任意）ユーザ設定のマルチキャスト エントリだけを表示します。
ip_address	（任意）指定グループ IP アドレスのマルチキャスト グループの特性を表示します。
vlan *vlan-id*	（任意）VLAN を指定します。指定できる範囲は 1 ～ 1001 および 1006 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(18)SE	このコマンドが追加されました。**show ip igmp snooping multicast** コマンドに替わるものです。

使用上のガイドライン

マルチキャスト情報またはマルチキャスト テーブルを表示するには、このコマンドを使用します。

VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、キーワードの指定をしない **show ip igmp snooping groups** コマンドの出力を示します。スイッチのマルチキャスト テーブルが表示されます。

```
Switch# show ip igmp snooping groups
Vlan      Group           Type        Version     Port List
------------------------------------------------------------
1         224.1.4.4       igmp                    Fa1/0/11
1         224.1.4.5       igmp                    Fa1/0/11
2         224.0.1.40      igmp        v2          Fa1/0/15
```

次の例では、**show ip igmp snooping groups count** コマンドの出力を示します。スイッチ上のマルチキャスト グループの総数が表示されます。

```
Switch# show ip igmp snooping groups count
Total number of multicast groups: 2
```

次の例では、**show ip igmp snooping groups dynamic** コマンドの出力を示します。IGMP スヌーピングにより学習したエントリだけを表示します。

```
Switch# show ip igmp snooping groups vlan 1 dynamic
Vlan      Group           Type        Version     Port List
------------------------------------------------------------
104       224.1.4.2       igmp        v2          Gi2/0/1, Fa1/0/15
104       224.1.4.3       igmp        v2          Gi2/0/1, Fa1/0/15
```

次の例では、**show ip igmp snooping groups vlan** *vlan-id ip-address* コマンドの出力を示します。指定された IP アドレスのグループのエントリを表示します。

```
Switch# show ip igmp snooping groups vlan 104 224.1.4.2
Vlan      Group           Type        Version     Port List
------------------------------------------------------------
104       224.1.4.2       igmp        v2          Gi2/0/1, Fa1/0/15
```

関連コマンド

コマンド	説明
ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピングをイネーブルにします。
ip igmp snooping vlan mrouter	マルチキャスト ルータ ポートを設定します。
ip igmp snooping vlan static	レイヤ 2 ポートをマルチキャスト グループのメンバとして静的に追加します。
show ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピング設定を表示します。
show ip igmp snooping mrouter	スイッチまたは指定されたマルチキャスト VLAN の IGMP スヌーピング マルチキャスト ルータ ポートを表示します。

show ip igmp snooping mrouter

スイッチまたは指定されたマルチキャスト VLAN の、動的に学習されたインターネット グループ管理プロトコル（IGMP）スヌーピングと、手動で設定されたマルチキャスト ルータ ポートを表示するには、**show ip igmp snooping mrouter** 特権 EXEC コマンドを使用します。

show ip igmp snooping mrouter [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

vlan *vlan-id*	（任意）VLAN を指定します。指定できる範囲は 1 ～ 1001 および 1006 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

スイッチまたは特定の VLAN 上のマルチキャスト ルータ ポートを表示するには、このコマンドを使用します。

VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

Multicast VLAN Registration（MVR; マルチキャスト VLAN レジストレーション）がイネーブルの場合、**show ip igmp snooping mrouter** コマンドは MVR マルチキャスト ルータの情報および IGMP スヌーピング情報を表示します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show ip igmp snooping mrouter** コマンドの出力を示します。スイッチ上でマルチキャスト ルータ ポートを表示します。

```
Switch# show ip igmp snooping mrouter
Vlan    ports
----    -----
   1    Gi2/0/1(dynamic)
```

関連コマンド

コマンド	説明
ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピングをイネーブルにします。
ip igmp snooping vlan mrouter	マルチキャスト ルータ ポートを追加します。
ip igmp snooping vlan static	レイヤ 2 ポートをマルチキャスト グループのメンバとして静的に追加します。
show ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピング設定を表示します。
show ip igmp snooping groups	スイッチまたは指定されたパラメータの IGMP スヌーピング マルチキャスト情報を表示します。

show ip igmp snooping querier

スイッチで設定された IGMP クエリアの設定および動作情報を表示するには、**show ip igmp snooping querier detail** ユーザ EXEC コマンドを使用します。

show ip igmp snooping querier [**detail** | **vlan** *vlan-id* [**detail**]] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

detail	（任意）IGMP クエリアの詳細情報を表示します。
vlan *vlan-id* [**detail**]	（任意）指定された VLAN の IGMP クエリア情報を表示します。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。詳細情報を表示するには、**detail** キーワードを使用します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)SEA	このコマンドが追加されました。

使用上のガイドライン

クエリアとも呼ばれ、IGMP クエリー メッセージを送信する検出装置の IGMP バージョンおよび IP アドレスを表示するには、**show ip igmp snooping querier** コマンドを使用します。サブネットは複数のマルチキャスト ルータを保有できますが、IGMP クエリアは 1 つしか保有できません。IGMPv2 を実行しているサブネットでは、マルチキャスト ルータの 1 つがクエリアとして設定されます。クエリアには、レイヤ 3 スイッチを指定できます。

show ip igmp snooping querier コマンド出力でも、検出されたクエリアの VLAN およびインターフェイスを表示します。クエリアがスイッチの場合、出力では *Port* フィールドに *Router* が表示されます。クエリアがルータの場合、出力では、*Port* フィールドにクエリアを学習したポート番号が表示されます。

show ip igmp snooping querier detail ユーザ EXEC コマンドは、**show ip igmp snooping querier** コマンドに類似しています。ただし、**show ip igmp snooping querier** コマンドでは、スイッチ クエリアにより直前に検出されたデバイス IP アドレスだけが表示されます。

show ip igmp snooping querier detail コマンドは、スイッチ クエリアによって最後に検出されたデバイスの IP アドレスのほか、次の追加情報を表示します。

- VLAN で選択されている IGMP クエリア
- VLAN で設定されたスイッチ クエリア（ある場合）に関連する設定および動作情報

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show ip igmp snooping querier** コマンドの出力を示します。

```
Switch> show ip igmp snooping querier
Vlan       IP Address      IGMP Version         Port
-----------------------------------------------------
1          172.20.50.11    v3                   Gi1/0/1
2          172.20.40.20    v2                   Router
```

次の例では、**show ip igmp snooping querier detail** コマンドの出力を示します。

```
Switch> show ip igmp snooping querier detail

Vlan       IP Address      IGMP Version    Port
-------------------------------------------------------------
1          1.1.1.1         v2              Fa8/0/1

Global IGMP switch querier status
-------------------------------------------------------
admin state                     : Enabled
admin version                   : 2
source IP address               : 0.0.0.0
query-interval (sec)            : 60
max-response-time (sec)         : 10
querier-timeout (sec)           : 120
tcn query count                 : 2
tcn query interval (sec)        : 10

Vlan 1:   IGMP switch querier status

-------------------------------------------------------
elected querier is 1.1.1.1          on port Fa8/0/1
-------------------------------------------------------
admin state                     : Enabled
admin version                   : 2
source IP address               : 10.1.1.65
query-interval (sec)            : 60
max-response-time (sec)         : 10
querier-timeout (sec)           : 120
tcn query count                 : 2
tcn query interval (sec)        : 10
operational state               : Non-Querier
operational version             : 2
tcn query pending count         : 0
```

関連コマンド

コマンド	説明
ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピングをイネーブルにします。
ip igmp snooping querier	レイヤ 2 ネットワークの IGMP クエリア機能をイネーブルにします。
show ip igmp snooping	スイッチまたは指定されたマルチキャスト VLAN の IGMP スヌーピング マルチキャスト ルータ ポートを表示します。

show ip source binding

スイッチ上の IP 送信元バインディングを表示するには、**show ip source binding** ユーザ EXEC コマンドを使用します。

show ip source binding [*ip-address*] [*mac-address*] [**dhcp-snooping** | **static**] [**interface** *interface-id*] [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

ip-address	（任意）特定の IP アドレスの IP 送信元バインディングを表示します。
mac-address	（任意）特定の MAC アドレスの IP 送信元バインディングを表示します。
dhcp-snooping	（任意）DHCP スヌーピングによって学習された IP 送信元バインディングを表示します。
static	（任意）スタティック IP 送信元バインディングを表示します。
interface *interface-id*	（任意）特定のインターフェイス上の IP 送信元バインディングを表示します。
vlan *vlan-id*	（任意）特定の VLAN 上の IP 送信元バインディングを表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

show ip source binding コマンドの出力は、DHCP スヌーピング バインディング データベース内のダイナミックおよびスタティックに設定されたバインディングを表示します。ダイナミックに設定されたバインディングだけを表示するには、**show ip dhcp snooping binding** 特権 EXEC コマンドを使用します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show ip source binding** コマンドの出力を示します。

```
Switch> show ip source binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
--------------      ---------------  ----------  -------------  ----  --------------------
00:00:00:0A:00:0B   11.0.0.1         infinite    static         10    GigabitEthernet1/0/1
00:00:00:0A:00:0A   11.0.0.2         10000       dhcp-snooping  10    GigabitEthernet1/0/1
```

関連コマンド

コマンド	説明
ip dhcp snooping binding	DHCP スヌーピング バインディング データベースを設定します。
ip source binding	スイッチにスタティック IP 送信元バインディングを設定します。

show ip verify source

スイッチ上または特定のインターフェイス上の IP 送信元ガードの設定を表示するには、**show ip verify source** ユーザ EXEC コマンドを使用します。

show ip verify source [**interface** *interface-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface *interface-id*	（任意）特定のインターフェイス上の IP 送信元ガードの設定を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show ip verify source** コマンドの出力を示します。

```
Switch> show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
gi1//1      ip           active       10.0.0.1                          10
gi1//1      ip           active       deny-all                          11-20
gi1//2      ip           inactive-trust-port
gi1//3      ip           inactive-no-snooping-vlan
gi1//4      ip-mac       active       10.0.0.2         aaaa.bbbb.cccc  10
gi1//4      ip-mac       active       11.0.0.1         aaaa.bbbb.cccd  11
gi1//4      ip-mac       active       deny-all         deny-all        12-20
gi1//5      ip-mac       active       10.0.0.3         permit-all      10
gi1//5      ip-mac       active       deny-all         permit-all      11-20
```

上記の例では、IP 送信元ガードの設定は次のようになります。

- Gigabit Ethernet 1 インターフェイスでは、DHCP スヌーピングは VLAN 10 ～ 20 上でイネーブルです。VLAN 10 では、IP アドレス フィルタリングによる IP ソース ガードがインターフェイスで設定され、バインディングがインターフェイスに存在します。VLAN 11 ～ 20 では、2 番目のエントリが、IP ソース ガードが設定されていない VLAN のインターフェイスで、デフォルト ポートのアクセス コントロール リスト（ACL）が適用されていることを示します。
- Gigabit Ethernet 2 インターフェイスは、信頼性のある DHCP スヌーピングとして設定されています。
- Gigabit Ethernet 3 インターフェイスでは、DHCP スヌーピングは、インターフェイスが所属する VLAN 上でイネーブルではありません。

- Gigabit Ethernet 4 インターフェイスでは、送信元 IP および MAC アドレスのフィルタリングによる IP ソース ガードがイネーブルで、スタティックな IP 送信元バインディングが VLAN 10 と 11 で設定されます。VLAN 12 ～ 20 では、IP ソース ガードが設定されていない VLAN のインターフェイスで、デフォルト ポートの ACL が適用されています。
- Gigabit Ethernet 5 インターフェイスでは、送信元 IP および MAC アドレスのフィルタリングによる IP ソース ガードがイネーブルで、スタティックな IP バインディングで設定されていますが、ポート セキュリティはディセーブルです。スイッチは、送信元 MAC アドレスをフィルタリングできません。

次の例では、IP 送信元ガードがディセーブルにされたインターフェイスの出力を示します。

```
Switch> show ip verify source gigabitethernet1/0/6
IP source guard is not configured on the interface gi1/6.
```

関連コマンド

コマンド	説明
ip verify source	インターフェイス上の IP 送信元ガードをイネーブルにします。

show ipc

スイッチ スタックまたはスタンドアロン スイッチ上の Interprocess Communications（IPC; プロセス間通信）プロトコルの設定、ステータス、および統計情報を表示するには、**show ipc** ユーザ EXEC コマンドを使用します。

show ipc {**mcast** {**appclass** | **groups** | **status**} | **nodes** | **ports** [**open**] | **queue** | **rpc** | **session** {**all** | **rx** | **tx**} [**verbose**] | **status** [**cumlulative**] | **zones**} [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

mcast {**appclass** | **groups** | **status**}	IPC マルチキャスト ルーティング情報を表示します。キーワードの意味は次のとおりです。 • **appclass**：IPC マルチキャスト アプリケーション クラスを表示します。 • **groups**：IPC マルチキャスト グループを表示します。 • **status**：IPC マルチキャスト ルーティング ステータスを表示します。
nodes	参加ノードを表示します。
ports [**open**]	ローカル IPC ポートを表示します。キーワードの意味は次のとおりです。 • **open**：（任意）オープン ポートだけを表示します。
queue	IPC 送信キューの内容を表示します。
rpc	IPC リモート プロシージャの統計情報を表示します。
session {**all** | **rx** | **tx**}	IPC セッションの統計情報を表示します（特権 EXEC モードの場合だけ使用可能）。キーワードの意味は次のとおりです。 • **all**：セッションの統計情報をすべて表示します。 • **rx**：スイッチが受信したトラフィックのセッション統計情報を表示します。 • **tx**：スイッチが転送したトラフィックのセッション統計情報を表示します。
verbose	（任意）詳細な統計情報を表示します（特権 EXEC モードの場合だけ使用可能）。
status [**cumlulative**]	ローカル IPC サーバのステータスを表示します。キーワードの意味は次のとおりです。 • **cumlulative**：（任意）スイッチが起動または再起動した後のローカル IPC サーバのステータスを表示します。
zones	参加している IPC ゾーンを表示します。スイッチは 1 つの IPC ゾーンをサポートします。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(18)SE	**mcast** {**appclass** | **groups** | **status**}、**rpc**、**session** {**all** | **rx** | **tx**} [**verbose**]、および **cumulative** キーワードが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、IPC ルーティング ステータスを表示する方法を示します。

```
Switch> show ipc mcast status
                          IPC Mcast Status
                                                          Tx         Rx

 Total Frames                                             0          0
 Total control Frames                                     0          0
 Total Frames dropped                                     0          0
 Total control Frames dropped                             0          0

 Total Reliable messages                                  0          0
 Total Reliable messages acknowledged                     0          0
 Total Out of Band Messages                               0          0
 Total Out of Band messages acknowledged                  0          0

 Total No Mcast groups                                    0          0

 Total Retries                    0  Total Timeouts                     0
 Total OOB Retries                0  Total OOB Timeouts                 0
 Total flushes                    0  Total No ports                     0
```

次の例では、参加ノードを表示する方法を示します。

```
Switch> show ipc nodes
There is 1 node in this IPC realm.
   ID    Type       Name           Last  Last
                                   Sent  Heard
   10000 Local      IPC Master     0      0
```

次の例では、ローカル IPC ポートを表示する方法を示します。

```
Switch> show ipc ports
There are 8 ports defined.

Port ID        Type       Name                    (current/peak/total)
There are 8 ports defined.
   10000.1     unicast    IPC Master:Zone
   10000.2     unicast    IPC Master:Echo
   10000.3     unicast    IPC Master:Control
   10000.4     unicast    IPC Master:Init
   10000.5     unicast    FIB Master:DFS.process_level.msgs
   10000.6     unicast    FIB Master:DFS.interrupt.msgs
   10000.7     unicast    MDFS RP:Statistics
     port_index = 0  seat_id = 0x10000    last sent = 0     last heard = 0
  0/2/159

   10000.8     unicast    Slot 1 :MDFS.control.RIL
     port_index = 0  seat_id = 0x10000    last sent = 0     last heard = 0
  0/0/0
```

```
RPC packets:current/peak/total
                                                                0/1/4
```

次の例では、IPC 再送信キューの内容を表示する方法を示します。

```
Switch> 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 0 IPC messages currently on the IPC inboundQ.
Messages currently in use                    :         3
Message cache size                           :      1000
Maximum message cache usage                  :      1000

0  times message cache crossed       5000 [max]

Emergency messages currently in use          :         0

There are 2 messages currently reserved for reply msg.

Inbound message queue depth 0
Zone inbound message queue depth 0
```

次の例では、すべての IPC セッションの統計情報を表示する方法を示します。

```
Switch# show ipc session all
Tx Sessions:
Port ID        Type       Name
   10000.7     Unicast    MDFS RP:Statistics
     port_index = 0  type = Unreliable      last sent = 0     last heard = 0
     Msgs requested = 180  Msgs returned = 180

   10000.8     Unicast    Slot 1 :MDFS.control.RIL
     port_index = 0  type = Reliable        last sent = 0     last heard = 0
     Msgs requested = 0    Msgs returned = 0

Rx Sessions:
Port ID        Type       Name
   10000.7     Unicast    MDFS RP:Statistics
     port_index = 0  seat_id = 0x10000    last sent = 0     last heard = 0
     No of msgs requested = 180   Msgs returned = 180

   10000.8     Unicast    Slot 1 :MDFS.control.RIL
     port_index = 0  seat_id = 0x10000    last sent = 0     last heard = 0
     No of msgs requested = 0     Msgs returned = 0
```

次の例では、ローカル IPC サーバのステータスを表示する方法を示します。

```
Switch> show ipc status cumulative
                         IPC System Status

 Time last IPC stat cleared :never

 This processor is the IPC master server.
Do not drop output of IPC frames for test purposes.

1000 IPC Message Headers Cached.

                                                     Rx Side     Tx Side

 Total Frames                                          12916         608
     0          0
 Total from Local Ports                                13080         574
 Total Protocol Control Frames                           116          17
```

```
 Total Frames Dropped                                        0           0

                              Service Usage

 Total via Unreliable Connection-Less Service            12783         171
 Total via Unreliable Sequenced Connection-Less Svc          0           0
 Total via Reliable Connection-Oriented Service             17         116
<output truncated>
```

関連コマンド

コマンド	説明
clear ipc	IPC マルチキャスト ルーティングの統計情報をクリアします。

show ipv6 access-list

現在の IPv6 アクセス リストのすべての内容を表示するには、**show ipv6 access-list** ユーザ EXEC コマンドを使用します。

show ipv6 access-list [*access-list-name*]

（注）このコマンドは、スイッチでデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートが設定されている場合に限り使用可能です。

構文の説明

access-list-name	（任意）アクセス リストの名前

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

IPv6 専用である点を除いて、**show ipv6 access-list** コマンドの出力は **show ip access-list** コマンドと類似しています。

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

例

次の例では、**show ipv6 access-list** コマンドで出力された inbound および outbound という名の IPv6 アクセス リストを示します。

```
Router# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp (8 matches) sequence 10
    permit tcp any any eq telnet (15 matches) sequence 20
    permit udp any any sequence 30
```

表 2-34 に、この出力で表示される重要なフィールドの説明を示します。

表 2-34　show ipv6 access-list のフィールドの説明

フィールド	説明
IPv6 access list inbound	IPv6 アクセス リスト名（例：inbound）。
permit	指定されたプロトコル タイプと一致するパケットを許可します。
tcp	Transmission Control Protocol（TCP）。パケットが一致しなければならない高いレベル（レイヤ 4）のプロトコル タイプ。
any	::/0 と同じです。
eq	TCP または UDP パケットの送信元または宛先ポートを比較する equal オペランド。

表 2-34　show ipv6 access-list のフィールドの説明 （続き）

フィールド	説明
bgp (matches)	Border Gateway Protocol（BGP）。パケットのプロトコル タイプおよび一致数。
sequence 10	着信パケットが比較されるアクセス リストの行のシーケンス。アクセス リストの行は、最初のプライオリティ（最低の数、たとえば 10）から最後のプライオリティ（最高の数、たとえば 80）の順に並んでいます。

関連コマンド

コマンド	説明
clear ipv6 access-list	IPv6 アクセス リスト一致カウンタをリセットします。
ipv6 access-list	IPv6 アクセス リストを定義し、スイッチを IPv6 アクセス リスト コンフィギュレーション モードにします。
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。

show ipv6 dhcp conflict

アドレスをクライアントに示すときに、Dynamic Host Configuration Protocol for IPv6（DHCPv6）サーバで見つかったアドレス競合を表示するには、**show ipv6 dhcp conflict** 特権 EXEC コマンドを使用します。

show ipv6 dhcp conflict

（注）　このコマンドは、スイッチでデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートが設定されている場合に限り使用可能です。

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(46)SE	このコマンドが追加されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

競合を検出するように DHCPv6 サーバを設定する場合、DHCPv6 サーバは ping を使用します。クライアントは近隣探索を使用してクライアントを検出し、DECLINE メッセージを介してサーバに報告します。アドレス競合が検出されると、このアドレスはプールから削除されます。管理者がこのアドレスを競合リストから削除するまでこのアドレスは割り当てることができません。

例

次の例では、**show ipv6 dhcp conflict** コマンドの出力を示します。

```
Switch# show ipv6 dhcp conflict
Pool 350, prefix 2001:1005::/48
        2001:1005::10
```

関連コマンド

コマンド	説明
ipv6 dhcp pool	DHCPv6 プールを設定して、DHCPv6 プール コンフィギュレーション モードを開始します。
clear ipv6 dhcp conflict	DHCPv6 サーバ データベースからアドレス競合をクリアします。

show ipv6 mld snooping

スイッチまたは VLAN の IP Version 6（IPv6）Multicast Listener Discovery（MLD）スヌーピング設定を表示するには、**show ipv6 mld snooping** ユーザ EXEC コマンドを使用します。

show ipv6 mld snooping [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

（注）　このコマンドは、スイッチでデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートが設定されている場合だけ使用可能です。

構文の説明

vlan *vlan-id*	（任意）VLAN を指定します。指定できる範囲は 1 ～ 1001 および 1006 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

スイッチまたは特定の VLAN の MLD スヌーピングの設定を表示するのにこのコマンドを使用します。

1002 ～ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show ipv6 mld snooping vlan** コマンドの出力を示します。ここでは、特定の VLAN のスヌーピング特性を表示します。

```
Switch> show ipv6 mld snooping vlan 100
Global MLD Snooping configuration:
-------------------------------------------
MLD snooping                   : Enabled
MLDv2 snooping (minimal)       : Enabled
Listener message suppression   : Enabled
TCN solicit query              : Disabled
TCN flood query count          : 2
Robustness variable            : 3
Last listener query count      : 2
```

```
Last listener query interval  : 1000
Vlan 100:
--------
MLD snooping                        : Disabled
MLDv1 immediate leave               : Disabled
Explicit host tracking              : Enabled
Multicast router learning mode      : pim-dvmrp
Robustness variable                 : 3
Last listener query count           : 2
Last listener query interval        : 1000
```

次の例では、**show ipv6 mld snooping** コマンドの出力を示します。ここでは、スイッチ上の VLAN すべてのスヌーピング特性を表示します。

```
Switch> show ipv6 mld snooping
Global MLD Snooping configuration:
------------------------------------------
MLD snooping                  : Enabled
MLDv2 snooping (minimal)      : Enabled
Listener message suppression  : Enabled
TCN solicit query             : Disabled
TCN flood query count         : 2
Robustness variable           : 3
Last listener query count     : 2
Last listener query interval  : 1000

Vlan 1:
--------
MLD snooping                        : Disabled
MLDv1 immediate leave               : Disabled
Explicit host tracking              : Enabled
Multicast router learning mode      : pim-dvmrp
Robustness variable                 : 1
Last listener query count           : 2
Last listener query interval        : 1000

<output truncated>

Vlan 951:
--------
MLD snooping                        : Disabled
MLDv1 immediate leave               : Disabled
Explicit host tracking              : Enabled
Multicast router learning mode      : pim-dvmrp
Robustness variable                 : 3
Last listener query count           : 2
Last listener query interval        : 1000
```

関連コマンド

コマンド	説明
ipv6 mld snooping	スイッチ上または VLAN 上の MLD スヌーピングをイネーブルにし、設定を行います。
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。

show ipv6 mld snooping address

Multicast Listener Discovery（MLD）スヌーピングが保持するすべての、または指定された IP version 6（IPv6）マルチキャスト アドレス情報を表示するには、**show ipv6 mld snooping address** ユーザ EXEC コマンドを使用します。

show ipv6 mld snooping address [[**vlan** *vlan-id*] [*ipv6 address*]] [**vlan** *vlan-id*] [**count** | **dynamic** | **user**] [| {**begin** | **exclude** | **include**} *expression*]

（注）　このコマンドは、スイッチでデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートが設定されている場合だけ使用可能です。

構文の説明

vlan *vlan-id*	（任意）MLD スヌーピング マルチキャスト アドレス情報を表示する VLAN を指定します。指定できる VLAN ID 範囲は 1 ～ 1001 および 1006 ～ 4094 です。
ipv6-multicast-address	（任意）指定された IPv6 マルチキャスト アドレスに関する情報を表示します。このキーワードは、VLAN ID を入力した場合だけ使用できます。
count	（任意）スイッチ上または指定された VLAN のマルチキャスト グループ数を表示します。
dynamic	（任意）MLD スヌーピング学習グループ情報を表示します。
user	（任意）MLD スヌーピング ユーザ設定グループ情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

IPv6 マルチキャスト アドレス情報を表示するのに、このコマンドを使用します。

VLAN ID を入力した後に限り、IPv6 マルチキャスト アドレスを入力できます。

1002 ～ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

学習されたグループに関する情報だけを表示するには、**dynamic** キーワードを使用します。設定されたグループに関する情報だけを表示するには、**user** キーワードを使用します。

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show snooping address** ユーザ EXEC コマンドの出力を示します。

```
Switch> show ipv6 mld snooping address
Vlan Group   Type Version Port List
------------------------------------------------------------
2    FF12::3 user         Fa1/0/2, Gi2/0/2, Gi3/0/1,Gi3/0/3
```

次の例では、**show snooping address count** ユーザ EXEC コマンドの出力を示します。

```
Switch> show ipv6 mld snooping address count
Total number of multicast groups: 2
```

次の例では、**show snooping address user** ユーザ EXEC コマンドの出力を示します。

```
Switch> show ipv6 mld snooping address user
Vlan Group  Type Version Port List
------------------------------------------------------------
2    FF12::3 user  v2    Fa1/0/2, Gi2/0/2, Gi3/0/1,Gi4/0/3
```

関連コマンド

コマンド	説明
ipv6 mld snooping vlan	VLAN で IPv6 MLD スヌーピングを設定します。
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。

show ipv6 mld snooping mrouter

スイッチまたは VLAN の、動的に学習され、手動で設定した IP Version 6（IPv6）Multicast Listener Discovery（MLD）ルータ ポートを表示するには、**show ipv6 mld snooping mrouter** ユーザ EXEC コマンドを使用します。

show ipv6 mld snooping mrouter [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

（注）　このコマンドは、スイッチでデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートが設定されている場合だけ使用可能です。

構文の説明

vlan *vlan-id*	（任意）VLAN を指定します。指定できる範囲は 1 ～ 1001 および 1006 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

スイッチまたは特定の VLAN の MLD スヌーピング ルータ ポートを表示するには、このコマンドを使用します。

1002 ～ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show ipv6 mld snooping mrouter** コマンドの出力を示します。MLD スヌーピングに参加する、スイッチのすべての VLAN のスヌーピング特性が表示されます。

```
Switch> show ipv6 mld snooping mrouter
Vlan    ports
----    -----
   2    Gi1/0/11(dynamic)
  72    Gi1/0/11(dynamic)
 200    Gi1/0/11(dynamic)
```

次の例では、**show ipv6 mld snooping mrouter vlan** コマンドの出力を示します。特定の VLAN のマルチキャスト ルータ ポートが表示されます。

```
Switch> show ipv6 mld snooping mrouter vlan 100
Vlan    ports
----    -----
   2    Gi1/0/11(dynamic)
```

関連コマンド

コマンド	説明
ipv6 mld snooping	スイッチ上または VLAN 上の MLD スヌーピングをイネーブルにし、設定を行います。
ipv6 mld snooping vlan mrouter interface *interface-id* | **static** *ipv6-multicast-address* **interface** *interface-id*]	VLAN にマルチキャスト ルータ ポートを設定します。
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。

show ipv6 mld snooping querier

スイッチまたは VLAN が受信した最新の IP Version 6（IPv6）Multicast Listener Discovery（MLD）スヌーピング クエリア関連情報を表示するには、**show ipv6 mld snooping querier** ユーザ EXEC コマンドを使用します。

show ipv6 mld snooping querier [**vlan** *vlan-id*] [**detail**] [| {**begin** | **exclude** | **include**} *expression*]

（注）　このコマンドは、スイッチでデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートが設定されている場合だけ使用可能です。

構文の説明

vlan *vlan-id*	（任意）VLAN を指定します。指定できる範囲は 1 ～ 1001 および 1006 ～ 4094 です。
detail	（任意）スイッチまたは VLAN の MLD スヌーピングの詳細なクエリア情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

MLD クエリー メッセージを送信する検出された装置（**クエリア**とも呼ばれる）の MLD バージョンおよび IPv6 アドレスを表示するには、*show ipv6 mld snooping querier* コマンドを使用します。サブネットは複数のマルチキャスト ルータを持つことができますが、MLD クエリアは 1 つだけです。クエリアには、レイヤ 3 スイッチを指定できます。

show ipv6 mld snooping querier コマンド出力は、クエリアが検出された VLAN およびインターフェイスも表示します。クエリアがスイッチの場合、出力では *Port* フィールドに *Router* が表示されます。クエリアがルータの場合、出力では、*Port* フィールドにクエリアを学習したポート番号が表示されます。

show ipv6 mld snoop querier vlan コマンドの出力では、外部または内部クエリアからのクエリー メッセージに応答して受信された情報を表示します。特定の VLAN 上のスヌーピング ロバストネス変数などのユーザ設定の VLAN 値は表示されません。このクエリア情報は、スイッチが送信する MASQ メッセージ上だけで使用されます。クエリー メッセージに応答しないメンバを期限切れにするのに使用するユーザ設定のロバストネス変数は無効にはなりません。

1002 ～ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show ipv6 mld snooping querier** コマンドの出力を示します。

```
Switch> show ipv6 mld snooping querier
Vlan      IP Address               MLD Version Port
-----------------------------------------------------------
2         FE80::201:C9FF:FE40:6000 v1          Gi3/0/1
```

次の例では、**show ipv6 mld snooping querier detail** コマンドの出力を示します。

```
Switch> show ipv6 mld snooping querier detail
Vlan      IP Address               MLD Version Port
-----------------------------------------------------------
2         FE80::201:C9FF:FE40:6000 v1          Gi3/0/1
```

次の例では、**show ipv6 mld snooping querier vlan** コマンドの出力を示します。

```
Switch> show ipv6 mld snooping querier vlan 2
IP address : FE80::201:C9FF:FE40:6000
MLD version : v1
Port : Gi3/0/1
Max response time : 1000s
```

関連コマンド

コマンド	説明
ipv6 mld snooping	スイッチ上または VLAN 上の IPv6 MLD スヌーピングをイネーブルにし、設定を行います。
ipv6 mld snooping last-listener-query-count	MLD クライアントが期限切れになる前にスイッチが送信するクエリーの最大数を設定します。
ipv6 mld snooping last-listener-query-interval	スイッチがクエリーを送信してから、マルチキャスト グループからポートを削除する前に待機する最大応答時間を設定します。
ipv6 mld snooping robustness-variable	応答がない場合、マルチキャスト アドレスが期限切れになる前にスイッチが送信するクエリーの最大数を設定します。
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。
ipv6 mld snooping	スイッチ上または VLAN 上の IPv6 MLD スヌーピングをイネーブルにし、設定を行います。

show ipv6 route updated

IPv6 ルーティング テーブルの現在の内容を表示するには、ユーザ EXEC コマンドの **show ipv6 route updated** コマンドを使用します。

show ipv6 route [*protocol*] **updated** [**boot-up**]{*hh:mm* | *day*{*month* [*hh:mm*]} [{*hh:mm* | *day*{*month* [*hh:mm*]}] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

protocol	（任意）次のいずれかのキーワードを使用して指定したルーティング プロトコルのルートを表示します。 • **bgp** • **isis** • **ospf** • **rip** または、次のいずれかのキーワードを使用して指定したルート タイプのルートを表示します。 • **connected** • **local** • **static** • **interface** *interface id*
boot-up	IPv6 ルーティング テーブルの現在の内容を表示します。
hh:mm	24 時間表記の 2 桁の数値で時刻を入力します。必ずコロン（:）を使用してください。たとえば、**13:32** のように入力します。
day	日にちを入力します。指定できる範囲は 1 ～ 31 です。
month	月を大文字または小文字で入力します。**January** または **august** など、月の名前をすべて入力することも、**jan** または **Aug** のように月の名前の最初の 3 文字を入力することもできます。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(37)SE	このコマンドが追加されました。

使用上のガイドライン

IPv6 ルーティング テーブルの現在の内容を表示するには、**show ipv6 route** 特権 EXEC コマンドを使用します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show ipv6 route updated rip** コマンドの出力を示します。

```
Switch> show ipv6 route rip updated
IPv6 Routing Table - 12 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
IA - ISIS interarea, IS - ISIS summary
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
R 2001::/64 [120/2]
via FE80::A8BB:CCFF:FE00:8D01, GigabitEthernet1/0/1
Last updated 10:31:10 27 February 2007
R 2004::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet1/0/2
Last updated 17:23:05 22 February 2007
R 4000::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet1/0/3
Last updated 17:23:05 22 February 2007
R 5000::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet1/0/4
Last updated 17:23:05 22 February 2007
R 5001::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet1/0/5
Last updated 17:23:05 22 February 2007
```

関連コマンド

コマンド	説明
show ipv6 route	IPv6 ルーティング テーブルの現在の内容を表示します。

show l2protocol-tunnel

レイヤ 2 プロトコル トンネル ポートに関する情報を表示するには、**show l2protocol-tunnel** ユーザ EXEC コマンドを使用します。プロトコル トンネリングがイネーブルにされたインターフェイスの情報が表示されます。

show l2protocol-tunnel [**interface** *interface-id*] [**summary**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface *interface-id*	（任意）プロトコル トンネリング情報を表示するインターフェイスを指定します。有効なインターフェイスは、物理ポートとポート チャネルです。ポート チャネルの使用範囲は 1 ～ 48 です。
summary	（任意）レイヤ 2 プロトコル サマリー情報だけを表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)SE	このコマンドが追加されました。

使用上のガイドライン

l2protocol-tunnel インターフェイス コンフィギュレーション コマンドを使用してアクセスまたは IEEE 802.1Q トンネル ポートのレイヤ 2 プロトコル トンネリングをイネーブルにした後、次のパラメータの一部またはすべてを設定できます。

- トンネリングするプロトコル タイプ
- シャットダウンしきい値
- ドロップしきい値

show l2protocol-tunnel [**interface** *interface-id*] コマンドを入力すると、すべてのパラメータが設定されたアクティブ ポートに関する情報だけが表示されます。

show l2protocol-tunnel summary コマンドを入力すると、一部またはすべてのパラメータが設定されたアクティブ ポートに関する情報だけが表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show l2protocol-tunnel** コマンドの出力を示します。

```
Switch> show l2protocol-tunnel
COS for Encapsulated Packets: 5
Drop Threshold for Encapsulated Packets: 0

Port       Protocol Shutdown  Drop      Encapsulation Decapsulation Drop
                    Threshold Threshold Counter       Counter       Counter
---------- -------- --------- --------- ------------- ------------- -------------
Fa3/0/3    ---           ----      ----          ----          ----          ----
           ---           ----      ----          ----          ----          ----
           ---           ----      ----          ----          ----          ----
           pagp          ----      ----             0        242500
           lacp          ----      ----         24268        242640
           udld          ----      ----             0        897960
Fa3/0/4    ---           ----      ----          ----          ----          ----
           ---           ----      ----          ----          ----          ----
           ---           ----      ----          ----          ----          ----
           pagp          1000      ----         24249        242700
           lacp          ----      ----         24256        242660
           udld          ----      ----             0        897960
Gi6/0/3    cdp           ----      ----        134482       1344820
           ---           ----      ----          ----          ----          ----
           ---           ----      ----          ----          ----          ----
           pagp          1000      ----             0        242500
           lacp           500      ----             0        485320
           udld           300      ----         44899        448980
Gi6/0/4    cdp           ----      ----        134482       1344820
           ---           ----      ----          ----          ----          ----
           ---           ----      ----          ----          ----          ----
           pagp          ----      1000             0        242700
           lacp          ----      ----             0        485220
           udld           300      ----         44899        448980
```

次の例では、**show l2protocol-tunnel summary** コマンドの出力を示します。

```
Switch> show l2protocol-tunnel summary
COS for Encapsulated Packets: 5
Drop Threshold for Encapsulated Packets: 0

Port    Protocol    Shutdown         Drop             Status
                    Threshold        Threshold
                    (cdp/stp/vtp)    (cdp/stp/vtp)
                    (pagp/lacp/udld) (pagp/lacp/udld)
------- ----------- ---------------- ---------------- ----------
Fa3/0/2  --- --- --- ----/----/----   ----/----/----   up
     pagp lacp udld ----/----/----   ----/----/----
Fa9/0/3  --- --- --- ----/----/----   ----/----/----   up
     pagp lacp udld 1000/----/----   ----/----/----
Fa9/0/4  --- --- --- ----/----/----   ----/----/----   up
     pagp lacp udld 1000/ 500/----   ----/----/----
Fa9/0/5  cdp stp vtp ----/----/----   ----/----/----   down
     ---- ---- ---- ----/----/----   ----/----/----
Gi4/0/1  --- --- --- ----/----/----   ----/----/----   down
     pagp ---- ---- ----/----/----   1000/----/----
Gi4/0/2  --- --- --- ----/----/----   ----/----/----   down
     pagp ---- ---- ----/----/----   1000/----/----
```

関連コマンド

コマンド	説明
clear l2protocol-tunnel counters	プロトコル トンネリング ポートのカウンタをクリアします。
l2protocol-tunnel	インターフェイス上の CDP、STP、または VTP パケットのレイヤ 2 プロトコル トンネリングをイネーブルにします。
l2protocol-tunnel cos	トンネリング レイヤ 2 プロトコル パケットに対してサービス クラス（CoS）値を設定します。

show lacp

Link Aggregation Control Protocol（LACP）チャネル グループ情報を表示するには、**show lacp** ユーザ EXEC コマンドを使用します。

show lacp [*channel-group-number*] {**counters** | **internal** | **neighbor** | **sys-id**} [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

channel-group-number	（任意）チャネル グループの番号です。指定できる範囲は 1 ～ 48 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	ネイバー情報を表示します。
sys-id	LACP で使用されるシステム ID を表示します。システム ID は、LACP システム プライオリティおよびスイッチ MAC アドレスで構成されています。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。
12.2(25)SE	*channel-group-number* 範囲が 1 ～ 12 から 1 ～ 48 に変更されました。

使用上のガイドライン

show lacp コマンドを入力すると、アクティブなチャネル グループの情報が表示されます。特定のチャネル情報を表示するには、チャネル グループ番号を指定して **show lacp** コマンドを入力します。

チャネル グループ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。

channel-group-number オプションを入力することで、**sys-id** 以外のすべてのキーワードでチャネル グループを指定できます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show lacp counters** ユーザ EXEC コマンドの出力を示します。表 2-35 に、この出力で表示されるフィールドの説明を示します。

```
Switch> show lacp counters
              LACPDUs         Marker      Marker Response    LACPDUs
Port         Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
---------------------------------------------------------------------
Channel group:1
Gi2/0/1      19     10       0      0        0      0         0
Gi2/0/2      14     6        0      0        0      0         0
```

表 2-35　show lacp counters のフィールドの説明

フィールド	説明
LACPDUs Sent および Recv	ポートによって送受信された LACP パケット数
Marker Sent および Recv	ポートによって送受信された LACP Marker パケット数
Marker Response Sent および Recv	ポートによって送受信された LACP Marker 応答パケット数
LACPDUs Pkts および Err	ポートの LACP によって受信された、未知で不正なパケット数

次の例では、**show lacp internal** コマンドの出力を示します。

```
Switch> show lacp 1 internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                             LACP port     Admin     Oper    Port     Port
Port        Flags   State    Priority      Key       Key     Number   State
Gi2/0/1     SA      bndl     32768         0x3       0x3     0x4      0x3D
Gi2/0/2     SA      bndl     32768         0x3       0x3     0x5      0x3D
```

表 2-36 に、この出力で表示されるフィールドの説明を示します。

表 2-36　show lacp internal のフィールドの説明

フィールド	説明
State	特定のポートの状態。次に使用可能な値を示します。 • – : ポートは unknown ステートです。 • **bndl** : ポートがアグリゲータに接続され、他のポートとバンドルされています。 • **susp** : ポートが中断されている状態で、アグリゲータには接続されていません。 • **hot-sby** : ポートがホットスタンバイの状態です。 • **indiv** : ポートをその他ポートとともにバンドルできません。 • **indep** : ポートは independent ステートです。バンドルされていませんが、データ トラフィックを切り替えることができます。この場合、LACP は相手側ポートで実行されていません。 • **down** : ポートがダウンしています。
LACP Port Priority	ポートのプライオリティ設定。互換性のあるすべてのポートが集約することを回避するため、ハードウェアの制限がある場合、LACP はポート プライオリティによりポートをスタンバイモードにします。
Admin Key	ポートに割り当てられた管理用のキー。LACP は自動的に管理用のキー値を生成します（16 進数）。管理用のキーは、ポートが他のポートと集約できる能力を定義します。その他のポートと統合するポートの機能は、ポートの物理特性（たとえば、データ レートやデュプレックス機能）と、設定した設定制限によって判断されます。

表 2-36　show lacp internal のフィールドの説明 （続き）

フィールド	説明
Oper Key	ポートで使用される実行時の操作キー。LACP は自動的に値を生成します（16 進数）。
Port Number	ポート番号。
Port State	ポートの状態変数。1 つのオクテット内で個々のビットとしてエンコードされ、次のような意味になります。 • bit0：LACP のアクティビティ • bit1：LACP のタイムアウト • bit2：集約 • bit3：同期 • bit4：収集 • bit5：配信 • bit6：デフォルト • bit7：期限切れ （注）　上のリストでは、bit7 が MSB で bit0 は LSB です。

次の例では、**show lacp neighbor** コマンドの出力を示します。

```
Switch> show lacp neighbor
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

Channel group 3 neighbors

Partner's information:

          Partner                Partner                      Partner
Port      System ID              Port Number     Age          Flags
Gi2/0/1   32768,0007.eb49.5e80   0xC              19s         SP

          LACP Partner          Partner          Partner
          Port Priority         Oper Key         Port State
          32768                 0x3              0x3C

Partner's information:

          Partner                Partner                      Partner
Port      System ID              Port Number     Age          Flags
Gi2/0/2   32768,0007.eb49.5e80   0xD              15s         SP

          LACP Partner          Partner          Partner
          Port Priority         Oper Key         Port State
          32768                 0x3              0x3C
```

次の例では、**show lacp sys-id** コマンドの出力を示します。

```
Switch> show lacp sys-id
32765,0002.4b29.3a00
```

システム ID は、システム プライオリティおよびシステム MAC アドレスで構成されています。最初の 2 バイトはシステム プライオリティ、最後の 6 バイトはグローバルに管理されているシステム関連の個々の MAC アドレスです。

関連コマンド

コマンド	説明
clear lacp	LACP チャネル グループ情報を消去します。
lacp port-priority	LACP ポート プライオリティを設定します。
lacp system-priority	LACP システム プライオリティを設定します。

show lldp

show lldp コマンドについては、
http://www.cisco.com/en/US/docs/ios/cether/command/reference/ce_04.html#wp1095571 を参照してください。

show location

エンドポイントのロケーション情報を表示するには、**show location** ユーザ EXEC コマンドを使用します。

show location admin-tag | [| {**begin** | **exclude** | **include**} *expression*]

show location civic-location {**identifier** *id number* | **interface** *interface-id* | **static**} | {**begin** | **exclude** | **include**} *expression*]

show location elin-location {**identifier** *id number* | **interface** *interface-id* | **static**} | {**begin** | **exclude** | **include**} *expression*]

構文の説明

admin-tag	管理タグまたはサイト情報を表示します。
civic-location	都市ロケーション情報を表示します。
elin-location	緊急ロケーション情報（ELIN）を表示します。
identifier id	都市ロケーションまたは elin ロケーションの ID を指定します。指定できる ID 範囲は 1 ～ 4095 です。
interface *interface-id*	（任意）指定されたインターフェイスまたはすべてのインターフェイスに対するロケーション情報を表示します。有効なインターフェイスには、物理ポートが含まれます。
static	スタティック コンフィギュレーション情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

エンドポイントのロケーション情報を表示するには、**show location** コマンドを使用します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、インターフェイスのロケーション情報を表示する **show location civic-location** コマンドの出力を示します。

```
Switch> show location civic interface gigibitethernet2/0/1
Civic location information
--------------------------
Identifier              : 1
County                  : Santa Clara
```

```
Street number           : 3550
Building                : 19
Room                    : C6
Primary road name       : Cisco Way
City                    : San Jose
State                   : CA
Country                 : US
```

次の例では、すべての都市ロケーション情報を表示する **show location civic-location** コマンドの出力を示します。

```
Switch> show location civic-location static
Civic location information
--------------------------
Identifier              : 1
County                  : Santa Clara
Street number           : 3550
Building                : 19
Room                    : C6
Primary road name       : Cisco Way
City                    : San Jose
State                   : CA
Country                 : US
Ports                   : Gi2/0/1
--------------------------
Identifier              : 2
Street number           : 24568
Street number suffix    : West
Landmark                : Golden Gate Bridge
Primary road name       : 19th Ave
City                    : San Francisco
Country                 : US
--------------------------
```

次の例では、緊急ロケーション情報を表示する **show location elin-location** コマンドの出力を示します。

```
Switch> show location elin-location identifier 1
Elin location information
--------------------------
Identifier : 1
Elin       : 14085553881
Ports      : Gi2/0/2
```

次の例では、すべての緊急ロケーション情報を表示する **show location elin static** コマンドの出力を示します。

```
Switch> show location elin static
Elin location information
--------------------------
Identifier : 1
Elin       : 14085553881
Ports      : Gi2/0/2
--------------------------
Identifier : 2
Elin       : 18002228999
--------------------------
```

関連コマンド

コマンド	説明
location（グローバル コンフィギュレーション）	エンドポイントにグローバル ロケーション情報を設定します。
location（インターフェイス コンフィギュレーション）	インターフェイスにロケーション情報を設定します。

show link state group

リンクステート グループ情報を表示するには、**show link state group** 特権 EXEC コマンドを使用します。

show link state group [*number*] [**detail**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

number	（任意）リンクステート グループの番号です。
detail	（任意）詳細情報を表示するよう指定します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

デフォルト

デフォルト設定はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

リンクステート グループ情報を表示するには、**show link state group** コマンドを使用します。キーワードを指定せずにこのコマンドを入力すると、すべてのリンクステート グループの情報が表示されます。特定のグループの情報を表示するには、グループ番号を入力します。

グループの詳細情報を表示するには、**detail** キーワードを入力します。**show link state group detail** コマンドの出力では、リンクステート トラッキングがイネーブルになっているか、またはアップストリームまたはダウンストリーム（あるいはその両方）インターフェイスが設定されたリンクステート グループだけが表示されます。グループにリンクステート グループ設定がない場合、イネーブルまたはディセーブルとして表示されません。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude outpu**t と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show link state group 1** コマンドの出力を示します。

```
Switch> show link state group 1
Link State Group: 1      Status: Enabled, Down
```

次の例では、**show link state group detail** コマンドの出力を示します。

```
Switch> show link state group detail
(Up):Interface up   (Dwn):Interface Down   (Dis):Interface disabled
```

```
Link State Group: 1 Status: Enabled, Down
Upstream Interfaces : Gi1/0/15(Dwn) Gi1/0/16(Dwn)
Downstream Interfaces : Gi1/0/11(Dis) Gi1/0/12(Dis) Gi1/0/13(Dis) Gi1/0/14(Dis)

Link State Group: 2 Status: Enabled, Down
Upstream Interfaces : Gi1/0/15(Dwn) Gi1/0/16(Dwn) Gi1/0/17(Dwn)
Downstream Interfaces : Gi1/0/11(Dis) Gi1/0/12(Dis) Gi1/0/13(Dis) Gi1/0/14(Dis)

(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
```

関連コマンド

コマンド	説明
link state group	リンクステート グループのメンバとしてインターフェイスを設定します。
link state track	リンクステート グループをイネーブルにします。
show running-config	現在の動作設定を表示します。

show mac access-group

あるインターフェイスまたはスイッチに設定されている MAC アクセス コントロール リスト（ACL）を表示するには、**show mac access-group** ユーザ EXEC コマンドを使用します。

show mac access-group [**interface** *interface-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface *interface-id*	（任意）特定のインターフェイスで設定された MAC ACL を表示します。有効なインターフェイスは物理ポートとポート チャネルです。ポート チャネル範囲は 1 ～ 48 です（特権 EXEC モードの場合だけ使用可能）。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mac-access group** ユーザ EXEC コマンドの出力を示します。ポート 2 には、適用される MAC アクセス リスト *macl_e1* があります。MAC ACL は他のインターフェイスに適用されません。

```
Switch> show mac access-group
Interface GigabitEthernet1/0/1:
   Inbound access-list is not set
Interface GigabitEthernet1/0/2:
   Inbound access-list is macl_e1
Interface GigabitEthernet1/0/3:
   Inbound access-list is not set
Interface GigabitEthernet1/0/4:
   Inbound access-list is not set

<output truncated>
```

次の例では、**show mac access-group interface** コマンドの出力を示します。

```
Switch# show mac access-group interface gigabitethernet1/0/1
Interface GigabitEthernet1/0/1:
   Inbound access-list is macl_e1
```

関連コマンド

コマンド	説明
mac access-group	インターフェイスに MAC アクセス グループを適用します。

show mac address-table

特定の MAC アドレス テーブルのダイナミック / スタティック エントリ、または特定のインターフェイスや VLAN 上の MAC アドレス テーブルのダイナミック / スタティック エントリを表示するには、**show mac address-table** ユーザ EXEC コマンドを使用します。

show mac address-table [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(19)EA1	**show mac-address-table**（ハイフン付き）コマンドは、**show mac address-table** （ハイフンなし）コマンドに替わりました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mac address-table** コマンドの出力を示します。

```
Switch> show mac address-table
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       ----        -----
 All    0000.0000.0001    STATIC      CPU
 All    0000.0000.0002    STATIC      CPU
 All    0000.0000.0003    STATIC      CPU
 All    0000.0000.0009    STATIC      CPU
 All    0000.0000.0012    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
   1    0030.9441.6327    DYNAMIC     Gi6/0/4
Total Mac Addresses for this criterion: 12
```

コマンド	説明
clear mac address-table dynamic	MAC アドレス テーブルから、特定のダイナミック アドレス、特定のインターフェイス上のすべてのダイナミック アドレス、または特定の VLAN 上のすべてのダイナミック アドレスを削除します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリだけを表示します。
show mac address-table interface	指定されたインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table notification	すべての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対する MAC アドレス通知設定を表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリだけを表示します。
show mac address-table vlan	指定された VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table address

指定された MAC アドレスの MAC アドレス テーブル情報を表示するには、**show mac address-table address** ユーザ EXEC コマンドを使用します。

show mac address-table address *mac-address* [**interface** *interface-id*] [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

mac-address	48 ビットの MAC アドレスを指定します。有効な形式は H.H.H です。
interface *interface-id*	（任意）特定のインターフェイスの情報を表示します。有効なインターフェイスには、物理ポートとポート チャネルが含まれます。
vlan *vlan-id*	（任意）特定の VLAN だけのエントリを表示します。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(19)EA1	**show mac-address-table address**（ハイフン付き）コマンドは、**show mac address-table address**（ハイフンなし）コマンドに替わりました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mac address-table address** コマンドの出力を示します。

```
Switch# show mac address-table address 0002.4b28.c482
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
 All    0002.4b28.c482  STATIC  CPU
Total Mac Addresses for this criterion: 1
```

関連コマンド

コマンド	説明
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリだけを表示します。
show mac address-table interface	指定されたインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table notification	すべての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対する MAC アドレス通知設定を表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリだけを表示します。
show mac address-table vlan	指定された VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table aging-time

特定のアドレス テーブル インスタンスのエージング タイム、指定された VLAN 上または指定がない場合はすべての VLAN 上のすべてのアドレス テーブル インスタンスのエージング タイムを表示するには、**show mac address-table aging-time** ユーザ EXEC コマンドを使用します。

show mac address-table aging-time [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

vlan *vlan-id*	（任意）特定の VLAN のエージング タイム情報を表示します。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(19)EA1	**show mac-address-table aging-time**（ハイフン付き）コマンドは、**show mac address-table aging-time**（ハイフンなし）コマンドに替わりました。

使用上のガイドライン

VLAN 番号が指定されない場合、すべての VLAN に対するエージング タイムが表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mac address-table aging-time** コマンドの出力を示します。

```
Switch> show mac address-table aging-time
Vlan    Aging Time
----    ----------
   1     300
```

次の例では、**show mac address-table aging-time vlan 10** コマンドの出力を示します。

```
Switch> show mac address-table aging-time vlan 10
Vlan    Aging Time
----    ----------
  10     300
```

関連コマンド

コマンド	説明
mac address-table aging-time	ダイナミック エントリが使用または更新された後、MAC アドレス テーブル内に保持される時間を設定します。
show mac address-table address	指定された MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリだけを表示します。
show mac address-table interface	指定されたインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table notification	すべての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対する MAC アドレス通知設定を表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリだけを表示します。
show mac address-table vlan	指定された VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table count

すべての VLAN または指定された VLAN に存在するアドレス数を表示するには、**show mac address-table count** ユーザ EXEC コマンドを使用します。

show mac address-table count [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

vlan *vlan-id*	（任意）特定の VLAN のアドレス数を表示します。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(19)EA1	**show mac-address-table count**（ハイフン付き）コマンドは、**show mac address-table count**（ハイフンなし）コマンドに替わりました。

使用上のガイドライン

VLAN 番号が指定されない場合、すべての VLAN に対するアドレス カウントが表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mac address-table count** コマンドの出力を示します。

```
Switch# show mac address-table count
Mac Entries for Vlan    : 1
---------------------------
Dynamic Address Count   : 2
Static  Address Count   : 0
Total Mac Addresses     : 2
```

関連コマンド

コマンド	説明
show mac address-table address	指定された MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリだけを表示します。

コマンド	説明
show mac address-table interface	指定されたインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table notification	すべての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対する MAC アドレス通知設定を表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリだけを表示します。
show mac address-table vlan	指定された VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table dynamic

ダイナミックな MAC アドレス テーブル エントリだけを表示するには、**show mac address-table dynamic** ユーザ EXEC コマンドを使用します。

show mac address-table dynamic [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]
[| {**begin** | **exclude** | **include**} *expression*]

構文の説明

address *mac-address*	（任意）48 ビットの MAC アドレスを指定します。有効なフォーマットは H.H.H です（特権 EXEC モードの場合だけ利用可能）。
interface *interface-id*	（任意）照合を行うインターフェイスを指定します。有効な*インターフェイス*には、物理ポートとポート チャネルが含まれます。
vlan *vlan-id*	（任意）特定の VLAN のエントリを表示します。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(19)EA1	**show mac-address-table dynamic**（ハイフン付き）コマンドは、**show mac address-table dynamic**（ハイフンなし）コマンドに替わりました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mac address-table dynamic** コマンドの出力を示します。

```
Switch> show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
   1    0030.b635.7862  DYNAMIC Gi6/0/2
   1    00b0.6496.2741  DYNAMIC Gi6/0/2
Total Mac Addresses for this criterion: 2
```

関連コマンド

コマンド	説明
clear mac address-table dynamic	MAC アドレス テーブルから、特定のダイナミック アドレス、特定のインターフェイス上のすべてのダイナミック アドレス、または特定の VLAN 上のすべてのダイナミック アドレスを削除します。
show mac address-table address	指定された MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。
show mac address-table interface	指定されたインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリだけを表示します。
show mac address-table vlan	指定された VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table interface

指定された VLAN の指定されたインターフェイスの MAC アドレス テーブル情報を表示するには、**show mac address-table interface** ユーザ EXEC コマンドを使用します。

show mac address-table interface *interface-id* [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface-id	（任意）インターフェイス タイプを指定します。有効なインターフェイスには、物理ポートとポート チャネルが含まれます。
vlan *vlan-id*	（任意）特定の VLAN のエントリを表示します。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(19)EA1	**show mac-address-table interface**（ハイフン付き）コマンドは、**show mac address-table interface**（ハイフンなし）コマンドに替わりました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mac address-table interface** コマンドの出力を示します。

```
Switch> show mac address-table interface gigabitethernet6/0/2
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
   1    0030.b635.7862  DYNAMIC Gi6/0/2
   1    00b0.6496.2741  DYNAMIC Gi6/0/2
Total Mac Addresses for this criterion: 2
```

関連コマンド

コマンド	説明
show mac address-table address	指定された MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリだけを表示します。
show mac address-table notification	すべての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対する MAC アドレス通知設定を表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリだけを表示します。
show mac address-table vlan	指定された VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table learning

すべての VLAN または指定した VLAN の MAC アドレス学習のステータスを表示するには、**show mac address-table learning** ユーザ EXEC コマンドを使用します。

show mac address-table learning [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

vlan *vlan-id*	（任意）特定の VLAN の情報を表示します。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(46)SE1	このコマンドが追加されました。

使用上のガイドライン

設定された VLAN と、その VLAN で MAC アドレス学習がイネーブルかディセーブルかを表示するには、キーワードを指定しないで **show mac address-table learning** コマンドを使用します。デフォルトは、すべての VLAN で MAC アドレス学習がイネーブルです。個々の VLAN の学習ステータスを表示するには、特定の VLAN ID を指定してこのコマンドを使用します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、MAC アドレス学習が VLAN 200 でディセーブルになっていることを示す **show mac address-table learning** ユーザ EXEC コマンドの出力を示します。

```
Switch> show mac address-table learning
VLAN    Learning Status
----    ---------------
1             yes
100           yes
200           no
```

関連コマンド

コマンド	説明
mac address-table learning vlan	VLAN の MAC アドレス学習をイネーブルまたはディセーブルにします。

show mac address-table move update

スイッチの MAC アドレス テーブル移行更新の情報を表示するには、**show mac address-table move update** ユーザ EXEC コマンドを使用します。

show mac address-table move update [| {**begin** | **exclude** | **include**} **expression**]

構文の説明

| **begin**	（任意）expression と一致する行から表示を開始します。
| **exclude**	（任意）expression と一致する行を表示から除外します。
| **include**	（任意）指定された expression と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、output を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mac address-table move update** コマンドの出力を示します。

```
Switch> show mac address-table move update
Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 10
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 0003.fd6a.8701
Rcv last switch-ID : 0303.fd63.7600
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
switch#
```

関連コマンド

コマンド	説明
clear mac address-table move update	MAC アドレス テーブル移行更新カウンタをクリアします。
mac address-table move update {**receive** | **transmit**}	スイッチ上の MAC アドレス テーブル移行更新を設定します。

show mac address-table notification

すべてのインターフェイスまたは指定されたインターフェイスの MAC アドレス通知設定を表示するには、**show mac address-table notification** ユーザ EXEC コマンドを使用します。

show mac address-table notification {**change** [**interface** [*interface-id*] | **mac-move** | **threshold**} [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

change	MAC 変更通知機能パラメータおよび履歴テーブルを表示します。
interface	（任意）すべてのインターフェイスの情報を表示します。有効なインターフェイスには、物理ポートとポート チャネルが含まれます。
interface-id	（任意）指定されたインターフェイスの情報を表示します。有効なインターフェイスには、物理ポートとポート チャネルが含まれます。
mac-move	MAC アドレス移動通知のステータスを表示します。
threshold	MAC アドレス テーブルしきい値モニタリングのステータスを表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(19)EA1	**show mac-address-table notification**（ハイフン付き）コマンドは、**show mac address-table notification**（ハイフンなし）コマンドに替わりました。
12.2(40)SE	**change**、**mac-move**、および **threshold** キーワードが追加されました。

使用上のガイドライン

キーワードを指定しないで **show mac address-table notification change** コマンドを使用すると、MAC アドレス変更通知機能がイネーブルかディセーブルか、MAC 通知間隔、履歴テーブルの最大許容エントリ数、および履歴テーブルの内容を表示します。

すべてのインターフェイスの通知を表示するには、**interface** キーワードを使用します。*interface-id* が含まれる場合、そのインターフェイスのフラグだけが表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mac address-table notification change** コマンドの出力を示します。

```
Switch> show mac address-table notification change
MAC Notification Feature is Enabled on the switch
Interval between Notification Traps : 60 secs
Number of MAC Addresses Added : 4
Number of MAC Addresses Removed : 4
Number of Notifications sent to NMS : 3
Maximum Number of entries configured in History Table : 100
Current History Table Length : 3
MAC Notification Traps are Enabled
History Table contents
----------------------
History Index 0, Entry Timestamp 1032254, Despatch Timestamp 1032254
MAC Changed Message :
Operation: Added   Vlan: 2     MAC Addr: 0000.0000.0001 Module: 0   Port: 1

History Index 1, Entry Timestamp 1038254, Despatch Timestamp 1038254
MAC Changed Message :
Operation: Added   Vlan: 2     MAC Addr: 0000.0000.0000 Module: 0   Port: 1
Operation: Added   Vlan: 2     MAC Addr: 0000.0000.0002 Module: 0   Port: 1
Operation: Added   Vlan: 2     MAC Addr: 0000.0000.0003 Module: 0   Port: 1

History Index 2, Entry Timestamp 1074254, Despatch Timestamp 1074254
MAC Changed Message :
Operation: Deleted Vlan: 2     MAC Addr: 0000.0000.0000 Module: 0   Port: 1
Operation: Deleted Vlan: 2     MAC Addr: 0000.0000.0001 Module: 0   Port: 1
Operation: Deleted Vlan: 2     MAC Addr: 0000.0000.0002 Module: 0   Port: 1
Operation: Deleted Vlan: 2     MAC Addr: 0000.0000.0003 Module: 0   Port: 1
```

関連コマンド

コマンド	説明
clear mac address-table notification	MAC アドレス通知グローバル カウンタをクリアします。
mac address-table notification	MAC アドレス変更、移動、またはアドレス テーブルしきい値の MAC アドレス通知機能をイネーブルにします。
show mac address-table address	指定された MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリだけを表示します。
show mac address-table interface	指定されたインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリだけを表示します。
show mac address-table vlan	指定された VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table static

スタティック MAC アドレス テーブル エントリだけを表示するには、**show mac address-table static** ユーザ EXEC コマンドを使用します。

show mac address-table static [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]
[| {**begin** | **exclude** | **include**} *expression*]

構文の説明

address *mac-address*	（任意）48 ビットの MAC アドレスを指定します。有効なフォーマットは H.H.H です（特権 EXEC モードの場合だけ利用可能）。
interface *interface-id*	（任意）照合を行うインターフェイスを指定します。有効なインターフェイスには、物理ポートとポート チャネルが含まれます。
vlan *vlan-id*	（任意）特定の VLAN のアドレスを表示します。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(19)EA1	**show mac-address-table static**（ハイフン付き）コマンドは、**show mac address-table static**（ハイフンなし）コマンドに替わりました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mac address-table static** コマンドの出力を示します。

```
Switch> show mac address-table static
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
 All    0100.0ccc.cccc  STATIC  CPU
 All    0180.c200.0000  STATIC  CPU
 All    0100.0ccc.cccd  STATIC  CPU
 All    0180.c200.0001  STATIC  CPU
 All    0180.c200.0004  STATIC  CPU
 All    0180.c200.0005  STATIC  CPU
   4    0001.0002.0004  STATIC  Drop
   6    0001.0002.0007  STATIC  Drop
```

```
Total Mac Addresses for this criterion: 8
```

関連コマンド

コマンド	説明
mac address-table static	MAC アドレス テーブルにスタティック アドレスを追加します。
mac address-table static drop	ユニキャスト MAC アドレス フィルタリングをイネーブルにし、特定の送信元または宛先 MAC アドレスを持つトラフィックをドロップするようにスイッチを設定します。
show mac address-table address	指定された MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリだけを表示します。
show mac address-table interface	指定されたインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table notification	すべての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対する MAC アドレス通知設定を表示します。
show mac address-table vlan	指定された VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table vlan

指定された VLAN の MAC アドレス テーブル情報を表示するには、**show mac address-table vlan** ユーザ EXEC コマンドを使用します。

show mac address-table vlan *vlan-id* [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

vlan-id	（任意）特定の VLAN のアドレスを表示します。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(19)EA1	**show mac-address-table vlan**（ハイフン付き）コマンドは、**show mac address-table vlan**（ハイフンなし）コマンドに替わりました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mac address-table vlan 1** コマンドの出力を示します。

```
Switch> show mac address-table vlan 1
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
   1    0100.0ccc.cccc  STATIC  CPU
   1    0180.c200.0000  STATIC  CPU
   1    0100.0ccc.cccd  STATIC  CPU
   1    0180.c200.0001  STATIC  CPU
   1    0180.c200.0002  STATIC  CPU
   1    0180.c200.0003  STATIC  CPU
   1    0180.c200.0005  STATIC  CPU
   1    0180.c200.0006  STATIC  CPU
   1    0180.c200.0007  STATIC  CPU
Total Mac Addresses for this criterion: 9
```

関連コマンド

コマンド	説明
show mac address-table address	指定された MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリだけを表示します。
show mac address-table interface	指定されたインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table notification	すべての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対する MAC アドレス通知設定を表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリだけを表示します。

show mls qos

グローバルな Quality of Service（QoS）設定情報を表示するには、**show mls qos** ユーザ EXEC コマンドを使用します。

show mls qos [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、QoS がイネーブルで DSCP 透過もイネーブルの場合の **show mls qos** コマンドの出力を示します。

```
Switch> show mls qos
QoS is enabled
QoS ip packet dscp rewrite is enabled
```

関連コマンド

コマンド	説明
mls qos	スイッチ全体に対して QoS をイネーブルにします。

show mls qos aggregate-policer

Quality of Service（QoS）集約ポリサー設定を表示するには、**show mls qos aggregate-policer** ユーザ EXEC コマンドを使用します。ポリサーは、最大許容伝送速度、最大バースト伝送サイズ、およびいずれかの最大値を超過した場合の対処法を定義します。

show mls qos aggregate-policer [*aggregate-policer-name*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

aggregate-policer-name	（任意）指定された名前のポリシー設定を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mls qos aggregate-policer** コマンドの出力を示します。

```
Switch> show mls qos aggregate-policer policer1
aggregate-policer policer1 1000000 2000000 exceed-action drop
Not used by any policy map
```

関連コマンド

コマンド	説明
mls qos aggregate-policer	ポリシー マップ内で複数のクラスが共有するポリサー パラメータを定義します。

show mls qos input-queue

入力キューの Quality of Service（QoS）を表示するには、**show mls qos input-queue** ユーザ EXEC コマンドを使用します。

show mls qos input-queue [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mls qos input-queue** コマンドの出力を示します。

```
Switch> show mls qos input-queue
Queue     :       1       2
----------------------------------------------
buffers   :       90      10
bandwidth :       4       4
priority  :       0       10
threshold1:       100     100
threshold2:       100     100
```

関連コマンド

コマンド	説明
mls qos srr-queue input bandwidth	Shaped Round Robin（SRR; シェイプド ラウンド ロビン）の重みを入力キューに割り当てます。
mls qos srr-queue input buffers	入力キュー間のバッファを割り当てます。
mls qos srr-queue input cos-map	割り当てられたサービス クラス（CoS）値を入力キューにマッピングし、CoS 値をキューとしきい値 ID に割り当てます。
mls qos srr-queue input dscp-map	割り当てられた Differentiated Service Code Point（DSCP）値を入力キューにマッピングし、DSCP 値をキューとしきい値 ID に割り当てます。
mls qos srr-queue input priority-queue	入力プライオリティ キューを設定し、帯域幅を保証します。
mls qos srr-queue input threshold	Weighted Tail-Drop（WTD）しきい値のパーセンテージを入力キューに割り当てます。

show mls qos interface

Quality of Service（QoS）情報をポート レベルで表示するには、**show mls qos interface** ユーザ EXEC コマンドを使用します。

show mls qos interface [*interface-id*] [**buffers** | **queueing** | **statistics**]
[| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface-id	（任意）指定されたポートの QoS 情報を表示します。有効なインターフェイスには、物理ポートが含まれます。
buffers	（任意）キュー間のバッファ割り当てを表示します。
queueing	（任意）キューイングの指針（共有またはシェーピング）およびキューに対応したウェイトを表示します。
statistics	（任意）送受信された Differentiated Service Code Point（DSCP）の統計情報、サービス クラス（CoS）値、キューに入れられたかまたは出力キュー単位で削除されたパケット数、各ポリサーのプロファイル内外のパケット数を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

（注）　**policer** キーワードは、コマンドラインのヘルプ ストリングには表示されますが、サポートされていません。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、VLAN ベース QoS がイネーブルの場合の **show mls qos interface** *interface-id* コマンドの出力を示します。

```
Switch> show mls qos interface gigabitethernet1/0/1
GigabitEthernet1/0/1
trust state:not trusted
trust mode:not trusted
trust enabled flag:ena
COS override:dis
default COS:0
DSCP Mutation Map:Default DSCP Mutation Map
```

```
Trust device:none
qos mode:vlan-based
```

次の例では、VLAN ベース QoS がディセーブルの場合の **show mls qos interface** *interface-id* コマンドの出力を示します。

```
Switch> show mls qos interface gigabitethernet1/0/2
GigabitEthernet1/0/2
trust state:not trusted
trust mode:not trusted
trust enabled flag:ena
COS override:dis
default COS:0
DSCP Mutation Map:Default DSCP Mutation Map
Trust device:none
qos mode:port-based
```

次の例では、**show mls qos interface** *interface-id* **buffers** コマンドの出力を示します。

```
Switch> show mls qos interface gigabitethernet1/0/2 buffers
GigabitEthernet1/0/2
The port is mapped to qset : 1
The allocations between the queues are : 25 25 25 25
```

次の例では、**show mls qos interface** *interface-id* **queueing** コマンドの出力を示します。出力緊急キューは、設定された Shaped Round Robin（SRR）の重みを無効にします。

```
Switch> show mls qos interface gigabitethernet1/0/2 queueing
GigabitEthernet1/0/2
Egress Priority Queue :enabled
Shaped queue weights (absolute) :  25 0 0 0
Shared queue weights  :  25 25 25 25
The port bandwidth limit : 100  (Operational Bandwidth:100.0)
The port is mapped to qset : 1
```

次の例では、**show mls qos interface** *interface-id* **statistics** コマンドの出力を示します。表 2-37 に、この出力で表示されるフィールドの説明を示します。

```
Switch> show mls qos interface gigabitethernet1/0/2 statistics
GigabitEthernet1/0/2

  dscp: incoming
-------------------------------

  0 -  4 :      4213          0          0          0          0
  5 -  9 :         0          0          0          0          0
 10 - 14 :         0          0          0          0          0
 15 - 19 :         0          0          0          0          0
 20 - 24 :         0          0          0          0          0
 25 - 29 :         0          0          0          0          0
 30 - 34 :         0          0          0          0          0
 35 - 39 :         0          0          0          0          0
 40 - 44 :         0          0          0          0          0
 45 - 49 :         0          0          0          6          0
 50 - 54 :         0          0          0          0          0
 55 - 59 :         0          0          0          0          0
 60 - 64 :         0          0          0          0
  dscp: outgoing
-------------------------------

  0 -  4 :    363949          0          0          0          0
  5 -  9 :         0          0          0          0          0
 10 - 14 :         0          0          0          0          0
 15 - 19 :         0          0          0          0          0
```

```
 20 - 24 :          0           0           0           0           0
 25 - 29 :          0           0           0           0           0
 30 - 34 :          0           0           0           0           0
 35 - 39 :          0           0           0           0           0
 40 - 44 :          0           0           0           0           0
 45 - 49 :          0           0           0           0           0
 50 - 54 :          0           0           0           0           0
 55 - 59 :          0           0           0           0           0
 60 - 64 :          0           0           0           0
  cos: incoming
-------------------------------

  0 -  4 :     132067           0           0           0           0
  5 -  9 :          0           0           0
  cos: outgoing
-------------------------------

  0 -  4 :     739155           0           0           0           0
  5 -  9 :         90           0           0

Policer: Inprofile:        0 OutofProfile:        0
```

表 2-37　show mls qos interface statistics のフィールドの説明

フィールド		説明
DSCP	incoming	DSCP 値ごとに受信したパケット数
	outgoing	DSCP 値ごとに送信したパケット数
CoS	incoming	CoS 値ごとに受信したパケット数
	outgoing	CoS 値ごとに送信したパケット数
Policer	Inprofile	ポリサーごとのプロファイル内パケット数
	OutofProfile	ポリサーごとのプロファイル外パケット数

関連コマンド

コマンド	説明
mls qos queue-set output buffers	バッファをキューセットに割り当てます。
mls qos queue-set output threshold	Weighted Tail-Drop（WTD）しきい値を設定し、バッファのアベイラビリティを保証し、キューセットに対する最大メモリ割り当てを設定します。
mls qos srr-queue input bandwidth	SRR の重みを入力キューに割り当てます。
mls qos srr-queue input buffers	入力キュー間のバッファを割り当てます。
mls qos srr-queue input cos-map	CoS 値を入力キューにマッピングするか、または CoS 値をキューとしきい値 ID にマッピングします。
mls qos srr-queue input dscp-map	DSCP 値を入力キューにマッピングするか、または DSCP 値をキューとしきい値 ID にマッピングします。
mls qos srr-queue input priority-queue	入力プライオリティ キューを設定し、帯域幅を保証します。
mls qos srr-queue input threshold	WTD しきい値のパーセンテージを入力キューに割り当てます。
mls qos srr-queue output cos-map	CoS 値を出力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue output dscp-map	DSCP 値を出力キュー、またはキューとしきい値 ID にマッピングします。
policy-map	ポリシー マップを作成または変更します。

コマンド	説明
priority-queue	ポート上で出力緊急キューをイネーブルにします。
queue-set	ポートをキューセットにマッピングします。
srr-queue bandwidth limit	ポートでの最大出力を制限します。
srr-queue bandwidth shape	シェーピングされた重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅シェーピングをイネーブルにします。
srr-queue bandwidth share	共有する重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅の共有をイネーブルにします。

show mls qos maps

Quality of Service（QoS）マッピング情報を表示するには、**show mls qos maps** ユーザ EXEC コマンドを使用します。分類では、QoS はマッピング テーブルを使用してトラフィックのプライオリティを表示し、受信したサービス クラス（CoS）、Differentiated Service Code Point（DSCP）、または IP precedence 値から対応する CoS または DSCP 値を取得します。

show mls qos maps [**cos-dscp** | **cos-input-q** | **cos-output-q** | **dscp-cos** | **dscp-input-q** | **dscp-mutation** *dscp-mutation-name* | **dscp-output-q** | **ip-prec-dscp** | **policed-dscp**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

cos-dscp	（任意）サービス クラス（CoS）/DSCP マップを表示します。
cos-input-q	（任意）CoS 入力キューのしきい値マップを表示します。
cos-output-q	（任意）CoS 出力キューのしきい値マップを表示します。
dscp-cos	（任意）DSCP/CoS マップを表示します。
dscp-input-q	（任意）DSCP 入力キューしきい値マップを表示します。
dscp-mutation *dscp-mutation-name*	（任意）指定された DSCP/DSCP-mutation マップを表示します。
dscp-output-q	（任意）DSCP 出力キューしきい値マップを表示します。
ip-prec-dscp	（任意）IP precedence/DSCP マップを表示します。
policed-dscp	（任意）ポリシング設定 DSCP マップを表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

ポリシング設定 DSCP、DSCP/CoS、および DSCP/DSCP-mutation マップは、マトリクスとして表示されます。d1 列では、DSCP で最も重要度の高い桁を指定します。d2 行では、DSCP で最も重要度の低い桁を指定します。d1 値および d2 値の共通部分では、ポリシング設定 DSCP、CoS、または Mutated-DSCP 値を提供します。たとえば、DSCP/CoS マップでは、DSCP 値 43 は CoS 値 5 に対応します。

DSCP 入力キューしきい値および DSCP 出力キューしきい値マップは、マトリクスとして表示されます。d1 列では、最も重要度の高い DSCP 番号の桁を指定します。d2 行では、最も重要度の低い DSCP 番号の桁を指定します。d1 値と d2 値の共通部分では、キュー ID としきい値 ID を提供します。たとえば、DSCP 入力キューしきい値マップでは、DSCP 値 43 はキュー 2 およびしきい値 1（02-01）に対応します。

CoS 入力キューしきい値および CoS 出力キューしきい値マップでは、CoS 値が一番上の行、対応するキュー ID およびしきい値 ID が 2 番目の行に表示されます。たとえば、CoS 入力キューしきい値マップでは、CoS 値 5 はキュー 2 およびしきい値 1（2-1）に対応することになります。

例

次の例では、**show mls qos maps** コマンドの出力を示します。

```
Switch> show mls qos maps
Policed-dscp map:
     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:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ----------------------------------------
      0 :    00 00 00 00 00 00 00 00 01 01
      1 :    01 01 01 01 01 01 02 02 02 02
      2 :    02 02 02 02 03 03 03 03 03 03
      3 :    03 03 04 04 04 04 04 04 04 04
      4 :    05 05 05 05 05 05 05 05 06 06
      5 :    06 06 06 06 06 06 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

Dscp-outputq-threshold map:
  d1 :d2    0     1     2     3     4     5     6     7     8     9
  ----------------------------------------------------------------------
   0 :    02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01
   1 :    02-01 02-01 02-01 02-01 02-01 02-01 03-01 03-01 03-01 03-01
   2 :    03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01
   3 :    03-01 03-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01
   4 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 04-01 04-01
   5 :    04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01
   6 :    04-01 04-01 04-01 04-01
```

```
Dscp-inputq-threshold map:
    d1 :d2    0     1     2     3     4     5     6     7     8     9
    ------------------------------------------------------------------
     0 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
     1 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
     2 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
     3 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
     4 :    02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 01-01 01-01
     5 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
     6 :    01-01 01-01 01-01 01-01

Cos-outputq-threshold map:
              cos:  0   1   2   3   4   5   6   7
              ------------------------------------
  queue-threshold: 2-1 2-1 3-1 3-1 4-1 1-1 4-1 4-1

   Cos-inputq-threshold map:
              cos:  0   1   2   3   4   5   6   7
              ------------------------------------
  queue-threshold: 1-1 1-1 1-1 1-1 1-1 2-1 1-1 1-1

Dscp-dscp mutation map:
   Default DSCP Mutation Map:
     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
```

関連コマンド

コマンド	説明
mls qos map	CoS/DSCP マップ、DSCP/CoS マップ、DSCP/DSCP-mutation マップ、IP precedence/DSCP マップ、およびポリシング設定 DSCP マップを定義します。
mls qos srr-queue input cos-map	CoS 値を入力キューにマッピングするか、または CoS 値をキューとしきい値 ID にマッピングします。
mls qos srr-queue input dscp-map	DSCP 値を入力キューにマッピングするか、または DSCP 値をキューとしきい値 ID にマッピングします。
mls qos srr-queue output cos-map	CoS 値を出力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue output dscp-map	DSCP 値を出力キュー、またはキューとしきい値 ID にマッピングします。

show mls qos queue-set

出力キューの Quality of Service（QoS）を表示するには、**show mls qos queue-set** ユーザ EXEC コマンドを使用します。

show mls qos queue-set [*qset-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

qset-id	（任意）キューセットの ID です。各ポートはキューセットに属し、ポート単位で出力キュー 4 つの特性すべてを定義します。指定できる範囲は 1 ～ 2 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mls qos queue-set** コマンドの出力を示します。

```
Switch> show mls qos queue-set
Queueset: 1
Queue    :        1       2       3       4
----------------------------------------------
buffers   :       25      25      25      25
threshold1:       100     200     100     100
threshold2:       100     200     100     100
reserved  :       50      50      50      50
maximum   :       400     400     400     400
Queueset: 2
Queue    :        1       2       3       4
----------------------------------------------
buffers   :       25      25      25      25
threshold1:       100     200     100     100
threshold2:       100     200     100     100
reserved  :       50      50      50      50
maximum   :       400     400     400     400
```

関連コマンド

コマンド	説明
mls qos queue-set output buffers	バッファをキューセットに割り当てます。
mls qos queue-set output threshold	Weighted Tail-Drop（WTD）しきい値を設定し、バッファのアベイラビリティを保証し、キューセットに対する最大メモリ割り当てを設定します。

show mls qos vlan

Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）に適用されているポリシー マップを表示するには、**show mls qos vlan** ユーザ EXEC コマンドを使用します。

show mls qos vlan *vlan-id* [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

vlan-id	ポリシー マップを表示するために SVI の VLAN ID を指定します。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.2(25)SE	このコマンドが追加されました。

使用上のガイドライン

show mls qos vlan コマンドからの出力は、VLAN ベースの Quality Of Service（QoS）がイネーブルで階層ポリシー マップが設定されている場合だけ意味があります。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mls qos vlan** コマンドの出力を示します。

```
Switch> show mls qos vlan 10
Vlan10
Attached policy-map for Ingress:pm-test-pm-2
```

関連コマンド

コマンド	説明
policy-map	複数のポートに適用できるポリシー マップを作成または変更し、ポリシー マップ コンフィギュレーション モードを開始します。

show monitor

スイッチのすべての Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）および Remote SPAN（RSPAN）セッションに関する情報を表示するには、**show monitor** ユーザ EXEC コマンドを使用します。キーワードを指定してコマンドを使用することで、特定のセッション、すべてのセッション、すべてのローカル セッション、すべてのリモート セッションが表示されます。

show monitor [**session** {*session_number* | **all** | **local** | **range** *list* | **remote**} [**detail**]] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

session	（任意）指定された SPAN セッションの情報を表示します。
session_number	SPAN または RSPAN のセッション番号を指定します。指定できる範囲は 1 ～ 66 です。
all	すべての SPAN セッションを表示します。
local	ローカルの SPAN セッションだけを表示します。
range *list*	SPAN セッションの範囲（*list* は有効なセッションの範囲）を表示します。1 つのセッションまたはセッションの範囲のいずれかが表示され、範囲の場合、2 つの数字のうち低い方が最初になります（ハイフンで区切られます）。カンマ区切りのパラメータ間、またはハイフン指定の範囲にスペースは入力しません。 **（注）**　このキーワードは、特権 EXEC モードの場合だけ使用可能です。
remote	リモートの SPAN セッションだけを表示します。
detail	（任意）指定されたセッションの詳細情報を表示します。
| begin	*expression* と一致する行から表示を開始します。
| exclude	*expression* と一致する行を表示から除外します。
| include	指定した *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**range** *list* および **detail** キーワードが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show monitor コマンドと **show monitor session all** コマンドの出力は同じです。

例

次に、**show monitor** ユーザ EXEC コマンドの出力例を示します。

```
Switch# show monitor
Session 1
---------
```

```
Type : Local Session
Source Ports :
RX Only : Fa4/0/1
Both : Fa4/0/2-3,Fa4/0/5-6
Destination Ports : Fa4/0/20
Encapsulation : Replicate
Ingress : Disabled

Session 2
---------
Type : Remote Source Session
Source VLANs :
TX Only : 10
Both : 1-9
Dest RSPAN VLAN : 105
```

次の例では、ローカル SPAN 送信元セッション 1 に対する **show monitor** ユーザ EXEC コマンドの出力を示します。

```
Switch# show monitor session 1
Session 1
---------
Type : Local Session
Source Ports :
RX Only : Fa4/0/1
Both : Fa4/0/2-3,Fa4/0/5-6
Destination Ports : Fa4/0/20
Encapsulation : Replicate
Ingress : Disabled
```

次の例では、入力トラフィック転送をイネーブルにした場合の **show monitor session all** ユーザ EXEC コマンドの出力を示します。

```
Switch# show monitor session all
Session 1
---------
Type : Local Session
Source Ports :
Both : Fa4/0/2
Destination Ports : Fa4/0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q

Session 2
---------
Type : Local Session
Source Ports :
Both : Fa4/0/8
Destination Ports : Fa4/0/2
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged
```

関連コマンド

コマンド	説明
monitor session	SPAN または RSPAN セッションを開始、または修正します。

show mvr

現在の Multicast VLAN Registration（MVR）グローバル パラメータ値を表示するには、キーワードを指定しないで **show mvr** 特権 EXEC コマンドを使用します。表示されるのは、MVR がイネーブルであるかどうか、MVR マルチキャスト VLAN、最大クエリー応答時間、マルチキャスト グループ数、および MVR モード（dynamic または compatible）です。

show mvr [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mvr** コマンドの出力を示します。

```
Switch# show mvr
MVR Running: TRUE
MVR multicast VLAN: 1
MVR Max Multicast Groups: 256
MVR Current multicast groups: 0
MVR Global query response time: 5 (tenths of sec)
MVR Mode: compatible
```

上記の例では、マルチキャスト グループの最大数は 256 です。MVR モードは、compatible（Catalyst 2900 XL および Catalyst 3500 XL スイッチと連動する場合）または dynamic（動作が IGMP スヌーピング動作と一貫性があり、送信元ポート上でダイナミック MVR メンバシップがサポートされている場合）のいずれかです。

関連コマンド

コマンド	説明
mvr（グローバル コンフィギュレーション）	スイッチ上で Multicast VLAN Registration（MVR）をイネーブルにして、設定します。
mvr（インターフェイス コンフィギュレーション）	MVR ポートを設定します。

コマンド	説明
show mvr interface	コマンドに **interface** および **members** キーワードを追加した場合、設定された MVR インターフェイス、指定されたインターフェイスのステータス、またはインターフェイスが属するすべてのマルチキャスト グループが表示されます。
show mvr members	MVR マルチキャスト グループのメンバであるポートすべてを表示します。グループ内にメンバがいない場合、グループは非アクティブであることを示します。

show mvr interface

Multicast VLAN Registration（MVR）レシーバおよび送信元ポートを表示するには、キーワードを指定せずに **show mvr interface** 特権 EXEC コマンドを使用します。キーワードを指定してこのコマンドを使用すると、特定のレシーバ ポートの MVR パラメータが表示されます。

show mvr interface [*interface-id* [**members** [**vlan** *vlan-id*]]] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface-id	（任意）インターフェイスの MVR タイプ、ステータス、および即時脱退設定を表示します。 **（注）**　有効なインターフェイスには、物理ポート（タイプ、スタック メンバ、モジュール、ポート番号を含む）が含まれます。
members	（任意）指定されたインターフェイスが属する MVR グループをすべて表示します。
vlan *vlan-id*	（任意）この VLAN 上の MVR グループ メンバをすべて表示します。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

入力したポートが非 MVR ポートまたは送信元ポートの場合は、エラー メッセージが戻されます。入力したポートがレシーバ ポートの場合は、ポート タイプ、ポート単位のステータス、および即時脱退設定が表示されます。

members キーワードを入力すると、インターフェイス上の MVR グループ メンバがすべて表示されます。VLAN ID を入力すると、VLAN の MVR グループ メンバがすべて表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mvr interface** コマンドの出力を示します。

```
Switch# show mvr interface
Port        Type            Status          Immediate Leave
----        ----            -------         ---------------
Gi1/0/1   SOURCE          ACTIVE/UP       DISABLED
Gi1/0/2   RECEIVER        ACTIVE/DOWN     DISABLED
```

上記の Status の定義は、次のとおりです。

- ACTIVE は、ポートが VLAN に含まれていることを意味します。
- UP/DOWN は、ポートが転送中か転送中でないかを示します。
- INACTIVE は、ポートが VLAN に含まれていないことを意味します。

次の例では、指定されたポートの **show mvr interface** コマンドの出力を示します。

```
Switch# show mvr interface gigabitethernet1/0/2
Type: RECEIVER Status: ACTIVE Immediate Leave: DISABLED
```

次の例では、**show mvr interface** *interface-id* **members** コマンドの出力を示します。

```
Switch# show mvr interface gigabitethernet1/0/2 members
239.255.0.0     DYNAMIC ACTIVE
239.255.0.1     DYNAMIC ACTIVE
239.255.0.2     DYNAMIC ACTIVE
239.255.0.3     DYNAMIC ACTIVE
239.255.0.4     DYNAMIC ACTIVE
239.255.0.5     DYNAMIC ACTIVE
239.255.0.6     DYNAMIC ACTIVE
239.255.0.7     DYNAMIC ACTIVE
239.255.0.8     DYNAMIC ACTIVE
239.255.0.9     DYNAMIC ACTIVE
```

関連コマンド

コマンド	説明
mvr（グローバル コンフィギュレーション）	スイッチ上で Multicast VLAN Registration（MVR）をイネーブルにして、設定します。
mvr（インターフェイス コンフィギュレーション）	MVR ポートを設定します。
show mvr	スイッチのグローバル MVR 設定を表示します。
show mvr members	MVR マルチキャスト グループのメンバであるすべてのレシーバ ポートを表示します。

show mvr members

現在 IP マルチキャスト グループのメンバであるすべてのレシーバおよび送信元ポートを表示するには、**show mvr members** 特権 EXEC コマンドを使用します。

show mvr members [*ip-address*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

ip-address	（任意）IP マルチキャスト アドレスです。アドレスを入力すると、マルチキャスト グループのメンバであるすべてのレシーバおよび送信元ポートが表示されます。アドレスを入力しない場合は、すべての Multicast VLAN Registration（MVR）グループのすべてのメンバがリストされます。グループ内にメンバがない場合は、グループは Inactive として表示されます。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

show mvr members コマンドは、レシーバおよび送信元ポートに適用されます。MVR 互換モードの場合、すべての送信元ポートは、すべてのマルチキャスト グループのメンバです。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show mvr members** コマンドの出力を示します。

```
Switch# show mvr members
MVR Group IP    Status          Members
------------    ------          -------
239.255.0.1     ACTIVE          Gi1/0/1(d), Gi1/0/2(s)
239.255.0.2     INACTIVE        None
239.255.0.3     INACTIVE        None
239.255.0.4     INACTIVE        None
239.255.0.5     INACTIVE        None
239.255.0.6     INACTIVE        None
239.255.0.7     INACTIVE        None
239.255.0.8     INACTIVE        None
239.255.0.9     INACTIVE        None
239.255.0.10    INACTIVE        None

<output truncated>
```

次の例では、**show mvr members** *ip-address* コマンドの出力を示します。次のアドレスを持った IP マルチキャスト グループのメンバを表示します。

```
Switch# show mvr members 239.255.0.2
239.255.003.--22     ACTIVE          Gi1/0/1(d), Gi1/0/2(d), Gi1/0/3(d),
                                     Gi1/0/4(d), Gi1/0/5(s)
```

関連コマンド

コマンド	説明
mvr（グローバル コンフィギュレーション）	スイッチ上で Multicast VLAN Registration（MVR）をイネーブルにして、設定します。
mvr（インターフェイス コンフィギュレーション）	MVR ポートを設定します。
show mvr	スイッチのグローバル MVR 設定を表示します。
show mvr interface	コマンドに **members** キーワードを追加した場合、設定された MVR インターフェイス、指定されたインターフェイスのステータス、またはインターフェイスが属するすべてのマルチキャスト グループが表示されます。

show network-policy profile

ネットワーク ポリシー プロファイルを表示するには、**show network policy profile** 特権 EXEC コマンドを使用します。

show network-policy profile [*profile number*] [**detail**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

profile number	（任意）ネットワーク ポリシー プロファイル番号を表示します。プロファイルが入力されていない場合、すべてのネットワーク ポリシー プロファイルが表示されます。
detail	（任意）詳細なステータスと統計情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

例

次の例では、**show network-policy profile** コマンドの出力を示します。

```
Switch# show network-policy profile
Network Policy Profile 10
   voice vlan 17 cos 4
  Interface:
   none
Network Policy Profile 30
   voice vlan 30 cos 5
  Interface:
   none
Network Policy Profile 36
   voice vlan 4 cos 3
  Interface:
   Interface_id
```

関連コマンド

コマンド	説明
network-policy	インターフェイスにネットワーク ポリシーを適用します。
network-policy profile（グローバル コンフィギュレーション）	ネットワーク ポリシー プロファイルを作成します。
network-policy profile（ネットワークポリシー コンフィギュレーション）	ネットワーク ポリシー プロファイルの属性を設定します。

show nmsp

スイッチの Network Mobility Services Protocol（NMSP）情報を表示するには、**show nmsp** 特権 EXEC コマンドを使用します。このコマンドは、スイッチで暗号化ソフトウェア イメージが実行されている場合にだけ利用できます。

show nmsp {**attachment suppress interface** | **capability** | **notification interval** | **statistics** {**connection** | **summary**} | **status** | **subscription** {**detail** | **summary**}} [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

attachment suppress interface	アタッチメント抑制インターフェイスを表示します。
capability	サポートされるサービスとサブサービスを含むスイッチ機能を表示します。
notification interval	サポートされるサービスの通知間隔を表示します。
statistics {**connection** | **summary**}	NMSP 統計情報を表示します。 • **connection**：各接続でのメッセージ カウンタを表示します。 • **summary**：グローバル カウンタを表示します。
status	NMSP 接続に関する情報を表示します。
subscription {**detail** | **summary**}	各 NMSP 接続に関するサブスクリプション情報を表示します。 • **detail**：各接続でサブスクライブしているすべてのサービスとサブサービスを表示します。 • **summary**：各接続でサブスクライブしているすべてのサービスを表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

例

次の例では、**show nmsp attachment suppress interface** コマンドの出力を示します。

```
Switch# show nmsp attachment suppress interface
NMSP Attachment Suppression Interfaces
--------------------------------------
GigabitEthernet1/1
GigabitEthernet1/2
```

次の例では、**show nmsp capability** コマンドの出力を示します。

```
Switch# show nmsp capability
NMSP Switch Capability
------------------------------
Service          Subservice
-----------       --------------
Attachment    Wired Station
Location        Subscription
```

次の例では、**show nmsp notification interval** コマンドの出力を示します。

```
Switch# show nmsp notification interval
NMSP Notification Intervals
----------------------------------
Attachment notify interval: 30 sec (default)
Location notify interval: 30 sec (default)
```

次の例では、**show nmsp statistics connection** コマンドと **show nmsp statistics summary** コマンドの出力を示します。

```
Switch# show nmsp statistics connection
NMSP Connection Counters
----------------------------------
Connection 1:
   Connection status: UP
   Freed connection: 0

   Tx message count       Rx message count
   ------------------------     ------------------------
   Subscr Resp: 1            Subscr Req: 1
   Capa Notif: 1              Capa Notif: 1
   Atta Resp: 1                Atta Req: 1
   Atta Notif: 0
   Loc Resp: 1                 Loc Req: 1
   Loc Notif: 0
Unsupported msg: 0

Switch# show nmsp statistics summary
NMSP Global Counters
----------------------------
  Send too big msg: 0
  Failed socket write: 0
  Partial socket write: 0
  Socket write would block: 0
  Failed socket read: 0
  Socket read would block: 0
  Transmit Q full: 0
  Max Location Notify Msg: 0
  Max Attachment Notify Msg: 0
Max Tx Q Size: 0
```

次の例では、**show nmsp status** コマンドの出力を示します。

```
Switch# show nmsp status
NMSP Status
----------------
NMSP: enabled
MSE IP Address    TxEchoResp RxEchoReq TxData RxData
172.19.35.109       5 5 4 4
```

次の例では、**show nmsp show subscription detail** コマンドと **show nmsp show subscription summary** コマンドの出力を示します。

```
Switch# show nmsp subscription detail
Mobility Services Subscribed by 172.19.35.109:
Services                Subservices
-----------------       -------------------
Attachment:           Wired Station
Location:               Subscription

Switch# show nmsp subscription summary
Mobility Services Subscribed:
MSE IP Address     Services
--------------------      ---------------------
172.19.35.109       Attachment, Location
```

関連コマンド

コマンド	説明
clear nmsp statistics	NMSP 統計カウンタをクリアします。
nmsp	スイッチ上で Network Mobility Services Protocol（NMSP）をイネーブルにします。

show pagp

Port Aggregation Protocol（PAgP; ポート集約プロトコル）チャネル グループ情報を表示するには、**show pagp** ユーザ EXEC コマンドを使用します。

show pagp [*channel-group-number*] {**counters** | **dual-active** | **internal** | **neighbor**} [| {**begin** | **exclude** | **include**} *expression*]]

構文の説明

channel-group-number	（任意）チャネル グループの番号です。指定できる範囲は 1 ～ 48 です。
counters	トラフィック情報を表示します。
dual-active	デュアル アクティブ ステータスを表示します。
internal	内部情報を表示します。
neighbor	ネイバー情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(25)SE	*channel-group-number* 範囲が 1 ～ 12 から 1 ～ 48 に変更されました。
12.2(46)SE	**dual-active** キーワードが追加されました。

使用上のガイドライン

show pagp コマンドを入力すると、アクティブなチャネル グループの情報が表示されます。非アクティブ ポート チャネルの情報を表示するには、チャネル グループ番号を指定して **show pagp** コマンドを入力します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show pagp 1 counters** コマンドの出力を示します。

```
Switch> show pagp 1 counters
             Information        Flush
Port         Sent   Recv     Sent   Recv
--------------------------------------
Channel group: 1
Gi1/0/1    45     42       0      0
  Gi1/0/2    45     41       0      0
```

次の例では、**show pagp 1 internal** コマンドの出力を示します。

```
Switch> 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
                                  Hello    Partner  PAgP     Learning  Group
Port        Flags State   Timers  Interval Count   Priority   Method  Ifindex
Gi1/0/1     SC    U6/S7   H       30s      1        128        Any      16
Gi1/0/2     SC    U6/S7   H       30s      1        128        Any      16
```

次の例では、**show pagp 1 neighbor** コマンドの出力を示します。

```
Switch> show pagp 1 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              Partner          Partner           Partner Group
    Port        Name                 Device ID        Port         Age  Flags   Cap.
    Gi1/0/1     switch-p2            0002.4b29.4600   Gi01//1        9s SC      10001
    Gi1/0/2     switch-p2            0002.4b29.4600   Gi1/0/2       24s SC      10001
```

次の例では、**show pagp dual-active** コマンドの出力を示します。

```
Switch> show pagp dual-active
PAgP dual-active detection enabled: Yes
PAgP dual-active version: 1.1

Channel group 1
          Dual-Active     Partner              Partner   Partner
Port      Detect Capable  Name                 Port      Version
Gi1/0/1   No              Switch               Gi3/0/3   N/A
Gi1/0/2   No              Switch               Gi3/0/4   N/A

<output truncated>
```

関連コマンド

コマンド	説明
clear pagp	PAgP チャネル グループ情報をクリアします。

show policy-map

着信トラフィックの分類基準を定義する Quality of Service（QoS）ポリシー マップを表示するには、**show policy-map** ユーザ EXEC コマンドを使用します。ポリシー マップには、帯域幅制限および制限を超過した場合の対処法を指定するポリサーを格納できます。

show policy-map [*policy-map-name* [**class** *class-map-name*]] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

policy-map-name	（任意）指定されたポリシー マップの名前を表示します。
class *class-map-name*	（任意）各クラスの QoS ポリシー アクションを表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

（注）**control-plane** および **interface** キーワードは、コマンドラインのヘルプ ストリングには表示されますが、サポートされていません。表示されている統計情報は無視してください。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show policy-map** コマンドの出力を示します。

```
Switch> show policy-map
Policy Map videowizard_policy2
  class  videowizard_10-10-10-10
   set dscp 34
   police 100000000 2000000 exceed-action drop

 Policy Map mypolicy
  class  dscp5
   set dscp 6
```

関連コマンド

コマンド	説明
policy-map	複数のポートに接続可能なポリシー マップを作成または変更して、サービス ポリシーを指定します。

show port-security

インターフェイスまたはスイッチのポート セキュリティ設定を表示するには、**show port-security** 特権 EXEC コマンドを使用します。

show port-security [**interface** *interface-id*] [**address** | **vlan**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface *interface-id*	（注）	（任意）指定されたインターフェイスのポート セキュリティ設定を表示します。有効なインターフェイスには、物理ポート（タイプ、スタック メンバ、モジュール、ポート番号を含む）が含まれます。
address		（任意）すべてのポートまたは指定されたポート上のすべてのセキュア MAC アドレスを表示します。
vlan		（任意）指定されたインターフェイスのすべての VLAN のポート セキュリティ設定を表示します。このキーワードは、スイッチポート モードが **trunk** に設定されているインターフェイス上だけで表示されます。
| begin		（任意）*expression* と一致する行から表示を開始します。
| exclude		（任意）*expression* と一致する行を表示から除外します。
| include		（任意）指定された *expression* と一致する行を表示に含めます。
expression		参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**vlan** キーワードが追加されました（トランク ポートだけで表示）。

使用上のガイドライン

キーワードを指定しないでこのコマンドを入力すると、スイッチのすべてのセキュア ポートの管理ステータスおよび動作ステータスが出力されます。

interface-id を入力した場合、コマンドはインターフェイスのポート セキュリティ設定を表示します。

address キーワードを指定してコマンドを入力すると、すべてのインターフェイスのセキュア MAC アドレス、および各セキュア アドレスのエージング情報が表示されます。

interface-id キーワードおよび **address** キーワードを指定してコマンドを入力すると、各セキュア アドレスのエージング情報を持ったインターフェイスの MAC アドレスがすべて表示されます。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でない場合も、このコマンドを使用して、そのインターフェイスの MAC アドレスをすべて表示できます。

vlan キーワードを指定してコマンドを入力すると、インターフェイスの VLAN すべてに対するセキュア MAC アドレスの最大設定数および現在数が表示されます。このオプションは、スイッチポート モードが **trunk** に設定されているインターフェイス上だけで表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show port-security** コマンドの出力を示します。

```
Switch# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                    (Count)        (Count)      (Count)
--------------------------------------------------------------------------------
     Gi1/0/1         1             0             0             Shutdown
--------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 6272
```

次の例では、**show port-security interface** *interface-id* コマンドの出力を示します。

```
Switch# show port-security interface gigabitethernet1/0/1
Port Security : Enabled
Port status : SecureUp
Violation mode : Shutdown
Maximum MAC Addresses : 1
Total MAC Addresses : 0
Configured MAC Addresses : 0
Aging time : 0 mins
Aging type : Absolute
SecureStatic address aging : Disabled
Security Violation count : 0
```

次の例では、**show port-security address** コマンドの出力を示します。

```
Switch# show port-security address
Secure Mac Address Table
-------------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                         (mins)
----    -----------       ----                -----   -------------
   1    0006.0700.0800    SecureConfigured    Gi1/0/2     1
-------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 6272
```

次の例では、**show port-security interface gigabitethernet**1/0/**2 address** コマンドの出力を示します。

```
Switch# show port-security interface gigabitethernet1/0/2 address
          Secure Mac Address Table
-------------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                         (mins)
----    -----------       ----                -----   -------------
   1    0006.0700.0800    SecureConfigured    Gi1/0/2     1
-------------------------------------------------------------------
Total Addresses: 1
```

次の例では、**show port-security interface** *interface-id* **vlan** コマンドの出力を示します。

```
Switch# show port-security interface gigabitethernet1/0/2 vlan
Default maximum:not set, using 5120
VLAN  Maximum    Current
    5    default          1
   10    default         54
   11    default        101
   12    default        101
   13    default        201
   14    default        501
```

関連コマンド

コマンド	説明
clear port-security	MAC アドレス テーブルからスイッチ上またはインターフェイス上の特定のタイプのセキュア アドレスまたはすべてのセキュア アドレスを削除します。
switchport port-security	ポート上でポート セキュリティをイネーブルにし、ポートの使用対象をユーザ定義のステーション グループに制限し、セキュア MAC アドレスを設定します。

show power inline

指定された Power over Ethernet（PoE）ポートまたはすべての PoE ポートの PoE ステータスを表示するには、**show power inline** ユーザ EXEC コマンドを使用します。

show power inline [[*interface-id* | **consumption**] | **module** *switch-number*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface-id	（任意）指定されたインターフェイスの PoE 関連電力管理情報を表示します。
consumption	（任意）PoE ポートに接続した装置に割り当てられた電力を表示します。
module *switch-number*	**（注）**（任意）指定されたスタック メンバのポートだけを表示します。スイッチ番号は 1 ～ 9 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。
12.2(25)SEC	**consumption** キーワードが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、output を含む行は表示されませんが、Output を含む行は表示されます。

例

次の例では、**show power inline** コマンドの出力を示します。出力では、ポート 2 がスタティックに設定されており、電力がこのポートに事前に割り当てられていますが、受電装置は接続されていません。ポート 6 は、最大ワット数が 10 W に設定されているために power-deny ステートになっているスタティック ポートです。接続された受電装置には、Class 0 または Class 3 装置について報告されたクラスの最大ワット数が設定されています。表 2-38 に、出力フィールドの説明を示します。

```
Switch> show power inline
Module   Available     Used     Remaining
          (Watts)     (Watts)    (Watts)
------   ---------   --------   ---------
1            370.0      114.9       255.1
2            370.0       34.3       335.

Interface Admin  Oper       Power   Device               Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Fa1/0/1   auto   on         6.3     IP Phone 7910       n/a   15.4
Fa1/0/2   static off        15.4    n/a                 n/a   15.4
Fa1/0/3   auto   on         6.3     IP Phone 7910       n/a   15.4
```

```
Fa1/0/4   auto   on         6.3     IP Phone 7960       2     15.4
Fa1/0/5   static on         15.4    IP Phone 7960       2     15.4
Fa1/0/6   static power-deny 10.0    n/a                 n/a   10.0
Fa1/0/7   auto   on         6.3     IP Phone 7910       n/a   15.4
<output truncated>
```

次の例では、ポートでの **show power inline** コマンドの出力を示します。

```
Switch> show power inline fastethernet2/0/1
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Fa2/0/1   auto   on         6.3     IP Phone 7910       n/a   15.4
```

次の例では、すべての PoE スイッチ ポートの **show power inline consumption** コマンドの出力を示します。

```
Switch> show power inline consumption
Default PD consumption : 15400 mW
```

次の例では、スタック メンバ 1 での **show power inline module** *switch-number* コマンドの出力を示します。

```
Switch> show power inline module 1
Module   Available     Used     Remaining
          (Watts)     (Watts)    (Watts)
------   ---------   --------   ---------
1           370.0      166.2       203.9
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Fa1/0/1   auto   on         6.3     IP Phone 7910       n/a   15.4
Fa1/0/2   auto   on         6.3     IP Phone 7910       n/a   15.4
Fa1/0/3   auto   on         6.3     IP Phone 7910       n/a   15.4
Fa1/0/4   auto   on         6.3     IP Phone 7910       n/a   15.4
Fa1/0/5   auto   on         6.3     IP Phone 7910       n/a   15.4
Fa1/0/6   auto   on         6.3     IP Phone 7910       n/a   15.4
<output truncated>
```

表 2-38　show power inline interface のフィールドの説明

フィールド	説明
Admin	管理モード：auto、off、static
Oper	動作モード： • on：受電装置が検出され、電力が適用されています。 • off：PoE が適用されていません。 • faulty：装置検出または受電装置が障害の状態です。 • power-deny：受電装置が検出されていますが、PoE が使用できない状態か、最大ワット数が検出された受電装置の最大数を超えています。
Power	PoE の供給ワット数
Device	検出された装置のタイプ：n/a、unknown、Cisco powered-device、IEEE powered-device、<CDP からの名前>
Class	IEEE 分類：n/a、Class <0 ～ 4>
Available	システム内の PoE の総数

表 2-38　show power inline interface のフィールドの説明 （続き）

フィールド	説明
Used	ポートに割り当てられている PoE の数
Remaining	システム内でポートに割り当てられていない PoE の数 （Available - Used = Remaining）

関連コマンド

コマンド	説明
logging event power-inline-status	PoE イベントのロギングをイネーブルにします。
power inline	指定した PoE ポートまたはすべての PoE ポートの電力管理モードを設定します。
show controllers power inline	指定した PoE コントローラのレジスタ値を表示します。

show sdm prefer

特定の機能に対するシステム リソースの割り当てに使用できる Switch Database Management（SDM）テンプレートに関する情報を表示するには、**show sdm prefer** 特権 EXEC コマンドを使用します。使用中のテンプレートを表示するには、キーワードを指定せずにこのコマンドを使用します。

show sdm prefer [**access** | **default** | **dual-ipv4-and-ipv6** {**default** | **routing** | **vlan**} | **routing** | **vlan** [**desktop**]] **[** | {**begin** | **exclude** | **include**} *expression*]

構文の説明

access	（任意）ACL 用のシステム リソースを最大化するテンプレートを表示します。
default	（任意）機能間のシステム リソースのバランスをとるテンプレートを表示します。
dual-ipv4-and-ipv6 {**default** | **routing** | **vlan**}	（任意）IPv4 と IPv6 の両方をサポートするデュアル テンプレートを表示します。 • **default** : デフォルトのデュアル テンプレート設定を表示します。 • **routing** : ルーティングのデュアル テンプレート設定を表示します。 • **vlan** : VLAN デュアル テンプレート設定を表示します。
routing	（任意）ルーティング用のシステム リソースを最大化するテンプレートを表示します。
vlan	（任意）レイヤ 2 VLAN 用のシステム リソースを最大化するテンプレートを表示します。
desktop	（任意）Catalyst 3750-12S アグリゲータ スイッチ専用で、デスクトップのテンプレートを表示します。このスイッチでは、**desktop** キーワードを入力しない場合、アグリゲータ テンプレートが表示されます。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**desktop** キーワードが追加されました。
12.2(25)SE	**dual-ipv4-and-ipv6** {**default** | **vlan**} キーワードが追加されました。
12.2(25)SED	**access** キーワードが追加されました。
12.2(25)SEE	**routing** デュアル IPv4 および IPv6 テンプレート用のキーワードが追加されました。

使用上のガイドライン

sdm prefer グローバル コンフィギュレーション コマンドを使用し、SDM テンプレートを変更した場合は、設定の変更を有効にするためスイッチをリロードする必要があります。**reload** 特権 EXEC コマンドを入力する前に、**show sdm prefer** コマンドを入力すると、**show sdm prefer** コマンドにより、現在使用しているテンプレートおよびリロード後にアクティブになるテンプレートが表示されます。

各テンプレートで表示される番号は、各機能のリソースにおけるおおよその最大数になります。他に設定された機能の実際の数字にもよるため、実際の数字とは異なる場合があります。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show sdm prefer** コマンドの出力を示します。使用中のテンプレートが示されています。

```
Switch# show sdm prefer
The current template is "desktop default" template.
The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:             6K
  number of igmp groups + multicast routes:    1K
  number of unicast routes:                    8K
    number of directly connected hosts:        6K
    number of indirect routes:                 2K
  number of policy based routing aces:         0
  number of qos aces:                          512
  number of security aces:                     1K
```

次の例では、アグリゲータ スイッチ上で入力された **show sdm prefer routing** コマンドの出力を示します。

```
Switch# show sdm prefer routing
"aggregate routing" template:
The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:             6K
  number of igmp groups + multicast routes:    1K
  number of unicast routes:                    20K
    number of directly connected hosts:        6K
    number of indirect routes:                 14K
  number of policy based routing aces:         512
  number of qos aces:                          512
  number of security aces:                     1K
```

次の例では、デスクトップ スイッチ上で入力された **show sdm prefer routing** コマンドの出力を示します。

```
Switch# show sdm prefer routing
"desktop routing" template:
The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:             3K
  number of igmp groups + multicast routes:    1K
  number of unicast routes:                    11K
    number of directly connected hosts:        3K
    number of indirect routes:                 8K
  number of policy based routing aces:         512
  number of qos aces:                          512
```

```
  number of security aces:                      1K
```

次の例では、デスクトップ スイッチ上で入力された **show sdm prefer dual-ipv4-and-ipv6 default** コマンドの出力を示します。

```
Switch# show sdm prefer dual-ipv4-and-ipv6 default
 "desktop IPv4 and IPv6 default" template:
The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:                  2K
  number of IPv4 IGMP groups + multicast routes:    1K
  number of IPv4 unicast routes:                    3K
    number of directly-connected IPv4 hosts:        2K
    number of indirect IPv4 routes:                 1K
  number of IPv6 multicast groups:                  1K
  number of directly-connected IPv6 addresses:      2K
  number of indirect IPv6 unicast routes:           1K
  number of IPv4 policy based routing aces:         0
  number of IPv4/MAC qos aces:                      512
  number of IPv4/MAC security aces:                 1K
  number of IPv6 policy based routing aces:         0
  number of IPv6 qos aces:                          510
  number of IPv6 security aces:                     510
```

次の例では、新しいテンプレートを設定し、まだリロードしていないスイッチ上での **show sdm prefer** コマンドの出力を示します。

```
Switch# show sdm prefer
 The current template is "desktop routing" template.
The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:            3K
  number of igmp groups + multicast routes:   1K
  number of unicast routes:                   11K
    number of directly connected hosts:       3K
    number of indirect routes:                8K
  number of qos aces:                         512
  number of security aces:                    1K

 On next reload, template will be "desktop vlan" template.
```

関連コマンド

コマンド	説明
sdm prefer	SDM テンプレートを、ルーティングまたは VLAN のリソースを最大限に活用するように設定、デフォルト テンプレートを使用するように設定、デュアル IPv4/IPv6 テンプレートを選択するように設定、またはデスクトップ、アグリゲータ テンプレートを選択するように設定します。

show setup express

Express Setup モードがスイッチでアクティブかどうかを表示するには、**show setup express** 特権 EXEC コマンドを使用します。

show setup express [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

例

次の例は、**show setup express** コマンドの出力を示しています。

```
Switch# show setup express
express setup mode is active
```

関連コマンド

コマンド	説明
setup express	Express Setup モードをイネーブルにします。

show spanning-tree

スパニングツリーの状態情報を表示するには、**show spanning-tree** ユーザ EXEC コマンドを使用します。

show spanning-tree [*bridge-group* | **active** [**detail**] | **backbonefast** | **blockedports** | **bridge** | **detail** [**active**] | **inconsistentports** | **interface** *interface-id* | **mst** | **pathcost method** | **root** | **summary** [**totals**] | **uplinkfast** | **vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree *bridge-group* [**active** [**detail**] | **blockedports** | **bridge** | **detail** [**active**] | **inconsistentports** | **interface** *interface-id* | **root** | **summary**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree vlan *vlan-id* [**active** [**detail**] | **blockedports** | **bridge** | **detail** [**active**] | **inconsistentports** | **interface** *interface-id* | **root** | **summary**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree {**vlan** *vlan-id* | *bridge-group*} **bridge** [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **priority** [**system-id**] | **protocol**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree {**vlan** *vlan-id* | *bridge-group*} **root** [**address** | **cost** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **port** | **priority** [**system-id**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree interface *interface-id* [**active** [**detail**] | **cost** | **detail** [**active**] | **inconsistency** | **portfast** | **priority** | **rootcost** | **state**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree mst [**configuration** [digest]] | [*instance-id* [**detail** | **interface** *interface-id* [**detail**]] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

bridge-group	（任意）ブリッジ グループ番号を指定します。指定できる範囲は 1 ～ 255 です。
active [**detail**]	（任意）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します（特権 EXEC モードの場合だけ使用可能）。
backbonefast	（任意）スパニング ツリー BackboneFast ステータスを表示します。
blockedports	（任意）ブロックされたポートの情報を表示します（特権 EXEC モードの場合だけ使用可能）。
bridge [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **priority** [**system-id**] | **protocol**]	（任意）このスイッチのステータスおよび設定を表示します（オプションのキーワードは特権 EXEC モードの場合だけ使用可能）。
detail [**active**]	（任意）インターフェイス情報の詳細サマリーを表示します（**active** キーワードは特権 EXEC モードの場合だけ使用可能）。
inconsistentports	（任意）矛盾するポートの情報を表示します（特権 EXEC モードの場合だけ使用可能）。

interface *interface-id* [**active** [**detail**] | **cost** | **detail** [**active**] | **inconsistency** | **portfast** | **priority** | **rootcost** | **state**]	（任意）指定されたインターフェイスのスパニング ツリー情報を表示します（**portfast** および **state** 以外のすべてのオプションは特権 EXEC モードの場合だけ使用可能）。各インターフェイスは、スペースで区切って入力します。インターフェイスの範囲は入力できません。有効なインターフェイスには、物理ポート、VLAN、およびポート チャネルが含まれます。指定できる VLAN 範囲は 1 ～ 4094 です。ポート チャネル範囲は 1 ～ 48 です。
mst [**configuration** [**digest**]] [*instance-id* [**detail** | **interface** *interface-id* [**detail**]]	（任意）Multiple Spanning-Tree（MST）のリージョン設定およびステータスを表示します（特権 EXEC モードの場合だけ使用可能）。 キーワードの意味は次のとおりです。 • **digest** :（任意）現在の MST 設定 ID（MSTCI）に含まれる MD5 ダイジェストを表示します。1 つは標準スイッチ、もう 1 つは先行標準スイッチ用の 2 つの別個ダイジェストが表示されます（特権 EXEC モードの場合だけ使用可能）。 IEEE 標準の実装のために専門用語が更新され、*txholdcount* フィールドが追加されました。 境界ポート用に新しいマスター ロールが表示されます。 IEEE 標準ブリッジがポートに先行標準 BPDU を送信した場合、*pre-standard* または *Pre-STD* という用語が表示されます。 ポートが先行標準 BPDU を送信するように設定され、ポートで先行標準 BPDU が受信されなかったとき、*pre-standard (config)* または *Pre-STD-Cf* という用語が表示されます。 先行標準 BPDU を送信するように設定されていないポートで先行標準 BPDU が受信された場合、*pre-standard (rcvd)* または *Pre-STD-Rx* という用語が表示されます。 下位指定情報が指定ポートで受信された場合、指定ポートがフォワーディング ステートに戻るか指定が中止されるまで、*dispute* フラグが表示されます。 • *instance-id* : 1 つのインスタンス ID、それぞれをハイフンで区切った ID の範囲、またはカンマで区切った一連の ID を指定できます。指定できる範囲は 1 ～ 4094 です。現在設定されているインスタンス数が表示されます。 • **interface** *interface-id* :（任意）有効なインターフェイスには、物理ポート、VLAN、およびポート チャネルが含まれます。指定できる VLAN 範囲は 1 ～ 4094 です。ポート チャネル範囲は 1 ～ 48 です。 • **detail** :（任意）インスタンスまたはインターフェイスの詳細情報を表示します。
pathcost method	（任意）デフォルトのパス コスト方式を表示します（特権 EXEC モードの場合だけ使用可能）。
root [**address** | **cost** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **port** | **priority** [**system-id**]]	（任意）ルート スイッチのステータスおよび設定を表示します（すべてのキーワードは特権 EXEC モードの場合だけ使用可能）。
summary [**totals**]	（任意）ポート状態のサマリー、またはスパニング ツリー ステート セクションの総行数を表示します。*IEEE Standard* という語は、スイッチ上で実行されている MST バージョンを識別します。

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* [**active** [**detail**] | **backbonefast** | **blockedports** | **bridge** [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **priority** [**system-id**] | **protocol**]	（任意）指定された VLAN のスパニング ツリー情報を表示します（キーワードの一部は特権 EXEC モードの場合だけ使用可能）。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**mst** キーワードおよびオプションが追加されました。

使用上のガイドライン

vlan-id 変数を省略した場合は、すべての VLAN のスパニング ツリー インスタンスにコマンドが適用されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show spanning-tree active** コマンドの出力を示します。

```
Switch# show spanning-tree active
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0001.42e2.cdd0
             Cost        3038
             Port        24 (GigabitEthernet2/0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    49153  (priority 49152 sys-id-ext 1)
             Address     0003.fd63.9580
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
  Uplinkfast enabled

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi2/0/1          Root FWD 3019      128.24   P2p
<output truncated>
```

次の例では、**show spanning-tree detail** コマンドの出力を示します。

```
Switch# show spanning-tree detail
VLAN0001 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 49152, sysid 1, address 0003.fd63.9580
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address 0001.42e2.cdd0
  Root port is 1 (GigabitEthernet2/0/1), cost of root path is 3038
  Topology change flag not set, detected flag not set
  Number of topology changes 0 last change occurred 1d16h ago
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300
  Uplinkfast enabled

 Port 1 (GigabitEthernet2/0/1) of VLAN0001 is forwarding
   Port path cost 3019, Port priority 128, Port Identifier 128.24.
   Designated root has priority 32768, address 0001.42e2.cdd0
   Designated bridge has priority 32768, address 00d0.bbf5.c680
   Designated port id is 128.25, designated path cost 19
   Timers: message age 2, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   BPDU: sent 0, received 72364
<output truncated>
```

次の例では、**show spanning-tree interface** *interface-id* コマンドの出力を示します。

```
Switch# show spanning-tree interface gigabitethernet2/0/1
Vlan             Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
VLAN0001         Root FWD 3019      128.24   P2p

Switch# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfiguration guard is enabled
Extended system ID   is enabled
Portfast             is disabled by default
PortFast BPDU Guard  is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard            is disabled by default
UplinkFast           is enabled
BackboneFast         is enabled
Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                  1        0         0        11         12
VLAN0002                  3        0         0        1          4
VLAN0004                  3        0         0        1          4
VLAN0006                  3        0         0        1          4
VLAN0031                  3        0         0        1          4
VLAN0032                  3        0         0        1          4
<output truncated>
---------------------- -------- --------- -------- ---------- ----------
37 vlans                  109      0         0        47         156
Station update rate set to 150 packets/sec.

UplinkFast statistics
-----------------------
Number of transitions via uplinkFast (all VLANs)            : 0
Number of proxy multicast addresses transmitted (all VLANs) : 0
```

```
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
```

次の例では、**show spanning-tree mst configuration** コマンドの出力を示します。

```
Switch# show spanning-tree mst configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
--------  ------------------
0         1-9,21-4094
1         10-20
----------------------------
```

次の例では、**show spanning-tree mst interface** *interface-id* コマンドの出力を示します。

```
Switch# show spanning-tree mst interface gigabitethernet2/0/1
GigabitEthernet2/0/1 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       (STP)            bpdu guard : disable     (default)
Bpdus sent 5, received 74

Instance role state cost      prio vlans mapped
0        root FWD   200000    128  1,12,14-4094
```

次の例では、**show spanning-tree mst 0** コマンドの出力を示します。

```
Switch# show spanning-tree mst 0
###### MST00        vlans mapped: 1-9,21-4094
Bridge      address 0002.4b29.7a00  priority  32768 (32768 sysid 0)
Root        address 0001.4297.e000  priority  32768 (32768 sysid 0)
            port    Gi1/0/1         path cost 200038
IST master *this switch
Operational hello time 2, forward delay 15, max age 20, max hops 20
Configured  hello time 2, forward delay 15, max age 20, max hops 20

Interface              role state cost      prio type
--------------------   ---- ----- --------- ---- --------------------------------
GigabitEthernet2/0/1   root FWD   200000    128  P2P bound(STP)
GigabitEthernet2/0/2   desg FWD   200000    128  P2P bound(STP)
Port-channel1          desg FWD   200000    128  P2P bound(STP)
```

関連コマンド

コマンド	説明
clear spanning-tree counters	スパニング ツリーのカウンタをクリアします。
clear spanning-tree detected-protocols	プロトコル移行プロセスを再開します。
spanning-tree backbonefast	BackboneFast 機能をイネーブルにします。
spanning-tree bpdufilter	インターフェイスでの UniDirectional Link Detection（UDLD; 単一方向リンク検出）の送受信を禁止します。
spanning-tree bpduguard	BPDU を受信したインターフェイスを、errdisable ステートにします。
spanning-tree cost	スパニング ツリーの計算に使用するパス コストを設定します。

コマンド	説明
spanning-tree extend system-id	拡張システム ID 機能をイネーブルにします。
spanning-tree guard	選択されたインターフェイスに対応するすべての VLAN に対して、ルート ガード機能またはループ ガード機能をイネーブルにします。
spanning-tree link-type	スパニング ツリーがフォワーディング ステートに高速移行するように、デフォルト リンクタイプ設定を上書きします。
spanning-tree loopguard default	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ないようにします。
spanning-tree mst configuration	Multiple Spanning-Tree（MST）リージョンを設定するための MST コンフィギュレーション モードを開始します。
spanning-tree mst cost	MST の計算に使用するパス コストを設定します。
spanning-tree mst forward-time	すべての MST インスタンスについて転送遅延時間を設定します。
spanning-tree mst hello-time	ルート スイッチ コンフィギュレーション メッセージが送信する hello BPDU の間隔を設定します。
spanning-tree mst max-age	スパニング ツリーがルート スイッチからメッセージを受信する間隔を設定します。
spanning-tree mst max-hops	BPDU をドロップしてインターフェイス用に保持していた情報を期限切れにするまでの、MST リージョンでのホップ数を設定します。
spanning-tree mst port-priority	インターフェイス プライオリティを設定します。
spanning-tree mst priority	指定したスパニング ツリー インスタンスのスイッチ プライオリティを設定します。
spanning-tree mst root	ネットワークの直径に基づいて、MST ルート スイッチのプライオリティおよびタイマーを設定します。
spanning-tree port-priority	インターフェイス プライオリティを設定します。
spanning-tree portfast（グローバル コンフィギュレーション）	PortFast 対応インターフェイス上で BPDU フィルタリング機能または BPDU ガード機能をグローバルにイネーブルにするか、またはすべての非トランク インターフェイスで PortFast 機能をイネーブルにします。
spanning-tree portfast（インターフェイス コンフィギュレーション）	特定のインターフェイスおよび対応するすべての VLAN 上で、PortFast 機能をイネーブルにします。
spanning-tree uplinkfast	リンクまたはスイッチに障害がある場合、またはスパニング ツリーが自動的に再設定された場合に、新しいルート ポートを短時間で選択できるようにします。
spanning-tree vlan	VLAN 単位でスパニング ツリーを設定します。

show storm-control

スイッチまたは指定されたインターフェイス上で、ブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御の設定を表示したり、ストーム制御履歴を表示したりするには、**show storm-control** ユーザ EXEC コマンドを使用します。

show storm-control [*interface-id*] [**broadcast** | **multicast** | **unicast**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface-id	（注）	（任意）物理ポートのインターフェイス ID（タイプ、スタック メンバ、モジュール、ポート番号を含む）
broadcast		（任意）ブロードキャスト ストームしきい値設定を表示します。
multicast		（任意）マルチキャスト ストームしきい値設定を表示します。
unicast		（任意）ユニキャスト ストームしきい値設定を表示します。
| begin		（任意）*expression* と一致する行から表示を開始します。
| exclude		（任意）*expression* と一致する行を表示から除外します。
| include		（任意）指定された *expression* と一致する行を表示に含めます。
expression		参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

interface-id を入力すると、指定されたインターフェイスのストーム制御しきい値が表示されます。

interface-id を入力しない場合、スイッチ上のポートすべてのトラフィック タイプの設定が表示されます。

トラフィック タイプを入力しない場合は、ブロードキャスト ストーム制御の設定が表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、キーワードを指定せずに入力した **show storm-control** コマンドの出力の一部を示します。トラフィック タイプのキーワードが入力されてないため、ブロードキャスト ストーム制御の設定が表示されます。

```
Switch> show storm-control
Interface    Filter State   Upper       Lower      Current
---------    -------------  ----------  ---------  ---------
Gi1/0/1      Forwarding     20 pps      10 pps     5 pps
Gi1/0/2      Forwarding     50.00%      40.00%     0.00%
<output truncated>
```

次の例では、指定されたインターフェイスの **show storm-control** コマンドの出力を示します。トラフィック タイプのキーワードが入力されてないため、ブロードキャスト ストーム制御の設定が表示されます。

```
Switch> show storm-control gigabitethernet 1/0/1
Interface    Filter State   Upper       Lower      Current
---------    -------------  ----------  ---------  ---------
Gi1/0/1      Forwarding     20 pps      10 pps     5 pps
```

表 2-39 に、**show storm-control** の出力で表示されるフィールドの説明を示します。

表 2-39　show storm-control のフィールドの説明

フィールド	説明
Interface	インターフェイスの ID を表示します。
Filter State	フィルタのステータスを表示します。 • blocking：ストーム制御はイネーブルであり、ストームが発生しています。 • forwarding：ストーム制御はイネーブルであり、ストームは発生していません。 • Inactive：ストーム制御はディセーブルです。
Upper	上限抑制レベルを利用可能な全帯域幅のパーセンテージとして、毎秒のパケット数または毎秒のビット数で表示します。
Lower	下限抑制レベルを利用可能な全帯域幅のパーセンテージとして、毎秒のパケット数または毎秒のビット数で表示します。
Current	ブロードキャスト トラフィックまたは指定されたトラフィック タイプ（ブロードキャスト、マルチキャスト、ユニキャスト）の帯域幅の使用状況を、利用可能な全帯域幅のパーセンテージで表示します。このフィールドは、ストーム制御がイネーブルの場合だけ有効です。

関連コマンド

コマンド	説明
storm-control	スイッチにブロードキャスト、マルチキャスト、およびユニキャスト ストーム制御レベルを設定します。

show switch

スタック メンバまたはスイッチ スタックに関連した情報を表示するには、**show switch** ユーザ EXEC コマンドを使用します。

show switch [*stack-member-number* | **detail** | **neighbors** | **stack-ports**[**summary**] | **stack-ring activity** [**detail**] | **speed**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

stack-member-number	（任意）指定されたメンバの情報を表示します。指定できる範囲は 1 ～ 9 です。
detail	（任意）スタック リングの詳細情報を表示します。
neighbors	（任意）スタック全体のネイバーを表示します。
stack-ports	（任意）スタック全体のポート情報を表示します。
stack-ports [**summary**]	（任意）StackWise ケーブルの長さ、スタック リンク ステータス、およびループバック ステータスを表示します。
stack-ring activity [**detail**]	（任意）スタック リングに送信されたフレーム数を、メンバ単位で表示します。スタック リング、受信キュー、および ASIC に送信されるフレーム数をメンバ単位で表示するには、**detail** キーワードを使用します。
stack-ring speed	（任意）スタック リングの速度を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	表示が、Switch Database Management（SDM）のミスマッチも含むよう拡張されました。
12.2(20)SE	表示が、プロビジョニング情報も含むよう拡張されました。**stack-ring activity** [**detail**] キーワードが追加されました。
12.2(50)SE	表示が、StackWise ケーブル、リンク、およびループバック情報を含むよう拡張されました。**stack ports** [**summary**] キーワードが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

このコマンドでは、次のステートが表示されます。

- Waiting：スイッチは起動中で、スタック内にある他のスイッチからの通信を待っています。スイッチはまだスタック マスターであるかどうかを判別していません。

  スタック マスター選出に参加していないスタック メンバは、スタック マスターが選出され準備ができるまで Waiting ステートのままです。

- Initializing：スイッチがそのスタック マスター ステータスを判別しました。スイッチがスタック マスターでない場合、このスイッチはスタック マスターからシステム レベルおよびインターフェイス レベルの設定を受信してロードしています。
- Ready：メンバがシステム レベルおよびインターフェイス レベルの設定のロードを完了し、トラフィックを転送できるようになっています。
- Master Re-Init：マスターの再選出で、異なるメンバがマスターに選出された直後のステート。新しいマスターがその設定を再初期化しています。このステートは、新しいマスターだけに適用されます。
- Ver Mismatch：Version-Mismatch モードのスイッチ。Version-Mismatch モードは、スタックに加入しているスイッチに、マスターとは異なるスタック プロトコル マイナー バージョン番号がある状態です。
- SDM Mismatch：Switch Database Management（SDM）ミスマッチ モードのスイッチ。SDM ミスマッチは、マスターで実行している SDM テンプレートをメンバがサポートしていない状態です。
- Provisioned：事前設定されたスイッチが、スタックのアクティブ メンバになる前のステート、またはスタック メンバがスタックから脱退した後のステート。プロビジョニングされたスイッチでは、MAC アドレスおよびプライオリティ番号は、常に 0 と表示されます。

起動中のメンバ（マスターを含む）の代表的なステート遷移は、Waiting -> Initializing -> Ready です。

マスター選出後にマスターになるメンバの代表的なステート遷移は、Ready -> Master Re-Init -> Ready です。

Version-Mismatch モードのメンバの代表的なステート遷移は、Waiting -> Ver Mismatch です。

スタックにプロビジョニングされたスイッチが存在するかどうかを識別するには、**show switch** コマンドを使用できます。**show running-config** および **show startup-config** 特権 EXEC コマンドでは、この情報は提供されません。

永続的 MAC アドレスがイネーブルになっている場合、スタックの MAC-persistency wait-time も表示されます。

例

次の例では、スタックのサマリー情報を示します。

```
Switch> show switch
                                                Current
Switch#  Role      Mac Address     Priority     State
-------------------------------------------------------
 6       Member    0003.e31a.1e00     1         Ready
*8       Master    0003.e31a.1200     1         Ready
 2       Member    0000.000.0000      0         Provisioned
```

次の例では、スタックの詳細情報を示します。

```
Switch> show switch detail
Switch/Stack Mac Address : 0013.c4db.7e00
Mac persistency wait time: 4 mins
                                            H/W   Current
Switch#  Role   Mac Address     Priority Version  State
-----------------------------------------------------------
*1       Master 0013.c4db.7e00     1      0       Ready
 2       Member 0000.000.0000      0      0       Provisioned
 6       Member 0003.e31a.1e00     1      0       Ready


         Stack Port Status             Neighbors
Switch#  Port 1     Port 2           Port 1   Port 2
-----------------------------------------------------------
```

```
  1        Ok        Down              6        None
  6        Down      Ok                None       1
```

次の例では、メンバ 6 のサマリー情報を示します。

```
Switch> show switch 6
                                                Current
Switch#  Role      Mac Address     Priority     State
-------------------------------------------------------
 6       Member    0003.e31a.1e00     1          Ready
```

次の例では、スタックのネイバー情報を示します。

```
Switch> show switch neighbors
  Switch #    Port A       Port B
  --------    ------       ------
      6        None           8
      8         6            None
```

次の例では、スタックポート情報を示します。

```
Switch> show switch stack-ports
  Switch #    Port A       Port B
  --------    ------       ------
    6          Down          Ok
    8           Ok          Down
```

表 2-40 に、**show switch stack-ports summary** コマンドの出力を示します。

```
Switch> show switch stack-ports summary
Switch#/  Stack   Neighbor   Cable    Link   Link   Sync      #         In
 Port#     Port              Length    OK   Active   OK    Changes   Loopback
           Status                                        To LinkOK
--------  ------  --------  --------  ----  ------  ----  ---------  --------
  1/1     Down      2       50 cm     No     NO      No      10         No
  1/2     Ok        3       1 m       Yes    Yes     Yes     0          No
  2/1     Ok        5       3 m       Yes    Yes     Yes     0          No
  2/2     Down      1       50 cm     No     No      No      10         No
  3/1     Ok        1       1 m       Yes    Yes     Yes     0          No
  3/2     Ok        5       1 m       Yes    Yes     Yes     0          No
  5/1     Ok        3       1 m       Yes    Yes     Yes     0          No
  5/2     Ok        2       3 m       Yes    Yes     Yes     0          No
```

表 2-40　show switch stack-ports summary コマンドの出力

フィールド	説明
Switch#/Port#	メンバ番号とその StackWise ポート番号。
Stack Port Status	• Absent：StackWise ポートではケーブルは検出されていません。 • Down：ケーブルが検出されましたが、接続済みのネイバーが起動していないか、StackWise ポートがディセーブルになっています。 • OK：ケーブルが検出され、接続済みのネイバーが起動しています。
Neighbor	StackWise ケーブルの一方の終端にあるアクティブ メンバのスイッチ番号。

表 2-40　show switch stack-ports summary コマンドの出力 （続き）

フィールド	説明
Cable Length	有効な長さは 50 cm、1 m、または 3 m です。 スイッチがケーブルの長さを検出できない場合は、値は *no cable* になります。ケーブルが接続されていないか、リンクが信頼できない可能性があります。
Link OK	これは、リンクが安定しているかどうかを示します。 *リンクの相手側*とは、ネイバー スイッチ上の StackWise ポートです。 • No：リンクの相手側は、ポートから無効なプロトコル メッセージを受信します。 • Yes：リンクの相手側は、ポートから有効なプロトコル メッセージを受信します。
Link Active	これは、StackWise ポートがリンクの相手側と同じステートになっているかどうかを示します。 • No：ポートはリンクの相手側にトラフィックを送信できません。 • Yes：ポートはリンクの相手側にトラフィックを送信できます。
Sync OK	• No：リンクの相手側は、StackWise ポートに有効なプロトコル メッセージを送信しません。 • Yes：リンクの相手側は、ポートに有効なプロトコル メッセージを送信します。
# Changes to LinkOK	これは、リンクの相対的安定性を示します。 短期間で多数の変更が行われた場合は、リンクのフラップが発生することがあります。
In Loopback	• No：メンバ上の少なくとも 1 つの StackWise ポートに接続済みの StackWise ケーブルがあります。 • Yes：メンバ上のどの StackWise ポートにも、接続済みの StackWise ケーブルはありません。

次の例では、スタックリングのアクティビティの詳細情報を示します。

```
Switch> show switch stack-ring activity detail
Switch   Asic  Rx Queue-1  Rx Queue-2  Rx Queue-3  Rx Queue-4       Total
---------------------------------------------------------------------------
1           0     2021864     1228937      281510           0     3532311
1           1          52           0       72678           0       72730
                                            ----------------------------
                                            Switch 1 Total:     3605041
---------------------------------------------------------------------------
2           0     2020901       90833      101680           0     2213414
2           1          52           0           0           0          52
                                            ----------------------------
                                            Switch 2 Total:     2213466
```

```
-----------------------------------------------------------------------------

Total frames sent to stack ring : 5818507

Note: these counts do not include frames sent to the ring
by certain output features, such as output SPAN and output
ACLs.
```

関連コマンド

コマンド	説明
reload	メンバをリロードし、設定の変更を有効にします。
remote command	すべてまたは指定されたメンバをモニタリングします。
session	特定のメンバにアクセスします。
switch	メンバのプライオリティ値を変更します。
switch provision	新しいスイッチがスタックに加入する前に、プロビジョニングします。
switch renumber	メンバ番号を変更します。

show system mtu

グローバル最大伝送ユニット（MTU）、またはスイッチの最大パケット サイズ設定を表示するには、**show system mtu** 特権 EXEC コマンドを使用します。

show system mtu [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

system mtu または **system mtu jumbo** 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 MTU の設定を変更した場合、スイッチをリセットしない限り、新しい設定は有効になりません。

システム MTU は 10/100 Mbps で動作するポートを、システム ジャンボ MTU はギガビット ポートを参照します。システム ルーティング MTU はルーテッド ポートを参照します。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show system mtu** コマンドの出力を示します。

```
Switch# show system mtu
System MTU size is 1500 bytes
System Jumbo MTU size is 1550 bytes
Routing MTU size is 1500 bytes.
```

関連コマンド

コマンド	説明
system mtu	ファスト イーサネット ポート、ギガビット イーサネット ポート、またはルーテッド ポートの MTU サイズを設定します。

show udld

すべてのポートまたは指定されたポートの UniDirectional Link Detection（UDLD; 単一方向リンク検出）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 udld** ユーザ EXEC コマンドを使用します。

show udld [*interface-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface-id	（任意）インターフェイスの ID およびポート番号です。有効なインターフェイスには、物理ポートと VLAN が含まれます。指定できる VLAN 範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

interface-id を入力しない場合は、すべてのインターフェイスの管理上および運用上の UDLD ステータスが表示されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show udld** *interface-id* コマンドの出力を示します。ここでは、UDLD はリンクの両端でイネーブルに設定されていて、リンクが双方向であることを UDLD が検出します。表 2-41 に、この出力で表示されるフィールドの説明を示します。

```
Switch> show udld gigabitethernet2/0/1
Interface gi2/0/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single Neighbor detected
Message interval: 60
Time out interval: 5
    Entry 1
    Expiration time: 146
    Device ID: 1
    Current neighbor state: Bidirectional
    Device name: Switch-A
    Port ID: Gi2/0/1
    Neighbor echo 1 device: Switch-B
    Neighbor echo 1 port: Gi2/0/2
```

```
Message interval: 5
CDP Device name: Switch-A
```

表 2-41　show udld のフィールドの説明

フィールド	説明
Interface	UDLD に設定されたローカル デバイスのインターフェイス。
Port enable administrative configuration setting	ポートでの UDLD の設定方法。UDLD がイネーブルまたはディセーブルの場合、ポートのイネーブル設定は運用上のイネーブル ステートと同じです。それ以外の場合、イネーブル動作設定は、グローバルなイネーブル設定によって決まります。
Port enable operational state	このポートで UDLD が実際に稼動しているかどうかを示す動作ステート。
Current bidirectional state	リンクの双方向ステート。リンクがダウンしているか、または UDLD 非対応デバイスに接続されている場合は、unknown ステートが表示されます。リンクが UDLD 対応デバイスに通常どおり双方向接続されている場合は、bidirectional ステートが表示されます。その他の値が表示されている場合は、正しく配線されていません。
Current operational state	UDLD ステート マシンの現在のフェーズ。通常の双方向リンクの場合、多くは、ステート マシンはアドバタイズ フェーズです。
Message interval	ローカル デバイスからアドバタイズ メッセージを送信する頻度。単位は秒です。
Time out interval	検出ウィンドウ中に、UDLD が近接デバイスからのエコーを待機する期間（秒）。
Entry 1	最初のキャッシュ エントリの情報。このエントリには、ネイバーから受信されたエコー情報のコピーが格納されます。
Expiration time	このキャッシュ エントリの期限が切れるまでの存続期間（秒）。
Device ID	近接デバイスの ID。
Current neighbor state	ネイバーの現在のステート。ローカル デバイスおよび近接装置の両方で UDLD が通常どおり稼動している場合、ネイバー ステートおよびローカル ステートは双方向です。リンクがダウンしているか、またはネイバーが UDLD 対応でない場合、キャッシュ エントリは表示されません。
Device name	装置名またはネイバーのシステム シリアル番号。装置名が設定されていないか、またはデフォルト（Switch）に設定されている場合、システムのシリアル番号が表示されます。
Port ID	UDLD に対してイネーブルに設定されたネイバーのポート ID。
Neighbor echo 1 device	エコーの送信元であるネイバーの装置名。
Neighbor echo 1 port	エコーの送信元であるネイバーのポート番号 ID。
Message interval	ネイバーがアドバタイズ メッセージを送信する速度（秒）。
CDP device name	CDP デバイス名またはシステム シリアル番号。装置名が設定されていないか、またはデフォルト（Switch）に設定されている場合、システムのシリアル番号が表示されます。

関連コマンド

コマンド	説明
udld	UDLD のアグレッシブ モードまたはノーマル モードをイネーブルにするか、または設定可能なメッセージ タイマーの時間を設定します。
udld port	個々のインターフェイスで UDLD をイネーブルにするか、または光ファイバ インターフェイスが **udld** グローバル コンフィギュレーション コマンドによってイネーブルになるのを防ぎます。
udld reset	UDLD によるすべてのインターフェイス シャットダウンをリセットし、トラフィックが通過するのを再び許可します。

show version

ハードウェアおよびファームウェアのバージョン情報を表示するには、**show version** ユーザ EXEC コマンドを使用します。

show version [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show version** コマンドの出力を示します。

（注）　**show version** 出力には表示されますが、*コンフィギュレーション* レジスタ情報はスイッチでサポートされていません。

```
Switch> show version
Cisco Internetwork Operating System Software
IOS (tm) C3750 Software (C3750-IPSERVICES-M), Version 12.2(25)SEB, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Tues 15-Feb-05 21:09 by antonino
Image text-base: 0x00003000, data-base: 0x008E36A4

ROM: Bootstrap program is C3750 boot loader
BOOTLDR: C3750 Boot Loader (C3750-HBOOT-M) Version 12.2(25)SEB,

Switch uptime is 2 days, 11 hours, 16 minutes
System returned to ROM by power-on
System image file is "flash:i5.709"

cisco WS-C3750-48TS (PowerPC405) processor with 120822K/10240K bytes of memory.
Last reset from power-on
Bridging software.
Target IOS Version 12.2(25)SEB
1 Virtual Ethernet/IEEE 802.3  interface(s)
48 FastEthernet/IEEE 802.3 interface(s)
32 Gigabit Ethernet/IEEE 802.3 interface(s)
```

```
The password-recovery mechanism is enabled.

512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:09:43:A7:F2:00
Motherboard assembly number     : 73-7056-05
Motherboard serial number       : CSJ0638004U
Motherboard revision number     : 05
Model number                    : 73-7056-05


Switch   Ports  Model              SW Version            SW Image
------   -----  -----              ----------            ----------
     1   28     WS-C3750G-24TS     12.2(25)SEB           C3750-IPSERVICES-M
*    8   52     WS-C3750-48TS      12.2(25)SEB           C3750-IPSERVICES-M


Switch 01
---------

Switch Uptime                   : 2 days, 11 hours, 17 minutes
Base ethernet MAC Address       : 00:0B:46:2E:35:80
Motherboard assembly number     : 73-7058-04
Power supply part number        : 341-0045-01
Motherboard serial number       : CSJ0640010L
Model number                    : WS-C3750-24TS-SMI
System serial number            : CSJ0642U00A

Configuration register is 0xF

<output truncated>
```

show vlan

スイッチ上のすべての設定済み VLAN またはある VLAN（VLAN ID または名前を指定した場合）のパラメータを表示するには、**show vlan** ユーザ EXEC コマンドを使用します。

show vlan [**brief** | **dot1q tag native** | **id** *vlan-id* | **internal usage** | **mtu** | **name** *vlan-name* | **private-vlan** [**type**] | **remote-span** | **summary**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

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。
dot1q tag native	（任意）IEEE 802.1Q ネイティブ VLAN タギング ステータスを表示します。
id *vlan-id*	（任意）VLAN ID 番号で特定された 1 つの VLAN に関する情報を表示します。*vlan-id* に指定できる範囲は 1 ～ 4094 です。
internal usage	（任意）スイッチが内部的に使用する VLAN のリストを表示します。これらの VLAN は常に拡張範囲（VLAN ID が 1006 ～ 4094）内のものです。これらの VLAN を内部使用から削除しないと、**vlan** 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、これらの IDS で VLAN を作成できません。
mtu	（任意）VLAN のリストと、VLAN のポートに設定されている最小および最大伝送ユニット（MTU）サイズを表示します。
name *vlan-name*	（任意）VLAN 名で特定された 1 つの VLAN に関する情報を表示します。VLAN 名は、1 ～ 32 文字の ASCII 文字列です。
private-vlan	（任意）プライマリおよびセカンダリ VLAN ID、タイプ（コミュニティ、独立、またはプライマリ）、およびプライベート VLAN に属するポートを含む、設定済みのプライベート VLAN の情報を表示します。このキーワードは、スイッチが IP サービス イメージを実行している場合だけサポートされます。
type	（任意）プライベート VLAN ID およびタイプだけを表示します。
remote-span	（任意）Remote SPAN（RSPAN）VLAN に関する情報を表示します。
summary	（任意）VLAN サマリー情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

（注）　**ifindex** キーワードは、コマンドラインのヘルプ ストリングには表示されていますが、サポートされていません。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(20)SE	**mtu** および **private-vlan** キーワードが追加されました。
12.2(25)SE	**dot1q tag native** キーワードが追加されました。

使用上のガイドライン

show vlan mtu コマンド出力では、MTU_Mismatch 列に VLAN 内のすべてのポートに同じ MTU があるかどうかを示します。この列に *yes* が表示されている場合、VLAN の各ポートに別々の MTU があり、パケットが、大きい MTU を持つポートから小さい MTU を持つポートにスイッチングされると、ドロップされることがあります。VLAN に SVI がない場合、ハイフン（-）記号が SVI_MTU 列に表示されます。MTU-Mismatch 列に *yes* が表示されている場合、MiniMTU を持つポートと MaxMTU を持つポート名が表示されます。

セカンダリ VLAN を定義する前にプライベート VLAN のセカンダリ VLAN をプライマリ VLAN に関連付けようとすると、セカンダリ VLAN が **show vlan private-vlan** コマンドの出力に含まれません。

show vlan private-vlan type コマンドの出力では、*normal* として表示されたタイプは、プライベート VLAN のアソシエーションを持っていても、プライベート VLAN の一部ではない VLAN であることを意味します。たとえば、2 つの VLAN をプライマリ VLAN およびセカンダリ VLAN と定義し、関連付けた後で、プライマリ VLAN からアソシエーションを削除せずにセカンダリ VLAN の設定を削除した場合、セカンダリ VLAN だった VLAN が出力に *normal* として表示されます。**show vlan private-vlan** 出力では、プライマリとセカンダリ VLAN のペアが *non-operational* と表示されます。

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show vlan** コマンドの出力を示します。表 2-42 に、この出力で表示されるフィールドの説明を示します。

```
Switch> show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/0/1, Fa1/0/2, Fa1/0/3
                                                Fa1/0/4, Fa1/0/5, Fa1/0/6
                                                Fa1/0/7, Fa1/0/8, Fa1/0/9
                                                Fa1/0/10, Fa1/0/11, Fa1/0/12
                                                Fa1/0/13, Fa1/0/14, Fa1/0/15
                                                Fa1/0/16, Fa1/0/17, Fa1/0/18
                                                Fa1/0/19, Fa1/0/20, Fa1/0/21
                                                Fa1/0/24, Gi1/0/1, Gi1/0/2
<output truncated>

2    VLAN0002                         active
3    VLAN0003                         active

<output truncated>

1000 VLAN1000                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
2    enet  100002     1500  -      -      -        -    -        0      0
```

```
3    enet  100003     1500  -      -      -        -    -        0      0

<output truncated>

1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------ --------- ----------------- ------------------------------------------

Primary Secondary Type Ports
------- --------- ----------------- ------------------------------------------
20      25     isolated  Fa1/0/13, Fa1/0/20, Fa1/0/22, Gi1/0/1, Fa2/0/13, Fa2/0/22,
                         Fa3/0/13, Fa3/0/14.Fa3/0/20, Gi3/0/1
20      30     community Fa1/0/13, Fa1/0/20, Fa1/0/21, Gi1/0/1, Fa2/0/13, Fa2/0/20,
                         Fa3/0/14, Fa3/0/20,Fa3/0/21, Gi3/0/1
20      35     community Fa1/0/13, Fa1/0/20, Fa1/0/23, Fa1/0/33, Gi1/0/1, Fa2/0/13,
                         Fa3/0/14, Fa3/0/20, Fa3/0/23, Fa3/0/33, Gi3/0/1

<output truncated>
```

表 2-42　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 の名前（設定されている場合）。
Status	VLAN のステータス（active または suspend）。
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 値。
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：可能な値はソースルート ブリッジング（SRB）およびソースルート トランスペアレント（SRT）で、デフォルトは SRB です。
Trans1	トランスレーション ブリッジ 1。
Trans2	トランスレーション ブリッジ 2。
Remote SPAN VLANs	設定されている RSPAN VLAN を識別します。
Primary/Secondary/Type/Ports	プライマリ VLAN ID、セカンダリ VLAN ID、セカンダリ VLAN のタイプ（コミュニティまたは隔離）、およびそれに所属するポートを含む、設定されたプライベート VLAN が含まれます。

次の例では、**show vlan dot1q tag native** コマンドの出力を示します。

```
Switch> show vlan dot1q tag native
dot1q native vlan tagging is disabled
```

次の例では、**show vlan private-vlan** コマンドの出力を示します。

```
Switch> show vlan private-vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
10      501       isolated          Gi3/0/3
10      502       community         Fa2/0/11
10      503       non-operational3      -
20       25       isolated          Fa1/0/13, Fa1/0/20, Fa1/0/22, Gi1/0/1, Fa2/0/13,
                                   Fa2/0/22, Fa3/0/13, Fa3/0/14, Fa3/0/20, Gi3/0/1
20       30       community         Fa1/0/13, Fa1/0/20, Fa1/0/21, Gi1/0/1, Fa2/0/13,
                                   Fa2/0/20, Fa3/0/14, Fa3/0/20, Fa3/0/21, Gi3/0/1
20       35       community         Fa1/0/13, Fa1/0/20, Fa1/0/23, Fa1/0/33.Gi1/0/1,
                                   Fa2/0/13, Fa3/0/14, Fa3/0/20.Fa3/0/23, Fa3/0/33,
                                   Gi3/0/1
20       55       non-operational
2000   2500       isolated          Fa1/0/5, Fa1/0/10, Fa2/0/5, Fa2/0/10, Fa2/0/15
```

次の例では、**show vlan private-vlan type** コマンドの出力を示します。

```
Switch> show vlan private-vlan type
Vlan Type
---- -----------------
10   primary
501  isolated
502  community
503  normal
```

次の例では、**show vlan summary** コマンドの出力を示します。

```
Switch> show vlan summary
Number of existing VLANs           : 45
 Number of existing VTP VLANs      : 45
 Number of existing extended VLANs : 0
```

次の例では、**show vlan id** コマンドの出力を示します。

```
Switch# show vlan id 2
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
2    VLAN0200                         active    Fa1/0/7, Fa1/0/8

2    VLAN0200                       active    Fa1/3, Fa2/5, Fa2/6
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled
```

次の例では、**show vlan internal usage** コマンドの出力を示します。これは、VLAN 1025 および 1026 が、スタック メンバ 1 のファスト イーサネット ルーテッド ポート 23 および 24 の内部 VLAN として使用されていることを示しています。これらの VLAN ID のいずれかを使用する場合は、ルーテッド ポートをシャットダウンする必要があります。これにより、内部 VLAN を解放して、拡張範囲 VLAN を作成します。ルーテッド ポートを開始すると、他の内部 VLAN 番号が割り当てられます。

```
Switch> show vlan internal usage
VLAN Usage
---- -------------
```

```
1025 FastEthernet1/0/23
1026 FastEthernet1/0/24
```

関連コマンド

コマンド	説明
private-vlan	VLAN をコミュニティ、隔離、またはプライマリ VLAN に設定するか、プライマリ VLAN をセカンダリ VLAN に関連付けます。
switchport mode	ポートの VLAN メンバシップ モードを設定します。
usb-inactivity-timeout	VLAN 1 ～ 4094 を設定できる場合、VLAN コンフィギュレーション モードをイネーブルにします。

show vlan access-map

特定の VLAN アクセス マップ、またはすべての VLAN アクセス マップに関する情報を表示するには、**show vlan access-map** 特権 EXEC コマンドを使用します。

show vlan access-map [*mapname*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

mapname	（任意）特定の VLAN アクセス マップ名。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show vlan access-map** コマンドの出力を示します。

```
Switch# show vlan access-map
Vlan access-map "SecWiz"  10
  Match clauses:
    ip  address: SecWiz_Gi0_3_in_ip
    ip  address: SecWiz_Fa10_3_in_ip

  Action:
    forward
```

関連コマンド

コマンド	説明
show vlan filter	VLAN フィルタすべてに関する情報、または特定の VLAN または VLAN アクセス マップに関する情報を表示します。
vlan access-map	VLAN パケット フィルタリングの VLAN マップ エントリを作成します。
vlan filter	1 つ以上の VLAN に、VLAN マップを適用します。

show vlan filter

VLAN フィルタすべてに関する情報、または特定の VLAN または VLAN アクセス マップに関する情報を表示するには、**show vlan filter** 特権 EXEC コマンドを使用します。

show vlan filter [**access-map** *name* | **vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

access-map *name*	（任意）指定された VLAN アクセス マップのフィルタリング情報を表示します。
vlan *vlan-id*	（任意）指定された VLAN のフィルタリング情報を表示します。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show vlan filter** コマンドの出力を示します。

```
Switch# show vlan filter
VLAN Map map_1 is filtering VLANs:
  20-22
```

関連コマンド

コマンド	説明
show vlan access-map	特定の VLAN アクセス マップまたはすべての VLAN アクセス マップに関する情報を表示します。
vlan access-map	VLAN パケット フィルタリングの VLAN マップ エントリを作成します。
vlan filter	1 つ以上の VLAN に、VLAN マップを適用します。

show vmps

VLAN Query Protocol（VQP）バージョン、再確認インターバル、再試行回数、VLAN メンバシップ ポリシー サーバ（VMPS）の IP アドレス、および現在のサーバやプライマリ サーバを表示するには、キーワードを指定しないで **show vmps** ユーザ EXEC コマンドを使用します。**statistics** キーワードを使用すると、クライアント側の統計情報が表示されます。

show vmps [**statistics**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

statistics	（任意）VQP のクライアント側統計情報およびカウンタを表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show vmps** コマンドの出力を示します。

```
Switch> show vmps
VQP Client Status:
--------------------
VMPS VQP Version:   1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server:

Reconfirmation status
---------------------
VMPS Action:         other
```

次の例では、**show vmps statistics** コマンドの出力を示します。表 2-43 に、表示される各フィールドの説明を示します。

```
Switch> show vmps statistics
VMPS Client Statistics
----------------------
VQP  Queries:               0
VQP  Responses:             0
VMPS Changes:               0
VQP  Shutdowns:             0
```

```
VQP  Denied:                0
VQP  Wrong Domain:          0
VQP  Wrong Version:         0
VQP  Insufficient Resource: 0
```

表 2-43　show vmps statistics のフィールドの説明

フィールド	説明
VQP Queries	クライアントから VMPS に送信されるクエリー数。
VQP Responses	VMPS からクライアントに送信される応答数。
VMPS Changes	サーバ間で VMPS を変更した回数。
VQP Shutdowns	ポートをシャットダウンするために VMPS が応答を送信した回数。クライアントはポートをディセーブルにし、このポート上のすべてのダイナミック アドレスをアドレス テーブルから削除します。接続を復元するには、ポートを再び管理上のイネーブル状態にする必要があります。
VQP Denied	VMPS がセキュリティ上の理由からクライアント要求を拒否した回数。VMPS の応答がアドレスを拒否した場合、そのアドレスでワークステーションとのフレーム伝送は実行されません（ポートが VLAN に割り当てられている場合、ブロードキャストまたはマルチキャスト フレームがワークステーションに対して配信されます）。クライアントは拒否されたアドレスをブロック済みアドレスとしてアドレス テーブルに保管します。これにより、このワークステーションから受信した各新規パケットに対するクエリーが、これ以上 VMPS に送信されなくなります。エージング タイム内に、このポートでこのワークステーションからの新規パケットを受信しない場合、クライアントはアドレスを期限切れにします。
VQP Wrong Domain	要求内の管理ドメインが VMPS の管理ドメインと一致しない回数。ポートの従来の VLAN 割り当ては変更されません。この応答は、サーバおよびクライアントに同じ VTP 管理ドメインが設定されていないことを意味します。
VQP Wrong Version	クエリー パケットのバージョン フィールドに、VMPS でサポートされているバージョンよりも大きい値が格納される回数。ポートの VLAN 割り当ては変更されません。スイッチは VMPS バージョン 1 要求だけを送信します。
VQP Insufficient Resource	リソースのアベイラビリティに問題があるために、VMPS が要求に応答できない回数。再試行制限に達していない場合、クライアントはサーバごとの再試行回数に達したかどうかに応じて、同じサーバまたは次の代替サーバに要求を再送信します。

関連コマンド

コマンド	説明
clear vmps statistics	VQP クライアントに保持されている統計情報をクリアします。
vmps reconfirm（特権 EXEC）	VQP クエリーを送信して、VMPS でのすべてのダイナミック VLAN 割り当てを再確認します。
vmps retry	VQP クライアントのサーバごとの再試行回数を設定します。
vmps server	プライマリ VMPS、および最大で 3 台のセカンダリ サーバを設定します。

show vtp

VLAN Trunking Protocol（VTP）の管理ドメイン、ステータス、およびカウンタに関する一般情報を表示するには、**show vtp** ユーザ EXEC コマンドを使用します。

show vtp {**counters** | **devices** [**conflicts**] | **interface** [*interface-id*] | **password** | **status**} [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

counters	スイッチの VTP 統計情報を表示します。
password	設定された VTP パスワードを表示します。
devices	ドメイン内のすべての VTP バージョン 3 デバイスに関する情報を表示します。このキーワードは、スイッチが VTP バージョン 3 を実行していない場合だけ適用されます。
conflicts	競合するプライマリ サーバを持つ VTP バージョン 3 デバイスに関する情報を表示します。このコマンドは、スイッチが VTP 透過モードまたは VPT オフ モードの場合、無視されます。
interface [*interface-id*]	すべての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対する VTP のステータスおよび設定を表示します。*interface-id* には物理インターフェイスまたはポート チャネルを指定できます。
status	VTP 管理ドメインのステータスに関する一般情報を表示します。
| **begin**	（任意）*expression* と一致する行から表示を開始します。
| **exclude**	（任意）*expression* と一致する行を表示から除外します。
| **include**	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**password** キーワードが追加されました。
12.2(52)SE	**devices** および **interface** キーワードが VTP バージョン 3 に追加されました。

使用上のガイドライン

スイッチが VTP バージョン 3 を実行中に **show vtp password** コマンドを入力すると、表示は次のルールに従います。

- **password** *password* グローバル コンフィギュレーション コマンドで **hidden** キーワードを指定せず、スイッチ上で暗号化がイネーブルでない場合、パスワードはクリア テキストで表示されます。
- **password** *password* コマンドで **hidden** キーワードを指定せず、スイッチ上で暗号化がイネーブルの場合、暗号化されたパスワードが表示されます。
- **password** *password* コマンドに **hidden** キーワードが含まれていた場合、16 進数の秘密キーが表示されます。

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show vtp devices** コマンドの出力を示します。*Conflict* 列の Yes は、応答するサーバがその機能のローカル サーバと競合していることを意味します。つまり、同じドメイン内の 2 つのスイッチは、データベースに対して同じプライマリ サーバを持ちません。

```
Switch# show vtp devices

Retrieving information from the VTP domain. Waiting for 5 seconds.
VTP Database Conf switch ID      Primary Server Revision   System Name
             lict
------------ ---- -------------- -------------- ---------- ----------------------
VLAN         Yes  00b0.8e50.d000 000c.0412.6300 12354      main.cisco.com
MST          No   00b0.8e50.d000 0004.AB45.6000 24         main.cisco.com
VLAN         Yes  000c.0412.6300=000c.0412.6300 67         qwerty.cisco.com
```

次の例では、**show vtp counters** コマンドの出力を示します。表 2-44 に、この出力で表示されるフィールドの説明を示します。

```
Switch> show vtp counters

VTP statistics:
Summary advertisements received    : 0
Subset advertisements received     : 0
Request advertisements received    : 0
Summary advertisements transmitted : 6970
Subset advertisements transmitted  : 0
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
                                                   non-pruning-capable device
---------------- ---------------- ---------------- ---------------------------
Fa1/0/47           0                0                0
Fa1/0/48           0                0                0
Gi2/0/1           0                0                0
Gi3/0/2           0                0                0
```

表 2-44　show vtp counters のフィールドの説明

フィールド	説明
Summary advertisements received	トランク ポート上でこのスイッチが受信するサマリー アドバタイズの数。サマリー アドバタイズには、管理ドメイン名、コンフィギュレーション リビジョン番号、更新タイムスタンプと ID、認証チェックサム、および関連するサブセット アドバタイズの数が含まれます。
Subset advertisements received	トランク ポート上でこのスイッチが受信するサブセット アドバタイズの数。サブセット アドバタイズには、1 つ以上の VLAN に関する情報がすべて含まれています。
Request advertisements received	トランク ポート上でこのスイッチが受信するアドバタイズ要求の数。アドバタイズ要求は、通常、すべての VLAN 上に関する情報を要求します。また、VLAN のサブセットに関する情報も要求できます。
Summary advertisements transmitted	トランク ポート上でこのスイッチが送信するサマリー アドバタイズの数。サマリー アドバタイズには、管理ドメイン名、コンフィギュレーション リビジョン番号、更新タイムスタンプと ID、認証チェックサム、および関連するサブセット アドバタイズの数が含まれます。
Subset advertisements transmitted	トランク ポート上でこのスイッチが送信するサブセット アドバタイズの数。サブセット アドバタイズには、1 つ以上の VLAN に関する情報がすべて含まれています。

表 2-44　show vtp counters のフィールドの説明 （続き）

フィールド	説明
Request advertisements transmitted	トランク ポート上でこのスイッチが送信するアドバタイズ要求の数。アドバタイズ要求は、通常、すべての VLAN 上に関する情報を要求します。また、VLAN のサブセットに関する情報も要求できます。
Number of configuration revision errors	リビジョン エラーの数。 新しい VLAN の定義、既存 VLAN の削除、中断、または再開、あるいは既存 VLAN のパラメータ変更を行うと、スイッチのコンフィギュレーション リビジョン番号が増加します。 リビジョン番号がスイッチのリビジョン番号と一致するにもかかわらず、MD5 ダイジェスト値が一致しないアドバタイズをスイッチが受信すると、リビジョン エラーが増加します。このエラーは、2 つのスイッチの VTP パスワードが異なるか、またはスイッチの設定が異なることを意味します。 これらのエラーが発生した場合、スイッチは着信アドバタイズのフィルタリング中であり、ネットワーク内で VTP データベースが同期しなくなります。
Number of configuration digest errors	MD5 ダイジェスト エラーの数。 サマリー パケット内の MD5 ダイジェストと、計算された受信済みアドバタイズの MD5 ダイジェストが一致しない場合は、ダイジェスト エラーが増加します。このエラーは、通常、2 つのスイッチの VTP パスワードが異なることを意味します。この問題を解決するには、すべてのスイッチで VTP パスワードが同じになるようにします。 これらのエラーが発生した場合、スイッチは着信アドバタイズのフィルタリング中であり、ネットワーク内で VTP データベースが同期しなくなります。
Number of V1 summary errors	バージョン 1 エラーの数。 VTP V2 モードのスイッチが VTP バージョン 1 フレームを受信すると、バージョン 1 サマリー エラーが増加します。これらのエラーは、少なくとも 1 つの近接スイッチ上で VTP バージョン 1 が稼動しているか、または V2 モードがディセーブルの状態で VTP バージョン 2 が稼動していることを意味します。この問題を解決するには、VTP V2 モードのスイッチの設定をディセーブルに変更します。
Join Transmitted	トランク上で送信された VTP プルーニング メッセージの数。
Join Received	トランク上で受信された VTP プルーニング メッセージの数。
Summary Advts Received from non-pruning-capable device	トランク上で受信された、プルーニングをサポートしていないデバイスからの VTP サマリー メッセージの数。

次の例では、VTP バージョン 2 を実行するスイッチに対する **show vtp status** コマンドの出力を示します。表 2-45 に、この出力で表示されるフィールドの説明を示します。

```
Switch> show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 45
VTP Operating Mode              : Transparent
VTP Domain Name                 : shared_testbed1
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Enabled
MD5 digest                      : 0x3A 0x29 0x86 0x39 0xB4 0x5D 0x58 0xD7
```

表 2-45　show vtp status のフィールドの説明

フィールド	説明
VTP Version	スイッチ上で動作している VTP バージョンを表示します。デフォルトでは、スイッチはバージョン 1 を実行しますが、バージョン 2 に設定することもできます。
Configuration Revision	このスイッチの現在のコンフィギュレーション リビジョン番号。
Maximum VLANs Supported Locally	ローカルにサポートされている VLAN の最大数。
Number of Existing VLANs	既存の VLAN 数。
VTP Operating Mode	VTP 動作モード（サーバ、クライアント、または透過）を表示します。 Server : VTP サーバ モードのスイッチは VTP に対してイネーブルであり、アドバタイズを送信します。スイッチで VLAN を設定できます。このスイッチを使用すると、起動後に、現在の VTP データベース内のすべての VLAN 情報を、NVRAM から復元できます。デフォルトでは、すべてのスイッチが VTP サーバです。 **（注）** スイッチが設定を NVRAM に書き込んでいる間に障害を検出し、NVRAM が機能するまでサーバ モードに戻ることができない場合、スイッチは VTP サーバ モードから VTP クライアント モードに自動的に変わります。 Client : VTP クライアント モードのスイッチは VTP に対してイネーブルであり、アドバタイズを送信できますが、VLAN 設定を格納するために十分な不揮発性ストレージがありません。スイッチでは VLAN を設定できません。VTP クライアントが起動すると、VTP クライアントはその VLAN データベースを初期化するアドバタイズを受信するまで、VTP アドバタイズを送信しません。 Transparent : VTP 透過モードのスイッチは、VTP に対してディセーブルであり、アドバタイズの送信や、他のデバイスから送信されたアドバタイズの学習を行いません。また、ネットワーク内の他のデバイスの VLAN 設定にも影響しません。スイッチは VTP アドバタイズを受信し、アドバタイズを受信したトランク ポートを除くすべてのトランク ポートにこれを転送します。
VTP Domain Name	スイッチの管理ドメインを特定する名前。
VTP Pruning Mode	プルーニングがイネーブルかまたはディセーブルかを表示します。VTP サーバでプルーニングをイネーブルにすると、管理ドメイン全体でプルーニングが有効になります。プルーニングを使用すると、トラフィックが適切なネットワーク デバイスにアクセスするために使用しなければならないトランク リンクへのフラッディング トラフィックが制限されます。

表 2-45　show vtp status のフィールドの説明 （続き）

フィールド	説明
VTP V2 Mode	VTP バージョン 2 モードがイネーブルかどうかを表示します。すべての VTP バージョン 2 スイッチは、デフォルトでバージョン 1 モードで動作します。各 VTP スイッチは他のすべての VTP デバイスの機能を自動的に検出します。VTP デバイス ネットワーク内のすべての VTP スイッチがバージョン 2 モードで動作可能な場合だけ、ネットワークをバージョン 2 に設定してください。
VTP Traps Generation	VTP トラップをネットワーク管理ステーションに送信するかどうかを表示します。
MD5 Digest	VTP 設定の 16 バイト チェックサム。
Configuration Last Modified	最後に行った設定変更の日付と時刻を表示します。データベースの設定変更の原因となったスイッチの IP アドレスを表示します。

次の例では、VTP バージョン 3 を実行するスイッチに対する **show vtp status** コマンドの出力を示します。

```
Switch> show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 3
VTP Domain Name                 : Cisco
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0021.1bcd.c700

Feature VLAN:
--------------
VTP Operating Mode                : Server
Number of existing VLANs          : 7
Number of existing extended VLANs : 0
Configuration Revision            : 0
Primary ID                        : 0000.0000.0000
Primary Description               :
MD5 digest                        : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
                                    0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
Feature MST:
--------------
VTP Operating Mode                : Client
Configuration Revision            : 0
Primary ID                        : 0000.0000.0000
Primary Description               :
MD5 digest                        : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
                                    0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

Feature UNKNOWN:
--------------
VTP Operating Mode                : Transparent
```

関連コマンド

コマンド	説明
clear vtp counters	VTP およびプルーニング カウンタをクリアします。
vtp（グローバル コンフィギュレーション）	VTP のファイル名、インターフェイス名、ドメイン名、およびモードを設定します。

shutdown

インターフェイスをディセーブルにするには、**shutdown** 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。ディセーブルされたインターフェイスを再起動するには、このコマンドの **no** 形式を使用します。

shutdown

no shutdown

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ポートはイネーブルです（シャットダウンしません）。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

shutdown コマンドを入力すると、ポートは転送を停止します。ポートをイネーブルにするには、**no shutdown** コマンドを使用します。

削除、中断、またはシャットダウンされた VLAN に割り当てられているスタティック アクセス ポートに **no shutdown** コマンドを使用しても、無効です。ポートを再びイネーブルにするには、まずポートをアクティブ VLAN のメンバにする必要があります。

shutdown コマンドは指定のインターフェイス上のすべての機能をディセーブルにします。

また、このコマンドはインターフェイスが使用不可であることをマーク付けします。インターフェイスがディセーブルかどうかを確認するには、**show interfaces** 特権 EXEC コマンドを使用します。シャットダウンされたインターフェイスは、管理上のダウンとして画面に表示されます。

例

次の例では、ポートをディセーブルにしてから、再びイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# shutdown

Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# no shutdown
```

設定を確認するには、**show interfaces** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces	すべてのインターフェイスまたは特定のインターフェイスに対する統計情報を表示します。

shutdown vlan

指定の VLAN のローカル トラフィックをシャットダウン（中断）するには、**shutdown vlan** グローバル コンフィギュレーション 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*

構文の説明

vlan-id	ローカルにシャットダウンする VLAN の ID です。指定できる範囲は 2 ～ 1001 です。VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）環境のデフォルト VLAN として定義された VLAN、および拡張範囲 VLAN（ID が 1005 を超える VLAN）は、シャットダウンできません。デフォルトの VLAN は 1 および 1002 ～ 1005 です。

デフォルト

デフォルト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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

shutdown vlan コマンドは、VTP データベース内の VLAN 情報を変更しません。このコマンドはローカル トラフィックをシャットダウンしますが、スイッチは VTP 情報をアドバタイズし続けます。

例

次の例では、VLAN 2 のトラフィックをシャットダウンする方法を示します。

```
Switch(config)# shutdown vlan 2
```

設定を確認するには、**show vlan** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
shutdown（config-vlan モード）	config-vlan モード（**vlan** *vlan-id* グローバル コンフィギュレーション コマンドで開始）の場合に、VLAN のローカル トラフィックをシャットダウンします。

small-frame violation rate

インターフェイスで受信する VLAN タグ付きパケットのフレームが小さく（67 バイト以下）、指定された伝送速度である場合に、インターフェイスが errdisable となる伝送速度（しきい値）を設定するには、**small-frame violation rate** ***pps*** 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。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。

small-frame violation rate *pps*

no small-frame violation rate *pps*

構文の説明

pps	小さいフレームを受信するインターフェイスが errdisable となるしきい値を指定します。指定できる範囲は、1 ～ 10,000 pps（パケット / 秒）です。

デフォルト

この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

コマンド履歴

リリース	変更内容
12.2(44)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ポートが小さいフレームを受信すると errdisable となる伝送速度（しきい値）をイネーブルにします。67 フレーム以下のパケットが小さいフレームと見なされます。

各ポートで小さいフレームと見なすしきい値をグローバルにイネーブルにするには、**errdisable detect cause small-frame** グローバル コンフィギュレーション コマンドを使用します。

ポートが自動的に再びイネーブルになるように設定するには、**errdisable recovery cause small-frame** グローバル コンフィギュレーション コマンドを使用します。回復時間を設定するには、**errdisable recovery interval** interval グローバル コンフィギュレーション コマンドを使用します。

例

次の例では、小さい着信フレームが 10,000 pps で到達した場合にポートが errdisable となるようにする小さいフレームの着信速度の機能をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# small-frame violation rate 10000
```

設定を確認するには、**show interfaces** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
errdisable detect cause small-frame	着信フレームが最小サイズより小さく、指定した伝送速度（しきい値）で到着したスイッチ ポートがあれば、そのポートを errdisable 状態にします。
errdisable recovery cause small-frame	回復タイマーをイネーブルにします。
show interfaces	入出力フロー制御を含むスイッチのインターフェイス設定を表示します。

snmp-server enable traps

スイッチで、さまざまなトラップの Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）通知の送信、または Network Management System（NMS; ネットワーク管理システム）への要求の通知をイネーブルにするには、**snmp-server enable traps** グローバル コンフィギュレーション 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。

snmp-server enable traps [**bgp** | **bridge** [**newroot**] [**topologychange**] | **cluster** | **config** | **copy-config** | **cpu threshold** | {**dot1x** [**auth-fail-vlan** | **guest-vlan** | **no-auth-fail-vlan** | **no-guest-vlan**] } | **entity** | **envmon** [**fan** | **shutdown** | **status** | **supply** | **temperature**] | **errdisable** [**notification-rate value**] | **flash** [**insertion** | **removal**] | **fru-ctrl** | **hsrp** | **ipmulticast** | **mac-notification** [**change**] [**move**] [**threshold**] | **msdp** | **ospf** [**cisco-specific** | **errors** | **lsa** | **rate-limit** | **retransmit** | **state-change**] | **pim** [**invalid-pim-message** | **neighbor-change** | **rp-mapping-change**] | **port-security** [**trap-rate** *value*] | **power-ethernet** {**group** *name* | **police**} | **rtr** | **snmp** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] | **stackwise** | **storm-control trap-rate** *value* | **stpx** [**inconsistency**] [**root-inconsistency**] [**loop-inconsistency**] | **syslog** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vtp**]

no snmp-server enable traps [**bgp** | **bridge** [**newroot**] [**topologychange**] | **cluster** | **config** | **copy-config** | **cpu threshold** | {**dot1x** [**auth-fail-vlan** | **guest-vlan** | **no-auth-fail-vlan** | **no-guest-vlan**] } | **entity** | **envmon** [**fan** | **shutdown** | **status** | **supply** | **temperature**] | **errdisable** [**notification-rate**] | **flash** [**insertion** | **removal**] | **fru-ctrl** | **hsrp** | **ipmulticast** | **mac-notification** [**change**] [**move**] [**threshold**] | **msdp** | **ospf** [**cisco-specific** | **errors** | **lsa** | **rate-limit** | **retransmit** | **state-change**] | **pim** [**invalid-pim-message** | **neighbor-change** | **rp-mapping-change**] | **port-security** [**trap-rate**] | **power-ethernet** {**group** *name* | **police**} | **rtr** | **snmp** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] | **stackwise** | **storm-control trap-rate** | **stpx** [**inconsistency**] [**root-inconsistency**] [**loop-inconsistency**] | **syslog** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vtp**]

構文の説明

bgp	（任意）Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）ステート変更トラップをイネーブルにします。 **（注）** このキーワードは、IP サービス イメージがスタック マスターにインストールされている場合にだけ使用できます。
bridge [**newroot**] [**topologychange**]	（任意）STP ブリッジ MIB トラップを生成します。キーワードの意味は次のとおりです。 • **newroot**：（任意）SNMP STP ブリッジ MIB の新しいルート トラップをイネーブルにします。 • **topologychange**：（任意）SNMP STP ブリッジ MIB のトポロジ変更トラップをイネーブルにします。
cluster	（任意）クラスタ トラップをイネーブルにします。
config	（任意）SNMP 設定トラップをイネーブルにします。
copy-config	（任意）SNMP コピー設定トラップをイネーブルにします。
cpu threshold	（任意）CPU 関連トラップを許可します。

dot1x [auth-fail-vlan | guest-vlan | no-auth-fail-vlan | no-guest-vlan]	（任意）IEEE 802.1x トラップをイネーブルにします。キーワードの意味は次のとおりです。 • **auth-fail-vlan**：（任意）ポートが設定された制限 VLAN に移行する場合にトラップを生成します。 • **guest-vlan**：（任意）ポートが設定されたゲスト VLAN に移行する場合にトラップを生成します。 • **no-auth-fail-vlan**：（任意）制限 VLAN が設定されていないために、ポートが制限 VLAN に移行しようとしてもできなかった場合にトラップを生成します。 • **no-guest-vlan**：（任意）ゲスト VLAN が設定されていないために、ポートがゲスト VLAN に移行しようとしてもできなかった場合にトラップを生成します。 **（注）**　キーワードを何も指定せずに **snmp-server enable traps dot1x** コマンドを入力すると、すべての IEEE 802.1x トラップがイネーブルになります。
entity	（任意）SNMP エンティティ トラップをイネーブルにします。
envmon [fan | shutdown | status | supply | temperature]	（任意）SNMP 環境トラップをイネーブルにします。キーワードの意味は次のとおりです。 • **fan**：（任意）ファン トラップをイネーブルにします。 • **shutdown**：（任意）環境モニタ シャットダウン トラップをイネーブルにします。 • **status**：（任意）SNMP 環境ステータス変更トラップをイネーブルにします。 • **supply**：（任意）環境モニタ電源トラップをイネーブルにします。 • **temperature**：（任意）環境モニタ温度トラップをイネーブルにします。
errdisable [notification-rate value]	（任意）errdisable トラップをイネーブルにします。notification-rate キーワードを使用して、分単位で送信される errdisable トラップの最大値を設定します。指定できる範囲は 0 ～ 10000 です。デフォルト値は 0 です（制限はなく、トラップは発生するたびに送信されます）。
flash [insertion | removal]	（任意）SNMP FLASH 通知をイネーブルにします。キーワードの意味は次のとおりです。 **insertion**：（任意）スイッチ（フラッシュ）がスタックに挿入されると（物理的に、または電源の再投入やリロードにより）、トラップを生成します。 **removal**：（任意）スイッチ（フラッシュ）がスタックから取り外されると（物理的に、または電源の再投入やリロードにより）、トラップを生成します。
fru-ctrl	（任意）エンティティ Field-Replaceable Unit（FRU）制御トラップを生成します。スタックでは、このトラップはスタックにおけるスイッチの挿入/取り外しを意味します。
hsrp	（任意）Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）トラップをイネーブルにします。
ipmulticast	（任意）IP マルチキャスト ルーティング トラップをイネーブルにします。
mac-notification	（任意）MAC アドレス通知トラップをイネーブルにします。
change	（任意）MAC アドレス変更通知トラップをイネーブルにします。
move	（任意）MAC アドレス移動通知トラップをイネーブルにします。
threshold	（任意）MAC アドレス テーブルしきい値トラップをイネーブルにします。

msdp	（任意）Multicast Source Discovery Protocol（MSDP）トラップをイネーブル にします。
ospf [**cisco-specific** | **errors** | **lsa** | **rate-limit** | **retransmit** | **state-change**]	（任意）Open Shortest Path First（OSPF）トラップをイネーブルにします。キーワードの意味は次のとおりです。 • **cisco-specific**：（任意）シスコ固有のトラップをイネーブルにします。 • **errors**：（任意）エラー トラップをイネーブルにします。 • **lsa**：（任意）Link-State Advertisement（LSA; リンクステート アドバタイズメント）トラップをイネーブルにします。 • **rate-limit**：（任意）速度制限トラップをイネーブルにします。 • **retransmit**：（任意）パケット再送信トラップをイネーブルにします。 • **state-change**：（任意）ステート変更トラップをイネーブルにします。
pim [**invalid-pim-message** | **neighbor-change** | **rp-mapping-change**]	（任意）Protocol-Independent Multicast（PIM）トラップをイネーブルにします。キーワードの意味は次のとおりです。 • **invalid-pim-message**：（任意）無効な PIM メッセージ トラップをイネーブルにします。 • **neighbor-change**：（任意）PIM ネイバー変更トラップをイネーブルにします。 • **rp-mapping-change**：（任意）Rendezvous Point（RP; ランデブー ポイント）マッピング変更トラップをイネーブルにします。
port-security [**trap-rate** *value*]	（任意）ポート セキュリティ トラップをイネーブルにします。1 秒間に送信するポート セキュリティ トラップの最大数を設定するには、**trap-rate** キーワードを使用します。指定できる範囲は 0 ～ 1000 です。デフォルトは 0 です（制限はなく、トラップは発生するたびに送信されます）。
power-ethernet {**group** *name* | **police**}	（任意）Power-over-Ethernet トラップをイネーブルにします。キーワードの意味は次のとおりです。 • **group** *name*：指定されたグループ番号またはリストのインライン パワー グループ ベースのトラップをイネーブルにします。 • **police**：インライン パワー ポリシング トラップをイネーブルにします。
rtr	（任意）SNMP Response Time Reporter トラップをイネーブルにします。
snmp [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]	（任意）SNMP トラップをイネーブルにします。キーワードの意味は次のとおりです。 • **authentication**：（任意）認証トラップをイネーブルにします。 • **coldstart**：（任意）コールド スタート トラップをイネーブルにします。 • **linkdown**：（任意）リンクダウン トラップをイネーブルにします。 • **linkup**：（任意）リンクアップ トラップをイネーブルにします。 • **warmstart**：（任意）ウォーム スタート トラップをイネーブルにします。
stackwise	（任意）SNMP StackWise トラップをイネーブルにします。
storm-control trap-rate *value*	（任意）ストーム制御トラップをイネーブルにします。分単位で送信されるストーム制御トラップの最大数を設定するには、**trap-rate** キーワードを使用します。指定できる範囲は 0 ～ 1000 です。デフォルト値は 0 です（制限はなく、トラップは発生するたびに送信されます）。

stpx	（任意）SNMP STPX MIB トラップをイネーブルにします。キーワードの意味は次のとおりです。 • **inconsistency**：（任意）SNMP STPX MIB の矛盾更新トラップをイネーブルにします。 • **root-inconsistency**：（任意）SNMP STPX MIB のルート矛盾更新トラップをイネーブルにします。 • **loop-inconsistency**：（任意）SNMP STPX MIB のループ矛盾更新トラップをイネーブルにします。
Syslog	（任意）SNMP Syslog トラップをイネーブルにします。
tty	（任意）TCP 接続トラップを送信します。デフォルトでイネーブルになっています。
vlan-membership	（任意）SNMP VLAN メンバシップ トラップをイネーブルにします。
vlancreate	（任意）SNMP VLAN 作成トラップをイネーブルにします。
vlandelete	（任意）SNMP VLAN 削除トラップをイネーブルにします。
vtp	（任意）VLAN Trunking Protocol（VTP）トラップをイネーブルにします。

（注）　**snmp-server enable informs** グローバル コンフィギュレーション コマンドは、サポートされていません。SNMP 情報通知の送信をイネーブルにするには、**snmp-server enable traps** グローバル コンフィギュレーション コマンドと **snmp-server host** *host-addr* **informs** グローバル コンフィギュレーション コマンドを組み合わせて使用します。

デフォルト

SNMP トラップの送信を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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**bgp**、**copy-config**、**envmon**、**flash**、**port-security**、**stpx**、**syslog**、**vlancreate**、および **vlandelete** キーワードが追加されました。
12.2(18)SE	**ipmulticast**、**msdp**、**ospf** [**cisco-specific** | **errors** | **lsa** | **rate-limit** | **retransmit** | **state-change**]、**pim** [**invalid-pim-message** | **neighbor-change** | **rp-mapping-change**]、および **tty** キーワードが追加されました。
12.2(25)SE	**storm-control trap-rate** *value* キーワードが追加されました。
12.2(37)SE	**errdisable notification-rate** *value* キーワードが追加されました。
12.2(40)SE	**change**、**move**、および **threshold** キーワードが mac-notification オプションに追加されました。
12.2(44)SE	**power-ethernet** {**group** *name* | **police**} キーワードが追加されました。
12.2(46)SE	**dot1x** [**auth-fail-vlan** | **guest-vlan** | **no-auth-fail-vlan** | **no-guest-vlan**] キーワードが追加されました。
12.2(50)SE	**cpu threshold** キーワードが追加されました。

使用上のガイドライン

snmp-server host 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、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのタイプが送信されます。

snmp-server enable traps コマンドは、トラップまたは情報がサポートされている場合に、これらの送信をイネーブルにします。

（注）　SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

CPU しきい値通知のタイプおよび値を設定するには、**process cpu threshold type** グローバル コンフィギュレーション コマンドを使用します。

例

次の例では、NMS に VTP トラップを送信する方法を示します。

```
Switch(config)# snmp-server enable traps vtp
```

設定を確認するには、**show vtp status** 特権 EXEC コマンド、または **show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	スイッチの実行コンフィギュレーションを表示します。
snmp-server host	SNMP トラップを受信するホストを指定します。

snmp-server host

Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）通知処理の受信側（ホスト）を指定するには、**snmp-server host** グローバル コンフィギュレーション コマンドを使用します。指定されたホ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。

snmp-server host *host-addr* [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth**| **priv**}] [**vrf** *vrf-instance*] {*community-string* [*notification-type*]}

no snmp-server host *host-addr* [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}] [**vrf** *vrf-instance*] *community-string*

構文の説明

host-addr	ホスト（ターゲットとなる受信側）の名前またはインターネット アドレスです。
udp-port *port*	（任意）トラップを受信するホストの User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ポート番号を設定します。指定できる範囲は 0 ～ 65535 です。
informs | **traps**	（任意）このホストに SNMP トラップまたは情報を送信します。
version 1 | **2c** | **3**	（任意）トラップの送信に使用する SNMP のバージョンです。 次のキーワードがサポートされています。 **1**：SNMPv1。情報の場合は、このオプションを使用できません。 **2c**：SNMPv2C **3**：SNMPv3。バージョン 3 キーワードの後に、次に示すオプション キーワードを指定できます。 • **auth**（任意）：Message Digest 5（MD5）および Secure Hash Algorithm（SHA）によるパケット認証をイネーブルにします。 • **noauth**（デフォルト）：noAuthNoPriv セキュリティ レベルです。[**auth** | **noauth** | **priv**] キーワードが指定されていない場合は、これがデフォルトです。 • **priv**（任意）：Data Encryption Standard（DES; データ暗号化規格）によるパケット暗号化（*プライバシー*ともいう）をイネーブルにします。 **（注）** **priv** キーワードは、暗号化ソフトウェア イメージがインストールされている場合にだけ利用できます。
vrf *vrf-instance*	（任意）Virtual Private Network（VPN; 仮想プライベート ネットワーク）ルーティング インスタンスとホスト名です。
community-string	通知処理にともなって送信される、パスワードと類似したコミュニティ ストリングです。**snmp-server host** コマンドを使用してこのストリングを設定できますが、このストリングを定義するには、**snmp-server community** 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から、**snmp-server host** コマンドを使用することを推奨します。 **（注）** コンテキスト情報を区切るには @ 記号を使用します。このコマンドの設定時に SNMP コミュニティ ストリングの一部として @ 記号を使用しないでください。

notification-type　（任意）ホストに送信される通知のタイプです。タイプが指定されていない場合、すべての通知が送信されます。通知タイプには、次のキーワードの 1 つまたは複数を指定できます。

- **bgp**：Border Gateway Protocol（BGP）ステート変更トラップを送信します。このキーワードは、IP サービス イメージがスタック マスターにインストールされている場合にだけ使用できます。
- **bridge**：SNMP Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）ブリッジ MIB トラップを送信します。
- **cluster**：クラスタ メンバ ステータス トラップを送信します。
- **config**：SNMP 設定トラップを送信します。
- **copy-config**：SNMP コピー設定トラップを送信します。
- **cpu threshold**：CPU 関連トラップを許可します。
- **entity**：SNMP エンティティ トラップを送信します。
- **envmon**：環境モニタ トラップを送信します。
- **errdisable**：SNMP errdisable 通知を送信します。
- **flash**：SNMP FLASH 通知を送信します。
- **fru-ctrl**：エンティティ FRU 制御トラップを送信します。スイッチ スタックでは、このトラップはスタックにおけるスイッチの挿入/取り外しを意味します。
- **hsrp**：SNMP Hot Standby Router Protocol（HSRP; ホット スタンバイ ルータ プロトコル）トラップを送信します。
- **ipmulticast**：SNMP IP マルチキャスト ルーティング トラップを送信します。
- **mac-notification**：SNMP MAC 通知トラップを送信します。
- **msdp**：SNMP Multicast Source Discovery Protocol（MSDP）トラップを送信します。
- **ospf**：Open Shortest Path First（OSPF）トラップを送信します。
- **pim**：SNMP Protocol-Independent Multicast（PIM）トラップを送信します。
- **port-security**：SNMP ポートセキュリティ トラップを送信します。
- **rtr**：SNMP Response Time Reporter トラップを送信します。
- **snmp**：SNMP タイプ トラップを送信します。
- **storm-control**：SNMP ストーム制御トラップを送信します。
- **stpx**：SNMP STP 拡張 MIB トラップを送信します。
- **syslog**：SNMP Syslog トラップを送信します。
- **tty**：TCP 接続トラップを送信します。
- **udp-port** *port* **：** トラップを受信するホストの User Datagram Protocol（UDP）ポート番号を設定します。指定できる範囲は 0 ～ 65535 です。
- **vlan-membership**：SNMP VLAN メンバシップ トラップを送信します。
- **vlancreate**：SNMP VLAN 作成トラップを送信します。
- **vlandelete**：SNMP VLAN 削除トラップを送信します。
- **vtp**：SNMP VLAN Trunking Protocol（VTP）トラップを送信します。

デフォルト

このコマンドは、デフォルトでディセーブルです。通知は送信されません。

キーワードを指定しないでこのコマンドを入力した場合は、デフォルトで、すべてのトラップ タイプがホストに送信されます。情報はこのホストに送信されません。

version キーワードがない場合、デフォルトはバージョン 1 になります。

バージョン 3 を選択し、認証キーワードを入力しなかった場合は、デフォルトで、**noauth**（noAuthNoPriv）セキュリティ レベルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**bgp**、**copy-config**、**flash**、**port-security**、**stpx**、**syslog**、**vlancreate**、および **vlandelete** キーワードが追加されました。
12.2(18)SE	**ipmulticast**、**msdp**、**ospf**、および **pim** キーワードが追加されました。コマンド構文が変更されました。
12.2(25)SE	**storm-control** および **vrf** *vrf-instance* キーワードが追加されました。
12.2(37)SE	**errdisable notification-rate** *value* キーワードが追加されました。
12.2(50)SE	**cpu threshold** キーワードが追加されました。

使用上のガイドライン

SNMP 通知は、トラップまたは情報要求として送信できます。トラップを受信しても受信側は確認応答を送信しないため、トラップは信頼できません。送信側では、トラップが受信されたかどうかを判別できません。ただし、情報要求を受信した SNMP エンティティは、SNMP 応答 PDU を使用してメッセージに確認応答します。送信側が応答を受信しなかった場合は、再び情報要求を送信できます。したがって、情報が目的の宛先に到達する可能性が高まります。

ただし、情報はエージェントおよびネットワークのリソースをより多く消費します。送信と同時にドロップされるトラップと異なり、情報要求は応答を受信するまで、または要求がタイムアウトになるまで、メモリ内に保持する必要があります。また、トラップの送信は 1 回限りですが、情報は数回にわたって再試行が可能です。再試行によってトラフィックが増え、ネットワークのオーバーヘッドが大きくなる原因になります。

snmp-server host コマンドを入力しなかった場合は、通知が送信されません。SNMP 通知を送信するようにスイッチを設定するには、**snmp-server host** コマンドを少なくとも 1 つ入力する必要があります。キーワードを指定しないでこのコマンドを入力した場合、そのホストではすべてのトラップ タイプがイネーブルになります。複数のホストをイネーブルにするには、ホストごとに **snmp-server host** コマンドを個別に入力する必要があります。コマンドには複数の通知タイプをホストごとに指定できます。

ローカル ユーザがリモート ホストと関連付けられていない場合、スイッチは **auth**（authNoPriv）および **priv**（authPriv）の認証レベルの情報を送信しません。

同じホストおよび同じ種類の通知（トラップまたは情報）に対して複数の **snmp-server host** コマンドを指定した場合は、後に入力されたコマンドによって前のコマンドが上書きされます。最後の **snmp-server host** コマンドだけが有効です。たとえば、ホストに **snmp-server host inform** を入力してから、同じホストに別の **snmp-server host inform** コマンドを入力した場合は、2 番目のコマンドによって最初のコマンドが置き換えられます。

snmp-server host コマンドは、**snmp-server enable traps** グローバル コンフィギュレーション コマンドと組み合わせて使用します。グローバルに送信される SNMP 通知を指定するには、**snmp-server enable traps** コマンドを使用します。1 つのホストでほとんどの通知を受信する場合は、このホストに対して、少なくとも 1 つの **snmp-server enable traps** コマンドと **snmp-server host** コマンドをイネーブルにする必要があります。一部の通知タイプは、**snmp-server enable traps** コマンドで制御できません。たとえば、ある通知タイプは常にイネーブルですが、別の通知タイプはそれぞれ異なるコマンドによってイネーブルになります。

キーワードを指定しないで **no snmp-server host** コマンドを使用すると、ホストへのトラップはディセーブルになりますが、情報はディセーブルになりません。情報をディセーブルにするには、**no snmp-server host informs** コマンドを使用してください。

例

次の例では、トラップに対して一意の SNMP コミュニティ ストリング *comaccess* を設定し、このストリングによる、アクセスリスト 10 を介した SNMP ポーリング アクセスを禁止します。

```
Switch(config)# snmp-server community comaccess ro 10
Switch(config)# snmp-server host 172.20.2.160 comaccess
Switch(config)# access-list 10 deny any
```

次の例では、名前 *myhost.cisco.com* で指定されたホストに SNMP トラップを送信する方法を示します。コミュニティ ストリングは、*comaccess* として定義されています。

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com comaccess snmp
```

次の例では、コミュニティ ストリング *public* を使用して、すべてのトラップをホスト *myhost.cisco.com* に送信するようにスイッチをイネーブルにする方法を示します。

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	スイッチの実行コンフィギュレーションを表示します。
snmp-server enable traps	各種トラップ タイプまたは情報要求の SNMP 通知をイネーブルにします。

snmp trap mac-notification change

特定のレイヤ 2 のインターフェイスで、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）MAC アドレス変更通知トラップをイネーブルにするには、**snmp trap mac-notification change** 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。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。

snmp trap mac-notification change {added | removed}

no snmp trap mac-notification change {added | removed}

構文の説明

added	MAC アドレスがインターフェイスに追加されると、MAC 通知トラップをイネーブルにします。
removed	MAC アドレスがインターフェイスから削除されると、MAC 通知トラップをイネーブルにします。

デフォルト

デフォルトでは、アドレス追加および削除に対するトラップは両方ともディセーブルです。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(40)SE	**change** という言葉がコマンドに追加されました。

使用上のガイドライン

snmp trap mac-notification change コマンドを使用して、特定のインターフェイスの通知トラップをイネーブルにできますが、トラップが生成されるのは、**snmp-server enable traps mac-notification change** および **mac address-table notification change** グローバル コンフィギュレーション コマンドをイネーブルにした場合だけです。

例

次の例では、MAC アドレスがポートに追加されたときに MAC 通知トラップをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# snmp trap mac-notification change added
```

show mac address-table notification change interface 特権 EXEC コマンドを入力すれば、設定を確認することができます。

関連コマンド

コマンド	説明
clear mac address-table notification	MAC アドレス通知グローバル カウンタをクリアします。
mac address-table notification	MAC アドレス通知機能をイネーブルにします。
show mac address-table notification	**interface** キーワードが追加されると、すべての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対する MAC アドレス通知設定を表示します。
snmp-server enable traps	**mac-notification** キーワードが追加された場合に SNMP MAC 通知トラップを送信します。

spanning-tree backbonefast

BackboneFast 機能をイネーブルにするには、**spanning-tree backbonefast** グローバル コンフィギュレーション コマンドを使用します。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。

spanning-tree backbonefast

no spanning-tree backbonefast

構文の説明

このコマンドには、引数またはキーワードはありません。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

BackboneFast 機能は、Rapid PVST+ または Multiple Spanning-Tree（MST）モード用に設定できますが、スパニング ツリー モードを PVST+ に変更するまでこの機能はディセーブル（非アクティブ）のままです。

スイッチのルート ポートまたはブロックされたポートが、指定スイッチから不良 BPDU を受信すると、BackboneFast が開始します。不良 BPDU は、ルート ブリッジと指定スイッチの両方を宣言しているスイッチを識別します。スイッチが不良 BPDU を受信した場合、そのスイッチが直接接続されていないリンク（*間接*リンク）で障害が発生したことを意味します（つまり、指定スイッチとルート スイッチ間の接続が切断されています）。ルート スイッチへの代替パスがある場合に BackboneFast を使用すると、不良 BPDU を受信するインターフェイスの最大エージング タイムが期限切れになり、ブロックされたポートをただちにリスニング ステートに移行できます。その後、BackboneFast はインターフェイスをフォワーディング ステートに移行させます。詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

間接リンク障害を検出し、スパニング ツリーの再認識をより短時間で開始できるようにするには、サポートするすべてのスイッチで BackboneFast をイネーブルにします。

例

次の例では、スイッチ上で BackboneFast をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree backbonefast
```

設定を確認するには、**show spanning-tree summary** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree summary	スパニング ツリー インターフェイス ステートのサマリーを表示します。

spanning-tree bpdufilter

インターフェイスでの UniDirectional Link Detection（UDLD; 単一方向リンク検出）の送受信を禁止するには、**spanning-tree bpdufilter** 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。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 bpdufilter {**disable** | **enable**}

no spanning-tree bpdufilter

構文の説明

disable	指定された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。
enable	指定された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。

デフォルト

BPDU フィルタリング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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

スイッチが Per-VLAN Spanning-Tree Plus（PVST+）モード、Rapid-PVST+ モード、または Multiple Spanning-Tree（MST）モードで稼動している場合は、BPDU フィルタリング機能をイネーブルにできます。

注意　BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニング ツリーをディセーブルにすることと同じであり、スパニング ツリー ループが発生することがあります。

すべての PortFast 対応インターフェイス上で BPDU フィルタリングをグローバルにイネーブルにするには、**spanning-tree portfast bpdufilter default** グローバル コンフィギュレーション コマンドを使用します。

spanning-tree bpdufilter インターフェイス コンフィギュレーション コマンドを使用すると、**spanning-tree portfast bpdufilter default** グローバル コンフィギュレーション コマンドの設定を上書きできます。

例

次の例では、ポート上で BPDU フィルタリング機能をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# spanning-tree bpdufilter enable
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	現在の動作設定を表示します。
spanning-tree portfast（グローバル コンフィギュレーション）	PortFast 対応インターフェイス上で BPDU フィルタリング機能または BPDU ガード機能をグローバルにイネーブルにするか、またはすべての非トランク インターフェイスで PortFast 機能をイネーブルにします。
spanning-tree portfast（インターフェイス コンフィギュレーション）	特定のインターフェイスおよび対応するすべての VLAN 上で、PortFast 機能をイネーブルにします。

spanning-tree bpduguard

UniDirectional Link Detection（UDLD; 単一方向リンク検出）を受信したインターフェイスを errdisable ステートにするには、**spanning-tree bpduguard** 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。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 {**disable** | **enable**}

no spanning-tree bpduguard

構文の説明

disable	指定された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。
enable	指定されたインターフェイス上で BPDU ガードをイネーブルにします。

デフォルト

BPDU ガ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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

インターフェイスを手動で再び動作させなければならない場合、無効な設定を防ぐには、BPDU ガード機能が役に立ちます。サービスプロバイダー ネットワーク内でインターフェイスがスパニング ツリー トポロジに参加しないようにするには、BPDU ガード機能を使用します。

スイッチが Per-VLAN Spanning-Tree Plus（PVST+）モード、Rapid-PVST+ モード、または Multiple Spanning-Tree（MST）モードで稼動している場合は、BPDU ガード機能をイネーブルにできます。

すべての PortFast 対応インターフェイス上で BPDU ガードをグローバルにイネーブルにするには、**spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドを使用します。

spanning-tree bpduguard インターフェイス コンフィギュレーション コマンドを使用すると、**spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドの設定を上書きできます。

例

次の例では、ポートで BPDU ガード機能をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# spanning-tree bpduguard enable
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	現在の動作設定を表示します。
spanning-tree portfast（グローバル コンフィギュレーション）	PortFast 対応インターフェイス上で BPDU フィルタリング機能または BPDU ガード機能をグローバルにイネーブルにするか、またはすべての非トランク インターフェイスで PortFast 機能をイネーブルにします。
spanning-tree portfast（インターフェイス コンフィギュレーション）	特定のインターフェイスおよび対応するすべての VLAN 上で、PortFast 機能をイネーブルにします。

spanning-tree cost

スパニング ツリー計算に使用するパス コストを設定するには、**spanning-tree cost** 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。ループが発生した場合、スパニング ツリーはパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。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*] **cost** *cost*

no spanning-tree [**vlan** *vlan-id*] **cost**

構文の説明

vlan *vlan-id*	（任意）スパニング ツリー インスタンスに関連付けられた VLAN 範囲です。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。
cost	パス コスト。指定できる範囲は 1 ～ 200000000 です。値が大きいほど、コストが高くなります。

デフォルト

デフォルト パス コストは、インターフェイス帯域幅の設定から計算されます。IEEE のデフォルト パス コスト値は、次のとおりです。

- 1000 Mb/s : 4
- 100 Mb/s : 19
- 10 Mb/s : 100

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	*vlan-id* 変数の値が変更されました。

使用上のガイドライン

コストを設定する場合は、値が大きいほどコストが高くなります。

spanning-tree vlan *vlan-id* **cost** *cost* コマンドおよび **spanning-tree cost** *cost* コマンドの両方を使用してインターフェイスを設定する場合、**spanning-tree vlan** *vlan-id* **cost** *cost* コマンドが有効になります。

例

次の例では、ポートでパス コストを 250 に設定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# spanning-tree cost 250
```

次の例では、VLAN 10、12 ～ 15、20 にパス コストとして 300 を設定する方法を示します。

```
Switch(config-if)# spanning-tree vlan 10,12-15,20 cost 300
```

設定を確認するには、**show spanning-tree interface** *interface-id* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree interface *interface-id*	指定したインターフェイスのスパニング ツリー情報を表示します。
spanning-tree port-priority	インターフェイス プライオリティを設定します。
spanning-tree vlan priority	指定したスパニング ツリー インスタンスのスイッチ プライオリティを設定します。

spanning-tree etherchannel guard misconfig

スイッチが EtherChannel の設定に矛盾を検出した場合にエラー メッセージを表示するには、**spanning-tree etherchannel guard misconfig** グローバル コンフィギュレーション コマンドを使用します。この機能をディセーブルにする場合は、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

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

EtherChannel ガードはスイッチ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

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

スイッチが EtherChannel の設定に矛盾を検出すると、次のエラー メッセージが表示されます。

```
PM-4-ERR_DISABLE: Channel-misconfig error detected on [chars], putting [chars] in
err-disable state.
```

設定に矛盾を持つ EtherChannel にあるスイッチ ポートを表示するには、**show interfaces status err-disabled** 特権 EXEC コマンドを使用します。リモート デバイスの EtherChannel 設定を確認するには、リモート デバイスで **show etherchannel summary** 特権 EXEC コマンドを使用します。

EtherChannel 設定の矛盾によりポートが errdisable ステートの場合は、**errdisable recovery cause channel-misconfig** 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 shut down** インターフェイス コンフィギュレーション コマンドを入力して、手動で再びイネーブルにすることができます。

例

次の例では、EtherChannel 設定矛盾のガード機能をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree etherchannel guard misconfig
```

設定を確認するには、**show spanning-tree summary** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
errdisable recovery cause channel-misconfig	EtherChannel 設定の矛盾による errdisable ステートから回復するタイマーをイネーブルにします。
show etherchannel summary	チャネルの EtherChannel 情報を、チャネルグループ単位で 1 行のサマリーとして表示します。
show interfaces status err-disabled	errdisable ステートのインターフェイスを表示します。

spanning-tree extend system-id

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** グローバル コンフィギュレーション コマンドを使用します。

spanning-tree extend system-id

（注）このコマンドの **no** バージョンは、コマンドラインのヘルプ ストリングには表示されますが、サポートされていません。拡張システム ID 機能をディセーブルにすることはできません。

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

拡張システム ID 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

スイッチは、IEEE 802.1t スパニング ツリー拡張をサポートします。以前スイッチ プライオリティに使用されたビットの一部を、現在は拡張システム ID（Per-VLAN Spanning-Tree Plus（PVST+）と Rapid PVST+ の VLAN 識別子、または Multiple Spanning-Tree（MST）のインスタンス識別子）に使用しています。

スパニング ツリーは、ブリッジ ID が VLAN または Multiple Spanning-Tree インスタンスごとに一意となるように、拡張システム ID、スイッチ プライオリティ、および割り当てられたスパニング ツリー MAC アドレスを使用しています。スイッチ スタックは他のネットワークからは単一のスイッチとして認識されるため、スタック内のすべてのスイッチは、指定のスパニング ツリーに対して同一のブリッジ ID を使用します。スタック マスターに障害が発生した場合、スタック メンバは、スタック マスターの新しい MAC アドレスに基づいて、実行しているスパニング ツリーすべてのブリッジ ID を再計算します。

拡張システム ID のサポートにより、ルート スイッチ、セカンダリ ルート スイッチ、および VLAN のスイッチ プライオリティの手動での設定方法に影響が生じます。詳細については、「spanning-tree mst root」および「spanning-tree vlan」の項を参照してください。

ネットワーク上に拡張システム ID をサポートするスイッチとサポートしないスイッチが混在する場合は、拡張システム ID をサポートするスイッチがルート スイッチになることはほぼありません。拡張システム ID によって、接続されたスイッチのプライオリティより VLAN 番号が大きくなるたびに、スイッチ プライオリティ値が増大します。

関連コマンド

コマンド	説明
show spanning-tree summary	スパニング ツリー インターフェイス ステートのサマリーを表示します。
spanning-tree mst root	ネットワークの直径に基づいて、MST ルート スイッチのプライオリティおよびタイマーを設定します。
spanning-tree vlan priority	指定したスパニング ツリー インスタンスのスイッチ プライオリティを設定します。

spanning-tree guard

選択されたインターフェイスに関連付けられたすべての VLAN 上でルート ガードまたはループ ガードをイネーブルにするには、**spanning-tree guard** 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。ルート ガードは、スパニング ツリー ルート ポートまたはスイッチのルートへのパスになることが可能なインターフェイスを制限します。ループ ガードは、障害によって単一方向リンクが作成された場合に、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ないようにします。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 | none | root}

no spanning-tree guard

構文の説明

loop	ループ ガードをイネーブルにします。
none	ルート ガードまたはループ ガードをディセーブルにします。
root	ルート ガードをイネーブルにします。

デフォルト

ルート ガードはディセーブルです。

ループ ガードは、**spanning-tree loopguard default** グローバル コンフィギュレーション コマンドに従って設定されます（グローバルにディセーブル化）。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

スイッチが Per-VLAN Spanning-Tree Plus（PVST+）モード、Rapid-PVST+ モード、または Multiple Spanning-Tree（MST）モードで稼動している場合は、ルート ガードまたはループ ガード機能をイネーブルにできます。

ルート ガードがイネーブルの場合に、スパニング ツリーを計算すると、インターフェイスがルート ポートとして選択され、root-inconsistent（ブロック）ステートに移行します。これにより、カスタマーのスイッチがルート スイッチになったり、ルートへのパスになったりすることはなくなります。ルート ポートは、スイッチからルート スイッチまでの最適パスを提供します。

no spanning-tree guard または **no spanning-tree guard none** コマンドを入力すると、ルート ガードは選択されたインターフェイスのすべての VLAN でディセーブルになります。このインターフェイスが root-inconsistent（ブロック）ステートの場合、インターフェイスはリスニング ステートに自動的に移行します。

UplinkFast 機能で使用するインターフェイスでは、ルート ガードをイネーブルにしないでください。UplinkFast を使用すると、障害発生時に（ブロック ステートの）バックアップ インターフェイスがルート ポートになります。しかし、同時にルート ガードもイネーブルになっていた場合は、UplinkFast 機能で使用されるすべてのバックアップ インターフェイスが root-inconsistent（ブロック）ステートになり、フォワーディング ステートに移行できなくなります。スイッチが Rapid-PVST+ モードまたは MST モードで稼動している場合、UplinkFast 機能は使用できません。

ループ ガード機能は、スイッチド ネットワーク全体に設定した場合に最も効果があります。スイッチが PVST+ モードまたは Rapid-PVST+ モードで動作している場合、ループ ガードによって、代替ポートおよびルート ポートが指定ポートとして使用されることを防ぎます。スパニング ツリーはルート ポートまたは代替ポートで UniDirectional Link Detection（UDLD; 単一方向リンク検出）を送信しません。スイッチが MST モードで動作している場合に、すべての MST インスタンスでインターフェイスがループ ガードによってブロックされているときは、BPDU は非境界インターフェイスからは送信されません。境界インターフェイスでは、ループ ガードによってすべての MST インスタンスでインターフェイスがブロックされます。

ルート ガードまたはループ ガードをディセーブルにする場合は、**spanning-tree guard none** 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。ルート ガードとループ ガードの両方を同時にイネーブルにすることはできません。

spanning-tree loopguard default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree guard loop** 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。

例

次の例では、指定のポートに関連付けられたすべての VLAN で、ルート ガードをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# spanning-tree guard root
```

次の例では、指定のポートに関連付けられたすべての VLAN で、ループ ガードをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# spanning-tree guard loop
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	現在の動作設定を表示します。
spanning-tree cost	スパニング ツリーの計算に使用するパス コストを設定します。
spanning-tree loopguard default	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ないようにします。
spanning-tree mst cost	MST の計算に使用するパス コストを設定します。
spanning-tree mst port-priority	インターフェイス プライオリティを設定します。
spanning-tree mst root	ネットワークの直径に基づいて、MST ルート スイッチのプライオリティおよびタイマーを設定します。
spanning-tree port-priority	インターフェイス プライオリティを設定します。
spanning-tree vlan priority	指定したスパニング ツリー インスタンスのスイッチ プライオリティを設定します。

spanning-tree link-type

インターフェイスのデュプレックス モードによって決まるデフォルトのリンクタイプ設定を上書きし、フォワーディング ステートへの Rapid Spanning-Tree 移行をイネーブルにするには、**spanning-tree link-type** 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。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

構文の説明

point-to-point	インターフェイスのリンク タイプがポイントツーポイントであることを指定します。
shared	インターフェイスのリンク タイプが共有であることを指定します。

デフォルト

スイッチは、デュプレックス モードからインターフェイスのリンク タイプを取得します。つまり、全二重インターフェイスはポイントツーポイント リンク、半二重インターフェイスは共有リンクであると見なされます。

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

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

リンク タイプのデフォルト設定を上書きするには、**spanning-tree link-type** コマンドを使用します。たとえば、半二重リンクは、Multiple Spanning-Tree Protocol（MSTP）または Rapid Per-VLAN Spanning-Tree Plus（Rapid-PVST+）プロトコルが稼動し高速移行がイネーブルであるリモート スイッチの 1 つのインターフェイスに、ポイントツーポイントで物理的に接続できます。

例

次の例では、（デュプレックスの設定に関係なく）リンク タイプを共有に指定し、フォワーディング ステートへの高速移行を禁止する方法を示します。

```
Switch(config-if)# spanning-tree link-type shared
```

設定を確認するには、**show spanning-tree mst interface** *interface-id* または show **spanning-tree interface** *interface-id* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
clear spanning-tree detected-protocols	すべてのインターフェイスまたは指定されたインターフェイスでプロトコル移行プロセスを再開（強制的に近接スイッチと再びネゴシエートさせる）します。
show spanning-tree interface *interface-id*	指定したインターフェイスのスパニング ツリー ステート情報を表示します。
show spanning-tree mst interface *interface-id*	指定したインターフェイスの MST 情報を表示します。

spanning-tree loopguard default

代替ポートまたはルート ポートが、単一方向リンクを発生させる障害が原因で指定ポートとして使用されないようにするには、**spanning-tree loopguard default** グローバル コンフィギュレーション 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 loopguard default

no spanning-tree loopguard default

構文の説明

このコマンドには、引数またはキーワードはありません。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

スイッチが Per-VLAN Spanning-Tree Plus（PVST+）モード、Rapid-PVST+ モード、または Multiple Spanning-Tree（MST）モードで稼動している場合は、ループ ガード機能をイネーブルにできます。

ループ ガード機能は、スイッチド ネットワーク全体に設定した場合に最も効果があります。スイッチが PVST+ モードまたは Rapid-PVST+ モードで動作している場合、ループ ガードによって、代替ポートおよびルート ポートが指定ポートとして使用されることを防ぎます。スパニング ツリーはルート ポートまたは代替ポートで UniDirectional Link Detection（UDLD; 単一方向リンク検出）を送信しません。スイッチが MST モードで動作している場合に、すべての MST インスタンスでインターフェイスがループ ガードによってブロックされているときは、BPDU は非境界インターフェイスからは送信されません。境界インターフェイスでは、ループ ガードによってすべての MST インスタンスでインターフェイスがブロックされます。

ループ ガードは、スパニング ツリーがポイントツーポイントと見なすインターフェイス上でだけ動作します。

spanning-tree loopguard default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree guard loop** 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。

例

次の例では、ループ ガードをグローバルにイネーブルする方法を示します。

```
Switch(config)# spanning-tree loopguard default
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	現在の動作設定を表示します。
spanning-tree guard loop	指定したインターフェイスに関連付けられたすべての VLAN で、ループ ガード機能をイネーブルにします。

spanning-tree mode

スイッチ上で Per-VLAN Spanning-Tree Plus（PVST+）、Rapid PVST+、または Multiple Spanning-Tree（MST）をイネーブルにするには、**spanning-tree mode** グローバル コンフィギュレーション 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 {mst | pvst | rapid-pvst}

no spanning-tree mode

構文の説明

mst	MST および Rapid Spanning-Tree Protocol（RSTP）をイネーブルにします（IEEE 802.1s および IEEE 802.1w に準拠）。
pvst	PVST+ をイネーブルにします（IEEE 802.1D に準拠）。
rapid-pvst	Rapid PVST+ をイネーブルにします（IEEE 802.1w に準拠）。

デフォルト

デフォルト モードは PVST+ 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**mst** および **rapid-pvst** キーワードが追加されました。

使用上のガイドライン

スイッチは PVST+、Rapid PVST+、および MSTP に対応していますが、PVST+、Rapid PVST+、または MSTP のいずれかをすべての VLAN が実行するというように、アクティブにできるのは常に 1 つのバージョンだけです。すべてのスタック メンバは、同一のスパニング ツリー バージョンを実行します。

MST モードをイネーブルにすると、RSTP が自動的にイネーブルになります。

注意　スパニング ツリー モードを変更すると、すべてのスパニング ツリー インスタンスは以前のモードであるため停止し、新しいモードで再起動するので、トラフィックを中断させる可能性があります。

例

次の例では、スイッチ上で MST および RSTP をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree mode mst
```

次の例では、スイッチ上で Rapid PVST+ をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree mode rapid-pvst
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	現在の動作設定を表示します。

spanning-tree mst configuration

Multiple Spanning-Tree（MST）リージョンを設定する場合に使用する MST コンフィギュレーション モードを開始するには、**spanning-tree mst configuration** グローバル コンフィギュレーション 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

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトでは、すべての VLAN が Common and Internal Spanning-Tree（CIST）インスタンス（インスタンス 0）にマッピングされます。

デフォルト名は空の文字列です。

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

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。
12.2(25)SEC	*instance-id* の範囲が 1 ～ 4094 に変更されました。

使用上のガイドライン

spanning-tree mst configuration コマンドを入力すると、MST コンフィギュレーション モードが開始します。使用できるコンフィギュレーション コマンドは、次のとおりです。

- **abort** : 設定変更を適用しないで、MST リージョン コンフィギュレーション モードを終了します。
- **exit** : MST リージョン コンフィギュレーション モードを終了し、すべての設定変更を適用します。
- **instance** *instance-id* **vlan** *vlan-range* : VLAN を MST インスタンスにマッピングします。*instance-id* に指定できる範囲は 1 ～ 4094 です。*vlan-range* に指定できる範囲は 1 ～ 4094 です。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。
- **name** *name* : 設定名を設定します。*name* ストリングには最大 32 文字使用でき、大文字と小文字が区別されます。
- **no** : **instance**、**name**、および **revision** コマンドを無視するか、またはデフォルト設定に戻します。
- **private-vlan** : このコマンドは、コマンドラインのヘルプ ストリングには表示されますが、サポートされていません。
- **revision** *version* : 設定のリビジョン番号を設定します。指定できる範囲は 0 ～ 65535 です。
- **show** [**current** | **pending**] : 現在のまたは保留中の MST リージョンの設定を表示します。

MST モードでは、スイッチ スタックは最大 65 個の MST インスタンスをサポートします。特定の MST インスタンスにマッピング可能な VLAN 数に制限はありません。

VLAN を MST インスタンスにマッピングすると、マッピングは増分で実行されます。コマンドで指定された VLAN は、すでにマッピング済みの VLAN に対して追加または削除されます。範囲を指定する場合はハイフンを使用します。たとえば、**instance 1 vlan 1-63** を指定した場合、VLAN 1 ～ 63 を MST インスタンス 1 にマッピングします。列挙して指定する場合はカンマを使用します。たとえば、**instance 1 vlan 10, 20, 30** を指定した場合、VLAN 10、20、および 30 を MST インスタンス 1 にマッピングします。

明示的に MST インスタンスにマッピングされていないすべての VLAN は、Common and Internal Spanning Tree（CIST）インスタンス（インスタンス 0）にマッピングされます。このマッピングは、このコマンドの **no** 形式では CIST から解除できません。

2 台以上のスイッチが同一 MST リージョン内に存在する場合、同じ VLAN マッピング、同じコンフィギュレーション リビジョン番号、および同じ名前が設定されている必要があります。

例

次の例では、MST コンフィギュレーション モードを開始して VLAN 10 ～ 20 を MST インスタンス 1 にマッピングし、リージョンに *region1* と名前を付けて、コンフィギュレーション リビジョンを 1 に設定します。その後、変更確認前の設定を表示して変更を適用し、グローバル コンフィギュレーション モードに戻る方法を示します。

```
Switch# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name region1
Switch(config-mst)# revision 1
Switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
--------  ---------------------
0         1-9,21-4094
1         10-20
-------------------------------

Switch(config-mst)# exit
Switch(config)#
```

次の例では、VLAN 1 ～ 100 を、すでに同じ VLAN がマッピングされている場合でも、インスタンス 2 に追加し、ここでインスタンス 2 にマッピングした VLAN 40 ～ 60 を CIST インスタンスに移動します。その後、インスタンス 10 に VLAN 10 を追加し、インスタンス 2 にマッピングされているすべての VLAN を削除して、それらを CIST インスタンスにマッピングする方法を示します。

```
Switch(config-mst)# instance 2 vlan 1-100
Switch(config-mst)# no instance 2 vlan 40-60
Switch(config-mst)# instance 10 vlan 10
Switch(config-mst)# no instance 2
```

設定を確認するには、**show pending** MST コンフィギュレーション コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst configuration	MST リージョンの設定を表示します。

spanning-tree mst cost

Multiple Spanning-Tree（MST）計算に使用するパス コストを設定するには、**spanning-tree mst cost** 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。ループが発生した場合、スパニング ツリーはパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。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*

no spanning-tree mst *instance-id* **cost**

構文の説明

instance-id	スパニング ツリー インスタンス範囲。1 つのインスタンス、それぞれをハイフンで区切ったインスタンス範囲、またはカンマで区切った一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。
cost	パス コストの範囲は 1 ～ 200000000 です。値が大きいほど、コストが高くなります。

デフォルト

デフォルト パス コストは、インターフェイス帯域幅の設定から計算されます。IEEE のデフォルト パス コスト値は、次のとおりです。

- 1000 Mb/s : 20000
- 100 Mb/s : 200000
- 10 Mb/s : 2000000

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

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。
12.2(25)SEC	*instance-id* の範囲が 1 ～ 4094 に変更されました。

使用上のガイドライン

コストを設定する場合は、値が大きいほどコストが高くなります。

例

次の例では、インスタンス 2 および 4 に関連付けられたポートにパス コストとして 250 を設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# spanning-tree mst 2,4 cost 250
```

設定を確認するには、**show spanning-tree mst interface** *interface-id* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst interface *interface-id*	指定したインターフェイスの MST 情報を表示します。
spanning-tree mst port-priority	インターフェイス プライオリティを設定します。
spanning-tree mst priority	指定したスパニング ツリー インスタンスのスイッチ プライオリティを設定します。

spanning-tree mst forward-time

すべての Multiple Spanning-Tree（MST）インスタンスに転送遅延時間を設定するには、**spanning-tree mst forward-time** グローバル コンフィギュレーション コマンドを使用します。転送遅延時間には、インターフェイスが転送を開始するまでに、リスニング ステートおよびラーニング ステートがそれぞれ継続する時間を指定します。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

構文の説明

seconds	リスニング ステートおよびラーニング ステートの継続時間です。指定できる範囲は 4 ～ 30 秒です。

デフォルト

デフォルト値は 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

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

spanning-tree mst forward-time コマンドを変更すると、すべてのスパニング ツリー インスタンスに影響します。

例

次の例では、すべての MST インスタンスについて、スパニング ツリーの転送遅延時間を 18 秒に設定する方法を示します。

```
Switch(config)# spanning-tree mst forward-time 18
```

設定を確認するには、**show spanning-tree mst** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst	MST 情報を表示します。
spanning-tree mst hello-time	ルート スイッチ コンフィギュレーション メッセージから送信される hello UniDirectional Link Detection（UDLD; 単一方向リンク検出）の間隔を設定します。
spanning-tree mst max-age	スパニング ツリーがルート スイッチからメッセージを受信する間隔を設定します。
spanning-tree mst max-hops	BPDU がドロップされるまでのリージョンのホップ数を設定します。

spanning-tree mst hello-time

ルート スイッチ コンフィギュレーション メッセージから送信される hello UniDirectional Link Detection（UDLD; 単一方向リンク検出）の間隔を設定するには、**spanning-tree mst hello-time** グローバル コンフィギュレーション 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

構文の説明

seconds	ルート スイッチ コンフィギュレーション メッセージから送信される hello BPDU の間隔です。指定できる範囲は 1 ～ 10 秒です。

デフォルト

デフォルト値は 2 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

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

spanning-tree mst max-age seconds グローバル コンフィギュレーション コマンドを設定した後に、スイッチが指定された間隔の間にルート スイッチから BPDU を受信しなかった場合は、スパニング ツリー トポロジが再計算されます。**max-age** の設定値は、**hello-time** の設定値よりも大きくなければなりません。

spanning-tree mst hello-time コマンドを変更すると、すべてのスパニング ツリー インスタンスに影響します。

例

次の例では、すべての Multiple Spanning-Tree（MST）インスタンスについて、スパニング ツリーの hello タイムを 3 秒に設定する方法を示します。

```
Switch(config)# spanning-tree mst hello-time 3
```

設定を確認するには、**show spanning-tree mst** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst	MST 情報を表示します。
spanning-tree mst forward-time	すべての MST インスタンスについて転送遅延時間を設定します。

コマンド	説明
spanning-tree mst max-age	スパニング ツリーがルート スイッチからメッセージを受信する間隔を設定します。
spanning-tree mst max-hops	BPDU がドロップされるまでのリージョンのホップ数を設定します。

spanning-tree mst max-age

スパニング ツリーがルート スイッチから受信するメッセージの間隔を設定するには、**spanning-tree mst max-age** グローバル コンフィギュレーション コマンドを使用します。スイッチがこのインターバル内にルート スイッチから UniDirectional Link Detection（UDLD; 単一方向リンク検出）メッセージを受信しなかった場合は、スパニング ツリー トポロジが再計算されます。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

構文の説明

seconds	スパニング ツリーがルート スイッチからメッセージを受信する間隔です。指定できる範囲は 6 ～ 40 秒です。

デフォルト

デフォルト値は 20 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

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

spanning-tree mst max-age seconds グローバル コンフィギュレーション コマンドを設定した後に、スイッチが指定された間隔の間にルート スイッチから BPDU を受信しなかった場合は、スパニング ツリー トポロジが再計算されます。**max-age** の設定値は、**hello-time** の設定値よりも大きくなければなりません。

spanning-tree mst max-age コマンドを変更すると、すべてのスパニング ツリー インスタンスに影響します。

例

次の例では、すべての Multiple Spanning-Tree（MST）インスタンスについて、スパニング ツリーの有効期限を 30 秒に設定する方法を示します。

```
Switch(config)# spanning-tree mst max-age 30
```

設定を確認するには、**show spanning-tree mst** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst	MST 情報を表示します。
spanning-tree mst forward-time	すべての MST インスタンスについて転送遅延時間を設定します。

コマンド	説明
spanning-tree mst hello-time	ルート スイッチ コンフィギュレーション メッセージが送信する hello BPDU の間隔を設定します。
spanning-tree mst max-hops	BPDU がドロップされるまでのリージョンのホップ数を設定します。

spanning-tree mst max-hops

UniDirectional Link Detection（UDLD; 単一方向リンク検出）がドロップされて、インターフェイス用に保持された情報が期限切れになるまでのリージョンのホップ数を設定するには、**spanning-tree mst max-hops** グローバル コンフィギュレーション 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 *hop-count*

no spanning-tree mst max-hops

構文の説明

hop-count	BPDU がドロップされるまでのリージョンのホップ数です。指定できるホップ数の範囲は 1 ～255 です。

デフォルト

デフォルトのホップ数は 20 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

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。
12.2(25)SEC	*hop-count* の範囲が 1 ～ 255 に変更されました。

使用上のガイドライン

インスタンスのルート スイッチは、常にコストを 0、ホップ カウントを最大値に設定して BPDU（または M レコード）を送信します。スイッチは、この BPDU を受信すると、受信した残りのホップ カウントを 1 つ減らして、生成する M レコードの残りのホップ カウントとしてこの値を伝播します。ホップ カウントが 0 になると、スイッチは BPDU をドロップして、インターフェイス用に保持された情報を期限切れにします。

spanning-tree mst max-hops コマンドを変更すると、すべてのスパニング ツリー インスタンスに影響します。

例

次の例では、すべての Multiple Spanning-Tree（MST）インスタンスについて、スパニング ツリーの最大ホップ数を 10 に設定する方法を示します。

```
Switch(config)# spanning-tree mst max-hops 10
```

設定を確認するには、**show spanning-tree mst** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst	MST 情報を表示します。
spanning-tree mst forward-time	すべての MST インスタンスについて転送遅延時間を設定します。
spanning-tree mst hello-time	ルートスイッチコンフィギュレーションメッセージが送信する hello BPDU の間隔を設定します。
spanning-tree mst max-age	スパニング ツリーがルート スイッチからメッセージを受信する間隔を設定します。

spanning-tree mst port-priority

インターフェイス プライオリティを設定するには、**spanning-tree mst port-priority** 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。ループが発生した場合、Multiple Spanning-Tree Protocol（MSTP）はフォワーディング ステートに設定するインターフェイスを判別できます。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* **port-priority** *priority*

no spanning-tree mst *instance-id* **port-priority**

構文の説明

instance-id	スパニング ツリー インスタンス範囲。1 つのインスタンス、それぞれをハイフンで区切ったインスタンス範囲、またはカンマで区切った一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。
priority	指定できる範囲は 0 ～ 240 で、16 ずつ増加します。有効なプライオリティ値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。それ以外の値はすべて拒否されます。値が小さいほど、プライオリティが高くなります。

デフォルト

デフォルト値は 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

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。
12.2(25)SEC	*instance-id* の範囲が 1 ～ 4094 に変更されました。

使用上のガイドライン

最初に選択させるインターフェイスには高いプライオリティ（小さい数値）を割り当て、最後に選択させるインターフェイスには低いプライオリティ（大きい数値）を割り当てることができます。すべてのインターフェイスに同じプライオリティ値が付けられている場合、Multiple Spanning-Tree（MST）はインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

スイッチがスイッチ スタックのメンバの場合、**spanning-tree mst** [*instance vlan-id*] **port-priority** *priority* インターフェイス コンフィギュレーション コマンドの代わりに、**spanning-tree mst** [*instance-id*] **cost** *cost* インターフェイス コンフィギュレーション コマンドを使用して、フォワーディング ステートにするインターフェイスを選択しなければなりません。最初に選択させるインターフェイスには低いコスト値を割り当て、最後に選択させるインターフェイスには高いコスト値を割り当てます。

例

次の例では、ループが発生した場合に、スパニング ツリー インスタンス 20 および 22 に関連付けられたインターフェイスがフォワーディング ステートになる可能性を高める方法を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# spanning-tree mst 20,22 port-priority 0
```

設定を確認するには、**show spanning-tree mst interface** *interface-id* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst interface *interface-id*	指定したインターフェイスの MST 情報を表示します。
spanning-tree mst cost	MST の計算に使用するパス コストを設定します。
spanning-tree mst priority	指定したスパニング ツリー インスタンスのスイッチ プライオリティを設定します。

spanning-tree mst pre-standard

先行標準 UniDirectional Link Detection（UDLD; 単一方向リンク検出）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** 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。

spanning-tree mst pre-standard

no spanning-tree mst pre-standard

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

デフォルトのステートは、先行標準ネイバーの自動検出です。

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

コマンド履歴

リリース	変更内容
12.2(25)SEC	このコマンドが追加されました。

使用上のガイドライン

ポートでは、先行標準と標準の両方の BPDU を受け入れることができます。ネイバー タイプが不一致の場合、Common and Internal Spanning Tree（CIST）だけがこのインターフェイスで実行されます。

（注）スイッチのポートが、先行標準の Cisco IOS ソフトウェアを実行しているスイッチに接続されている場合には、ポートに対して **spanning-tree mst pre-standard** インターフェイス コンフィギュレーション コマンドを使用する*必要があります*。先行標準 BPDU だけを送信するようにポートを設定していない場合、Multiple STP（MSTP）のパフォーマンスが低下することがあります。

自動的に先行標準ネイバーを検出するようにポートが設定されている場合、*show* **spanning-tree mst** コマンドに **prestandard** フラグが常に表示されます。

例

次の例では、先行標準 BPDU だけを送信するようにポートを設定する方法を示します。

```
Switch(config-if)# spanning-tree mst pre-standard
```

設定を確認するには、**show spanning-tree mst** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst *instance-id*	*prestandard* フラグなど、指定されたインターフェイスの Multiple Spanning-Tree（MST）情報を表示します。

spanning-tree mst priority

指定されたスパニング ツリーのインスタンスにスイッチ プライオリティを設定するには、**spanning-tree mst priority** グローバル コンフィギュレーション 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* **priority** *priority*

no spanning-tree mst *instance-id* **priority**

構文の説明

instance-id	スパニング ツリー インスタンス範囲。1 つのインスタンス、それぞれをハイフンで区切ったインスタンス範囲、またはカンマで区切った一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。
priority	指定したスパニング ツリー インスタンスのスイッチ プライオリティを設定します。この設定は、スイッチがルート スイッチとして選択される可能性を左右します。小さい値を設定すると、スイッチがルート スイッチとして選択される可能性が高まります。 指定できる範囲は 0 ～ 61440 で、4096 ずつ増加します。有効なプライオリティ値は 0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。それ以外の値はすべて拒否されます。

デフォルト

デフォルト値は 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

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。
12.2(25)SEC	*instance-id* の範囲が 1 ～ 4094 に変更されました。

例

次の例では、Multiple Spanning-Tree（MST）インスタンス 20 ～ 21 のスパニング ツリー プライオリティを 8192 に設定する方法を示します。

```
Switch(config)# spanning-tree mst 20-21 priority 8192
```

設定を確認するには、**show spanning-tree** mst *instance-id* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst *instance-id*	指定したインターフェイスの MST 情報を表示します。
spanning-tree mst cost	MST の計算に使用するパス コストを設定します。
spanning-tree mst port-priority	インターフェイス プライオリティを設定します。

spanning-tree mst root

ネットワークの直径に基づいて、Multiple Spanning-Tree（MST）ルート スイッチのプライオリティおよびタイマーを設定するには、**spanning-tree mst root** グローバル コンフィギュレーション 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**} [**diameter** *net-diameter* [**hello-time** *seconds*]]

no spanning-tree mst *instance-id* **root**

構文の説明

instance-id	スパニング ツリー インスタンス範囲。1 つのインスタンス、それぞれをハイフンで区切ったインスタンス範囲、またはカンマで区切った一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。
root primary	このスイッチを強制的にルート スイッチに設定します。
root secondary	プライマリ ルート スイッチに障害が発生した場合に、このスイッチをルート スイッチに設定します。
diameter *net-diameter*	（任意）任意の 2 つのエンド ステーション間にスイッチの最大数を設定します。指定できる範囲は 2 ～ 7 です。このキーワードは、MST インスタンス 0 にだけ使用できます。
hello-time *seconds*	（任意）ルート スイッチ コンフィギュレーション メッセージから送信される hello UniDirectional Link Detection（UDLD; 単一方向リンク検出）の間隔を設定します。指定できる範囲は 1 ～ 10 秒です。このキーワードは、MST インスタンス 0 にだけ使用できます。

デフォルト

プライマリ ルート スイッチのプライオリティは 24576 です。

セカンダリ ルート スイッチのプライオリティは 28672 です。

hello タイムは 2 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

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

spanning-tree mst *instance-id* **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。

spanning-tree mst *instance-id* **root** コマンドを入力すると、ソフトウェアはこのスイッチをスパニング ツリー インスタンスのルートに設定するのに十分なプライオリティを設定しようとします。拡張システム ID がサポートされているため、スイッチはインスタンスのスイッチ プライオリティを 24576 に設定します（この値によってこのスイッチが指定されたインスタンスのルートになる場合）。指定されたインスタンスのルート スイッチに、24576 に満たないスイッチ プライオリティが設定されている場合は、スイッチは自身のプライオリティを最小のスイッチ プライオリティより 4096 だけ小さい値に設定します（4096 は 4 ビット スイッチ プライオリティの最下位ビットの値です）。

spanning-tree mst *instance-id* **root secondary** コマンドを入力すると、拡張システム ID がサポートされているため、ソフトウェアはスイッチ プライオリティをデフォルト値（32768）から 28672 に変更します。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（ネットワーク内の他のスイッチがデフォルトのスイッチ プライオリティである 32768 を使用しているため、ルート スイッチになる可能性が低い場合）。

例

次の例では、スイッチをインスタンス 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 に設定する方法を示します。

```
Switch(config)# spanning-tree mst 10 root primary diameter 4
```

次の例では、スイッチをインスタンス 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 に設定する方法を示します。

```
Switch(config)# spanning-tree mst 10 root secondary diameter 4
```

設定を確認するには、**show spanning-tree mst** *instance-id* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst *instance-id*	指定したインスタンスの MST 情報を表示します。
spanning-tree mst forward-time	すべての MST インスタンスについて転送遅延時間を設定します。
spanning-tree mst hello-time	ルート スイッチ コンフィギュレーション メッセージが送信する hello BPDU の間隔を設定します。
spanning-tree mst max-age	スパニング ツリーがルート スイッチからメッセージを受信する間隔を設定します。
spanning-tree mst max-hops	BPDU がドロップされるまでのリージョンのホップ数を設定します。

spanning-tree port-priority

インターフェイス プライオリティを設定するには、**spanning-tree port-priority** 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。ループが発生した場合、スパニング ツリーはフォワーディング ステートにするインターフェイスを判別できます。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*] **port-priority** *priority*

no spanning-tree [**vlan** *vlan-id*] **port-priority**

構文の説明

vlan *vlan-id*	（任意）スパニング ツリー インスタンスに関連付けられた VLAN 範囲です。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。
priority	指定できる番号は 0 ～ 240 で、16 ずつ増加します。有効な値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。それ以外の値はすべて拒否されます。値が小さいほど、プライオリティが高くなります。

デフォルト

デフォルト値は 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	*vlan-id* 変数の値が変更されました。プライオリティ範囲の値が変更されました。

使用上のガイドライン

変数 *vlan-id* を省略した場合、このコマンドは VLAN 1 に関連付けられたスパニング ツリー インスタンスに適用されます。

インターフェイスが割り当てられていない VLAN にプライオリティを設定できます。このインターフェイスを VLAN に割り当てると、設定が有効になります。

spanning-tree vlan *vlan-id* **port-priority** *priority* コマンドおよび **spanning-tree port-priority** *priority* コマンドの両方を使用してインターフェイスを設定する場合、**spanning-tree vlan** *vlan-id* **port-priority** *priority* コマンドが有効になります。

スイッチがスイッチ スタックのメンバの場合、**spanning-tree** [**vlan** *vlan-id*] **port-priority** *priority* インターフェイス コンフィギュレーション コマンドの代わりに、**spanning-tree** [**vlan** *vlan-id*] **cost** *cost* インターフェイス コンフィギュレーション コマンドを使用して、フォワーディング ステートにするインターフェイスを選択しなければなりません。最初に選択させるインターフェイスには、低いコスト値を割り当て、最後に選択させるインターフェイスには高いコスト値を割り当てます。

例

次の例では、ループが発生した場合にポートがフォワーディング ステートになる可能性を高める方法を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# spanning-tree vlan 20 port-priority 0
```

次の例では、VLAN 20 ～ 25 のポート プライオリティ値を設定する方法を示します。

```
Switch(config-if)# spanning-tree vlan 20-25 port-priority 0
```

設定を確認するには、**show spanning-tree interface** *interface-id* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree interface *interface-id*	指定したインターフェイスのスパニング ツリー情報を表示します。
spanning-tree cost	スパニング ツリーの計算に使用するパス コストを設定します。
spanning-tree vlan priority	指定したスパニング ツリー インスタンスのスイッチ プライオリティを設定します。

spanning-tree portfast（グローバル コンフィギュレーション）

PortFast 対応のインターフェイス上で、UniDirectional Link Detection（UDLD; 単一方向リンク検出）のフィルタリングおよび BPDU ガード機能をグローバルにイネーブルにしたり、またはすべての非トランク インターフェイス上で PortFast 機能をグローバルにイネーブルにするには、**spanning-tree portfast** グローバル コンフィギュレーション コマンドを使用します。BPDU フィルタリング機能を使用すると、スイッチ インターフェイスでの BPDU の送受信を禁止できます。BPDU ガード機能は、BPDU を受信する PortFast 対応インターフェイスを errdisable ステートにします。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 {**bpdufilter default** | **bpduguard default** | **default**}

no spanning-tree portfast {**bpdufilter default** | **bpduguard default** | **default**}

構文の説明

bpdufilter default	PortFast 対応インターフェイス上で BPDU フィルタリングをグローバルにイネーブルにし、エンド ステーションに接続されたスイッチ インターフェイスでの BPDU の送受信を禁止します。
bpduguard default	PortFast 対応インターフェイス上で BPDU ガード機能をグローバルにイネーブルにし、BPDU を受信する PortFast 対応インターフェイスを errdisable ステートにします。
default	すべての非トランク インターフェイス上で PortFast 機能をグローバルにイネーブルにします。PortFast 機能がイネーブルの場合、インターフェイスはブロッキング ステートからフォワーディング ステートに直接移行します。その際に、中間のスパニング ツリー ステートは変わりません。

デフォルト

BPDU フィルタリング、BPDU ガード、および PortFast 機能は、個別に設定しない限り、すべてのインターフェイス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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

スイッチが Per-VLAN Spanning-Tree Plus（PVST+）モード、Rapid-PVST+ モード、または Multiple Spanning-Tree（MST）モードで稼動している場合は、これらの機能をイネーブルにできます。

PortFast 対応インターフェイス（PortFast 動作ステートのインターフェイス）上で BPDU フィルタリングをグローバルにイネーブルにするには、**spanning-tree portfast bpdufilter default** グローバル コンフィギュレーション コマンドを使用します。ただし、リンクが確立してからスイッチが発信 BPDU のフィルタリングを開始するまでの間に、このインターフェイスから BPDU がいくつか送信されます。スイッチ インターフェイスに接続されたホストが BPDU を受信しないようにするには、スイッチ上で

BPDU フィルタリングをグローバルにイネーブルにする必要があります。BPDU を受信した PortFast 対応インターフェイスでは、PortFast 動作ステータスが解除され、BPDU フィルタリングがディセーブルになります。

spanning-tree portfast bpdufilter default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree bdpufilter** 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　BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニング ツリーをディセーブルにすることと同じであり、スパニング ツリー ループが発生することがあります。

PortFast 動作ステートのインターフェイス上で BPDU ガードをグローバルにイネーブルにするには、**spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドを使用します。有効な設定では、PortFast 対応インターフェイスは BPDU を受信しません。PortFast 対応インターフェイスが BPDU を受信した場合は、認可されていないデバイスの接続などの無効な設定が存在することを示しており、BPDU ガード機能によってインターフェイスは errdisable ステートになります。インターフェイスを手動で再び動作させなければならない場合、無効な設定を防ぐには、BPDU ガード機能が役に立ちます。サービスプロバイダー ネットワーク内でアクセス ポートがスパニング ツリーに参加しないようにするには、BPDU ガード機能を使用します。

spanning-tree portfast bpduguard default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree bdpuguard** 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。

すべての非トランク インターフェイス上で PortFast 機能をグローバルにイネーブルにするには、**spanning-tree portfast default** グローバル コンフィギュレーション コマンドを使用します。PortFast は、エンド ステーションに接続するインターフェイスに限って設定します。そうしないと、予期しないトポロジ ループが原因でデータのパケット ループが発生し、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。リンクが確立すると、PortFast 対応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。

spanning-tree portfast default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree portfast** 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。**no spanning-tree portfast default** グローバル コンフィギュレーション コマンドを使用すると、**spanning-tree portfast** インターフェイス コンフィギュレーション コマンドを使用して個別に設定した場合を除き、すべてのインターフェイス上で PortFast をディセーブルにできます。

例

次の例では、BPDU フィルタリング機能をグローバルにイネーブルにする方法を示します。

```
Switch(config)# spanning-tree portfast bpdufilter default
```

次の例では、BPDU ガード機能をグローバルにイネーブルにする方法を示します。

```
Switch(config)# spanning-tree portfast bpduguard default
```

次の例では、すべての非トランク インターフェイス上で PortFast 機能をグローバルにイネーブルにする方法を示します。

```
Switch(config)# spanning-tree portfast default
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	現在の動作設定を表示します。
spanning-tree bpdufilter	インターフェイスが BPDU を送受信しないようにします。
spanning-tree bpduguard	BPDU を受信したインターフェイスを、errdisable ステートにします。
spanning-tree portfast（インターフェイス コンフィギュレーション）	対応するすべての VLAN 内の特定のインターフェイスで、PortFast 機能をイネーブルにします。

spanning-tree portfast（インターフェイス コンフィギュレーション）

対応するすべての VLAN 内の特定のインターフェイス上で PortFast 機能をイネーブルにするには、**spanning-tree portfast** 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。PortFast 機能がイネーブルの場合、インターフェイスはブロッキング ステートからフォワーディング ステートに直接移行します。その際に、中間のスパニング ツリー ステートは変わりません。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 [**disable** | **trunk**]

no spanning-tree portfast

構文の説明

disable	（任意）指定されたインターフェイスの PortFast 機能をディセーブルにします。
trunk	（任意）トランキング インターフェイスの PortFast 機能をイネーブルにします。

デフォルト

すべてのインターフェイスで PortFast 機能はディセーブルですが、ダイナミック アクセス ポートでは自動的にイネーブルになります。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

この機能は、エンド ステーションに接続するインターフェイスに限って使用します。そうしないと、予期しないトポロジ ループが原因でデータのパケット ループが発生し、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。

トランク ポートで PortFast をイネーブルにするには、**spanning-tree portfast trunk** インターフェイス コンフィギュレーション コマンドを使用する必要があります。**spanning-tree portfast** コマンドは、トランク ポートではサポートされません。

スイッチが Per-VLAN Spanning-Tree Plus（PVST+）モード、Rapid-PVST+ モード、または Multiple Spanning-Tree（MST）モードで稼動している場合は、その機能をイネーブルにできます。

この機能はインターフェイス上のすべての VLAN に影響します。

PortFast 機能がイネーブルに設定されている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。

spanning-tree portfast default グローバル コンフィギュレーション コマンドを使用すると、すべての非トランク インターフェイス上で PortFast 機能をグローバルにイネーブルにできます。ただし、**spanning-tree portfast** インターフェイス コンフィギュレーション コマンドを使用して、グローバル設定を上書きできます。

spanning-tree portfast default グローバル コンフィギュレーション コマンドを設定する場合は、**spanning-tree portfast disable** インターフェイス コンフィギュレーション コマンドを使用して、トランク インターフェイス以外のインターフェイス上で PortFast 機能をディセーブルにできます。

例

次の例では、特定のポート上で PortFast 機能をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# spanning-tree portfast
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	現在の動作設定を表示します。
spanning-tree bpdufilter	インターフェイスでの UniDirectional Link Detection（UDLD; 単一方向リンク検出）の送受信を禁止します。
spanning-tree bpduguard	BPDU を受信したインターフェイスを、errdisable ステートにします。
spanning-tree portfast（グローバル コンフィギュレーション）	PortFast 対応インターフェイス上で BPDU フィルタリング機能または BPDU ガード機能をグローバルにイネーブルにするか、またはすべての非トランク インターフェイスで PortFast 機能をイネーブルにします。

spanning-tree transmit hold-count

毎秒送信する UniDirectional Link Detection（UDLD; 単一方向リンク検出）の数を設定するには、**spanning-tree transmit hold-count** グローバル コンフィギュレーション 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 [*value*]

構文の説明

value	（任意）毎秒送信される BPDU 数。指定できる範囲は 1 ～ 20 です。

デフォルト

デフォルト値は 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

コマンド履歴

リリース	変更内容
12.2(25)SEC	このコマンドが追加されました。

使用上のガイドライン

スイッチが Rapid-Per-VLAN Spanning-Tree Plus（Rapid-PVST+）モードの場合、伝送ホールド カウント値が増加すると、CPU の使用率に大きく影響する可能性があります。この値を減らすと、コンバージェンスの速度が低下します。デフォルト設定を使用することを推奨します。

例

次の例では、伝送ホールド カウントを 8 に設定する方法を示します。

```
Switch(config)# spanning-tree transmit hold-count 8
```

設定を確認するには、**show spanning-tree mst** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst	伝送ホールド カウントを含む、Multiple Spanning-Tree（MST）のリージョン設定およびステータスを表示します。

spanning-tree uplinkfast

リンクやスイッチに障害が発生した場合、またはスパニング ツリーが自動的に再設定された場合に、新しいルート ポートを短時間で選択できるようにするには、**spanning-tree uplinkfast** グローバル コンフィギュレーション 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 uplinkfast [**max-update-rate** *pkts-per-second*]

no spanning-tree uplinkfast [**max-update-rate**]

構文の説明

max-update-rate *pkts-per-second*	（任意）更新パケット送信時の 1 秒あたりのパケット数です。指定できる範囲は 0 ～ 32000 です。

デフォルト

UplinkFast はディセーブルです。

更新速度は 150 パケット / 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**max-update-rate** キーワードが追加されました。

使用上のガイドライン

このコマンドは、アクセス スイッチ上だけで使用します。

UplinkFast 機能は、Rapid PVST+ モードまたは Multiple Spanning-Tree（MST）モードで設定できますが、スパニング ツリー モードを PVST+ に変更するまでこの機能はディセーブル（非アクティブ）のままです。

UplinkFast をイネーブルにすると、スイッチ全体に対してイネーブルになります。VLAN 単位でイネーブルにすることはできません。

UplinkFast をイネーブルまたはディセーブルにすると、すべての非スタック ポートのインターフェイス上で、Cross-Stack UplinkFast（CSUF）も自動的にイネーブルまたはディセーブルになります。CSUF は、リンクやスイッチに障害が発生した場合、またはスパニング ツリーが自動的に再設定された場合に、新しいルート ポートを短時間で選択できるようにします。

UplinkFast をイネーブルにすると、すべての VLAN のスイッチ プライオリティは 49152 に設定されます。UplinkFast をイネーブルにする場合、または UplinkFast がすでにイネーブルに設定されている場合に、パス コストを 3000 未満の値に変更すると、すべてのインターフェイスおよび VLAN トランクのパス コストが 3000 だけ増加します（パス コストを 3000 以上の値に変更した場合、パス コストは変更されません）。スイッチ プライオリティおよびパス コストを変更すると、スイッチがルート スイッチになる可能性が低下します。

デフォルト値を変更していない場合、UplinkFast をディセーブルにすると、すべての VLAN のスイッチ プライオリティとすべてのインターフェイスのパス コストがデフォルト値に設定されます。

ルート ポートに障害が発生していることがスパニング ツリーで検出されると、UplinkFast はスイッチをただちに代替ルート ポートに変更して、新しいルート ポート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、トポロジ変更通知が送信されます。

UplinkFast 機能で使用するインターフェイスでは、ルート ガードをイネーブルにしないでください。UplinkFast を使用すると、障害発生時に（ブロック ステートの）バックアップ インターフェイスがルート ポートになります。しかし、同時にルート ガードもイネーブルになっていた場合は、UplinkFast 機能で使用されるすべてのバックアップ インターフェイスが root-inconsistent（ブロック）ステートになり、フォワーディング ステートに移行できなくなります。

max-update-rate を 0 に設定すると、ステーションを学習するフレームが生成されず、接続の切断後、スパニング ツリー トポロジのコンバージェンスに要する時間が長くなります。

例

次の例では、UplinkFast をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree uplinkfast
```

設定を確認するには、**show spanning-tree summary** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree summary	スパニング ツリー インターフェイス ステートのサマリーを表示します。
spanning-tree vlan root primary	このスイッチを強制的にルート スイッチに設定します。

spanning-tree vlan

VLAN ベースでスパニングツリーを設定するには、**spanning-tree vlan** グローバル コンフィギュレーション 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** *seconds* | **max-age** *seconds* | **priority** *priority* | **root** {**primary** | **secondary**} [**diameter** *net-diameter* [**hello-time** *seconds*]]]

no spanning-tree vlan *vlan-id* [**forward-time** | **hello-time** | **max-age** | **priority** | **root**]

構文の説明

vlan-id	スパニング ツリー インスタンスに関連付けられた VLAN 範囲です。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。
forward-time *seconds*	（任意）指定したスパニング ツリー インスタンスの転送遅延時間を設定します。転送遅延時間には、インターフェイスが転送を開始するまでに、リスニング ステートおよびラーニング ステートがそれぞれ継続する時間を指定します。指定できる範囲は 4 ～ 30 秒です。
hello-time *seconds*	（任意）ルート スイッチ コンフィギュレーション メッセージから送信される hello UniDirectional Link Detection（UDLD; 単一方向リンク検出）の間隔を設定します。指定できる範囲は 1 ～ 10 秒です。
max-age *seconds*	（任意）スパニング ツリーがルート スイッチからメッセージを受信する間隔を設定します。スイッチがこの間隔の間にルート スイッチから BPDU メッセージを受信しなかった場合は、スパニング ツリー トポロジが再計算されます。指定できる範囲は 6 ～ 40 秒です。
priority *priority*	（任意）指定したスパニング ツリー インスタンスのスイッチ プライオリティを設定します。この設定は、スタンドアロン スイッチまたはスタックのスイッチがルート スイッチとして選択される可能性を左右します。小さい値を設定すると、スイッチがルート スイッチとして選択される可能性が高まります。 指定できる範囲は 0 ～ 61440 で、4096 ずつ増加します。有効なプライオリティ値は 4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。それ以外の値はすべて拒否されます。
root primary	（任意）このスイッチを強制的にルート スイッチに設定します。
root secondary	（任意）プライマリ ルート スイッチに障害が発生した場合に、このスイッチをルート スイッチに設定します。
diameter *net-diameter*	（任意）任意の 2 つのエンド ステーション間にスイッチの最大数を設定します。指定できる範囲は 2 ～ 7 です。

デフォルト

すべての VLAN でスパニング ツリーがイネーブルです。

転送遅延時間は 15 秒です。

hello タイムは 2 秒です。

有効期限は 20 秒です。

プライマリ ルート スイッチのプライオリティは 24576 です。

セカンダリ ルート スイッチのプライオリティは 28672 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	*vlan-id* 変数の値が変更されました。

使用上のガイドライン

STP をディセーブルにすると、VLAN はスパニング ツリー トポロジへの参加を停止します。管理上のダウン状態のインターフェイスは、ダウン状態のままです。受信した BPDU は、他のマルチキャスト フレームと同様に転送されます。STP がディセーブルの場合、VLAN はループの検出や禁止を行いません。

現在アクティブではない VLAN 上で STP をディセーブルにし、この変更を確認するには、**show running-config** または **show spanning-tree vlan** *vlan-id* 特権 EXEC コマンドを使用します。設定は、VLAN がアクティブである場合に有効となります。

STP をディセーブルにするか、再びイネーブルにすると、ディセーブルまたはイネーブルにする VLAN 範囲を指定できます。

VLAN をディセーブルにしてからイネーブルにした場合、その VLAN に割り当てられていたすべての VLAN は引き続きメンバとなります。ただし、すべてのスパニング ツリー ブリッジ パラメータは元の設定（VLAN がディセーブルになる直前の設定）に戻ります。

インターフェイスが割り当てられていない VLAN 上で、スパニング ツリー オプションをイネーブルにできます。インターフェイスを VLAN に割り当てると、設定が有効になります。

max-age seconds を設定すると、スイッチが指定された間隔の間にルート スイッチから BPDU を受信しなかった場合は、スパニング ツリー トポロジが再計算されます。**max-age** の設定値は、**hello-time** の設定値よりも大きくなければなりません。

spanning-tree vlan *vlan-id* **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。

spanning-tree vlan *vlan-id* **root** コマンドを入力すると、ソフトウェアは各 VLAN の現在のルート スイッチのスイッチ プライオリティを確認します。拡張システム ID がサポートされているため、スイッチは指定された VLAN のスイッチ プライオリティを 24576 に設定します（この値によってこのスイッチが指定された VLAN のルートになる場合）。指定された VLAN のルート スイッチに 24576 に満たないスイッチ プライオリティが設定されている場合は、スイッチはその VLAN について、自身のプライオリティを最小のスイッチ プライオリティより 4096 だけ小さい値に設定します（4096 は 4 ビット スイッチ プライオリティの最下位ビットの値です）。

spanning-tree vlan *vlan-id* **root secondary** コマンドを入力すると、拡張システム ID がサポートされているため、ソフトウェアはスイッチ プライオリティをデフォルト値（32768）から 28672 に変更します。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（ネットワーク内の他のスイッチがデフォルトのスイッチ プライオリティである 32768 を使用しているため、ルート スイッチになる可能性が低い場合）。

例

次の例では、VLAN 5 上で STP をディセーブルにする方法を示します。

```
Switch(config)# no spanning-tree vlan 5
```

設定を確認するには、**show spanning-tree** 特権 EXEC コマンドを入力します。このインスタンスのリストに、VLAN 5 は表示されません。

次の例では、VLAN 20 と VLAN 25 のスパニング ツリーについて、転送遅延時間を 18 秒に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 20,25 forward-time 18
```

次の例では、VLAN 20 ～ 24 のスパニング ツリーについて、hello 遅延時間を 3 秒に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 20-24 hello-time 3
```

次の例では、VLAN 20 のスパニング ツリーについて、有効期限を 30 秒に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 20 max-age 30
```

次の例では、スパニング ツリー インスタンス 100 および 105 ～ 108 の **max-age** パラメータをデフォルト値に戻す方法を示します。

```
Switch(config)# no spanning-tree vlan 100, 105-108 max-age
```

次の例では、VLAN 20 のスパニング ツリーについて、プライオリティを 8192 に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 20 priority 8192
```

次の例では、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 に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 10 root primary diameter 4
```

次の例では、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 に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 10 root secondary diameter 4
```

設定を確認するには、**show spanning-tree vlan** *vlan-id* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree vlan	スパニング ツリー情報を表示します。
spanning-tree cost	スパニング ツリーの計算に使用するパス コストを設定します。
spanning-tree guard	選択されたインターフェイスに対応するすべての VLAN に対して、ルート ガード機能またはループ ガード機能をイネーブルにします。
spanning-tree port-priority	インターフェイス プライオリティを設定します。
spanning-tree portfast（グローバル コンフィギュレーション）	PortFast 対応インターフェイス上で BPDU フィルタリング機能または BPDU ガード機能をグローバルにイネーブルにするか、またはすべての非トランク インターフェイスで PortFast 機能をイネーブルにします。
spanning-tree portfast（インターフェイス コンフィギュレーション）	対応するすべての VLAN 内の特定のインターフェイスで、PortFast 機能をイネーブルにします。
spanning-tree uplinkfast	UplinkFast 機能をイネーブルにし、新しいルート ポートを短時間で選択できるようにします。

speed

10/100 Mb/s ポートまたは 10/100/1000 Mb/s ポートの速度を指定するには、**speed** 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。ポートをデフォルト値に戻すには、このコマンドの **no** 形式または **default** 形式を使用します。

speed {**10** | **100** | **1000** | **auto** [**10** | **100** | **1000**] | **nonegotiate**}

no speed

構文の説明

10	ポートは 10 Mb/s で稼動します。
100	ポートは 100 Mb/s で稼動します。
1000	ポートは 1000 Mb/s で稼動します。このオプションは、10/100/1000 Mb/s ポートでだけ有効になって表示されます。
auto	ポートが自動的に、もう一方のリンクの終端ポートを基準にして速度を検出します。**10**、**100**、または **1000** キーワードと **auto** キーワードを一緒に使用する場合、ポートは指定した速度で自動ネゴシエーションだけを行います。
nonegotiate	自動ネゴシエーションはディセーブルになっており、ポートは 1000 Mb/s で稼動します（1000BASE-T SFP は nonegotiate キーワードをサポートしていません）。

デフォルト

デフォルトは **auto** 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(20)SE1	**auto** キーワードでの **10**、**100**、および **1000** キーワー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 ギガビット イーサネット ポートでは速度を設定できません。

1000BASE-T SFP モジュールを除き、SFP モジュール ポートが自動ネゴシエーションをサポートしていないデバイスに接続されている場合、ネゴシエートしないように（**nonegotiate**）速度を設定できます。

速度が **auto** に設定されている場合、スイッチはもう一方のリンクの終端にあるデバイスと速度設定についてネゴシエートし、速度をネゴシエートされた値に強制的に設定します。デュプレックス設定はリンクの両端での設定が引き継がれますが、これにより、デュプレックス設定に矛盾が生じることがあります。

ラインの両端が自動ネゴシエーションをサポートしている場合、デフォルトの自動ネゴシエーション設定を使用することを強く推奨します。一方のインターフェイスは自動ネゴシエーションをサポートし、もう一方の終端はサポートしていない場合、サポートしている側には **auto** 設定を使用し、サポートしていない終端にはデュプレックスおよび速度を設定します。

注意　インターフェイス速度とデュプレックス モードの設定を変更すると、再設定中にインターフェイスがシャットダウンし、再びイネーブルになる場合があります。

スイッチの速度およびデュプレックスのパラメータの設定に関する注意事項は、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring Interface Characteristics」の章を参照してください。

例

次の例では、ポートの速度を 100 Mb/s に設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# speed 100
```

次の例では、10 Mb/s だけで自動ネゴシエートするようにポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# speed auto 10
```

次の例では、10 Mb/s または 100 Mb/s だけで自動ネゴシエートするようにポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# speed auto 10 100
```

設定を確認するには、**show interfaces** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
duplex	デュプレックス モードの動作を指定します。
show interfaces	すべてのインターフェイスまたは特定のインターフェイスに対する統計情報を表示します。

srr-queue bandwidth limit

ポートの最大出力を制限するには、**srr-queue bandwidth limit** 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。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。

srr-queue bandwidth limit *weight1*

no srr-queue bandwidth limit

構文の説明

weight1	制限されるポート速度のパーセンテージ。指定できる範囲は 10 ～ 90 です。

デフォルト

ポートはレート制限されておらず、100% 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドを 80% に設定した場合、ポートは 20% の時間はアイドル状態になります。ライン レートは接続速度の 80% に下がります。ただし、ハードウェアはライン レートを 6% 単位で調整しているため、この値は厳密ではありません。

このコマンドは、10 ギガビット イーサネット インターフェイスでは使用できません。

（注）出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、これらの設定がユーザの Quality of Service（QoS）ソリューションを満たさないと判断した場合に限り、設定を変更することができます。

例

次の例では、ポートを 800 Mb/s に制限する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth limit 80
```

設定を確認するには、**show mls qos interface** [*interface-id*] **queueing** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos queue-set output buffers	バッファをキューセットに割り当てます。
mls qos srr-queue output cos-map	Class of Service（CoS; サービス クラス）値を出力キュー、またはキューとしきい値 ID にマッピングします。
mls qos srr-queue output dscp-map	Differentiated Service Code Point（DSCP）値を出力キュー、またはキューとしきい値 ID にマッピングします。
mls qos queue-set output threshold	Weighted Tail-Drop（WTD）しきい値を設定し、バッファのアベイラビリティを保証して、キューセットに対する最大メモリ割り当てを設定します。
queue-set	ポートをキューセットにマッピングします。
show mls qos interface queueing	QoS 情報を表示します。
srr-queue bandwidth shape	シェーピングされた重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅シェーピングをイネーブルにします。
srr-queue bandwidth share	共有する重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅の共有をイネーブルにします。

srr-queue bandwidth shape

シェーピングされた重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅シェーピングをイネーブルにするには、**srr-queue bandwidth shape** 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。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。

srr-queue bandwidth shape *weight1 weight2 weight3 weight4*

no srr-queue bandwidth shape

（注）

構文の説明

weight1 weight2 weight3 weight4	シェーピングされるポートのパーセンテージを判別する重みを指定します。インバース比（1/*weight*）は、このキューのシェーピング帯域幅を指定します。各値はスペースで区切ります。指定できる範囲は 0 ～ 65535 です。

デフォルト

weight1 は 25 に設定されています。weight2、weight3、および weight4 は 0 に設定されています。また、このキューは共有モードです。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

シェーピング モードでは、キューには帯域幅が割合で保証され、この総量までにレート制限されます。リンクがアイドルの場合でも、シェーピングされたトラフィックは割り当てられた帯域幅を超えて使用できません。バースト性のあるトラフィックをスムーズにする、または長期にわたって出力をスムーズにする場合に、シェーピングを使用します。

シェーピング モードは、共有モードを無効にします。

srr-queue bandwidth shape インターフェイス コンフィギュレーション コマンドを使用してシェーピングされたキューの重みを 0 に設定すると、このキューは共有モードで参加します。**srr-queue bandwidth shape** コマンドで指定された重みは無視され、**srr-queue bandwidth share** 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キューの重みが有効になります。

同じポートのキューをシェーピングと共有の両方に設定する場合、最小のキューをシェーピングに設定します。

このコマンドは、10 ギガビット イーサネット インターフェイスでは使用できません。

（注）出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

例

次の例では、同じポートのキューをシェーピングと共有の両方に設定する方法を示します。キュー 2、3、4 の重み比が 0 に設定されているので、これらのキューは共有モードで動作します。キュー 1 の帯域幅の重みは 1/8 で、これは 12.5% です。キュー 1 はこの帯域幅が保証され、またこの帯域幅までに制限されています。他のキューにトラフィックがなくアイドル状態であっても、他のキューにスロットを拡張しません。キュー 2、3、4 は共有モードで、キュー 1 の設定は無視されます。共有モードのキューに割り当てられた帯域幅比は、4/（4+4+4）で、これは 33% です。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth shape 8 0 0 0
Switch(config-if)# srr-queue bandwidth share 4 4 4 4
```

設定を確認するには、**show mls qos interface** [*interface-id*] **queueing** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos queue-set output buffers	バッファをキューセットに割り当てます。
mls qos srr-queue output cos-map	Class of Service（CoS）値を出力キュー、またはキューとしきい値 ID にマッピングします。
mls qos srr-queue output dscp-map	Differentiated Service Code Point（DSCP）値を出力キュー、またはキューとしきい値 ID にマッピングします。
mls qos queue-set output threshold	Weighted Tail-Drop（WTD）しきい値を設定し、バッファのアベイラビリティを保証し、キューセットに対する最大メモリ割り当てを設定します。
priority-queue	ポート上で出力緊急キューをイネーブルにします。
queue-set	ポートをキューセットにマッピングします。
show mls qos interface queueing	Quality of Service（QoS）情報を表示します。
srr-queue bandwidth share	共有する重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅の共有をイネーブルにします。

srr-queue bandwidth share

共有する重みを割り当てて、ポートにマッピングされた 4 つの出力キューの帯域幅の共有をイネーブルにするには、**srr-queue bandwidth share** 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。重み比は、Shaped Round Robin（SRR）スケジューラが各キューからパケットを取り出す頻度の比率です。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。

srr-queue bandwidth share *weight1 weight2 weight3 weight4*

no srr-queue bandwidth share

構文の説明

weight1 weight2 weight3 weight4	*weight1*、*weight2*、*weight3*、および *weight4* は、SRR スケジューラがパケットを取り出す頻度の比率を指定します。各値はスペースで区切ります。指定できる範囲は 1 ～ 255 です。

デフォルト

weight1、weight2、weight3 および weight4 は 25 に設定されています（各キューに帯域幅の 1/4 を割り当て）。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

各重みの絶対値は意味がないので、パラメータ比だけを使用します。

共有モードでは、設定された重みによりキュー間で帯域幅が共有されます。このレベルでは帯域幅は保証されていますが、このレベルに限定されていません。たとえば、キューが空でリンク共有を必要としない場合、残りのキューは未使用の帯域幅まで拡大し、キュー間でこの帯域幅を共有できます。

srr-queue bandwidth shape インターフェイス コンフィギュレーション コマンドを使用してシェーピングされたキューの重みを 0 に設定すると、このキューは SRR 共有モードで参加します。**srr-queue bandwidth shape** コマンドで指定された重みは無視され、**srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドで指定されたキューの重みが有効になります。

同じポートのキューをシェーピングと共有の両方に設定する場合、最小のキューをシェーピングに設定します。

（注）　出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

例

次の例では、出力ポートで稼動する SRR スケジューラの重み比を設定する方法を示します。キュー 4 つを使用します。共有モードの各キューに割り当てられた帯域幅の比率は、1/（1+2+3+4）、2/（1+2+3+4）、3/（1+2+3+4）、4/（1+2+3+4）で、これは、キュー 1、2、3、4 それぞれに対して 10%、20%、30%、40% です。キュー 4 はキュー 1 の帯域幅の 4 倍、キュー 2 の帯域幅の 2 倍、キュー 3 の帯域幅の 1 と 1/3 倍であることを示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth share 1 2 3 4
```

設定を確認するには、**show mls qos interface** [*interface-id*] **queueing** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos queue-set output buffers	バッファをキューセットに割り当てます。
mls qos srr-queue output cos-map	Class of Service（CoS）値を出力キュー、またはキューとしきい値 ID にマッピングします。
mls qos srr-queue output dscp-map	Differentiated Service Code Point（DSCP）値を出力キュー、またはキューとしきい値 ID にマッピングします。
mls qos queue-set output threshold	Weighted Tail-Drop（WTD）しきい値を設定し、バッファのアベイラビリティを保証し、キューセットに対する最大メモリ割り当てを設定します。
priority-queue	ポート上で出力緊急キューをイネーブルにします。
queue-set	ポートをキューセットにマッピングします。
show mls qos interface queueing	Quality of Service（QoS）情報を表示します。
srr-queue bandwidth shape	シェーピングされた重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅シェーピングをイネーブルにします。

stack-mac persistent timer

固定 MAC アドレス機能をイネーブルにするには、スイッチ スタック上で **stack-mac persistent timer** グローバル コンフィギュレーション コマンドを使用します。この機能をイネーブルにすると、スタック マスターが変更された場合、スタックの MAC アドレスは約 4 分間、無期限、または設定された値の間、変更されません。この間に以前のスタック マスターがスタックに再加入すると、現在はスタック メンバであっても、スタックはこのスイッチの MAC アドレスをスタックの MAC アドレスとして引き続き使用します。固定 MAC アドレス機能をディセーブルにする場合は、このコマンドの **no** 形式を使用します。

stack-mac persistent timer [**0** | *time-value*]

no stack-mac persistent timer

構文の説明

0	（任意）新しいスタック マスターが引き継いだ後も、現在のスタック マスターの MAC アドレスを引き続き使用する場合に入力します。
time-value	（任意）スタック MAC アドレスが新しいスタック マスターの MAC アドレスに変わるまでの時間を分単位で設定します。指定できる範囲は 1 ～ 60 分です。値を入力しない場合、デフォルト値は 4 分です。このコマンドには明示的な値を設定することを推奨します。

コマンド デフォルト

固定 MAC アドレスはディセーブルに設定されています。スタックの MAC アドレスは常に、スタック マスターの MAC アドレスです。

このコマンドに値を入力しない場合、MAC アドレスが変更されるまでのデフォルトの時間は 4 分です。このコマンドには、明示的な値を設定することを推奨します。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SE	このコマンドが追加されました。
12.2(35)SE	*time-value* 変数が追加されました。

使用上のガイドライン

スイッチ スタックの MAC アドレスは、スタック マスターの MAC アドレスにより決定します。デフォルト ステート（固定 MAC アドレスがディセーブル）で、新しいスイッチがスタック マスターになると、スタックの MAC アドレスは新しいスタック マスターの MAC アドレスに変更されます。

固定 MAC アドレスがイネーブルの場合、スタックの MAC アドレスは一定の時間変更されません。この間に以前のスタック マスターがスタック メンバとしてスタックに再加入した場合、スタックではこのスイッチがスタック内に存在する限り、以前のスタック マスターの MAC アドレスを保持します。以前のスタック マスターが指定された時間内にスタックに再加入しない場合、スイッチ スタックは新しいスタック マスターの MAC アドレスをスタックの MAC アドレスとします。

この時間を 0 ～ 60 分に設定できます。

- このコマンドに値を入力しない場合、デフォルトの遅延は 4 分です。
- **0** を入力すると、**no stack-mac persistent timer** コマンドを入力するまで、スタックは現在のスタック MAC アドレスを引き続き使用します。
- 遅延時間に 1 ～ 60 分を入力すると、設定された時間が過ぎるまで、または **no stack-mac persistent timer** コマンドを入力するまで、以前のスタック マスターのスタック MAC アドレスが使用されます。

（注）　キーワードの指定にかかわらず、**stack-mac persistent timer** コマンドを入力した場合、以前のマスター MAC アドレスがネットワーク ドメインのいずれかに表示されるとトラフィックが失われる可能性があるという警告メッセージが表示されます。この機能は慎重に使用してください。

スイッチオーバーの後、時間切れになる前に **no stack-mac persistent timer** コマンドを入力した場合、スイッチ スタックは現在のスタック マスター MAC アドレスに移行します。

スタック全体がリロードする場合、このスタックが復元すると、スタック マスターの MAC アドレスがスタックの MAC アドレスとなります。

例

次の例では、設定ごとに警告メッセージを表示する固定 MAC アドレス機能を設定する方法を示します。また、設定を確認する方法も示します。

```
Switch(config)# stack-mac persistent timer
WARNING: Use of an explicit timer value with the command is recommended
WARNING: Default value of 4 minutes is being used.
WARNING: The stack continues to use the base MAC of the old Master
WARNING: as the stack MAC after a master switchover until the MAC
WARNING: persistency timer expires.During this time the Network
WARNING: Administrators must make sure that the old stack-mac does
WARNING: not appear elsewhere in this network domain.If it does,
WARNING: user traffic may be blackholed.

Switch(config)# stack-mac persistent timer 0
WARNING: Stack MAC persistency timer value of 0 means that, after a
WARNING: master switchover, the current stack-mac will continue
WARNING: to be used indefinitely.
WARNING: The Network Administrators must make sure that the old
WARNING: stack-mac does not appear elsewhere in this network
WARNING: domain.If it does, user traffic may be blackholed.

Switch(config)# stack-mac persistent timer 7
WARNING: The stack continues to use the base MAC of the old Master
WARNING: as the stack MAC after a master switchover until the MAC
WARNING: persistency timer expires.During this time the Network
WARNING: Administrators must make sure that the old stack-mac does
WARNING: not appear elsewhere in this network domain.If it does,
WARNING: user traffic may be blackholed.

Switch(config)# end
Switch# show switch
Switch/Stack Mac Address : 0016.4727.a900
Mac persistency wait time: 7 mins
                                            H/W   Current
Switch#  Role   Mac Address     Priority Version  State
-----------------------------------------------------------
*1       Master 0016.4727.a900     1      0       Ready
```

設定を確認するには、次の 2 つの特権 EXEC コマンドのうちいずれかを入力します。

- **show running-config**：イネーブルの場合、出力に `stack-mac persistent timer` と時間が分単位で表示されます。
- **show switch**：イネーブルの場合、出力に `Mac persistency wait time` と時間（分）が表示されます。

関連コマンド

コマンド	説明
show running-config	固定 MAC アドレスが設定されている場合、スタックの MAC persistency wait time を含む現在の動作設定を表示します。
show switch	固定 MAC アドレスがイネーブルである場合、スタックの MAC persistency wait time を含むスイッチ スタックに関連した情報を表示します。

storm-control

インターフェイス上でブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御をイネーブルにし、しきい値のレベルを設定するには、**storm-control** 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。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。

storm-control {{**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **bps** *bps* [*bps-low*] | **pps** *pps* [*pps-low*]}} | {**action** {**shutdown** | **trap**}}

no storm-control {{**broadcast** | **multicast** | **unicast**} **level**} | {**action** {**shutdown** | **trap**}}

構文の説明

broadcast	インターフェイス上でブロードキャスト ストーム制御をイネーブルにします。
multicast	インターフェイス上でマルチキャスト ストーム制御をイネーブルにします。
unicast	インターフェイス上でユニキャスト ストーム制御をイネーブルにします。
level *level* [*level-low*]	上限および下限抑制レベルをポートの全帯域幅の割合で指定します。 • *level*：上限抑制レベル（小数点以下第 2 位まで）。指定できる範囲は 0.00 ～ 100.00 です。指定した *level* の値に達した場合、ストーム パケットのフラッディングをブロックします。 • *level-low*：（任意）下限抑制レベル（小数点以下第 2 位まで）。指定できる範囲は 0.00 ～ 100.00 です。この値は上限抑制値より小さいか、または等しくなければなりません。下限抑制レベルを設定しない場合、上限抑制レベルの値に設定されます。
level bps *bps* [*bps-low*]	上限および下限抑制レベルを、ポートで受信するトラフィックの速度（ビット/秒）で指定します。 • *bps*：上限抑制レベル（小数点以下第 1 位まで）。指定できる範囲は 0.0 ～ 10000000000.0 です。指定した *bps* の値に達した場合、ストーム パケットのフラッディングをブロックします。 • *bps-low*：（任意）下限抑制レベル（小数点以下第 1 位まで）。指定できる範囲は 0.0 ～ 10000000000.0 です。この値は上限抑制値に等しいか、または小さくなければなりません。 大きい数値のしきい値には、k、m、g などのメトリック サフィクスを使用できます。
level pps *pps* [*pps-low*]	上限および下限抑制レベルを、ポートで受信するトラフィックの速度（パケット/秒）で指定します。 • *pps*：上限抑制レベル（小数点以下第 1 位まで）。指定できる範囲は 0.0 ～ 10000000000.0 です。指定した *pps* の値に達した場合、ストーム パケットのフラッディングをブロックします。 • *pps-low*：（任意）下限抑制レベル（小数点以下第 1 位まで）。指定できる範囲は 0.0 ～ 10000000000.0 です。この値は上限抑制値に等しいか、または小さくなければなりません。 大きい数値のしきい値には、k、m、g などのメトリック サフィクスを使用できます。

action {**shutdown** | **trap**}	ポートでストームが発生した場合に実行されるアクション。デフォルト アクションは、トラフィックをフィルタリングし、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）トラップを送信しません。 キーワードの意味は次のとおりです。 • **shutdown**：ストームの間、ポートをディセーブルにします。 • **trap**：ストーム発生時に、SNMP トラップを送信します。

デフォルト

ブロードキャスト、マルチキャスト、およびユニキャスト ストーム制御はディセーブルです。

デフォルト アクションは、トラフィックをフィルタリングし、SNMP トラップを送信しません。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(25)SE	**level** *level* [*.level*] オプションは、**level** {*level* [*level-low*] | **pps** *pps* [*pps-low*] | **bps** *bps* [*bps-low*]} **action** {**shutdown** | **trap**}} オプションに替わりました。

使用上のガイドライン

ストーム制御抑制レベルは、ポートの全帯域幅の割合、またはトラフィックを受信する速度（1 秒あたりのパケット数、または 1 秒あたりのビット数）で入力できます。

全帯域幅の割合で指定した場合、100% の抑制値は、指定したトラフィック タイプに制限が設定されていないことを意味します。**level 0 0** の値は、ポート上のすべてのブロードキャスト、マルチキャスト、ユニキャスト トラフィックをブロックします。ストーム制御は、上限抑制レベルが 100% 未満の場合にだけイネーブルになります。他のストーム制御設定が指定されていない場合、デフォルト アクションは、ストームの原因となっているトラフィックをフィルタリングし、SNMP トラップを送信しません。

（注）　マルチキャスト トラフィックのストーム制御しきい値に達した場合、UniDirectional Link Detection（UDLD; 単一方向リンク検出）および Cisco Discovery Protocol（CDP）フレームなどの制御トラフィック以外のマルチキャスト トラフィックはすべてブロックされます。ただし、スイッチは、Open Shortest Path First（OSPF）および通常のマルチキャスト データ トラフィック間のように、ルーティング アップデート間を区別しないため、両方のタイプのトラフィックがブロックされます。

trap および **shutdown** オプションは、互いに独立しています。

パケット ストームが検出されたときにシャットダウンを行う（ストームの間、ポートが errdisable になる）ようにアクションを設定する場合、インターフェイスをこのステートから解除するには **no shutdown** インターフェイス コンフィギュレーション コマンドを使用する必要があります。**shutdown** アクションを指定しない場合、アクションを **trap**（ストーム検出時にスイッチがトラップを生成する）に指定してください。

ストームが発生し、実行されるアクションがトラフィックのフィルタリングである場合、下限抑制レベルが指定されていないと、トラフィック レートが上限抑制レベルより低くなるまでスイッチはすべてのトラフィックをブロックします。下限抑制レベルが指定されている場合、トラフィック レートがこのレベルより低くなるまでスイッチはトラフィックをブロックします。

（注）　ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

ブロードキャスト ストームが発生し、実行されるアクションがトラフィックのフィルタである場合、スイッチはブロードキャスト トラフィックだけをブロックします。

詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、75.5% の上限抑制レベルでブロードキャスト ストーム制御をイネーブルにする方法を示します。

```
Switch(config-if)# storm-control broadcast level 75.5
```

次の例では、87% の上限抑制レベルと 65% の下限抑制レベルのポートでユニキャスト ストーム制御をイネーブルにする方法を示します。

```
Switch(config-if)# storm-control unicast level 87 65
```

次の例では、2000 パケット/秒の上限抑制レベルと 1000 パケット/秒の下限抑制レベルのポートでマルチキャスト ストーム制御をイネーブルにする方法を示します。

```
Switch(config-if)# storm-control multicast level pps 2k 1k
```

次の例では、ポートで **shutdown** アクションをイネーブルにする方法を示します。

```
Switch(config-if)# storm-control action shutdown
```

設定を確認するには、**show storm-control** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show storm-control	すべてのインターフェイス上、または指定のインターフェイス上で、ブロードキャスト、マルチキャストまたはユニキャスト ストーム制御の設定を表示します。

switch

指定されたスタック メンバの StackWise ポートをディセーブルまたはイネーブルにするには、そのスタック メンバ上で **switch** 特権 EXEC を使用します。

switch *stack-member-number* **stack port** *port-number* {**disable** | **enable**}

構文の説明

stack-member-number	現在のスタック メンバ番号を指定します。指定できる範囲は 1 ～ 9 です。
stack port *port-number*	メンバの StackWise ポートを指定します。指定できる範囲は 1 ～ 2 です。
disable	指定されたポートをディセーブルにします。
enable	指定されたポートをイネーブルにします。

デフォルト

StackWise ポートはイネーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

（注）　**switch** *stack-member-number* **stack port** *port-number* **disable** コマンドの使用には注意が必要です。StackWise ポートをディセーブルにする場合、スタックは帯域幅の半分または全体を使用して動作します。

すべてのメンバが StackWise ポートを介して接続されていて ready ステートである場合、スタックは *full-ring* ステートの状態です。

スタックが *partial-ring* ステートになるのは次のような場合です。

- すべてのメンバが StackWisestack ポートを介して接続されているが、一部のメンバは ready ステートではない。
- 一部のメンバが StackWisestack ポートを介して接続されていない。

switch *stack-member-number* **stack port** *port-number* **disable** 特権 EXEC コマンドを入力した場合、

- スタックが full-ring ステートのときは、1 つの StackWise ポートだけをディセーブルにできます。次のメッセージが表示されます。

  ```
  Enabling/disabling a stack port may cause undesired stack changes.Continue?[confirm]
  ```

- スタックが partial-ring ステートのときは、ポートをディセーブルにできません。次のメッセージが表示されます。

  ```
  Disabling stack port not allowed with current stack configuration.
  ```

例

次の例では、メンバ 4 の StackWise ポート 2 をディセーブルにする方法を示します。

```
Switch# switch 4 stack port 2 disable
```

関連コマンド

コマンド	説明
show switch	スイッチ スタックおよびスタック メンバの情報を表示します。

switch priority

スタック メンバのプライオリティ値を変更するには、スタック マスター上から **switch priority** グローバル コンフィギュレーション コマンドを使用します。

switch *stack-member-number* **priority** *new-priority-value*

構文の説明

stack-member-number	現在のスタック メンバ番号を指定します。指定できる範囲は 1 ～ 9 です。
priority *new-priority-value*	新しいスタック メンバのプライオリティ値を指定します。指定できる範囲は 1 ～ 15 です。

デフォルト

デフォルトのプライオリティ値は 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

新しいプライオリティ値はスタックマスターの再選出にとって重要な要素になります。そのため、プライオリティ値の変更がただちにスタック マスターを変更するわけではありません。

例

次の例では、スタック メンバ 6 のプライオリティ値を 9 に変更する方法を示します。

```
Switch(config)# switch 6 priority 9
Changing the Switch Priority of Switch Number 6 to 9
Do you want to continue?[confirm]
```

関連コマンド

コマンド	説明
reload	スタック メンバをリロードし、設定の変更を有効にします。
session	特定のスタック メンバにアクセスします。
switch renumber	スタック メンバ番号を変更します。
show switch	スイッチ スタックおよびスタック メンバの情報を表示します。

switch provision

新しいスイッチがスイッチ スタックに加入する前に、プロビジョニングして設定を提供するには、スタック マスターから **switch provision** グローバル コンフィギュレーション コマンドを使用します。削除されたスイッチ（スタックを脱退したスタック メンバ）に関連付けられたすべての設定情報を削除するには、このコマンドの **no** 形式を使用します。

switch *stack-member-number* **provision** *type*

no switch *stack-member-number* **provision**

構文の説明

stack-member-number	スタック メンバ番号を指定します。指定できる範囲は 1 ～ 9 です。
provision *type*	新しいスイッチがスタックに加入する前に、このスイッチのタイプを指定します。 *type* には、コマンドライン ヘルプ ストリングに示されたサポート対象のスイッチのモデル番号を入力します。

デフォルト

スイッチは、プロビジョニングされていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

エラー メッセージを受信しないようにするには、このコマンドの **no** 形式を使用してプロビジョニングされた設定を削除する前に、スイッチ スタックから指定のスイッチを削除する必要があります。

スイッチ タイプを変更する場合も、スイッチ スタックから指定のスイッチを削除する必要があります。スイッチ タイプを変更しない場合でも、スイッチ スタック内に物理的に存在するプロビジョニングされたスイッチのスタック メンバ番号を変更できます。

プロビジョニングされたスイッチのタイプが、スタック上のプロビジョニングされた設定のスイッチ タイプと一致しない場合、スイッチ スタックはプロビジョニングされたスイッチにデフォルト設定を適用し、これをスタックに追加します。スイッチ スタックでは、デフォルト設定を適用する場合にメッセージを表示します。

プロビジョニング情報は、スイッチ スタックの実行コンフィギュレーションで表示されます。**copy running-config startup-config** 特権 EXEC コマンドを入力すると、プロビジョニングされた設定がスイッチ スタックのスタートアップ コンフィギュレーション ファイルに保存されます。

注意　このコマンドを使用すると、プロビジョニングされた設定にメモリが割り当てられます。新しいスイッチ タイプが設定されたときに、以前割り当てられたメモリのすべてが解放されるわけではありません。そのため、このコマンドをおおよそ 200 回を超えて使用しないようにしてください。スイッチのメモリが不足し、予期せぬ動作が発生する可能性があります。

例

次の例では、スイッチ スタックにスタック メンバ番号が 2 の Catalyst 3750G-12S スイッチをプロビジョニングする方法を示します。**show running-config** コマンドの出力は、プロビジョニングされたスイッチに関連付けられたインターフェイスを示します。

```
Switch(config)# switch 2 provision WS-C3750G-12S
Switch(config)# end
Switch# show running-config | include switch 2
!
interface GigabitEthernet2/0/1
!
interface GigabitEthernet2/0/2
!
interface GigabitEthernet2/0/3
<output truncated>
```

また、**show switch** ユーザ EXEC コマンドを入力すると、スイッチ スタックのプロビジョニングされたステータスを表示できます。

次の例では、スイッチがスタックから削除される場合に、スタック メンバ 5 についてのすべての設定情報が削除される方法を示します。

```
Switch(config)# no switch 5 provision
```

プロビジョニングされたスイッチが、実行コンフィギュレーションで追加または削除されたことを確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	現在の動作設定を表示します。
show switch	スイッチ スタックおよびスタック メンバの情報を表示します。

switch renumber

スタック メンバ番号を変更するには、スタック マスター上から **switch renumber** グローバル コンフィギュレーション コマンドを使用します。

switch *current-stack-member-number* **renumber** *new-stack-member-number*

構文の説明

current-stack-member-number	現在のスタック メンバ番号を指定します。指定できる範囲は 1 ～ 9 です。
renumber *new-stack-member-number*	スタック メンバに新しいスタック メンバ番号を指定します。指定できる範囲は 1 ～ 9 です。

デフォルト

デフォルトのスタック メンバ番号は 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

他のスタック メンバがすでに指定したメンバ番号を使用している場合、スタック マスターは、スタック メンバをリロードする際に、使用可能な一番低い番号を割り当てます。

（注）スタック メンバ番号を変更し、新しいスタック メンバ番号がどの設定にも関連付けされていない場合、そのスタック メンバは現在の設定を廃棄してリセットを行い、デフォルトの設定に戻ります。スタック メンバ番号および設定に関する詳細については、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。

プロビジョニングされたスイッチでは、**switch** *current-stack-member-number* **renumber** *new-stack-member-number* コマンドを使用しないでください。使用すると、コマンドは拒否されます。

スタック メンバをリロードし、設定変更を適用するには、**reload slot** *current stack member number* 特権 EXEC コマンドを使用します。

例

次の例では、スタック メンバ 6 のメンバ番号を 7 に変更する方法を示しています。

```
Switch(config)# switch 6 renumber 7
WARNING:Changing the switch number may result in a configuration change for that switch.
The interface configuration associated with the old switch number will remain as a
provisioned configuration.
Do you want to continue?[confirm]
```

関連コマンド

コマンド	説明
reload	スタック メンバをリロードし、設定の変更を有効にします。
session	特定のスタック メンバにアクセスします。
switch	スタック メンバのプライオリティ値を変更します。
show switch	スイッチ スタックおよびスタック メンバの情報を表示します。

switchport

レイヤ 3 モードにあるインターフェイスをレイヤ 2 モードに移行して、レイヤ 2 の設定を行うには、キーワードを指定せずに **switchport** 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。レイヤ 3 モードにインターフェイスを戻す場合は、このコマンドの **no** 形式を使用します。

switchport

no switchport

インターフェイスをルーテッド インターフェイスの状態に設定して、レイヤ 2 の設定をすべて削除するには、**no switchport** コマンド（パラメータの指定なし）を使用します。このコマンドは、ルーテッド ポートに IP アドレスを割り当てる前に使用する必要があります。

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトでは、すべてのインターフェイスがレイヤ 2 モードです。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

no switchport コマンドが入力されると、ポートをシャットダウンし、再びイネーブルにします。ポートが接続されている装置上ではメッセージが生成される可能性があります。

レイヤ 2 モードからレイヤ 3 モード（またはその逆）にインターフェイスを変更すると、影響を受けたインターフェイスに関連する以前の設定情報が失われる可能性があり、インターフェイスがデフォルト設定に戻ります。

（注）インターフェイスがレイヤ 3 インターフェイスとして設定されている場合、最初にキーワードを指定せずに **switchport** コマンドを入力し、インターフェイスをレイヤ 2 ポートとして設定する必要があります。その後、ここで記載されているようにキーワードを指定して別の switchport コマンドを入力できます。

例

次の例では、インターフェイスをレイヤ 2 ポートとして運用することを中止し、シスコのルーテッド ポートにする方法を示します。

```
Switch(config-if)# no switchport
```

次の例では、ポートのインターフェイスをシスコのルーテッド ポートとして運用することを中止し、レイヤ 2 のスイッチド インターフェイスに変更する方法を示します。

```
Switch(config-if)# switchport
```

（注）キーワードを指定しない **switchport** コマンドは、シスコのルーテッド ポートをサポートしないプラットフォーム上では使用できません。このようなプラットフォーム上のすべての物理ポートは、レイヤ 2 のスイッチド インターフェイスとして想定されます。

インターフェイスのスイッチ ポートのステータスを確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces switchport	ポート ブロッキング、ポート保護設定など、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。
show running-config	現在の動作設定を表示します。

switchport access

ポートをスタティック アクセスまたはダイナミック アクセス ポートとして設定するには、**switchport access** 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。スイッチポートのモードが、**access** に設定されている場合、ポートは指定の VLAN のメンバとして動作します。**dynamic** として設定されている場合、ポートは受信した着信パケットに基づいて、VLAN 割り当ての検出を開始します。アクセス モードをスイッチのデフォルト 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* | **dynamic**}

no switchport access vlan

構文の説明

vlan *vlan-id*	インターフェイスを、アクセス モード VLAN の VLAN ID を持つスタティック アクセス ポートとして設定します。指定できる範囲は 1 ～ 4094 です。
vlan dynamic	VLAN Membership Policy Server（VMPS; VLAN メンバシップ ポリシー サーバ）プロトコルによってアクセス モード VLAN が決まるように指定します。ポートに接続されたホスト（複数可）の送信元 MAC アドレスに基づいて、ポートが VLAN に割り当てられます。スイッチは、新しい MAC アドレスを受信するたびに VMPS サーバに送信して、ダイナミック アクセス ポートに割り当てる VLAN の名前を取得します。すでに、ポートには VLAN が割り当てられていて、送信元が VMPS によって承認されている場合、スイッチはパケットを該当する VLAN に転送します。

デフォルト

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 は、プラットフォームまたはインターフェイス ハードウェアに対応したデフォルト VLAN です。

ダイナミック アクセス ポートは、最初はどの VLAN のメンバにも属さず、受信したパケットに基づいて割り当てを受信します。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

no switchport access コマンドは、アクセス モード VLAN をデバイスの適切なデフォルト VLAN にリセットします。

switchport access vlan コマンドを有効にするには、事前にポートをアクセス モードにする必要があります。

アクセス ポートを割り当てることができるのは、1 つの VLAN だけです。

ポートをダイナミックとして設定するには、事前に VMPS サーバ（Catalyst 6000 シリーズ スイッチなど）を設定する必要があります。

ダイナミック アクセス ポートには、次の制限事項が適用されます。

- ソフトウェアは、Catalyst 6000 シリーズ スイッチなどの VMPS をクエリーできる VLAN Query Protocol（VQP）クライアントを実装します。Catalyst 3750 スイッチは、VMPS サーバではありません。ポートをダイナミックとして設定するには、事前に VMPS サーバを設定する必要があります。
- ダイナミック アクセス ポートは、エンド ステーションの接続にだけ使用します。ブリッジング プロトコルを使用するスイッチまたはルータにダイナミック アクセス ポートを接続すると、接続が切断されることがあります。
- STP がダイナミック アクセス ポートを STP ブロッキング ステートにしないように、ネットワークを設定します。ダイナミック アクセス ポートでは、PortFast 機能が自動的にイネーブルになります。
- ダイナミック アクセス ポートは、1 つの VLAN にだけ属することができ、VLAN タギングは使用しません。
- ダイナミック アクセス ポートを次のように設定することはできません。
  - EtherChannel ポート グループのメンバ（ダイナミック アクセス ポートは、他のダイナミック ポートなど、他のポートとはグループ化できません）
  - スタティック アドレス エントリ内の送信元または宛先ポート
  - モニタ ポート

例

次の例では、アクセス モードで動作するスイッチド ポート インターフェイスが、デフォルト VLAN ではなく VLAN 2 で動作するように変更します。

```
Switch(config-if)# switchport access vlan 2
```

設定を確認するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力して、Administrative Mode 行および Operational Mode 行の情報を調べます。

関連コマンド

コマンド	説明
show interfaces switchport	ポート ブロッキング、ポート保護設定など、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	ポートの VLAN メンバシップ モードを設定します。

switchport autostate exclude

VLAN インターフェイス（Switch Virtual Interface（SVI; スイッチ仮想インターフェイス））のラインステート アップまたはダウン計算からインターフェイスを除外するには、**switchport autostate exclude** 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。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

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

VLAN 上のすべてのポートを VLAN インターフェイス リンクアップ計算に含めます。

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

コマンド履歴

リリース	変更内容
12.2(46)SE	このコマンドが追加されました。

使用上のガイドライン

SVI に属するレイヤ 2 アクセス ポートまたはトランク ポートで **switchport autostate exclude** コマンドを入力します。

ポートが関連 VLAN のトラフィックを転送している場合、VLAN インターフェイス（SVI）は起動しています。VLAN 上のすべてのポートがダウンしているかブロックしている場合、SVI はダウンしています。SVI ライン ステートを起動するには、VLAN 上の少なくとも 1 つのポートを起動して、転送させる必要があります。**switchport autostate exclude** コマンドを使用すると、SVI インターフェイスのラインステート アップまたはダウン計算からポートを除外できます。たとえば、モニタリング ポートがアクティブなだけで VLAN が起動していると見なされないようにするために、計算からモニタリング ポートを除外できます。

ポートで **switchport autostate exclude** コマンドを入力すると、このコマンドはポートでイネーブルになっているすべての VLAN に適用されます。

インターフェイスの autostate モードを確認するには、**show interface interface-id switchport** 特権 EXEC コマンドを入力します。モードが設定されていないと、autostate モードが表示されません。

例

次の例では、インターフェイスで autostate 除外を設定して、設定を確認する方法を示します。

```
Switch(config)#interface gigabitethernet 1/0/1
Switch(config-if)# switchport autostate exclude
Switch(config-if)# end
Switch# show interface gigabitethernet1/0/1 switchport
Name: Gi1/0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
```

```
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Autostate mode exclude
```

関連コマンド

コマンド	説明
show interfaces [*interface-id*] **switchport**	autostate モード（設定されている場合）を含む、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。
show running-config	現在の動作設定を表示します。

switchport backup interface

1 組のインターフェイスで、相互にバックアップを提供する Flex Link を設定するには、レイヤ 2 インターフェイスで、**switchport backup interface** 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。Flex Link 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。

switchport backup interface [**FastEthernet** *interface-id* | **GigabitEthernet** *interface-id* | **Port-channel** *interface-id* | **TenGigabitEthernet** *interface-id*] {**mmu primary vlan** *interface-id* | **multicast fast-convergence** | **preemption** {**delay** *delay-time* | **mode**} | **prefer vlan** *vlan-id*}

no switchport backup interface [**FastEthernet** *interface-id* | **GigabitEthernet** *interface-id* | **Port-channel** *interface-id* | **TenGigabitEthernet** *interface-id*] {**mmu primary vlan** *interface-id* | **multicast fast-convergence** | **preemption** {**delay** *delay-time* | **mode**} | **prefer vlan** *vlan-id*}

構文の説明

FastEthernet	FastEthernet IEEE 802.3 ポート名です。指定できる範囲は 0 ～ 9 です。
GigabitEthernet	GigabitEthernet IEEE 802.3z ポート名です。指定できる範囲は 0 ～ 9 です。
Port-channel	インターフェイスのイーサネット チャネルです。指定できる範囲は 0 ～ 48 です。
TenGigabitEthernet	10 ギガビット イーサネット ポート名です。指定できる範囲は 0 ～ 9 です。
interface-id	設定されるインターフェイスへのバックアップ リンクとしてレイヤ 2 インターフェイスが機能するように指定します。このインターフェイスには物理インターフェイスまたはポート チャネルを指定できます。ポート チャネル範囲は 1 ～ 48 です。
mmu	MAC アドレス移行更新です。バックアップ インターフェイス ペアの Mac Move Update（MMU）を設定します。
primary vlan *vlan-id*	プライベート VLAN プライマリ VLAN の VLAN ID。指定できる範囲は、1 ～ 4,094 です。
multicast fast-convergence	マルチキャスト高速コンバージェンス パラメータです。
preemption	バックアップ インターフェイス ペアのプリエンプション スキームを設定します。
delay *delay-time*	（任意）プリエンプション遅延を指定します。指定できる範囲は、1 ～ 300 秒です。
mode	プリエンプション モードを bandwidth、forced、または off に設定します。
prefer vlan *vlan-id*	VLAN が Flex Link ペアのバックアップ インターフェイスで実行されるように指定します。VLAN ID 範囲は 1 ～ 4,094 です。
off	（任意）バックアップからアクティブへ移行する際、プリエンプションを行わないように指定します。
delay *delay-time*	（任意）プリエンプション遅延を指定します。指定できる範囲は、1 ～ 300 秒です。

デフォルト

デフォルトは、Flex Link が定義されていません。プリエンプション モードはオフです。プリエンプションを行いません。プリエンプション遅延は 35 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

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。
12.2(25)SEE	**preemption**、**mode**、**forced**、**bandwidth**、**off**、および **delay** キーワードが追加されました。
12.2(37)SE	**prefer vlan** キーワードが追加されました。
12.2(44)SE	**multicast**、**fast-convergence**、**delay**、**mode**、**prefer**、および **vlan** キーワードが追加されました。

使用上のガイドライン

Flex Link を設定すると、1 つのリンクがプライマリ インターフェイスとして機能してトラフィックを転送し、もう一方のインターフェイスがスタンバイ モードになり、プライマリ リンクがシャットダウンされた場合に転送を開始できるように準備されます。設定されるインターフェイスはアクティブ リンクと呼ばれ、指定されたインターフェイスはバックアップ リンクとして識別されます。この機能は Spanning Tree Protocol（STP; スパニング ツリー プロトコル）の代わりに提供され、ユーザが STP をオフにしても基本的なリンク冗長性を維持できます。

- このコマンドは、レイヤ 2 インターフェイスに対してだけ使用可能です。
- 任意のアクティブ リンクに対して設定可能な Flex Link バックアップ リンクは 1 つだけで、アクティブ インターフェイスとは異なるインターフェイスでなければなりません。
- インターフェイスが所属できる Flex Link ペアは 1 つだけです。インターフェイスがバックアップ リンクになるのは、1 つのアクティブ リンクに対してだけです。アクティブ リンクは別の Flex Link ペアに属することはできません。
- バックアップ リンクはアクティブ リンクと同じタイプ（たとえばファスト イーサネットやギガビット イーサネット）でなくてもかまいません。ただし、スタンバイ リンクがトラフィック転送を開始した場合にループが発生したり動作が変更したりしないように、両方の Flex Link を同様の特性で設定する必要があります。
- いずれのリンクも EtherChannel に属するポートにはなれません。ただし、2 つのポート チャネル（EtherChannel 論理インターフェイス）を Flex Link として設定できます。また、ポート チャネルか物理インターフェイスのいずれか一方をアクティブ リンクにして、ポート チャネルと物理インターフェイスポートを Flex Link として設定できます。
- STP がスイッチに設定されている場合、Flex Link はすべての有効な VLAN で STP に参加しません。STP が動作していない場合、設定されているトポロジでループが発生していないことを確認してください。

例

次の例では、2 つのインターフェイスを Flex Link として設定する例を示します。

```
Switch# configure terminal
Switch(conf)# interface fastethernet1/0/1
Switch(conf-if)# switchport backup interface fastethernet1/0/2
Switch(conf-if)# end
```

次の例では、常にバックアップのプリエンプションを行うようファスト イーサネット インターフェイスを設定する方法を示します。

```
Switch# configure terminal
Switch(conf)# interface fastethernet1/0/1
Switch(conf-if)# switchport backup interface fastethernet1/0/2 preemption forced
```

```
Switch(conf-if)# end
```

次の例では、ファスト イーサネット インターフェイスのプリエンプション遅延時間を設定する方法を示します。

```
Switch# configure terminal
Switch(conf)# interface fastethernet1/0/1
Switch(conf-if)# switchport backup interface fastethernet1/0/2 preemption delay 150
Switch(conf-if)# end
```

次の例では、MMU プライマリ VLAN としてファスト イーサネット インターフェイスを設定する方法を示します。

```
Switch# configure terminal
Switch(conf)# interface fastethernet1/0/1
Switch(conf-if)# switchport backup interface fastethernet1/0/2 mmu primary vlan 1021
Switch(conf-if)# end
```

設定を確認するには、**show interfaces switchport backup** 特権 EXEC コマンドを入力します。

次の例では、優先 VLAN の設定方法を示します。

```
Switch(config)# interface gigabitethernet 1/0/6
Switch(config-if)# switchport backup interface gigabitethernet 1/0/8 prefer vlan
60,100-120
```

設定を確認するには、**show interfaces switchport backup** 特権 EXEC コマンドを入力します。

この例では、VLAN 60 および 100 ～ 120 がスイッチに設定されています。

```
Switch(config)# interface gigabitEthernet 1/0/6
Switch(config-if)# switchport backup interface gigabitEthernet 1/0/8 prefer vlan
60,100-120
```

両方のインターフェイスが起動している場合、Gi1/0/6 が VLAN 1 ～ 50 のトラフィックを転送し、Gi1/0/8 が VLAN 60 および 100 ～ 120 のトラフィックを転送します。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet1/0/6 GigabitEthernet1/0/8 Active Up/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

Flex Link インターフェイスがダウンすると（LINK_DOWN）、このインターフェイスで優先される VLAN は、Flex Link ペアのピア インターフェイスに移動します。この例では、インターフェイス Gi1/0/6 がダウンして、Gi1/0/8 が Flex Link ペアのすべての VLAN を引き継ぎます。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet1/0/61/0/8 GigabitEthernet Active Down/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

Flex Link インターフェイスがアップになると、このインターフェイスで優先される VLAN はピア インターフェイスでブロックされ、アップしたインターフェイスでフォワーディング ステートになります。この例では、インターフェイス Gi1/0/6 がアップになると、このインターフェイスで優先される VLAN はピア インターフェイス Gi1/0/8 でブロックされ、Gi1/0/6 で転送されます。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet1/0/6 GigabitEthernet1/0/8 Active Up/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

次の例では、マルチキャスト高速コンバージェンスをインターフェイス Gi1/0/11 で設定する方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet 1/0/11
Switch(config-if)# switchport backup interface gigabitEthernet 1/0/12 multicast
fast-convergence
Switch(config-if)# end
```

設定を確認するには、**show interfaces switchport backup detail** 特権 EXEC コマンドを入力します。

```
Switch# show interfaces switchport backup detail

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet1/0/11 GigabitEthernet1/0/12 Active Up/Backup Standby
        Preemption Mode  : off
        Multicast Fast Convergence  : On
        Bandwidth : 1000000 Kbit (Gi1/0/11), 1000000 Kbit (Gi1/0/12)
        Mac Address Move Update Vlan : auto
```

関連コマンド

コマンド	説明
show interfaces [*interface-id*] **switchport backup**	スイッチまたは指定したインターフェイスに設定されている Flex Link とそのステータスを表示します。

switchport block

不明なマルチキャストまたはユニキャストのパケットが転送されないようにするには、**switchport block** 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。未知のマルチキャストまたはユニキャスト 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 {**multicast** | **unicast**}

no switchport block {**multicast** | **unicast**}

構文の説明

multicast	不明なマルチキャスト トラフィックをブロックするよう指定します。 （注）　純粋なレイヤ 2 マルチキャスト トラフィックだけがブロックされます。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。
unicast	不明なユニキャスト トラフィックをブロックするよう指定します。

デフォルト

不明なマルチキャストおよびユニキャスト トラフィックはブロックされていません。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、不明な 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。保護ポートまたは非保護ポート上の不明なマルチキャストまたはユニキャスト トラフィックをブロックすることができます。不明なマルチキャストまたはユニキャスト トラフィックが保護ポートでブロックされない場合、セキュリティに問題のある場合があります。

マルチキャスト トラフィックでは、ポート ブロッキング機能は純粋なレイヤ 2 パケットだけをブロックします。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。

不明なマルチキャストまたはユニキャスト トラフィックのブロックは、保護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。

パケットのブロックに関する情報は、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、インターフェイス上で不明なユニキャスト トラフィックをブロックする方法を示します。

```
Switch(config-if)# switchport block unicast
```

設定を確認するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces switchport	ポート ブロッキング、ポート保護設定など、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 host

レイヤ 2 ポートのホスト接続を最適化するには、**switchport host** 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。システム上への影響をなくすには、このコマンドの **no** 形式を使用します。

switchport host

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ポートのデフォルトは、ホストへの接続が最適化されていません。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

ホスト接続のためポートを最適化するには、**switchport host** コマンドで、アクセスするスイッチ ポート モードを設定し、スパニング ツリー PortFast をイネーブルにして、チャネル グルーピングをディセーブルにします。エンド ステーションにだけこの設定を適用することができます。

スパニング ツリー PortFast はイネーブルであるため、**switchport host** コマンドをシングルホストと接続するポートにだけ入力します。その他のスイッチ、ハブ、コンセントレータ、またはブリッジと fast-start ポートを接続すると、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。

switchport host コマンドをイネーブルにし、パケット転送の開始における遅延時間を減少させることができます。

例

次の例では、ポートのホスト接続の設定を最適化する方法を示します。

```
Switch(config-if)# switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
Switch(config-if)#
```

設定を確認するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces switchport	スイッチポート モードを含む、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

ポートの VLAN メンバシップ モードを設定するには、**switchport mode** インターフェイス コンフィギュレーション コマンドを入力します。モードをデバイスの適切なデフォルト設定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 | dot1q-tunnel | dynamic {auto | desirable} | private-vlan | trunk}

no switchport mode {access | dot1q-tunnel | dynamic | trunk}

構文の説明

access	アクセス モード（**switchport access vlan** インターフェイス コンフィギュレーション コマンドの設定に応じて、スタティック アクセスまたはダイナミック アクセスのいずれか）を設定します。ポートは無条件にアクセスするように設定され、非カプセル化（タグなし）フレームを送受信する単一の非トランク VLAN インターフェイスとして動作します。アクセス ポートを割り当てることができるのは、1 つの VLAN だけです。
dot1q-tunnel	ポートを IEEE 802.1Q トンネル ポートとして設定します。
dynamic auto	インターフェイス トランキング モード ダイナミック パラメータを auto に設定して、インターフェイスがリンクをトランク リンクに変換するように指定します。これがデフォルトのスイッチポート モードになります。
dynamic desirable	インターフェイス トランキング モード ダイナミック パラメータを desirable に設定して、インターフェイスがリンクをトランク リンクにアクティブに変換するように指定します。
private-vlan	**switchport mode private-vlan** コマンドを参照してください。
trunk	無条件にポートをトランクに設定します。ポートは VLAN レイヤ 2 インターフェイスをトランキングします。ポートは、送信元の VLAN を識別するカプセル化（タグ付き）フレームを送受信します。トランクは、2 つのスイッチ間、またはスイッチとルータ間のポイントツーポイント リンクです。

デフォルト

デフォルト モードは **dynamic auto** 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(20)SE	**private-vlan** キーワードが追加されました。
12.2(25)SE	**dot1q-tunnel** キーワードが追加されました。

使用上のガイドライン

access、**dot1q-tunnel**、または **trunk** キーワードによる設定が有効となるのは、**switchport mode** コマンドを使用して、適切なモードでポートを設定した場合だけです。スタティック アクセスおよびトランクの設定は保存されますが、同時にアクティブにできるのはいずれかの設定だけです。

access モードを入力すると、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 モードを入力すると、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、接続先の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 モードを入力した場合に、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 モードを入力した場合に、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。

トランキングを自動ネゴシエーションするには、インターフェイスが同じ VLAN Trunking Protocol（VTP）ドメインに存在する必要があります。トランク ネゴシエーションは、ポイントツーポイント プロトコルである Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）によって管理されます。ただし、一部のインターネットワーキング デバイスによって DTP フレームが不正に転送されて、矛盾した設定となる場合があります。この事態を避けるには、DTP をサポートしない装置に接続されたインターフェイスが DTP フレームを転送しないように、つまり DTP をオフにするように設定する必要があります。

- これらのリンク上でトランキングを行わない場合は、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用して、トランキングをディセーブルにします。
- DTP をサポートしていない装置でトランキングをイネーブルにするには、**switchport mode** trunk および **switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。

dot1q-tunnel を入力すると、ポートは IEEE 802.1Q トンネル ポートとして無条件に設定されます。

アクセス ポート、トランク ポート、およびトンネル ポートは、相互に排他的な関係にあります。

トンネル ポートで受信された IEEE 802.1Q カプセル化 IP パケットはすべて MAC Access Control List（ACL; アクセス コントロール リスト）でフィルタリングできますが、IP ACL ではフィルタリングできません。これは、スイッチが IEEE 802.1Q ヘッダー内部のプロトコルを認識しないためです。ルータ ACL、ポート ACL、および VLAN マップに、この制限が適用されます。

ポートを IEEE 802.1Q トンネル ポートとして設定する場合、次の制限事項が適用されます。

- IP ルーティングおよびフォールバック ブリッジングは、トンネル ポートではサポートされません。
- トンネル ポートは、IP ACL をサポートしません。
- IP ACL がトンネル ポートを含む VLAN 内のトランク ポートに適用されている場合、または VLAN マップがトンネル ポートを含む VLAN に適用されている場合は、トンネル ポートから受信したパケットは、非 IP パケットとして取り扱われ、MAC アクセス リストでフィルタリングされます。
- レイヤ 3 の Quality of Service（QoS）ACL およびレイヤ 3 情報に関連する他の QoS 機能は、トンネル ポートではサポートされていません。

IEEE 802.1Q トンネル ポートの設定に関する詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

IEEE 802.1x 機能は、次の方法でスイッチポート モードに作用します。

- トランク ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートのモードをトランクに変更しようとしても、ポート モードは変更されません。
- ポート設定で IEEE 802.1x を **dynamic auto** または **dynamic desirable** にイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートのモードを **dynamic auto** または **dynamic desirable** に変更しようとしても、ポート モードは変更されません。
- ダイナミック アクセス（VLAN Query Protocol（VQP））ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートをダイナミック VLAN 割り当てに変更しようとしても、エラー メッセージが表示され、VLAN 設定は変更されません。

例

次の例では、ポートをアクセス モードに設定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode access
```

次の例では、ポートを dynamic desirable モードに設定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode dynamic desirable
```

次の例では、ポートをトランク モードに設定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode trunk
```

次の例では、ポートを IEEE 802.1Q トンネル ポートとして設定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode dot1q-tunnel
```

設定を確認するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力して、Administrative Mode 列および Operational Mode 列を調べます。

関連コマンド

コマンド	説明
show interfaces switchport	ポート ブロッキング、ポート保護設定など、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	ポートをスタティック アクセス ポートまたはダイナミック アクセス ポートとして設定します。
switchport trunk	インターフェイスがトランキング モードの場合、トランクの特性を設定します。

switchport mode private-vlan

ポートを混合ポートまたはホストのプライベート VLAN ポートとして設定するには、**switchport mode private-vlan** 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。モードをデバイスの適切なデフォルト設定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 private-vlan {host | promiscuous}

no switchport mode private-vlan

構文の説明

host	インターフェイスをプライベート VLAN ホスト ポートとして設定します。ホスト ポートは、プライベート VLAN のセカンダリ VLAN に所属し、所属する VLAN に応じてコミュニティ ポートまたは隔離ポートのいずれかになります。
promiscuous	インターフェイスをプライベート VLAN 混合ポートとして設定します。混合ポートは、プライベート VLAN のプライマリ VLAN のメンバです。

デフォルト

デフォルトのプライベート VLAN モードは、ホストまたは混合のどちらでもありません。

デフォルトのスイッチポート モードは **dynamic auto** 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

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

プライベート VLAN のホスト ポートまたは混合ポートは、Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）宛先ポートには設定できません。SPAN 宛先ポートをプライベート VLAN のホスト ポートまたは混合ポートとして設定する場合、ポートが非アクティブになります。

ポート上のプライベート VLAN に他の機能（以下）を設定しないでください。

- ダイナミック アクセス ポート VLAN メンバシップ
- Dynamic Trunking Protocol（DTP）
- Port Aggregation Protocol（PAgP）
- Link Aggregation Control Protocol（LACP）
- Multicast VLAN Registration（MVR）
- Voice VLAN

プライベート VLAN ポートは、SPAN 宛先ポートには設定できません。

ポートがプライベート VLAN 設定に含まれていると、ポートの EtherChannel 設定が非アクティブになります。

プライベート VLAN ポートはセキュア ポートにはできないので、保護ポートとして設定できません。

プライベート VLAN の他の機能との相互作用に関する詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

設定の矛盾による STP ループの発生を防ぎ、STP コンバージェンスをより速く行うために、隔離およびコミュニティ ホスト ポート上でスパニング ツリー PortFast および UniDirectional Link Detection（UDLD; 単一方向リンク検出）ガードをイネーブルにすることを強く推奨します。

ポートをプライベート VLAN ホスト ポートとして設定し、**switchport private-vlan host-association** インターフェイス コンフィギュレーション コマンドを使用して有効なプライベート VLAN のアソシエーションを設定しない場合、インターフェイスが非アクティブになります。

ポートをプライベート VLAN 混合ポートとして設定し、**switchport private-vlan mapping** インターフェイス コンフィギュレーション コマンドを使用して有効なプライベート VLAN のマッピングを設定しない場合、インターフェイスが非アクティブになります。

例

次の例では、インターフェイスをプライベート VLAN ホスト ポートとして設定し、それをプライマリ VLAN 20 に関連付ける方法を示します。インターフェイスは、セカンダリ隔離 VLAN 501 およびプライマリ VLAN 20 のメンバです。

（注）　ポートをプライベート VLAN ホスト ポートとして設定する場合は、**spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドおよび **spanning-tree portfast** インターフェイス コンフィギュレーション コマンドを使用して、BPDU ガードと PortFast もイネーブルにする必要があります。

```
Switch# configure terminal
Switch(config)# interface fastethernet 1/0/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 501
Switch(config-if)# end
```

次の例では、インターフェイスをプライベート VLAN 混合ポートとして設定し、それをプライベート VLAN にマッピングする方法を示します。インターフェイスは、プライマリ VLAN 20 のメンバで、セカンダリ VLAN 501 ～ 503 がマッピングされます。

```
Switch# configure terminal
Switch(config)# interface fastethernet 1/0/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 501-503
Switch(config-if)# end
```

プライベート VLAN のスイッチポート モードを確認するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
private-vlan	VLAN をコミュニティ、隔離、またはプライマリ VLAN に設定するか、プライマリ VLAN をセカンダリ VLAN に関連付けます。
show interfaces switchport	プライベート VLAN の設定を含む、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 private-vlan	インターフェイス上のプライマリおよびセカンダリ VLAN 間のプライベート VLAN のアソシエーションとマッピングを設定します。

switchport nonegotiate

レイヤ 2 インターフェイス上で Dynamic Trunking Protocol（DTP）ネゴシエーション パケットが送信されないように指定するには、**switchport nonegotiate** 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。スイッチは、このインターフェイス上で DTP ネゴシエーションを行いません。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 nonegotiate

no switchport nonegotiate

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトでは、トランキング ステータスを学習するために、DTP ネゴシエーションを使用します。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

nonegotiate ステータスを解除するには、**switchport nonegotiate** コマンドの **no** 形式を使用します。

このコマンドが有効なのは、インターフェイス スイッチポート モードがアクセスまたはトランク（**switchport mode access** または **switchport mode trunk** 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）の場合だけです。**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と、エラーが返されます。

DTP をサポートしないインターネットワーキング デバイスでは、DTP フレームが正しく転送されず、設定に矛盾が生じることがあります。この問題を回避するには、**switchport nonegotiate** コマンドを使用して DTP をオフにし、DTP をサポートしていないデバイスに接続されたインターフェイスが DTP フレームを転送しないように設定します。

switchport nonegotiate コマンドを入力した場合、このインターフェイスでは DTP ネゴシエーション パケットが送信されません。デバイスがトランキングを実行するかどうかは、**mode** パラメータ（**access** または **trunk**）によって決まります。

- これらのリンク上でトランキングを行わない場合は、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用して、トランキングをディセーブルにします。
- DTP をサポートしていないデバイスでのトランキングをイネーブルにするには、**switchport mode** trunk および **switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。

例

次の例では、ポートに対してトランキング モードのネゴシエートを制限し、（モードの設定に応じて）トランク ポートまたはアクセス ポートとして動作させる方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport nonegotiate
```

設定を確認するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces switchport	ポート ブロッキング、ポート保護設定など、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	ポートの VLAN メンバシップ モードを設定します。

switchport port-security

インターフェイス上のポート セキュリティをイネーブルにするには、キーワードを指定せずに **switchport port-security** 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。キーワードを指定すると、セキュア MAC アドレス、スティッキ MAC アドレス ラーニング、セキュア MAC アドレスの最大数、または違反モードが設定されます。ポート セキュリティをディセーブルにしたり、またはパラメータをデフォルト状態に戻すには、このコマンドの **no** 形式を使用します。

switchport port-security [**mac-address** *mac-address* [**vlan** {*vlan-id* | {**access** | **voice**}}] | **mac-address sticky** [*mac-address* | **vlan** {*vlan-id* | {**access** | **voice**}}]] [**maximum** *value* [**vlan** {*vlan-list* | {**access** | **voice**}}]]

no switchport port-security [**mac-address** *mac-address* [**vlan** {*vlan-id* | {**access** | **voice**}}] | **mac-address sticky** [*mac-address* | **vlan** {*vlan-id* | {**access** | **voice**}}]] [**maximum** *value* [**vlan** {*vlan-list* | {**access** | **voice**}}]]

switchport port-security [**aging**] [**violation** {**protect** | **restrict** | **shutdown** | **shutdown vlan**}]

no switchport port-security [**aging**] [**violation** {**protect** | **restrict** | **shutdown** | **shutdown vlan**}]

構文の説明

aging	（任意）**switchport port-security aging** コマンドを参照してください。
mac-address *mac-address*	（任意）48 ビット MAC アドレスを入力して、インターフェイスのセキュア MAC アドレスを指定します。設定された最大数まで、セキュア MAC アドレスを追加できます。
vlan *vlan-id*	（任意）トランク ポート上でだけ、VLAN ID および MAC アドレスを指定します。VLAN ID を指定しない場合は、ネイティブ VLAN が使用されます。
vlan access	（任意）アクセス ポートでだけ、VLAN をアクセス VLAN として指定します。
vlan voice	（任意）アクセス ポートでだけ、VLAN を音声 VLAN として指定します。 **（注）** **voice** キーワードは、音声 VLAN がポートに設定されてそのポートがアクセス VLAN でない場合に限り利用可能です。
mac-address sticky [*mac-address*]	（任意）*mac-address sticky* キーワードだけを入力して、インターフェイスの**スティッキ ラーニング**をイネーブルにします。スティッキ ラーニングをイネーブルにすると、インターフェイスは動的に学習したすべてのセキュア MAC アドレスを実行コンフィギュレーションに追加して、これらのアドレスをスティッキ セキュア MAC アドレスに変換します。 （任意）*mac-address* を入力し、スティッキ セキュア MAC アドレスを指定します。

maximum *value*	（任意）インターフェイスのセキュア MAC アドレスの最大数を設定します。スイッチ スタックで設定できるセキュア MAC アドレスの最大数は、システムで使用が許可されている MAC アドレスの最大数によって決まります。この数字はアクティブな Switch Database Management（SDM）テンプレートによって決められます。詳細は、**sdm prefer** グローバル コンフィギュレーション コマンドを参照してください。この数字は、インターフェイスで設定された他のレイヤ 2 機能やその他のセキュア MAC アドレスなど、利用可能な MAC アドレスの合計数を示します。 デフォルトの設定は 1 です。
vlan [*vlan-list*]	（任意）トランク ポートに対して、VLAN のセキュア MAC アドレスの最大数を設定できます。**vlan** キーワードが入力されていない場合、デフォルト値が使用されます。 • **vlan** : VLAN ごとに最大値を設定します。 • **vlan** *vlan-list* : VLAN 範囲、または一連の VLAN 内の VLAN ごとに最大値を設定します。VLAN 範囲はハイフン、一連の VLAN はカンマで区切ります。VLAN を指定しない場合、VLAN ごとの最大値が使用されます。
violation	（任意）セキュリティ違反モード、またはポート セキュリティに違反した場合に実行するアクションを設定します。デフォルトは **shutdown** です。
protect	セキュリティ違反保護モードを設定します。このモードでは、ポートのセキュア MAC アドレス数がポートで許可されている最大数に到達した場合、不明な送信元アドレスのパケットはドロップされます。ドロップすることでセキュア MAC アドレス数を上限よりも少なくするか、許容できるアドレスの最大数を増やさない限り、この状態が続きます。セキュリティ違反が起こっても、ユーザには通知されません。 **（注）** トランク ポート上に保護モードを設定することは推奨できません。保護モードでは、ポートが最大数に達していなくても VLAN が保護モードの最大数に達すると、ラーニングがディセーブルになります。
restrict	セキュリティ違反制限モードを設定します。このモードでは、セキュア MAC アドレス数がポートで許可されている最大数に到達した場合、不明な送信元アドレスのパケットはドロップされます。セキュア MAC アドレス数を上限よりも少なくするか、許容できるアドレスの最大数を増やさない限り、この状態が続きます。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。
shutdown	セキュリティ違反シャットダウン モードを設定します。このモードでは、違反が発生し、ポートの LED がオフになると、インターフェイスが errdisable の状態になります。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。セキュア ポートが errdisable ステートの場合は、**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 shut down** インターフェイス コンフィギュレーション コマンドを入力したりして、手動で再びイネーブルにすることができます。
shutdown vlan	VLAN ごとのシャットダウンにセキュリティ違反モードを設定します。このモードでは、違反が発生した VLAN だけが errdisable になります。

デフォルト

デフォルトでは、ポート セキュリティはディセーブルです。

ポート セキュリティをイネーブルにしてキーワードを入力しない場合、デフォルトのセキュア MAC アドレスの最大数は 1 です。

デフォルトの違反モードは、**shutdown** です。

スティッキ ラーニング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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**sticky** および **vlan** キーワードが追加されました。
12.2(25)SEB	**access** および **voice** キーワードが追加されました。
12.2(35)SE	**shutdown vlan** キーワードが追加されました。

使用上のガイドライン

セキュア ポートに関する制限事項は、次のとおりです。

- セキュア ポートはアクセス ポートまたはトランク ポートにすることはできますが、ダイナミック アクセス ポートには設定できません。
- セキュア ポートはルーテッド ポートにはできません。
- セキュア ポートは保護ポートにはできません。
- セキュア ポートを Switched Port Analyzer（SPAN）の宛先ポートにすることはできません。
- セキュア ポートはプライベート VLAN ポートにはできません。
- セキュア ポートを Fast EtherChannel または Gigabit EtherChannel ポート グループに含めることはできません。
- 音声 VLAN では、スタティック セキュアまたはスティッキ セキュア MAC アドレスを設定できません。
- 音声 VLAN が設定されたインターフェイス上でポート セキュリティをイネーブルにする場合は、ポートの最大セキュア アドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合、MAC アドレスの追加は必要ありません。2 台以上の PC を Cisco IP Phone に接続する場合、各 PC に 1 つ、さらに Cisco IP Phone に 1 つ割り当てるよう十分なセキュア アドレスを設定する必要があります。
- 音声 VLAN はアクセス ポート上でだけサポートされます。トランク ポート上ではサポートされません。
- インターフェイスのセキュア アドレスの最大値を入力する場合、新しい値が前回の値より大きいと、新しい値によって前回の設定値が上書きされます。新しい値が前回の値より小さく、インターフェイスで設定されているセキュア アドレス数が新しい値より大きい場合、コマンドは拒否されます。
- スイッチはスティッキ セキュア MAC アドレスのポート セキュリティ エージングをサポートしていません。

セキュア MAC アドレスの最大値がアドレス テーブルに存在し、アドレス テーブルに存在しない MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合、または別のセキュア ポートのセキュア MAC アドレスとして設定された MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合に、セキュリティ違反が起こります。

セキュア ポートが errdisable ステートの場合は、**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、このステートから回復させることができます。**shutdown** および **no shut down** インターフェイス コンフィギュレーション コマンドを入力するか、**clear errdisable interface** 特権 EXEC コマンドを使用して、ポートを手動で再びイネーブルにすることができます。

アドレスの最大数を 1 に設定し、接続されたデバイスの MAC アドレスを設定すると、確実にデバイスがポートの帯域幅を完全に使用できます。

インターフェイスのセキュア アドレスの最大値を入力すると、次の事象が発生します。

- 新しい値が前回の値より大きい場合、新しい値によって前回の設定値が上書きされます。
- 新しい値が前回の値より小さく、インターフェイスで設定されているセキュア アドレス数が新しい値より大きい場合、コマンドは拒否されます。

スティッキ セキュア MAC アドレスには、次の特性があります。

- **switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイス上でスティッキ ラーニングをイネーブルにした場合、インターフェイスはすべてのダイナミック セキュア MAC アドレスを（スティッキ ラーニングがイネーブルになる前にダイナミックに学習されたアドレスも含め）、スティッキ セキュア MAC アドレスに変換し、すべてのスティッキ セキュア MAC アドレスを実行コンフィギュレーションに追加します。
- **no switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用して、スティッキ ラーニングをディセーブルする場合、または実行コンフィギュレーションを削除する場合は、スティッキ セキュア MAC アドレスは実行コンフィギュレーションの一部に残りますが、アドレス テーブルからは削除されます。削除されたアドレスはダイナミックに再設定することができ、ダイナミック アドレスとしてアドレス テーブルに追加されます。
- **switchport port-security mac-address sticky** *mac-address* インターフェイス コンフィギュレーション コマンドを使用して、スティッキ セキュア MAC アドレスを設定する場合、アドレスはアドレス テーブルと実行コンフィギュレーションに追加されます。ポート セキュリティがディセーブルの場合、スティッキ セキュア MAC アドレスは実行コンフィギュレーションに残ります。
- スティッキ セキュア MAC アドレスがコンフィギュレーション ファイルに保存されていると、スイッチの再起動時、またはインターフェイスのシャットダウン時に、インターフェイスはこれらのアドレスを再学習しなくてすみます。スティッキ セキュア アドレスを保存しない場合、アドレスは失われます。スティッキ ラーニングがディセーブルの場合、スティッキ セキュア MAC アドレスはダイナミック セキュア アドレスに変換され、実行コンフィギュレーションから削除されます。
- スティッキ ラーニングをディセーブルにして、**switchport port-security mac-address sticky** *mac-address* インターフェイス コンフィギュレーション コマンドを入力した場合、エラー メッセージが表示され、スティッキ セキュア MAC アドレスは実行コンフィギュレーションに追加されません。

例

次の例では、ポートでポート セキュリティをイネーブルにし、セキュア アドレスの最大数を 5 に設定する方法を示します。違反モードはデフォルトで、セキュア MAC アドレスは設定されていません。

```
Switch(config)# interface gigabitethernet 2/0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
```

次の例では、ポートでセキュア MAC アドレスと VLAN ID を設定する方法を示します。

```
Switch(config)# interface gigabitethernet 2/0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 1000.2000.3000 vlan 3
```

次の例では、スティッキ ラーニングをイネーブルにして、ポート上で 2 つのスティッキ セキュア MAC アドレスを入力する方法を示します。

```
Switch(config)# interface gigabitethernet 2/0/2
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.4141
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.000f
```

次の例では、違反が発生した場合に VLAN だけをシャットダウンするようにポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet 2/0/2
Switch(config)# switchport port-security violation shutdown vlan
```

設定を確認するには、**show port-security** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
clear port-security	MAC アドレス テーブルからスイッチ上またはインターフェイス上の特定のタイプのセキュア アドレスまたはすべてのセキュア アドレスを削除します。
show port-security address	スイッチで設定されているすべてのセキュア アドレスを表示します。
show port-security interface *interface-id*	スイッチまたは指定されたインターフェイスのポート セキュリティ設定を表示します。

switchport port-security aging

セキュア アドレス エントリのエージング タイムおよびタイプを設定したり、特定のポートのセキュア アドレスのエージング動作を変更するには、**switchport port-security aging** 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。ポート セキュリティのエージングをディセーブルにしたり、またはパラメータをデフォルト状態に戻すには、このコマンドの **no** 形式を使用します。

switchport port-security aging {**static** | **time** *time* | **type** {**absolute** | **inactivity**}}

no switchport port-security aging {**static** | **time** | **type**}

構文の説明

static	このポートに静的に設定されたセキュア アドレスのエージングをイネーブルにします。
time *time*	このポートのエージング タイムを指定します。指定できる範囲は 0 ～ 1440 分です。time が 0 の場合、このポートのエージングはディセーブルです。
type	エージング タイプを設定します。
absolute	absolute エージング タイプを設定します。このポートのすべてのセキュア アドレスは、指定された時間（分）が経過した後に期限切れとなり、セキュア アドレス リストから削除されます。
inactivity	inactivity エージング タイプを設定します。指定された時間内にセキュア送信元アドレスからのデータ トラフィックがない場合だけ、このポートのセキュア アドレスが期限切れになります。

デフォルト

ポート セキュリティ エージング機能はディセーブルです。デフォルトの時間は 0 分です。

デフォルトのエージング タイプは absolute です。

デフォルトのスタティック エージング動作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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

特定のポートのセキュア アドレス エージングをイネーブルにするには、ポート エージング タイムを 0 以外の値に設定します。

特定のセキュア アドレスに時間を限定してアクセスできるようにするには、エージング タイプを **absolute** に設定します。エージング タイムの期限が切れると、セキュア アドレスが削除されます。

継続的にアクセスできるセキュア アドレス数を制限するには、エージング タイプを **inactivity** に設定します。このようにすると、非アクティブになったセキュア アドレスが削除され、他のアドレスがセキュアになることができます。

セキュア アドレスへのアクセス制限を解除するには、セキュア アドレスとして設定し、**no switchport port-security aging static** インターフェイス コンフィギュレーション コマンドを使用して、静的に設定されたセキュア アドレスのエージングをディセーブルにします。

例

次の例では、ポートのすべてのセキュア アドレスに対して、エージング タイプを absolute、エージング タイムを 2 時間に設定します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport port-security aging time 120
```

次の例では、ポートに設定されたセキュア アドレスに対して、エージング タイプを inactivity、エージング タイムを 2 分に設定します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

次の例では、設定されたセキュア アドレスのエージングをディセーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# no switchport port-security aging static
```

関連コマンド

コマンド	説明
show port-security	ポートに定義されたポート セキュリティ設定を表示します。
switchport port-security	ポート上でポート セキュリティをイネーブルにし、ポートの使用対象をユーザ定義のステーション グループに制限し、セキュア MAC アドレスを設定します。

switchport priority extend

着信したタグなしフレームのポート プライオリティ、または指定されたポートに接続された IP Phone が受信するフレームのプライオリティを設定するには、**switchport priority extend** 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。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 priority extend {**cos** *value* | **trust**}

no switchport priority extend

構文の説明

cos *value*	PC から受信したか、または指定した Class of Service（CoS）値を持つ接続装置から受信した IEEE 802.1p プライオリティを上書きするよう IP Phone ポートを設定します。指定できる範囲は 0 ～ 7 です。7 が最も高いプライオリティです。デフォルト値は 0 です。
trust	PC または接続装置から受信した IEEE 802.1p プライオリティを信頼するように IP Phone のポートを設定します。

デフォルト

ポートで受信したタグなしフレームには、デフォルト ポート プライオリティは、CoS 値 0 で設定されています。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

音声 VLAN をイネーブルにした場合、スイッチを設定して、Cisco Discovery Protocol（CDP）パケットを送信し、Cisco IP Phone のアクセス ポートに接続される装置からデータ パケットを送信する方法を IP Phone に指示できます。Cisco IP Phone に設定を送信するには、Cisco IP Phone に接続しているスイッチ ポートの CDP をイネーブルにする必要があります（デフォルトでは、CDP はすべてのスイッチ インターフェイスでグローバルにイネーブルです）。

スイッチ アクセス ポート上で音声 VLAN を設定する必要があります。音声 VLAN は、レイヤ 2 ポート上にだけ設定できます。

音声 VLAN をイネーブルにする前に、**mls qos** 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スイッチの Quality of Service（QoS）をイネーブルにし、**mls qos trust cos** インターフェイス コンフィギュレーション コマンドを入力して、信頼するようにポート信頼状態を設定することを推奨します。

例

次の例では、受信した IEEE 802.1p プライオリティを信頼するように、指定されたポートに接続された IP Phone を設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport priority extend trust
```

設定を確認するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力します。

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 voice vlan {vlan-id | dot1p | none | untagged}	ポートに音声 VLAN を設定します。

switchport private-vlan

隔離ポートまたはコミュニティ ポートへのプライベート VLAN のアソシエーション、または混合ポートへのマッピングを定義するには、**switchport private-vlan** 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。ポートからプライベート VLAN のアソシエーション、または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 {**association** {**host** *primary-vlan-id secondary-vlan-id* | **mapping** *primary-vlan-id* {**add** | **remove**} *secondary-vlan-list*} | **host-association** *primary-vlan-id secondary-vlan-id* | **mapping** *primary-vlan-id* {**add** | **remove**} *secondary-vlan-list*}

no switchport private-vlan {**association** {**host** | **mapping**} | **host-association** | **mapping**

構文の説明

association	ポートに対するプライベート VLAN のアソシエーションを定義します。
host	コミュニティまたは隔離ホスト ポートに対するプライベート VLAN のアソシエーションを定義します。
primary-vlan-id	プライベート VLAN のプライマリ VLAN の VLAN ID。指定できる範囲は 2 ～ 1001 および 1006 ～ 4094 です。
secondary-vlan-id	プライベート VLAN のセカンダリ（隔離またはコミュニティ）VLAN の VLAN ID。指定できる範囲は 2 ～ 1001 および 1006 ～ 4094 です。
mapping	混合ポートに対するプライベート VLAN のマッピングを定義します。
add	セカンダリ VLAN をプライマリ VLAN に関連付けます。
remove	セカンダリ VLAN とプライマリ VLAN 間のアソシエーションをクリアします。
secondary-vlan-list	プライマリ VLAN にマッピングされる 1 つまたは複数のセカンダリ（隔離またはコミュニティ）VLAN
host-association	コミュニティまたは隔離ホスト ポートに対するプライベート VLAN のアソシエーションを定義します。

デフォルト

デフォルトでは、プライベート VLAN のアソシエーションまたは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

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

switchport mode private-vlan {**host** | **promiscuous**} インターフェイス コンフィギュレーション コマンドを使用して、ポートがプライベート VLAN のホスト ポートまたは混合ポートとして設定されていないと、プライベート VLAN のアソシエーションまたはマッピングはポートで作用しません。

ポートがプライベート VLAN のホスト モードまたは混合モードであっても、VLAN が存在しない場合、コマンドは許可されますが、ポートは非アクティブになります。

secondary_vlan_list パラメータには、スペースを含めないでください。複数のカンマ区切りの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、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。リストには、1 つの隔離 VLAN と複数のコミュニティ VLAN を含めることができます。

混合ポートを 1 つのプライマリ VLAN だけにマッピングできます。プライマリおよびセカンダリ VLAN にすでにマッピングされている混合ポート上で **switchport private-vlan mapping** コマンドを入力すると、プライマリ VLAN のマッピングが上書きされます。

add および **remove** キーワードを使用して、混合ポートのプライベート VLAN のマッピングからセカンダリ VLAN を追加または削除できます。

switchport private-vlan association host コマンドを入力することは、**switchport private-vlan host-association** インターフェイス コンフィギュレーション コマンドを入力することと同じ効果があります。

switchport private-vlan association mapping コマンドを入力することは、**switchport private-vlan mapping** インターフェイス コンフィギュレーション コマンドを入力することと同じ効果があります。

例

次の例では、インターフェイスをプライベート VLAN ホスト ポートとして設定し、それをプライマリ VLAN 20 およびセカンダリ VLAN 501 に関連付ける方法を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet 1/0/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 501
Switch(config-if)# end
```

次の例では、インターフェイスをプライベート VLAN 混合ポートとして設定し、それをプライマリ VLAN とセカンダリ VLAN にマッピングする方法を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet 1/0/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 501-502
Switch(config-if)# end
```

プライベート VLAN のマッピングを確認するには、**show interfaces private-vlan mapping** 特権 EXEC コマンドを使用します。スイッチ スタック上で設定されたプライベート VLAN およびインターフェイスを確認するには、**show vlan private-vlan** 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show interfaces private-vlan mapping	VLAN SVI に対するプライベート VLAN のマッピング情報を表示します。
show vlan private-vlan	スイッチ スタックで設定されたすべてのプライベート VLAN 関係およびタイプを表示します。

switchport protected

同じスイッチの他の保護ポートから送信されるレイヤ 2 のユニキャスト、マルチキャスト、およびブロードキャスト トラフィックを分離するには、**switchport protected** 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。ポートで保護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 protected

no switchport protected

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

保護ポートは定義されていません。すべてのポートが保護されていません。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

スイッチポート保護機能はスイッチ内に限定され、同一スイッチ上の保護ポート間では、レイヤ 3 デバイスを介してだけ通信できます。異なるスイッチ上の保護ポート間の通信を禁止するには、各スイッチの保護ポートを一意の VLAN に設定し、そのスイッチ間にトランク リンクを設定する必要があります。保護ポートはセキュア ポートとは異なります。

保護ポートは、同様に保護ポートになっている他のポートに対して、ユニキャスト、マルチキャスト、またはブロードキャスト トラフィックを転送しません。データ トラフィックはレイヤ 2 の保護ポート間で転送されません。PIM パケットなどは CPU で処理されてソフトウェアで転送されるため、このような制御トラフィックだけが転送されます。保護ポート間を通過するすべてのデータ トラフィックは、レイヤ 3 デバイスを介して転送されなければなりません。

スイッチ スタックは論理的には 1 つのスイッチを表しているため、レイヤ 2 トラフィックは、スタック内の同一スイッチか異なるスイッチかにかかわらず、スイッチ スタックの保護ポート間では転送されません。

モニタリングするポートおよびモニタリングされるポートの両方が保護ポートの場合、ポート モニタリングは機能しません。

例

次の例では、インターフェイス上で保護ポートをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport protected
```

設定を確認するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力します。

構文の説明

コマンド	説明
show interfaces switchport	ポート ブロッキング、ポート保護設定など、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 block	インターフェイス上で不明なマルチキャストまたはユニキャスト トラフィックを防ぎます。

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** 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。トランキング特性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。

switchport trunk {**allowed vlan** *vlan-list* | **encapsulation** {**dot1q** | **isl** | **negotiate**} | **native vlan** *vlan-id* | **pruning vlan** *vlan-list*}

no switchport trunk {**allowed vlan** | **encapsulation** | **native vlan** | {**pruning vlan**}

構文の説明

allowed vlan *vlan-list*	トランキング モードの場合に、このインターフェイス上でタグ付き形式のトラフィックを送受信できる許可 VLAN のリストを設定します。次の *vlan-list* 形式を参照してください。**none** キーワードは無効です。デフォルトは **all** です。
encapsulation dot1q	トランク ポートのカプセル化フォーマットを IEEE 802.1Q に設定します。このフォーマットでは、スイッチはポートでタグ付きおよびタグなしトラフィックの両方を同時にサポートします。
encapsulation isl	トランク ポートのカプセル化フォーマットを Inter-Switch Link（ISL; スイッチ間リンク）に設定します。スイッチは、送受信したすべての ISL ヘッダー付きパケットをカプセル化し、ISL トランク ポートから受信したネイティブ フレームをフィルタリングします。
encapsulation negotiate	Dynamic Inter-Switch Link（DISL）および Dynamic Trunking Protocol（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は、ISL を形式として選択することを指定します。
native vlan *vlan-id*	インターフェイスが IEEE 802.1Q トランキング モードの場合に、タグなしトラフィックを送受信するようにネイティブ VLAN を設定します。指定できる範囲は 1 ～ 4094 です。
pruning vlan *vlan-list*	トランキング モードの場合に、VTP プルーニングに適格な VLAN のリストを設定します。**all** キーワードは無効です。

vlan-list の形式は、**all** | **none** | [**add** | **remove** | **except**] *vlan-atom* [**,***vlan-atom...*] です。各キーワードの意味は、次のとおりです。

- **all** は、1 ～ 4094 のすべての VLAN を指定します。このキーワードは、リストのすべての VLAN を同時に設定することを許可しないコマンド上では使用できません。
- **none** は空のリストを意味します。特定の VLAN を設定するか、または少なくとも 1 つの VLAN を設定する必要があるコマンドでは、このキーワードを使用できません。
- **add** は現在設定されている VLAN リストを置き換えないで、定義済み VLAN リストを追加します。有効な ID は 1 ～ 1005 です。場合によっては、拡張範囲 VLAN（VLAN ID が 1005 より上）を使用できます。

（注） 許可 VLAN リストに拡張範囲 VLAN を追加できますが、プルーニング適格 VLAN リストには追加できません。

カンマを使い、連続しない VLAN ID を区切ります。ID の範囲を指定するには、ハイフンを使用します。

- **remove** は現在設定されている VLAN リストを置き換えないで、リストから定義済み VLAN リストを削除します。有効な ID は 1 ～ 1005 です。場合によっては、拡張範囲 VLAN ID を使用できます。

（注）　許可 VLAN リストから拡張範囲 VLAN を削除できますが、プルーニング適格リストからは削除できません。

カンマを使い、連続しない VLAN ID を区切ります。ID の範囲を指定するには、ハイフンを使用します。

- **except** は定義済み VLAN リスト以外の、計算する必要がある VLAN を示します（指定した VLAN を除く VLAN が追加されます）。有効な ID は 1 ～ 1005 です。カンマを使い、連続しない VLAN ID を区切ります。ID の範囲を指定するには、ハイフンを使用します。
- *vlan-atom* は、1 ～ 4094 内の単一の VLAN 番号、または 2 つの VLAN 番号で指定された連続した範囲の VLAN で、小さい方の値を先頭にハイフンで区切ります。

デフォルト

デフォルト カプセル化はネゴシエートされます。

VLAN 1 は、ポートのデフォルトのネイティブ VLAN ID です。

すべての VLAN リストのデフォルトには、すべての VLAN が含まれます。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	VLAN 1 および VLAN 1002 ～ 1005 の値を受け入れるため、**allowed vlan** *vlan-list* の add、remove、および except キーワードは変更されました。

使用上のガイドライン

カプセル化：

- **switchport trunk encapsulation** コマンドをサポートするのは、ISL と IEEE 802.1Q の形式を両方サポートできるプラットフォームおよびインターフェイス ハードウェアの場合だけです。
- トランクの一方の終端を IEEE 802.1Q トランクとして、もう一方の終端を ISL または非トランク ポートとして設定することはできません。ただし、ポート 1 つを ISL トランクとして、同じスイッチの別のポートを IEEE 802.1Q トランクとして設定できます。
- **negotiate** キーワードを入力し、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は、ISL が形式として選択されます。コマンドの **no** 形式は、トランク カプセル化形式をデフォルトにリセットします。
- **encapsulation コマンド**の no 形式は、カプセル化フォーマットをデフォルトにリセットします。

ネイティブ VLAN：

- IEEE 802.1Q トランク ポートで受信されたすべてのタグなしトラフィックは、ポートに設定されたネイティブ VLAN によって転送されます。
- パケットの VLAN ID が送信側ポートのネイティブ VLAN ID と同じであれば、そのパケットはタグなしで送信されます。ネイティブ VLAN ID と異なる場合は、スイッチはそのパケットをタグ付きで送信します。
- **native vlan** コマンドの **no** 形式は、ネイティブ モード VLAN を、デバイスに適したデフォルト VLAN にリセットします。

許可 VLAN：

- スパニング ツリー ループまたはストームのリスクを減らすには、許可リストから VLAN 1 を削除して個々の VLAN トランク ポートの VLAN 1 をディセーブルにできます。トランク ポートから VLAN 1 を削除した場合、インターフェイスは管理トラフィック（Cisco Discovery Protocol（CDP）、Port Aggregation Protocol（PAgP; ポート集約プロトコル）、Link Aggregation Control Protocol（LACP）、Dynamic Trunking Protocol（DTP）、および VLAN 1 の VLAN Trunking Protocol（VTP））を送受信し続けます。
- **allowed vlan** コマンドの **no** 形式は、リストをデフォルト リスト（すべての VLAN を許可）にリセットします。

トランク プルーニング：

- プルーニング適格リストは、トランク ポートだけに適用されます。
- トランク ポートごとに独自の適格リストがあります。
- VLAN をプルーニングしない場合は、プルーニング適格リストから VLAN を削除します。プルーニング不適格の VLAN は、フラッディング トラフィックを受信します。
- VLAN 1、VLAN 1002 ～ 1005、および拡張範囲 VLAN（VLAN 1006 ～ 4094）は、プルーニングできません。

例

次の例では、スイッチド インターフェイスとして設定されたポートを、トランキング モードのデフォルト トランキング形式に関係なく、IEEE 802.1Q トランキング形式にカプセル化させる方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport trunk encapsulation dot1q
```

次の例では、すべてのタグなしトラフィックを送信するポートのデフォルトとして、VLAN 3 を設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport trunk native vlan 3
```

次の例では、許可リストに VLAN 1、2、5、および 6 を追加する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport trunk allowed vlan add 1,2,5,6
```

次の例では、プルーニング適格リストから VLAN 3 および 10 ～ 15 を削除する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport trunk pruning vlan remove 3,10-15
```

設定を確認するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces switchport	ポート ブロッキング、ポート保護設定など、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	ポートの VLAN メンバシップ モードを設定します。

switchport voice detect

Cisco IP Phone を検出および認識するには、**switchport voice detect** 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。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 voice detect cisco-phone [**full-duplex**]

no switchport voice detect cisco-phone [**full-duplex**]

構文の説明

cisco-phone	Cisco IP Phone を検出して認識するようにスイッチを設定します。
full-duplex	（任意）全二重 Cisco IP Phone だけを受け入れるようにスイッチを設定します。

コマンド履歴

リリース	変更内容
12.2(37)SE	このコマンドが追加されました。

使用上のガイドライン

Cisco IP Phone を検出して認識するには、このコマンドを使用します。

例

次の例では、スイッチ上でスイッチポート音声検出機能をイネーブルにする方法を示します。

```
Switch(config)# interface fastethernet 1/0/1
Switch(config-if)# switchport voice detect cisco-phone
```

次の例では、スイッチ上でスイッチポート音声検出機能をディセーブルにする方法を示します。

```
Switch(config)# interface fastethernet 1/0/1
Switch(config-if)# no switchport voice detect cisco-phone
```

設定を確認するには、**show run interfaces** *interface-id* 特権 EXEC コマンドを入力します。

関連コマンド

関連コマンドはありません。

switchport voice vlan

ポートに音声 VLAN を設定するには、**switchport voice vlan** 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。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 voice vlan {*vlan-id* | **dot1p** | **none** | **untagged**}

no switchport voice vlan

構文の説明

vlan-id	音声トラフィックに使用する VLAN を設定します。指定できる範囲は 1 ～ 4094 です。デフォルトでは、Cisco IP Phone は IEEE 802.1Q プライオリティ 5 を使用して音声トラフィックを転送します。
dot1p	IEEE 802.1p プライオリティ タギングおよび VLAN 0（ネイティブ VLAN）を使用するように電話機を設定します。デフォルトでは、Cisco IP Phone は IEEE 802.1p プライオリティ 5 を使用して音声トラフィックを転送します。
none	音声 VLAN に関して IP Phone に指示しません。IP Phone のキー パッドから入力された設定を使用します。
untagged	IP Phone をタグなしの音声トラフィックを送信するよう設定します。これが IP Phone のデフォルト設定になります。

デフォルト

デフォルトでは、スイッチは IP Phone を自動設定しません（**none**）。

デフォルトでは、IP Phone はフレームにタグを付けません。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

レイヤ 2 アクセス ポート上で音声 VLAN を設定する必要があります。

スイッチの Cisco IP Phone に接続しているスイッチ ポート上の Cisco Discovery Protocol（CDP; シスコ検出プロトコル）をイネーブルにし、Cisco IP Phone に設定情報を送信する必要があります。デフォルトでは、CDP はインターフェイス上でグローバルにイネーブルです。

音声 VLAN をイネーブルにする前に、**mls qos** 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スイッチの Quality of Service（QoS）をイネーブルにし、**mls qos trust cos** インターフェイス コンフィギュレーション コマンドを入力して、信頼するポート信頼状態を設定することを推奨します。

VLAN ID を入力すると、IP Phone は IEEE 802.1Q フレームの音声トラフィックを指定された VLAN ID タグ付きで転送します。スイッチは IEEE 802.1Q 音声トラフィックを音声 VLAN に入れます。

dot1q、**none**、または **untagged** を選択した場合、スイッチは指定の音声トラフィックをアクセス VLAN に入れます。

すべての設定で、音声トラフィックはレイヤ 2 の IP precedence 値を運びます。音声トラフィックのデフォルトは 5 です。

音声 VLAN が設定されたインターフェイス上でポート セキュリティをイネーブルにする場合は、ポートの最大セキュア アドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合、MAC アドレスの追加は必要ありません。2 台以上の PC を Cisco IP Phone に接続する場合、各 PC に 1 つ、さらに Cisco IP Phone に 1 つ割り当てるよう十分なセキュア アドレスを設定する必要があります。

アクセス VLAN で任意のポート セキュリティ タイプがイネーブルにされた場合、音声 VLAN でダイナミック ポート セキュリティは自動的にイネーブルになります。

音声 VLAN では、スタティック セキュア MAC アドレスを設定できません。

音声 VLAN ポートは、プライベート VLAN ポートにはできません。

音声 VLAN を設定すると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。

例

次の例では、VLAN 2 をポート用音声 VLAN として設定します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport voice vlan 2
```

設定を確認するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces *interface-id* **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 priority extend	指定されたポートに接続されたデバイスが、着信ポートで受信したプライオリティ トラフィックを処理する方法を指定します。

system env temperature threshold yellow

イエローのしきい値を決める、イエローとレッドの温度しきい値の差を設定するには、**system env temperature threshold yellow** グローバル コンフィギュレーション 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。

system env temperature threshold yellow *value*

no system env temperature threshold yellow *value*

構文の説明

value	イエローとレッドのしきい値の差を指定します（摂氏）。指定できる範囲は 10 ～ 25 です。デフォルト値は 10 です。

デフォルト

デフォルト値は次のとおりです。

表 2-46　温度しきい値のデフォルト値

スイッチ	イエローとレッドの差	レッド[1]
Catalyst 3750G-48TS	10 ℃	66 ℃
Catalyst 3750G-48PS	10 ℃	68 ℃
Catalyst 3750G-24TS-1U	10 ℃	65 ℃
Catalyst 3750G-24PS	10 ℃	61 ℃

1. レッドの温度しきい値を設定することはできません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(25)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、すべてのスイッチ上に表示されますが、次のスイッチだけで有効です。

- Catalyst 3750G-48TS
- Catalyst 3750G-48PS
- Catalyst 3750G-24TS-1U
- Catalyst 3750G-24PS

グリーンとレッドのしきい値を設定することはできませんが、イエローのしきい値を設定することはできます。イエローとレッドのしきい値の差を指定して、イエローのしきい値を設定するには、**system env temperature threshold yellow** *value* グローバル コンフィギュレーション コマンドを使用します。たとえば、レッドのしきい値が 66 ℃の場合に、イエローのしきい値を 51 ℃ に設定するには、**system env temperature threshold yellow 15** コマンドを使用してしきい値の差を 15 に設定します。

（注）　スイッチ内部の温度センサーでシステム内の温度を測定するため、±5℃の差が生じる可能性があります。

例

次の例では、イエローとレッドのしきい値の差を 15 に設定する方法を示します。

```
Switch(config)# system env temperature threshold yellow 15
Switch(config)#
```

関連コマンド

コマンド	説明
show env temperature status	温度ステータスとしきい値レベルを表示します。

system mtu

ギガビット イーサネット ポート、ルーテッド ポート、またはファスト イーサネット（10/100）ポートの最大パケット サイズまたは Maximum Transmission Unit（MTU; 最大伝送ユニット）を設定するには、**system mtu** グローバル コンフィギュレーション コマンドを使用します。グローバル MTU 値を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。

system mtu {*bytes* | **jumbo** *bytes* | **routing** *bytes*}

no system mtu

構文の説明

bytes	10 または 100 Mbps に設定されているポートのシステム MTU を設定します。指定できる範囲は 1500 ～ 1998 バイトです。これは、10/100 Mbps イーサネット スイッチ ポートで受信する最大 MTU です。
jumbo *bytes*	1000 Mbps 以上で稼動しているギガビット イーサネット ポートのシステム ジャンボ MTU を設定します。指定できる範囲は 1500 ～ 9000 バイトです。これは、ギガビット イーサネット ポートの物理ポートで受信する最大 MTU です。
routing *bytes*	ルーテッド パケットの最大 MTU を設定します。また、設定した MTU サイズをサポートするルーティング プロトコルがアドバタイズする最大 MTU も設定できます。指定できる範囲は 1500 バイト～システム MTU 値です。システム ルーティング MTU は、ルーテッド パケットの最大 MTU であり、また OSPF などのプロトコルのルーティング アップデートでスイッチがアドバタイズする最大 MTU でもあります。

デフォルト

すべてのポートのデフォルトの MTU サイズは 1500 バイトです。ただし、システム MTU に別の値を設定した場合、その値はスイッチのリセット後に適用され、ルーテッド ポートのデフォルトの MTU サイズになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(25)SEC	指定できる範囲が 1500 ～ 1998 *バイト*になりました。
12.2(25)SED	**routing** *bytes* キーワードが追加されました。

使用上のガイドライン

このコマンドでシステム MTU またはジャンボ MTU のサイズを変更した場合、新しい設定内容を反映させるには、スイッチをリセットする必要があります。**system mtu routing** コマンドを使用する場合は、変更内容を反映させるためにスイッチをリセットする必要はありません。

システム MTU 設定は、NVRAM のスイッチ環境変数に保存され、スイッチをリロードするときに有効になります。システム MTU ルーティング設定とは異なり、**system mtu** および **system mtu jumbo** コマンドで入力した MTU 設定は、**copy running-config startup-config** 特権 EXEC コマンドを入力しても、スイッチ IOS コンフィギュレーション ファイルに保存されません。したがって、Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）を使用し、バックアップ コンフィギュレー

ション ファイルで新しいスイッチを設定して、システム MTU をデフォルト以外の値にしたい場合、新しいスイッチ上で **system mtu** および **system mtu jumbo** を明示的に設定し、スイッチをリロードする必要があります。

1000 Mbps で稼動しているギガビット イーサネット ポートは **system mtu** コマンドによる影響を受けません。10/100 Mbps ポートは **system mtu jumbo** コマンドによる影響を受けません。

ルーテッド ポートで MTU サイズを設定するには、**system mtu routing** コマンドを使用できます。

（注）システム MTU サイズを超えるルーティング MTU サイズは設定できません。システム MTU サイズを現在設定されているルーティング MTU サイズより小さい値に変更すると、設定変更は受け入れられますが、次にスイッチをリセットするまで適用されません。設定変更が有効になると、ルーティング MTU サイズは新しいシステム MTU サイズのデフォルトになります。

特定のスイッチ タイプに許容範囲外の値を入力すると、値が拒否されます。

（注）スイッチは、インターフェイスごとの MTU の設定をサポートしません。

スイッチの CPU で受信できるフレーム サイズは、**system mtu** コマンドで入力した値に関係なく、1998 バイトに制限されます。転送されたフレームまたはルーテッド フレームは、通常 CPU では受信しませんが、一部のパケット（制御トラフィック、SNMP、Telnet、およびルーティング プロトコルなど）は CPU に送信されます。

スイッチはパケットを分割しないので、次のパケットをドロップします。

- *出力*インターフェイスでサポートされるパケット サイズより大きい、スイッチド パケット
- ルーティング MTU 値より大きいルーテッド パケット

たとえば、**system mtu** 値が 1998 バイトで、**system mtu jumbo** 値が 5000 バイトの場合、1000 Mbps で稼動するインターフェイスでは、最大 5000 バイトのパケットを受信できます。ただし、1998 バイトを超えるパケットは 1000 Mbps で稼動するインターフェイスで受信できますが、宛先インターフェイスが 10 または 100 Mbps で稼動している場合、パケットはドロップされます。

例

次の例では、1000 Mbps 以上で稼動しているギガビット イーサネット ポートの最大ジャンボ パケット サイズを 1800 バイトに設定する方法を示します。

```
Switch(config)# system mtu jumbo 1800
Switch(config)# exit
Switch# reload
```

設定を確認するには、**show system mtu** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show system mtu	ファスト イーサネット ポート、ギガビット イーサネット ポート、およびルーテッド ポートに設定されたパケット サイズを表示します。

test cable-diagnostics tdr

インターフェイス上で Time Domain Reflector（TDR）機能を実行するには、**test cable-diagnostics tdr** 特権 EXEC コマンドを使用します。

test cable-diagnostics tdr interface *interface-id*

構文の説明

interface-id	TDR を実行するインターフェイスを指定します。

デフォルト

デフォルト設定はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。

使用上のガイドライン

TDR は、銅線のイーサネット 10/100/100 ポートだけでサポートされます。10/100 ポート、10 ギガビット モジュール ポート、または SFP モジュール ポートではサポートされません。TDR の詳細については、このリリースに対応する *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。

test cable-diagnostics tdr interface *interface-id* コマンドを使用して TDR を実行した後、結果を表示するには **show cable-diagnostics tdr interface** *interface-id* 特権 EXEC コマンドを使用します。

例

次の例では、インターフェイス上で TDR を実行する方法を示します。

```
Switch# test cable-diagnostics tdr interface gigabitethernet1/0/2
TDR test started on interface Gi1/0/2
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

インターフェイスのリンク ステータスがアップ状態で速度が 10 Mb/s または 100 Mb/s である場合、**test cable-diagnostics tdr interface** *interface-id* コマンドを入力すると、次のメッセージが表示されます。

```
Switch# test cable-diagnostics tdr interface gigabitethernet1/0/3
TDR test on Gi1/0/3 will affect link state and traffic
TDR test started on interface Gi1/0/3
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

関連コマンド

コマンド	説明
show cable-diagnostics tdr	TDR 結果が表示されます。

traceroute mac

指定の送信元 MAC アドレスから指定の宛先 MAC アドレスまでを通過するパケットのレイヤ 2 パスを表示するには、**traceroute mac** 特権 EXEC コマンドを使用します。

traceroute mac [**interface** *interface-id*] {*source-mac-address*} [**interface** *interface-id*] {*destination-mac-address*} [**vlan** *vlan-id*] [**detail**]

構文の説明

interface *interface-id*	（任意）送信元または宛先スイッチ上のインターフェイスを指定します。
source-mac-address	送信元スイッチの MAC アドレスを指定します（16 進数）。
destination-mac-address	宛先スイッチの MAC アドレスを指定します（16 進数）。
vlan *vlan-id*	（任意）送信元スイッチから宛先スイッチを通過するパケットのレイヤ 2 のパスをトレースする VLAN を指定します。指定できる VLAN ID の範囲は 1 ～ 4094 です。
detail	（任意）詳細情報を表示するよう指定します。

デフォルト

デフォルト設定はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

レイヤ 2 の traceroute を適切に機能させるには、Cisco Discovery Protocol（CDP）がネットワークのすべてのスイッチでイネーブルになっている必要があります。CDP をディセーブルにすることは避けてください。

スイッチがレイヤ 2 パス内でレイヤ 2 traceroute をサポートしていないデバイスを検知した場合、スイッチはレイヤ 2 trace クエリーを送信し続け、タイムアウトにします。

パス内で識別できるホップ数は最大で 10 です。

レイヤ 2 traceroute はユニキャスト トラフィックだけをサポートします。マルチキャストの送信元または宛先 MAC アドレスを指定しても、物理的なパスは識別されず、エラー メッセージが表示されます。

指定された送信元および宛先アドレスが同じ VLAN にある場合、**traceroute mac** コマンド出力はレイヤ 2 パスを表示します。異なる VLAN にある送信元および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、エラー 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 にある場合、送信元および宛先 MAC アドレス両方の属する VLAN を指定する必要があります。VLAN が指定されないと、パスは識別されず、エラー メッセージが表示されます。

複数の装置がハブを介して 1 つのポートに接続されている場合（たとえば、複数の CDP ネイバーがポートで検出されるなど）、レイヤ 2 traceroute 機能はサポートされません。複数の CDP ネイバーが 1 つのポートで検出された場合、レイヤ 2 パスは特定されず、エラー メッセージが表示されます。

この機能は、トークンリング VLAN ではサポートされません。

例

次の例では、送信元および宛先 MAC アドレスを指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Source 0000.0201.0601 found on con6[switch_mmodel] (2.2.6.6)
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5                 (2.2.5.5        )  :    Gi0/0/3 => Gi0/0/1
con1                 (2.2.1.1        )  :    Gi0/0/1 => Gi0/0/2
con2                 (2.2.2.2        )  :    Gi0/0/2 => Gi0/0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

次の例では、**detail** キーワードを使用することで、レイヤ 2 のパスを表示する方法を示します。

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201 detail
Source 0000.0201.0601 found on con6[switch_mmodel] (2.2.6.6)
con6 /switch_mmodel/ 2.2.6.6 :
        Gi0/2 [auto, auto] => Gi0/3 [auto, auto]
con5 / switch_mmodel / 2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / switch_mmodel / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 /switch_mmodel / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

次の例では、送信元および宛先スイッチのインターフェイスを指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Switch# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3
0000.0201.0201
Source 0000.0201.0601 found on con6[switch_mmodel] (2.2.6.6)
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5                 (2.2.5.5        )  :    Gi0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/1 => G0/2
con2                 (2.2.2.2        )  :    Gi0/2 => Gi0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

次の例では、スイッチが送信元スイッチに接続されていない場合のレイヤ 2 のパスを示します。

```
Switch# traceroute mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source .....
Source 0000.0201.0501 found on con5[switch_mmodel] (2.2.5.5)
con5 / switch_mmodel / 2.2.5.5 :
        Gi0/1 [auto, auto] => Gi0/3 [auto, auto]
con1 / switch_mmodel / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / switch_mmodel / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

次の例では、送信元 MAC アドレスの宛先ポートが見つからない場合のレイヤ 2 のパスを示します。

```
Switch# traceroute mac 0000.0011.1111 0000.0201.0201
Error:Source Mac address not found.
Layer2 trace aborted.
```

次の例では、送信元および宛先デバイスが異なる VLAN にある場合のレイヤ 2 のパスを示します。

```
Switch# traceroute mac 0000.0201.0601 0000.0301.0201
Error:Source and destination macs are on different vlans.
Layer2 trace aborted.
```

次の例では、宛先 MAC アドレスがマルチキャスト アドレスの場合のレイヤ 2 のパスを示します。

```
Switch# traceroute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
```

次の例では、送信元および宛先スイッチが複数の VLAN にある場合のレイヤ 2 のパスを示しています。

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
```

関連コマンド

コマンド	説明
traceroute mac ip	指定の送信元 IP アドレスまたはホスト名から、指定の宛先 IP アドレスまたはホスト名を通過するパケットのレイヤ 2 パスを表示します。

traceroute mac ip

指定の送信元 IP アドレスまたはホスト名から、指定の宛先 IP アドレスまたはホスト名までを通過するパケットのレイヤ 2 パスを表示するには、**traceroute mac ip** 特権 EXEC コマンドを使用します。

traceroute mac ip {*source-ip-address* | *source-hostname*} {*destination-ip-address* | *destination-hostname*} [**detail**]

構文の説明

source-ip-address	送信元スイッチの IP アドレスを、32 ビットの値で指定します（ドット付き 10 進数）。
destination-ip-address	宛先スイッチの IP アドレスを、32 ビットの値で指定します（ドット付き 10 進数）。
source-hostname	送信元スイッチの IP ホスト名を指定します。
destination-hostname	宛先スイッチの IP ホスト名を指定します。
detail	（任意）詳細情報を表示するよう指定します。

デフォルト

デフォルト設定はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

レイヤ 2 の traceroute を適切に機能させるには、Cisco Discovery Protocol（CDP）がネットワークのすべてのスイッチでイネーブルになっている必要があります。CDP をディセーブルにすることは避けてください。

スイッチがレイヤ 2 パス内でレイヤ 2 traceroute をサポートしていないデバイスを検知した場合、スイッチはレイヤ 2 trace クエリーを送信し続け、タイムアウトにします。

パス内で識別できるホップ数は最大で 10 です。

指定された送信元および宛先の IP アドレスが同一のサブネット内にある場合、**traceroute mac ip** コマンド出力はレイヤ 2 パスを表示します。IP アドレスを指定した場合、スイッチは Address Resolution Protocol（ARP; アドレス解決プロトコル）を使用し、IP アドレスとそれに対応する MAC アドレスおよび VLAN ID を関連付けます。

- 指定の IP アドレスの ARP のエントリが存在している場合、スイッチは関連付けられた MAC アドレスを使用し、物理パスを識別します。
- ARP のエントリが存在しない場合、スイッチは ARP クエリーを送信し、IP アドレスを解決しようと試みます。IP アドレスは同一のサブネットにある必要があります。IP アドレスが解決されないと、パスは識別されず、エラー メッセージが表示されます。

複数の装置がハブを介して 1 つのポートに接続されている場合（たとえば、複数の CDP ネイバーがポートで検出されるなど）、レイヤ 2 traceroute 機能はサポートされません。複数の CDP ネイバーが 1 つのポートで検出された場合、レイヤ 2 パスは特定されず、エラー メッセージが表示されます。

この機能は、トークンリング VLAN ではサポートされません。

例

次の例では、**detail** キーワードを使用して、送信元および宛先 IP アドレスを指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Switch# 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-C2950G-24-EI] (2.2.6.6)
con6 / switch_mmodel / 2.2.6.6 :
        Gi0/1 [auto, auto] => Gi0/3 [auto, auto]
con5 / switch_mmodel / 2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / switch_mmodel / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / switch_mmodel / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

次の例では、送信元および宛先ホスト名を指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Switch# 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) :Gi0/1 => Gi0/3
con5                (2.2.5.5        )  :    Gi0/3 => 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
```

次の例では、ARP が送信元 IP アドレスと対応する MAC アドレスを関連付けられない場合の、レイヤ 2 のパスを示します。

```
Switch# traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
```

関連コマンド

コマンド	説明
traceroute mac	指定の送信元 MAC アドレスから、指定の宛先 MAC アドレスまでをパケットが通過するレイヤ 2 パスを表示します。

trust

class ポリシー マップ コンフィギュレーション コマンドまたは **class-map** グローバル コンフィギュレーション コマンドで分類されたトラフィックの信頼状態を定義するには、**trust** 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。

trust [**cos** | **dscp** | **ip-precedence**]

no trust [**cos** | **dscp** | **ip-precedence**]

構文の説明

cos	（任意）パケットの Class of Service（CoS）値を使用して、入力パケットを分類します。タグのない IP パケットの場合、ポートのデフォルトの CoS 値が使用されます。
dscp	（任意）パケットの Differentiated Service Code Point（DSCP）値（8 ビット サービス タイプ フィールドの上位 6 ビット）を使用することにより、入力パケットを分類します。パケットがタグ付きの場合、非 IP パケットにはパケットの CoS 値が使用されます。パケットがタグなしの場合、CoS の DSCP マッピングにデフォルト ポートの CoS 値が使用されます。
ip-precedence	（任意）パケットの IP precedence 値（8 ビット サービスタイプ フィールドの上位 3 ビット）を使用して、入力パケットを分類します。パケットがタグ付きの場合、非 IP パケットにはパケットの CoS 値が使用されます。パケットがタグなしの場合、CoS の DSCP マッピングにポートのデフォルト CoS 値が使用されます。

デフォルト

アクションは信頼されていません。キーワードを指定せずにコマンドを入力した場合、デフォルトは **dscp** です。

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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

特定のトラフィックの Quality of Service（QoS）の信頼動作を他のトラフィックと区別するために、このコマンドを使用します。たとえば、特定の DSCP 値を持つ着信トラフィックが信頼されます。着信トラフィックの DSCP 値と一致し、信頼するクラス マップを設定できます。

このコマンドで設定された信頼性の値は、**mls qos trust** 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信頼性の値を上書きします。

trust コマンドは、同一ポリシー マップ内の **set** ポリシー マップ クラス コンフィギュレーション コマンドと相互に排他的な関係にあります。

trust cos を指定した場合、QoS は受信した CoS 値、またはデフォルト ポートの CoS 値および CoS/DSCP マップを使用して、パケットの DSCP 値を生成します。

trust dscp を指定した場合、QoS は入力パケットから DSCP 値を使用します。タグ付きの非 IP パケットに対しては、QoS は受信した CoS 値を、タグなしの非 IP パケットに対しては、デフォルト ポートの CoS 値を使用します。どちらの場合も、パケットの DSCP 値は CoS/DSCP マップから抽出されます。

trust ip-precedence を指定した場合、QoS は入力パケットおよび IP precedence/DSCP マップから IP precedence 値を使用します。タグ付きの非 IP パケットに対しては、QoS は受信した CoS 値を、タグなしの非 IP パケットに対しては、デフォルト ポートの CoS 値を使用します。どちらの場合も、パケットの DSCP 値は CoS/DSCP マップから抽出されます。

ポリシー マップ コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

例

次の例では、*class1* で分類されたトラフィックの着信 DSCP 値を信頼するようにポート信頼状態を定義する方法を示します。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
```

設定を確認するには、**show policy-map** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
class	指定されたクラスマップ名のトラフィック分類一致条件（**police**、**set**、および **trust** ポリシー マップ クラス コンフィギュレーション コマンドによる）を定義します。
police	分類したトラフィックにポリサーを定義します。
policy-map	複数のポートに接続可能なポリシー マップを作成または変更して、サービス ポリシーを指定します。
set	パケットに DSCP 値または IP precedence 値を設定することによって、IP トラフィックを分類します。
show policy-map	QoS ポリシー マップを表示します。

udld

UniDirectional Link Detection（UDLD; 単一方向リンク検出）でアグレッシブ モードまたはノーマル モードをイネーブルにし、設定可能なメッセージ タイマー時間を設定するには、**udld** グローバル コンフィギュレーション コマンドを使用します。すべての光ファイバ ポートでアグレッシブ モードまたはノーマル モードの 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 {**aggressive** | **enable** | **message time** *message-timer-interval*}

no udld {**aggressive** | **enable** | **message**}

構文の説明

aggressive	すべての光ファイバ インターフェイスにおいて、アグレッシブ モードで UDLD をイネーブルにします。
enable	すべての光ファイバ インターフェイスにおいて、ノーマル モードで UDLD をイネーブルにします。
message time *message-timer-interval*	アドバタイズ フェーズにあり、双方向と判別されたポートにおける UDLD プローブ メッセージ間の時間間隔を設定します。指定できる範囲は 1 ～ 90 秒です。

デフォルト

すべてのインターフェイスで UDLD はディセーブルです。

メッセージ タイマーは 15 秒に設定されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(25)SEC	*message-timer-interval* の範囲が 7 ～ 90 から 1 ～ 90 秒に変更されました。

使用上のガイドライン

UDLD は、ノーマル（デフォルト）とアグレッシブの 2 つの動作モードをサポートしています。ノーマル モードでは、UDLD は、光ファイバ接続において誤って接続されたインターフェイスによる単一方向リンクを検出します。アグレッシブ モードでは、UDLD はまた、光ファイバおよびツイストペア リンクの単一方向トラフィックによる単一方向リンク、および光ファイバ リンクにおいて誤って接続されたインターフェイスによる単一方向リンクを検出します。ノーマル モードおよびアグレッシブ モードの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Understanding UDLD」を参照してください。

プローブ パケット間のメッセージ時間を変更する場合、検出速度と CPU 負荷のトレードオフを行っていることになります。時間を減少させると、検出応答を高速にすることができますが、CPU の負荷も高くなります。

このコマンドが作用するのは、光ファイバ インターフェイスだけです。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** 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。

UDLD によるインターフェイス シャットダウンをリセットするのに、次のコマンドを使用できます。

- **udld reset** 特権 EXEC コマンド - UDLD によってシャットダウンされたすべてのインターフェイスをリセットします。
- **shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンド
- **no udld enable** グローバル コンフィギュレーション コマンドの後に **udld** {**aggressive** | **enable**} グローバル コンフィギュレーション コマンドを入力 - グローバルに UDLD を再びイネーブルにします。
- **no udld port** インターフェイス コンフィギュレーション コマンドの後に **udld port** または **udld port aggressive** インターフェイス コンフィギュレーション コマンドを入力：指定されたインターフェイスの UDLD を再びイネーブルにします。
- **errdisable recovery cause udld** および **errdisable recovery interval** *interval* グローバル コンフィギュレーション コマンド：自動的に UDLD errdisable ステートから回復します。

例

次の例では、すべての光ファイバ インターフェイスで UDLD をイネーブルにする方法を示します。

```
Switch(config)# udld enable
```

設定を確認するには、**show udld** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show udld	すべてのポートまたは指定されたポートの UDLD の管理ステータスおよび動作ステータスを表示します。
udld port	個々のインターフェイスで UDLD をイネーブルにするか、または光ファイバ インターフェイスが **udld** グローバル コンフィギュレーション コマンドによってイネーブルになるのを防ぎます。
udld reset	UDLD によってシャットダウンされたすべてのインターフェイスをリセットし、トラフィックを再び通過させるようにします。

udld port

個々のインターフェイスで UniDirectional Link Detection（UDLD; 単一方向リンク検出）をイネーブルにするか、または光ファイバ インターフェイスが **udld** グローバル コンフィギュレーション コマンドによってイネーブルにされるのを防ぐには、**udld port** 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。**udld** グローバル コンフィギュレーション コマンド設定に戻したり、非光ファイバ ポートで入力された場合に UDLD をディセーブルにしたりするには、このコマンドの **no** 形式を使用します。

udld port [**aggressive**]

no udld port [**aggressive**]

構文の説明

aggressive	指定されたインターフェイスにおいて、アグレッシブ モードで UDLD をイネーブルにします。

デフォルト

光ファイバ インターフェイスでは、UDLD はイネーブル、アグレッシブ モード、ディセーブルのいずれでもありません。このため、光ファイバ インターフェイスは、**udld enable** または **udld aggressive** グローバル コンフィギュレーション コマンドのステートに従い UDLD をイネーブルにします。

非光ファイバ インターフェイスでは、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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(20)SE	**disable** キーワードが削除されました。

使用上のガイドライン

UDLD 対応ポートが別のスイッチの UDLD 非対応ポートに接続されている場合、このポートは単一方向リンクを検出できません。

UDLD は、ノーマル（デフォルト）とアグレッシブの 2 つの動作モードをサポートしています。ノーマル モードでは、UDLD は、光ファイバ接続において誤って接続されたインターフェイスによる単一方向リンクを検出します。アグレッシブ モードでは、UDLD はまた、光ファイバおよびツイストペア リンクの単一方向トラフィックによる単一方向リンク、および光ファイバ リンクにおいて誤って接続されたインターフェイスによる単一方向リンクを検出します。ノーマル モードおよびアグレッシブ モードの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring UDLD」の章を参照してください。

UDLD をノーマル モードでイネーブルにするには、**udld port** 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。UDLD をアグレッシブ モードでイネーブルにするには、**udld port aggressive** 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。

UDLD の制御を **udld enable** グローバル コンフィギュレーション コマンドに戻したり、UDLD を非光ファイバ ポートでディセーブルにしたりする場合は、光ファイバ ポートで **no udld port** コマンドを使用します。

udld enable または **udld aggressive** グローバル コンフィギュレーション コマンドの設定を無効にする場合は、光ファイバ ポートで **udld port aggressive** コマンドを使用します。この設定を削除して UDLD イネーブル化の制御を **udld** グローバル コンフィギュレーション コマンドに戻したり、UDLD を非光ファイバ ポートでディセーブルにしたりする場合は、光ファイバ ポートで **no** 形式を使用します。

UDLD によってシャットダウンされたインターフェイスをリセットするのに、次のコマンドを使用できます。

- **udld reset** 特権 EXEC コマンド：UDLD によってシャットダウンされたすべてのインターフェイスをリセットします。
- **shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンド
- **no udld enable** グローバル コンフィギュレーション コマンドの後に **udld** {**aggressive** | **enable**} グローバル コンフィギュレーション コマンドを入力：グローバルに UDLD を再びイネーブルにします。
- **no udld port** インターフェイス コンフィギュレーション コマンドの後に **udld port または udld port aggressive** インターフェイス コンフィギュレーション コマンドを入力：指定されたインターフェイスの UDLD を再びイネーブルにします。
- **errdisable recovery cause udld** および **errdisable recovery interval** *interval* グローバル コンフィギュレーション コマンド：自動的に UDLD errdisable ステートから回復します。

例

次の例では、ポート上で UDLD をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet6/0/1
Switch(config-if)# udld port
```

次の例では、**udld** グローバル コンフィギュレーション コマンドの設定に関係なく、光ファイバ インターフェイス上で UDLD をディセーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet6/0/1
Switch(config-if)# no udld port
```

設定を確認するには、**show running-config** または **show udld** *interface* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	スイッチの実行コンフィギュレーションを表示します。
show udld	すべてのポートまたは指定されたポートの UDLD の管理ステータスおよび動作ステータスを表示します。
udld	UDLD のアグレッシブ モードまたはノーマル モードをイネーブルにするか、または設定可能なメッセージ タイマーの時間を設定します。
udld reset	UDLD によってシャットダウンされたすべてのインターフェイスをリセットし、トラフィックを再び通過させるようにします。

udld reset

UniDirectional Link Detection（UDLD; 単一方向リンク検出）によりディセーブルにされたインターフェイスをすべてリセットし、インターフェイスのトラフィックを再開させるには、**udld reset** 特権 EXEC コマンドを使用します（イネーブルの場合には、スパニング ツリー、Port Aggregation Protocol（PAgP）、Dynamic Trunking Protocol（DTP）などの他の機能を介することで有効になります）。

udld reset

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

インターフェイスの設定で、UDLD がまだイネーブルである場合、これらのポートは再び UDLD の稼動を開始し、問題が修正されていない場合には同じ理由でディセーブルになります。

例

次の例では、UDLD によってディセーブルにされたすべてのインターフェイスをリセットする方法を示します。

```
Switch# udld reset
1 ports shutdown by UDLD were reset.
```

設定を確認するには、**show udld** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	スイッチの実行コンフィギュレーションを表示します。
show udld	すべてのポートまたは指定されたポートの UDLD の管理ステータスおよび動作ステータスを表示します。
udld	UDLD のアグレッシブ モードまたはノーマル モードをイネーブルにするか、または設定可能なメッセージ タイマーの時間を設定します。
udld port	個々のインターフェイスで UDLD をイネーブルにするか、または光ファイバ インターフェイスが **udld** グローバル コンフィギュレーション コマンドによってイネーブルになるのを防ぎます。

aaa authentication dot1x

IEEE 802.1x 認証に準拠するポートで Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）メソッドを使用するように指定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **aaa authentication dot1x** グローバル コンフィギュレーション コマンドを使用します。認証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。

aaa authentication dot1x {**default**} *method1*

no aaa authentication dot1x {**default**}

構文の説明

default	この引数の後に続く、リストされた認証方式をログイン時のデフォルトの方式として使用します。
method1	認証用にすべての RADIUS サーバのリストを使用するには、**group radius** キーワードを入力します。

（注）　他のキーワードがコマンドラインのヘルプ ストリングに表示されますが、サポートされているのは **default** および **group radius** キーワードだけです。

デフォルト

認証は実行されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(35)SE2	このコマンドが追加されました。

使用上のガイドライン

method 引数には、認証アルゴリズムがクライアントからのパスワードを確認するために一定の順序で試みる方式を指定します。実際に IEEE 802.1x に準拠している唯一の方式は、クライアント データが RADIUS 認証サーバに対して確認される **group radius** 方式です。

group radius を指定した場合、**radius-server host** 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 RADIUS サーバを設定する必要があります。

設定された認証方式リストを表示するには、**show running-config** 特権 EXEC コマンドを使用します。

例

次の例では AAA をイネーブルにして IEEE 802.1x 準拠の認証リストを作成する方法を示します。この認証は、最初に RADIUS サーバとの交信を試みます。この動作でエラーが返信された場合、ユーザはネットワークへのアクセスが許可されません。

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
show running-config	動作設定を表示します。構文情報については、『Cisco IOS Release 12.2 Command Reference』一覧ページへのリンク（http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html）を使用してください。 コマンドに移動するには、「Cisco IOS Commands Master List, Release 12.2」を選択します。

vlan（VLAN コンフィギュレーション）

このコマンドは現在サポートされていません。

VLAN データベースに標準範囲 VLAN（VLAN ID 1 ～ 1005）の VLAN 特性を設定するには、**vlan** VLAN コンフィギュレーション コマンドを使用します。VLAN コンフィギュレーション モードを開始する場合は、**vlan database** 特権 EXEC コマンドを入力します。

vlan *vlan-id* [**are** *are-number*] [**backupcrf** {**enable** | **disable**}] [**bridge** *bridge-number* | **type** {**srb** | **srt**}] [**media** {**ethernet** | **fddi** | **fdi-net** | **tokenring** | **tr-net**}] [**mtu** mtu-size] [**name** *vlan-name*] [**parent** *parent-vlan-id*] [**ring** *ring-number*] [**said** *said-value*] [**state** {**suspend** | **active**}] [**ste** *ste-number*] [**stp type** {**ieee** | **ibm** | **auto**}] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id]*

vlan access-map

VLAN パケット フィルタリング用の VLAN マップ エントリを作成または修正するには、**vlan access-map** グローバル コンフィギュレーション コマンドを使用します。このエントリは、モードを VLAN アクセス マップ コンフィギュレーションに変更します。VLAN マップ エントリを削除するには、このコマンドの **no** 形式を使用します。**vlan filter** インターフェイス コンフィギュレーション コマンドは、VLAN マップを 1 つまたは複数の VLAN に適用します。

vlan access-map *name* [*number*]

no vlan access-map *name* [*number*]

構文の説明

name	VLAN マップ名
number	（任意）作成または変更するマップ エントリのシーケンス番号（0 ～ 65535）。VLAN マップを作成する際にシーケンス番号を指定しない場合、番号は自動的に割り当てられ、10 から開始して 10 ずつ増加します。この番号は、VLAN アクセス マップ エントリに挿入するか、または VLAN アクセス マップ エントリから削除する順番です。

デフォルト

VLAN に適用する VLAN マップ エントリまたは VLAN マップはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

グローバル コンフィギュレーション モードでは、このコマンドは VLAN マップを作成または修正します。このエントリは、モードを VLAN アクセス マップ コンフィギュレーションに変更します。**match** アクセス マップ コンフィギュレーション コマンドを使用して、一致する IP または非 IP トラフィック用にアクセス リストを指定します。**action** コマンドは、この一致によりパケットを転送またはドロップするかどうかを設定します。

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

- **action**：実行するアクションを設定します（転送またはドロップ）。
- **default**：コマンドをそのデフォルトに設定します。
- **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**：一致する値を設定します（IP アドレスまたは MAC アドレス）。
- **no**：コマンドを無効にするか、デフォルト値を設定します。

エントリ番号（シーケンス番号）を指定しない場合、マップの最後に追加されます。

VLAN ごとに VLAN マップは 1 つだけ設定できます。VLAN マップは、VLAN でパケットを受信すると適用されます。

シーケンス番号を指定して **no vlan access-map** *name* [*number*] コマンドを使用すると、エントリを 1 つ削除できます。

グローバル コンフィギュレーション モードでは、**vlan filter** インターフェイス コンフィギュレーション コマンドを使用して、VLAN マップを 1 つまたは複数の VLAN に適用します。

VLAN マップ エントリの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、*vac1* という名の VLAN マップを作成し、一致条件とアクションをその VLAN マップに適用する方法を示します。他のエントリがマップに存在しない場合、これはエントリ 10 になります。

```
Switch(config)# vlan access-map vac1
Switch(config-access-map)# match ip address acl1
Switch(config-access-map)# action forward
```

次の例では、VLAN マップ *vac1* を削除する方法を示します。

```
Switch(config)# no vlan access-map vac1
```

関連コマンド

コマンド	説明
action	VLAN アクセス マップ エントリのアクションを設定します。
match（アクセス マップ コンフィギュレーション）	1 つまたは複数のアクセス リストとパケットが一致するように VLAN マップを設定します。
show vlan access-map	特定の VLAN アクセス マップまたはすべての VLAN アクセス マップに関する情報を表示します。
vlan filter	1 つまたは複数の VLAN に、VLAN アクセス マップを適用します。

vlan database

このコマンドは現在サポートされていません。

VLAN コンフィギュレーション モードを開始するには、**vlan database** 特権 EXEC コマンドを入力します。このモードから、標準範囲 VLAN の VLAN 設定の追加、削除、および修正を行い、VLAN Trunking Protocol（VTP）を使用してこれらの変更をグローバルに伝播できます。コンフィギュレーション情報は、VLAN データベースに保存されます。

vlan database

vlan dot1q tag native

すべての IEEE 802.1Q トランク ポートでネイティブ VLAN フレームのタギングをイネーブルにするには、**vlan dot1q tag native** グローバル コンフィギュレーション 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 dot1q tag native

no vlan dot1q tag native

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

IEEE 802.1Q ネイティブ VLAN タギング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

コマンド履歴

リリース	変更内容
12.2(25)EA1	このコマンドが追加されました。

使用上のガイドライン

イネーブルの場合は、すべての IEEE 802.1Q トランク ポートから出るネイティブ VLAN パケットがタグ付けされます。

ディセーブルの場合は、すべての IEEE 802.1Q トランク ポートから出るネイティブ VLAN パケットがタグ付けされません。

このコマンドを IEEE 802.1Q トンネリング機能とともに使用できます。この機能は、サービス プロバイダー ネットワークのエッジ スイッチで動作し、VLAN 内 VLAN 階層構造を使用し、タグ付きパケットをタグ付けして VLAN スペースを拡張します。サービス プロバイダー ネットワークへのパケット送信に IEEE 802.1Q トランク ポートを使用する必要があります。ただし、サービス プロバイダー ネットワークのコアを通過するパケットも IEEE 802.1Q トランクで伝送される可能性があります。IEEE 802.1Q トランクのネイティブ VLAN が同一スイッチ上のトンネリング ポートのネイティブ VLAN と一致する場合は、ネイティブ VLAN 上のトラフィックは送信トランク ポートでタグ付けされません。このコマンドは、すべての IEEE 802.1Q トランク ポート上のネイティブ VLAN パケットが確実にタグ付けされるようにします。

IEEE 802.1Q トンネリングに関する詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、ネイティブ VLAN フレームの IEEE 802.1Q タギングをイネーブルにする方法を示します。

```
Switch# configure terminal
Switch (config)# vlan dot1q tag native
Switch (config)# end
```

設定を確認するには、**show vlan dot1q tag native** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show vlan dot1q tag native	IEEE 802.1Q ネイティブ VLAN タギング ステータスを表示します。

vlan filter

VLAN マップを 1 つまたは複数の VLAN に適用するには、**vlan filter** 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。マップを削除する場合は、このコマンドの **no** 形式を使用します。

vlan filter *mapname* **vlan-list** {*list* | **all**}

no vlan filter *mapname* **vlan-list** {*list* | **all**}

構文の説明

mapname	VLAN マップ エントリ名
list	tt、uu-vv、xx、および yy-zz 形式での 1 つまたは複数の VLAN リスト。カンマとダッシュの前後のスペースは任意です。指定できる範囲は 1 ～ 4094 です。
all	すべての VLAN からフィルタを削除します。

デフォルト

VLAN フィルタはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

パケットを誤って過剰にドロップし、設定プロセスの途中で接続が無効になることがないように、VLAN アクセス マップを完全に定義してから VLAN に適用することを推奨します。

VLAN マップ エントリの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、VLAN マップ エントリ *map1* を VLAN 20 および 30 に適用します。

```
Switch(config)# vlan filter map1 vlan-list 20, 30
```

次の例では、VLAN マップ エントリ *map1* を VLAN 20 から削除する方法を示します。

```
Switch(config)# no vlan filter map1 vlan-list 20
```

設定を確認するには、**show vlan filter** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show vlan access-map	特定の VLAN アクセス マップまたはすべての VLAN アクセス マップに関する情報を表示します。
show vlan filter	VLAN フィルタすべてに関する情報、または特定の VLAN または VLAN アクセス マップに関する情報を表示します。
vlan access-map	VLAN パケット フィルタリングの VLAN マップ エントリを作成します。

vmps reconfirm（特権 EXEC）

ただちに VLAN Query Protocol（VQP）クエリーを送信して、VLAN Membership Policy Server（VMPS）でのすべてのダイナミック VLAN 割り当てを再確認するには、**vmps reconfirm** 特権 EXEC コマンドを使用します。

vmps reconfirm

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

例

次の例では、VQP クエリーを VMPS にただちに送信する方法を示します。

```
Switch# vmps reconfirm
```

設定を確認するには、**show vmps** 特権 EXEC コマンドを入力して、Reconfirmation Status セクションの VMPS Action 列を調べます。**show vmps** コマンドは、再確認タイマーの期限切れ、または **vmps reconfirm** コマンドの入力のいずれかにより最後に割り当てが再確認されたときの結果を表示します。

関連コマンド

コマンド	説明
show vmps	VQP および VMPS 情報を表示します。
vmps reconfirm（グローバル コンフィギュレーション）	VQP クライアントの再確認間隔を変更します。

vmps reconfirm（グローバル コンフィギュレーション）

VLAN Query Protocol（VQP）クライアントの再確認間隔を変更するには、**vmps reconfirm** グローバル コンフィギュレーション 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。

vmps reconfirm *interval*

no vmps reconfirm

構文の説明

interval	ダイナミック VLAN 割り当てを再確認するための VLAN Membership Policy Server（VMPS）への VQP クライアント クエリーの再確認間隔。指定できる範囲は 1 ～ 120 分です。

デフォルト

デフォルトの再確認間隔は 60 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

例

次の例では、VQP クライアントが 20 分ごとにダイナミック VLAN エントリを再確認するように設定する方法を示します。

```
Switch(config)# vmps reconfirm 20
```

設定を確認するには、**show vmps** 特権 EXEC コマンドを入力して、Reconfirm Interval 列を調べます。

関連コマンド

コマンド	説明
show vmps	VQP および VMPS 情報を表示します。
vmps reconfirm（特権 EXEC）	VQP クエリーを送信して、VMPS でのすべてのダイナミック VLAN 割り当てを再確認します。

vmps retry

VLAN Query Protocol（VQP）クライアントのサーバあたりの再試行回数を設定するには、**vmps retry** グローバル コンフィギュレーション 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。

vmps retry *count*

no vmps retry

構文の説明

count	リストの次のサーバに照会する前にクライアントが VLAN Membership Policy Server（VMPS）との通信を試行する回数。指定できる範囲は 1 ～ 10 です。

デフォルト

デフォルトの再試行回数は 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

例

次の例では、再試行回数を 7 に設定する方法を示します。

```
Switch(config)# vmps retry 7
```

設定を確認するには、**show vmps** 特権 EXEC コマンドを入力して、Server Retry Count 列を調べます。

関連コマンド

コマンド	説明
show vmps	VQP および VMPS 情報を表示します。

vmps server

プライマリ VLAN Membership Policy Server（VMPS）および最大 3 つまでのセカンダリ サーバを設定するには、**vmps server** グローバル コンフィギュレーション コマンドを使用します。VMPS サーバを削除するには、このコマンドの **no** 形式を使用します。

vmps server *ipaddress* [**primary**]

no vmps server [*ipaddress*]

構文の説明

ipaddress	プライマリまたはセカンダリ VMPS サーバの IP アドレスまたはホスト名。ホスト名を指定する場合には、Domain Name System（DNS; ドメイン ネーム システム）サーバが設定されている必要があります。
primary	（任意）プライマリとセカンダリのどちらの VMPS サーバを設定するのかを決定します。

デフォルト

プライマリまたはセカンダリ VMPS サーバ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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

primary が入力されているかどうかにかかわらず、最初に入力されたサーバは自動的にプライマリ サーバとして選択されます、最初のサーバ アドレスは、次のコマンドで **primary** を使用することにより無効にすることができます。

クラスタ コンフィギュレーションのメンバ スイッチに IP アドレスがない場合、クラスタはそのメンバ スイッチに設定された VMPS サーバを使用しません。その代わり、クラスタはコマンド スイッチの VMPS サーバを使用し、コマンド スイッチは VMPS 要求のプロキシとなります。VMPS サーバは、クラスタを単一スイッチとして扱い、コマンド スイッチの IP アドレスを使用して要求に応答します。

ipaddress を指定せずに *no* 形式を使用すると、設定されたすべてのサーバが削除されます。ダイナミック アクセス ポートが存在するときにすべてのサーバを削除すると、スイッチは、VMPS に照会できないため、これらのポートの新しい送信元からのパケットを転送できません。

例

次の例では、IP アドレス 191.10.49.20 のサーバをプライマリ VMPS サーバとして設定する方法を示します。IP アドレス 191.10.49.21 および 191.10.49.22 のサーバは、セカンダリ サーバとして設定されます。

```
Switch(config)# vmps server 191.10.49.20 primary
Switch(config)# vmps server 191.10.49.21
Switch(config)# vmps server 191.10.49.22
```

次の例では、IP アドレス 191.10.49.21 のサーバを削除する方法を示します。

```
Switch(config)# no vmps server 191.10.49.21
```

設定を確認するには、**show vmps** 特権 EXEC コマンドを入力して、VMPS Domain Server 列を調べます。

関連コマンド

コマンド	説明
show vmps	VQP および VMPS 情報を表示します。

vtp（グローバル コンフィギュレーション）

VLAN Trunking Protocol（VTP）コンフィギュレーション特性を設定または修正するには、**vtp** グローバル コンフィギュレーション コマンドを使用します。設定を削除したり、デフォルト設定に戻したりする場合は、このコマンドの **no** 形式を使用します。

vtp {**domain** *domain-name* | **file** *filename* | **interface** *name* [**only**] | **mode** {**client** | **off** | **server** | **transparent**} [**mst** | **unknown** | **vlan**] | **password** *password* [**hidden** | **secret**] | **pruning** | **version** *number*}

no vtp {**file** | **interface** | **mode** [**client** | **off** | **server** | **transparent**] [**mst** | **unknown** | **vlan**] | **password** | **pruning** | **version**}

構文の説明

domain *domain-name*	VTP ドメイン名をスイッチの VTP 管理ドメインを識別する 1 ～ 32 文字の ASCII 文字列で指定します。ドメイン名では大文字と小文字が区別されます。
file *filename*	VTP VLAN 設定が保存されている Cisco IOS ファイル システム ファイルを指定します。
interface *name*	このデバイスで更新された VTP ID を提供するインターフェイスの名前を指定します。
only	（任意）VTP IP アップデータとしてこのインターフェイスの IP アドレスだけで使用します。
mode	VTP 装置モードをクライアント、サーバ、または透過型に指定します。
client	スイッチを VTP クライアント モードにします。VTP クライアント モードのスイッチは VTP に対してイネーブルであり、アドバタイズを送信できますが、VLAN 設定を格納するために必要な不揮発性メモリがありません。スイッチで VLAN を設定することはできません。VTP クライアントが起動すると、VTP クライアントはその VLAN データベースを初期化するアドバタイズを受信するまで、VTP アドバタイズを送信しません。
off	スイッチを VTP オフ モードにします。VTP オフ モードのスイッチは、トランク ポート上で VTP アドバタイズメントを転送しないことを除いて、VTP 透過型デバイスと同様に機能します。
server	スイッチを VTP サーバ モードにします。VTP サーバ モードのスイッチは VTP に対してイネーブルであり、アドバタイズを送信します。スイッチでは VLAN を設定できます。スイッチは、再起動後に、不揮発性メモリから現在の VTP データベース内のすべての VLAN 情報を回復できます。
transparent	スイッチを VTP 透過モードにします。VTP 透過モードのスイッチは、VTP に対してディセーブルであり、アドバタイズの送信や、他のデバイスから送信されたアドバタイズからの学習を行いません。また、ネットワーク内の他のデバイスの VLAN 設定に影響を与えることはありません。スイッチは VTP アドバタイズを受信し、アドバタイズを受信したトランク ポートを除くすべてのトランク ポートにこれを転送します。 VTP モードが透過型である場合、モードおよびドメイン名はスイッチの実行コンフィギュレーション ファイルに保存されます。この情報をスイッチのスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを入力します。
mst	（任意）Multiple Spanning Tree（MST）VTP データベース（VTP バージョン 3 に限る）にモードを設定します。
unknown	（任意）未知の VTP データベース（VTP バージョン 3 に限る）にモードを設定します。

vlan	（任意）VLAN VTP データベースにモードを設定します。これがデフォルトです（VTP バージョン 3 に限る）。
password *password*	VTP アドバタイズで送信され、受信 VTP アドバタイズを確認するための MD5 ダイジェスト計算で使用される 16 バイトの秘密値を生成するための管理ドメイン パスワードを設定します。パスワードは、1 ～ 32 文字の ASCII 文字列です。パスワードでは大文字と小文字が区別されます。
hidden	（任意）パスワード ストリングから生成されたキーが VLAN データベース ファイルに保存されることを指定します。**hidden** キーワードを指定しない場合、パスワード ストリングはクリア テキストに保存されます。**hidden** パスワードを入力した場合、そのパスワードを再入力し、ドメイン内でコマンドを発行する必要があります。このキーワードは、VTP バージョン 3 だけでサポートされています。
secret	（任意）ユーザがパスワードの秘密キーを直接設定できるようにします（VTP バージョン 3 に限る）。
pruning	スイッチ上で VTP プルーニングをイネーブルに設定します。
version *number*	VTP バージョンをバージョン 1、バージョン 2、またはバージョン 3 に設定します。

デフォルト

デフォルトのファイル名は *flash:vlan.dat* です。

デフォルト モードはサーバ モードで、デフォルトのデータベースは VLAN です。

VTP バージョン 3 では、MST データベースのデフォルト モードは透過型です。

ドメイン名またはパスワードは定義されていません。

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。

デフォルトのバージョンはバージョン 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

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(52)SE	**mode off** キーワードが追加され、VTP バージョン 3 に対するサポートが追加され、password **hidden** および **secret** キーワード、およびモード データベース キーワード（**vlan**、**mst**、および **unknown**）が VTP バージョン 3 とともに追加されました。

使用上のガイドライン

VTP モード、ドメイン名、および VLAN 設定をスイッチのスタートアップ コンフィギュレーション ファイルに保存して、スイッチを再起動すると、VTP および VLAN 設定は次の条件によって選択されます。

- VLAN データベースとコンフィギュレーション ファイルの両方の VTP モードが透過型であり、VTP ドメイン名が一致する場合、VLAN データベースは無視されます。スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ VTP モードがサーバ モードの場合、またはスタートアップ VTP モードまたはドメイン名が VLAN データベースと一致しない場合、最初の 1005 の VLAN の VTP モードおよび VLAN 設定は、VLAN データベース情報によって選択され、1005 を超える VLAN は、スイッチ コンフィギュレーション ファイルから設定されます。

新規データベースをロードするのに **vtp file** *filename* を使用することはできません。これは、既存のデータベースが保存されているファイルの名前を変更するだけです。

VTP ドメイン名を設定するときには、次の注意事項に従ってください。

- ドメイン名を設定するまで、スイッチは非管理ドメイン ステートの状態です。非管理ドメイン ステートの間は、ローカル VLAN 設定に変更が生じても、スイッチは VTP アドバタイズを送信しません。スイッチは、トランキングを行っているポートで最初の VTP サマリー パケットを受信した後、または **vtp domain** コマンドでドメイン名を設定した後で、非管理ドメイン ステートから抜け出します。スイッチは、サマリー パケットからドメインを受信した場合、そのコンフィギュレーション リビジョン番号を 0 にリセットします。スイッチが非管理ドメイン ステートから抜け出した後、NVRAM（不揮発性 RAM）をクリアしてソフトウェアをリロードするまで、スイッチがこのステートに再び入るよう設定することはできません。
- ドメイン名では、大文字と小文字が区別されます。
- 設定したドメイン名は、削除できません。別のドメインに再度割り当てるしかありません。

VTP モードを設定するときには、次の注意事項に従ってください。

- **no vtp mode** コマンドを使用すると、スイッチを VTP サーバ モードに戻すことができます。
- **vtp mode server** コマンドは、スイッチがクライアント モードまたは透過モードでない場合にエラーを返さないことを除けば、**no vtp mode** と同じです。
- 受信スイッチがクライアント モードである場合、クライアント スイッチはその設定を変更して、サーバのコンフィギュレーションをコピーします。クライアント モードのスイッチがある場合には、必ずサーバ モードのスイッチですべての VTP または VLAN 設定変更を行ってください。受信スイッチがサーバ モードまたは透過モードである場合、スイッチの設定は変更されません。
- 透過モードのスイッチは、VTP に参加しません。透過モードのスイッチで VTP または VLAN 設定の変更を行った場合、変更はネットワーク内の他のスイッチには伝播されません。
- サーバ モードのスイッチで VTP または VLAN 設定を変更した場合、その変更は同じ VTP ドメインのすべてのスイッチに伝播されます。
- **vtp mode transparent** コマンドは、ドメインの VTP をディセーブルにしますが、スイッチからドメインを削除しません。
- VTP バージョン 1 および 2 では、拡張範囲 VLAN を追加したり、VTP および VLAN 情報を実行コンフィギュレーション ファイルに保存したりする場合には、VTP モードは透過型に設定してください。VTP は拡張範囲 VLAN をクライアントおよびサーバ モードでサポートし、VLAN データベースに保存します。
- VTP バージョン 1 および 2 では、拡張範囲 VLAN がスイッチで設定され、VTP モードをサーバまたはクライアントに設定しようとした場合、エラー メッセージが表示され、その設定は許可されません。VTP モードは、VTP バージョン 3 で拡張 VLAN を使用することにより変更できます。

- ダイナミック VLAN 作成がディセーブルの場合、VTP に設定できるモードは、サーバ モードまたはクライアント モードのいずれかに限ります。
- **vtp mode off** コマンドを使用すると、デバイスをオフに設定します。**no vtp mode off** コマンドを使用すると、デバイスを VTP サーバ モードにリセットします。

VTP パスワードを設定するときには、次の注意事項に従ってください。

- パスワードでは、大文字と小文字が区別されます。パスワードは、同じドメイン内のすべてのスイッチで一致している必要があります。
- スイッチをパスワードが設定されていない状態に戻す場合は、このコマンドの **no vtp password** 形式を使用します。
- **hidden** および **secret** キーワードは、VTP バージョン 3 だけでサポートされています。VTP バージョン 2 から VTP バージョン 3 に変換する場合、変換前に **hidden** または **secret** キーワードを削除する必要があります。

VTP プルーニングを設定するときには、次の注意事項に従ってください。

- VTP プルーニングは、プルーニング適格 VLAN に所属するステーションがない場合、その VLAN の情報を VTP 更新から削除します。
- VTP サーバでプルーニングをイネーブルにすると、プルーニングは VLAN ID 1 ～ 1005 の管理ドメイン全体でイネーブルになります。
- プルーニング適格リストに指定された VLAN だけが、プルーニングの対象になります。
- プルーニングは、VTP バージョン 1 およびバージョン 2 でサポートされています。

VTP バージョンを設定するときには、次の注意事項に従ってください。

- バージョン 2（v2）モード ステートを切り替えると、ある一定のデフォルト VLAN のパラメータが変更されます。
- 各 VTP スイッチは他のすべての VTP デバイスの機能を自動的に検出します。VTP バージョン 2 を使用するには、ネットワーク内のすべての VTP スイッチでバージョン 2 がサポートされている必要があります。そうでない場合、VTP バージョン 1 モードで稼動するよう設定する必要があります。
- ドメイン内のすべてのスイッチが VTP バージョン 2 対応である場合、1 つのスイッチでバージョン 2 を設定すれば、バージョン番号は、VTP ドメイン内の他のバージョン 2 対応スイッチに伝播されます。
- トークンリング環境で VTP を使用している場合、VTP バージョン 2 もイネーブルである必要があります。
- Token Ring Bridge Relay Function（TrBRF）または Token Ring Concentrator Relay Function（TrCRF）VLAN メディア タイプを設定している場合には、バージョン 2 を使用してください。
- トークンリングまたはトークンリング NET VLAN メディア タイプを設定している場合には、バージョン 1 を使用してください。
- VTP バージョン 3 では、VLAN データベース情報だけでなく、すべてのデータベース VTP 情報が VTP ドメインに伝播します。
- 2 つの VTP バージョン 3 の領域は、トランスペアレント モードの VTP バージョン 1 または VTP バージョン 2 の領域でだけ通信できます。

スイッチ コンフィギュレーション ファイルにパスワード、プルーニング、およびバージョン コンフィギュレーションを保存することはできません。

例

次の例では、VTP コンフィギュレーション メモリのファイル名を *vtpfilename* に変更する方法を示します。

```
Switch(config)# vtp file vtpfilename
```

次の例では、デバイス ストレージのファイル名をクリアする方法を示します。

```
Switch(config)# no vtp file vtpconfig
Clearing device storage filename.
```

次の例では、このデバイスの VTP アップデータ ID を提供するインターフェイスの名前を指定する方法を示します。

```
Switch(config)# vtp interface gigabitethernet
```

次の例では、スイッチの管理ドメインを設定する方法を示します。

```
Switch(config)# vtp domain OurDomainName
```

次の例では、スイッチを VTP 透過モードにする方法を示します。

```
Switch(config)# vtp mode transparent
```

次の例では、VTP ドメイン パスワードを設定する方法を示します。

```
Switch(config)# vtp password ThisIsOurDomain'sPassword
```

次の例では、VLAN データベースでのプルーニングをイネーブルにする方法を示します。

```
Switch(config)# vtp pruning
Pruning switched ON
```

次の例では、VLAN データベースのバージョン 2 モードをイネーブルにする方法を示します。

```
Switch(config)# vtp version 2
```

設定を確認するには、**show vtp status** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show vtp status	スイッチの VTP 統計情報および VTP 管理ドメイン ステータスの一般情報を表示します。
vtp（インターフェイス コンフィギュレーション）	インターフェイスで VTP をイネーブルまたはディセーブルにします。

vtp（インターフェイス コンフィギュレーション）

ポート単位で VLAN Trunking Protocol（VTP）をイネーブルにするには、**vtp** 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。インターフェイスで VTP をディセーブルにする場合は、このコマンドの **no** 形式を使用します。

vtp

no vtp

（注）　このコマンドは、スイッチが LAN ベース イメージおよび VTP バージョン 3 を実行している場合だけサポートされます。

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

このコマンドには、デフォルト設定はありません。

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

コマンド履歴

リリース	変更内容
12.2(52)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、スイッチポートがトランク モードであるインターフェイスだけに入力します。

このコマンドは、VTP バージョン 3 に設定されているスイッチ上だけでサポートされています。

例

次の例では、インターフェイス上で VTP をイネーブルにする方法を示します。

```
Switch(config-if)# vtp
```

次の例では、インターフェイス上で VTP をディセーブルにする方法を示します。

```
Switch(config-if)# no vtp
```

関連コマンド

コマンド	説明
vtp（グローバル コンフィギュレーション）	VTP のドメイン名、パスワード、プルーニング、バージョン、およびモードをグローバルに設定します。

vtp（VLAN コンフィギュレーション）

このコマンドは現在サポートされていません。

VLAN Trunking Protocol（VTP）の特性を設定するには、**vtp** VLAN コンフィギュレーション コマンドを使用します。VLAN コンフィギュレーション モードを開始する場合は、**vlan database** 特権 EXEC コマンドを入力します。

vtp {**domain** *domain-name* | **password** *password* | **pruning** | **v2-mode** | {**server** | **client** | **transparent**}}

no vtp {**client** | **password** | **pruning** | **transparent** | **v2-mode**}

vtp primary

スイッチを VLAN Trunking Protocol（VTP）プライマリ サーバとして設定するには、**vtp primary** 特権 EXEC コマンドを使用します。

vtp primary [**mst** | **vlan**] [**force**]

このコマンドには、**no** 形式はありません。

（注）　このコマンドは、スイッチが LAN ベース イメージおよび VTP バージョン 3 を実行している場合だけサポートされます。

（注）　**vtp** {**password** *password* | **pruning** | **version** *number*} コマンドはコマンドライン ヘルプに表示されますが、サポートされていません。

構文の説明

mst	（任意）スイッチを Multiple Spanning Tree（MST）機能のプライマリ VTP サーバとして設定します。
vlan	（任意）スイッチを VLAN のプライマリ VTP サーバとして設定します。
force	（任意）プライマリ サーバを設定する場合、スイッチが競合するデバイスをチェックしないように設定します。

デフォルト

スイッチは VTP セカンダリ サーバです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(52)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、VTP バージョン 3 に設定されているスイッチ上だけでサポートされています。

VTP プライマリ サーバはデータベース情報をアップデートし、システム内のすべてのデバイスによって行われるアップデートを送信します。VTP セカンダリ サーバは、プライマリ サーバから受信したアップデートされた VTP のコンフィギュレーションを NVRAM にバックアップすることだけができます。

デフォルトでは、すべてのデバイスはセカンダリ サーバとして起動します。プライマリ サーバのステータスは、管理者がドメイン内のテイクオーバー メッセージを発行する場合のデータベース アップデートのためだけに必要です。プライマリ サーバなしで実用 VTP ドメインを持つことができます。

デバイスがリロードするかドメイン パラメータが変更された場合、プライマリ サーバのステータスは失われます。

例

次の例では、スイッチを VLAN のプライマリ VTP サーバとして設定する方法を示します。

```
Switch# vtp primary vlan
Setting device to VTP TRANSPARENT mode.
```

設定を確認するには、**show vtp status** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show vtp status	スイッチの VTP 統計情報および VTP 管理ドメイン ステータスの一般情報を表示します。
vtp（グローバル コンフィギュレーション）	VTP ファイル名、インターフェイス、ドメイン名、モード、およびバージョンを設定します。

APPENDIX A

Catalyst 3750 スイッチ ブート ローダー コマンド

通常のブート ローダー処理中は、ブート ローダー コマンドライン プロンプトが表示されません。ブート ローダー コマンド ラインは、スイッチが手動ブートに設定されている場合、Power-on Self-Test（POST; 電源投入時セルフテスト）DRAM テスト中にエラーが発生した場合、またはオペレーティング システム（破壊された Cisco IOS イメージ）のロード中にエラーが発生した場合に使用できます。スイッチのパスワードを忘れた場合にも、ブート ローダーを使用できます。

（注） スイッチのデフォルトの設定を使用すると、スイッチに物理的にアクセスするエンド ユーザは、スイッチの電源投入時にブート プロセスを中断して新しいパスワードを入力することにより、パスワードを失った状態から回復できます。パスワード回復ディセーブル機能を使用すると、システム管理者は、この機能の一部をディセーブルにし、システムをデフォルト設定に戻すことに同意するだけでユーザがブート プロセスを中断できるようにすることにより、スイッチのパスワードへのアクセスを防止できます。パスワード回復をディセーブルにすることにより、ユーザはブート プロセスを中断してパスワードを変更できますが、コンフィギュレーション ファイル（config.text）および VLAN データベース ファイル（vlan.dat）は削除されます。詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

ブートローダーには、9600 bps のスイッチ コンソール接続を介してアクセスできます。

スイッチの電源コードを取り外し、電源コードの再接続中に Mode ボタンを押します。ポート 1X の上の LED が消灯してから 1 ～ 2 秒後に、Mode ボタンを離します。その後、ブート ローダーの `Switch:` プロンプトが表示されます。ブート ローダーは低レベルの CPU 初期化および POST を実行し、デフォルトのオペレーティング システム イメージをメモリにロードします。

boot

実行可能イメージをロードおよび起動して、コマンドライン インターフェイスを開始するには、**boot** ブート ローダー コマンドを使用します。

boot [**-post** | **-n** | **-p** | *flag*] *filesystem:/file-url ...*

構文の説明

-post	（任意）拡張および総合 POST によってロードされたイメージを実行します。このキーワードを使用すると、POST の完了に要する時間が長くなります。
-n	（任意）起動後すぐに、Cisco IOS デバッガが休止します。
-p	（任意）イメージのロード後すぐに、JTAG デバッガが休止します。
filesystem:	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスには **flash:** を使用します。
/file-url	（任意）ブート可能イメージのパス（ディレクトリ）および名前です。各イメージ名はセミコロンで区切ります。

デフォルト

スイッチは、BOOT 環境変数内の情報を使用して、自動的にシステムを起動しようとします。この変数が設定されていない場合、スイッチは、フラッシュ ファイル システム全体に再帰的に縦型検索し、最初の実行可能イメージをロードして実行しようとします。ディレクトリの縦型検索では、検出した各サブディレクトリを完全に検索してから元のディレクトリでの検索を続けます。

コマンド モード

ブート ローダー

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

引数を何も指定しないで **boot** コマンドを入力した場合、スイッチは、BOOT 環境変数が設定されていればその中の情報を使用して、システムを自動的に起動しようとします。*file-url* 変数にイメージ名を指定した場合、**boot** コマンドは指定されたイメージを起動しようとします。

ブート ローダー **boot** コマンドのオプションを設定した場合は、このコマンドがただちに実行され、現在のブート ローダー セッションだけに適用されます。これらの設定が保存されて、次の起動処理に使用されることはありません。

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

例

次の例では、*new-image.bin* イメージを使用してスイッチを起動する方法を示します。

```
switch: boot flash:/new-images/new-image.bin
```

このコマンドを入力すると、セットアップ プログラムを開始するように求められます。

関連コマンド

コマンド	説明
set	コマンドに **BOOT** キーワードを追加して、特定のイメージを起動するように BOOT 環境変数を設定します。

cat

1 つ以上のファイルの内容を表示するには、**cat** ブート ローダー コマンドを使用します。

cat *filesystem*:/*file-url* ...

構文の説明

filesystem:	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスには **flash:** を使用します。
/*file-url*	表示するファイルのパス（ディレクトリ）および名前です。ファイル名はスペースで区切ります。

コマンド モード

ブート ローダー

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

ファイルのリストを指定した場合は、各ファイルの内容が順に表示されます。

例

次の例では、2 つのファイル内容を表示する方法および出力例を示します。

```
switch: cat flash:/new-images/info flash:env_vars
version_suffix: image-version
version_directory: image-name
image_name: image-name.bin
ios_image_file_size: 6398464
total_image_file_size: 8133632
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family:switch-family
info_end:
BAUD=57600
MANUAL_BOOT=no
```

関連コマンド

コマンド	説明
more	1 つ以上のファイルの内容を表示します。
type	1 つ以上のファイルの内容を表示します。

copy

ファイルをコピー元からコピー先にコピーするには、**copy** ブート ローダー コマンドを使用します。

copy [**-b** *block-size*] *filesystem*:/*source-file-url filesystem*:/*destination-file-url*

構文の説明

-b *block-size*	（任意）このオプションは、内部開発およびテスト専用です。
filesystem:	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスには **flash:** を使用します。
/*source-file-url*	コピー元のパス（ディレクトリ）およびファイル名です。
/*destination-file-url*	コピー先のパス（ディレクトリ）およびファイル名です。

デフォルト

デフォルトのブロック サイズは 4 KB です。

コマンド モード

ブート ローダー

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

スラッシュ（/）間に指定できるディレクトリ名は最大 45 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

指定できるファイル名は最大 45 文字です。ファイル名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

ファイルを別のディレクトリにコピーする場合は、そのディレクトリが存在していなければなりません。

例

次の例では、ルートにあるファイルをコピーする方法を示します。

```
switch: copy flash:test1.text flash:test4.text
.
File "flash:test1.text" successfully copied to "flash:test4.text"
```

ファイルがコピーされたかどうかを確認するには、**dir** *filesystem*: ブート ローダー コマンドを入力します。

関連コマンド

コマンド	説明
delete	指定されたファイル システムから 1 つ以上のファイルを削除します。

delete

指定されたファイル システムから 1 つ以上のファイルを削除するには、**delete** ブート ローダー コマンドを使用します。

delete *filesystem***:***/file-url* ...

構文の説明

*filesystem***:**	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスには **flash:** を使用します。
/file-url	削除するファイルのパス（ディレクトリ）および名前です。ファイル名はスペースで区切ります。

コマンド モード

ブート ローダー

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

各ファイルを削除する前に、確認を求めるプロンプトが表示されます。

例

次の例では、2 つのファイルを削除します。

```
switch: delete flash:test2.text flash:test5.text
Are you sure you want to delete "flash:test2.text" (y/n)?y
File "flash:test2.text" deleted
Are you sure you want to delete "flash:test5.text" (y/n)?y
File "flash:test2.text" deleted
```

ファイルが削除されたかどうかを確認するには、**dir flash:** ブート ローダー コマンドを入力します。

関連コマンド

コマンド	説明
copy	コピー元からコピー先にファイルをコピーします。

dir

指定されたファイル システム上のファイルおよびディレクトリのリストを表示するには、**dir** ブート ローダー コマンドを使用します。

dir *filesystem***:**/*file-url* ...

構文の説明

*filesystem***:**	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスには **flash:** を使用します。
/*file-url*	（任意）内容を表示するパス（ディレクトリ）およびディレクトリ名です。ディレクトリ名はスペースで区切ります。

コマンド モード

ブート ローダー

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

ディレクトリ名では、大文字と小文字が区別されます。

例

次の例では、フラッシュ メモリ内のファイルを表示する方法を示します。

```
switch: dir flash:
Directory of flash:/

    3  -rwx        1839   Mar 01 2002 00:48:15  config.text
   11  -rwx        1140   Mar 01 2002 04:18:48  vlan.dat
   21  -rwx          26   Mar 01 2002 00:01:39  env_vars
    9  drwx         768   Mar 01 2002 23:11:42  html
   16  -rwx        1037   Mar 01 2002 00:01:11  config.text
   14  -rwx        1099   Mar 01 2002 01:14:05  homepage.htm
   22  -rwx          96   Mar 01 2002 00:01:39  system_env_vars
   17  drwx        192    Mar 06 2002 23:22:03  imnage-name

15998976 bytes total (6397440 bytes free)
```

表 A-1 に、この出力で表示されるフィールドの説明を示します。

表 A-1　dir のフィールドの説明

フィールド	説明
2	ファイルのインデックス番号
-rwx	ファイルのアクセス権（次のいずれか、またはすべて） • d：ディレクトリ • r：読み取り可能 • w：書き込み可能 • x：実行可能
1644045	ファイルのサイズ
<date>	最終変更日
env_vars	ファイル名

関連コマンド

コマンド	説明
mkdir	1 つ以上のディレクトリを作成します。
rmdir	1 つ以上のディレクトリを削除します。

flash_init

フラッシュ ファイル システムを初期化するには、**flash_init** ブート ローダー コマンドを使用します。

flash_init

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

フラッシュ ファイル システムは、通常のシステム動作中に自動的に初期化されます。

コマンド モード

ブート ローダー

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

フラッシュ ファイル システムは、通常の起動プロセス中に自動的に初期化されます。

このコマンドは、フラッシュ ファイル システムを手動で初期化します。たとえば、パスワードを忘れた場合には、回復手順中にこのコマンドを使用します。

format

指定されたファイル システムをフォーマットし、そのファイル システム内のすべてのデータを破棄するには、**format** ブート ローダー コマンドを使用します。

format *filesystem***:**

構文の説明

*filesystem***:**	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスには **flash:** を使用します。

コマンド モード

ブート ローダー

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

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。ファイル システム内のすべてのデータが破棄され、システムが使用不能になります。

fsck

ファイル システムの一貫性を確認するには、**fsck** ブート ローダー コマンドを使用します。

fsck [**-test** | **-f**] *filesystem***:**

構文の説明

-test	（任意）ファイル システム コードを初期化し、フラッシュ メモリ上で新しい POST を実行します。ファイル システムを構成するバイトごとに、広範なメモリ テストを実行します（メモリは破壊されません）。
-f	（任意）ファイル システム コードを初期化し、高速ファイル一貫性チェックを実行します。フラッシュ セクタ内の Cyclic Redundancy Check（CRC; 巡回冗長検査）は実行されません。
*filesystem***:**	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスには **flash:** を使用します。

デフォルト

ファイル システム チェックは実行されません。

コマンド モード

ブート ローダー

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

進行中のファイル システム一貫性チェックを停止するには、スイッチの電源を切断してから、電源を再接続します。

例

次の例では、フラッシュ メモリ上で広範なファイル システム チェックを実行する方法を示します。

```
switch: fsck -test flash:
```

help

使用可能なコマンドを表示するには、**help** ブート ローダー コマンドを使用します。

help

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド モード

ブート ローダー

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

疑問符（?）を使用して、使用可能なブート ローダー コマンドのリストを表示することもできます。

memory

メモリ ヒープ使用率情報を表示するには、**memory** ブート ローダー コマンドを使用します。

memory

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド モード

ブート ローダー

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

例

次の例では、メモリ ヒープ使用率情報を表示する方法を示します。

```
switch: memory
Text:   0x00700000 - 0x0071cf24 (0x0001cf24 bytes)
Rotext: 0x00000000 - 0x00000000 (0x00000000 bytes)
Data:   0x0071cf24 - 0x00723a0c (0x00006ae8 bytes)
Bss:    0x0072529c - 0x00746f94 (0x00021cf8 bytes)
Stack:  0x00746f94 - 0x00756f94 (0x00010000 bytes)
Heap:   0x00756f98 - 0x00800000 (0x000a9068 bytes)

Bottom heap utilization is 22 percent.
Top heap utilization is 0 percent.
Total heap utilization is 22 percent.
Total bytes: 0xa9068 (692328)
Bytes used: 0x26888 (157832)
Bytes available: 0x827e0 (534496)

Alternate heap utilization is 0 percent.
Total alternate heap bytes: 0x6fd000 (7327744)
Alternate heap bytes used: 0x0 (0)
Alternate heap bytes available: 0x6fd000 (7327744)
```

表 A-2 に、この出力で表示されるフィールドの説明を示します。

表 A-2　Memory のフィールドの説明

フィールド	説明
Text	テキスト記憶領域の先頭および末尾アドレス。
Rotext	読み取り専用テキスト記憶領域の先頭および末尾アドレス。データ セグメントのこの部分は、Text エントリとともにグループ化されます。
Data	データ セグメント記憶領域の先頭および末尾アドレス。
Bss	Block Started by Symbol（Bss）記憶領域から始まるブロックの先頭および末尾アドレス。ゼロに初期化されています。

表 A-2　Memory のフィールドの説明 （続き）

フィールド	説明
Stack	自動変数やリターン アドレスなどを格納するためにソフトウェアに割り当てられたメモリ領域の先頭および末尾アドレス。
Heap	メモリの割り当ておよび解放が動的に行われるメモリ領域の先頭および末尾アドレス。

mkdir

指定されたファイル システムに 1 つ以上のディレクトリを新規作成するには、**mkdir** ブート ローダー コマンドを使用します。

mkdir *filesystem***:**/*directory-url* ...

構文の説明

*filesystem***:**	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスには **flash:** を使用します。
/*directory-url*	作成するディレクトリの名前です。ディレクトリ名はスペースで区切ります。

コマンド モード

ブート ローダー

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

ディレクトリ名では、大文字と小文字が区別されます。

スラッシュ（/）間に指定できるディレクトリ名は最大 45 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

例

次の例では、ディレクトリ Saved_Configs を作成する方法を示します。

```
switch: mkdir flash:Saved_Configs
Directory "flash:Saved_Configs" created
```

次の例では、2 つのディレクトリを作成する方法をします。

```
switch: mkdir flash:Saved_Configs1 flash:Test
Directory "flash:Saved_Configs1" created
Directory "flash:Test" created
```

ディレクトリが作成されたかどうかを確認するには、**dir** *filesystem***:** ブート ローダー コマンドを入力します。

関連コマンド

コマンド	説明
dir	指定されたファイル システムのファイルおよびディレクトリのリストを表示します。
rmdir	指定されたファイル システムから 1 つ以上のディレクトリを削除します。

more

1 つ以上のファイルの内容を表示するには、**more** ブート ローダー コマンドを使用します。

more *filesystem*:/*file-url* ...

構文の説明

filesystem:	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスには **flash:** を使用します。
/*file-url*	表示するファイルのパス（ディレクトリ）および名前です。ファイル名はスペースで区切ります。

コマンド モード

ブート ローダー

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

ファイルのリストを指定した場合は、各ファイルの内容が順に表示されます。

例

次の例では、2 つのファイル内容を表示する方法を示します。

```
switch: more flash:/new-images/info flash:env_vars
version_suffix: image-version
version_directory: image-name
c3750-ipservices-mz.122-25.SEB
image_name:image-name.bin
ios_image_file_size: 6398464
total_image_file_size: 8133632
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128switch-family
info_end:
BAUD=57600
MANUAL_BOOT=no
```

関連コマンド

コマンド	説明
cat	1 つ以上のファイルの内容を表示します。
type	1 つ以上のファイルの内容を表示します。

rename

ファイルの名前を変更するには、**rename** ブート ローダー コマンドを使用します。

rename *filesystem*:/*source-file-url filesystem*:/*destination-file-url*

構文の説明

filesystem:	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスには **flash:** を使用します。
/*source-file-url*	元のパス（ディレクトリ）およびファイル名です。
/*destination-file-url*	新しいパス（ディレクトリ）およびファイル名です。

コマンド モード

ブート ローダー

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

スラッシュ（/）間に指定できるディレクトリ名は最大 45 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

指定できるファイル名は最大 45 文字です。ファイル名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

例

次の例では、ファイル *config.text* の名前を *config1.text* に変更します。

```
switch: rename flash:config.text flash:config1.text
```

ファイル名が変更されたかどうかを確認するには、**dir** *filesystem*: ブート ローダー コマンドを入力します。

関連コマンド

コマンド	説明
copy	コピー元からコピー先にファイルをコピーします。

reset

システムのハード リセットを実行するには、**reset** ブート ローダー コマンドを使用します。ハード リセットを行うと、スイッチの電源切断後に電源を投入する手順と同様に、プロセッサ、レジスタ、およびメモリの内容が消去されます。

reset

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド モード

ブート ローダー

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

例

次の例では、システムをリセットする方法を示します。

```
switch: reset
Are you sure you want to reset the system (y/n)?y
System resetting...
```

関連コマンド

コマンド	説明
boot	実行可能イメージをロードおよび起動して、コマンドライン インターフェイスを開始します。

rmdir

指定されたファイル システムから 1 つ以上の空のディレクトリを削除するには、**rmdir** ブート ローダー コマンドを使用します。

rmdir *filesystem*:/*directory-url* ...

構文の説明

filesystem:	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスには **flash:** を使用します。
/*directory-url*	削除する空のディレクトリのパス（ディレクトリ）および名前です。ディレクトリ名はスペースで区切ります。

コマンド モード

ブート ローダー

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

スラッシュ（/）間に指定できるディレクトリ名は最大 45 文字で、大文字と小文字の区別があります。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、およびコロンは使用できません。

ディレクトリを削除する前に、まずディレクトリ内のファイルをすべて削除する必要があります。

各ディレクトリを削除する前に、確認を求めるプロンプトが表示されます。

例

次の例では、ディレクトリを 1 つ削除する方法を示します。

```
switch: rmdir flash:Test
```

ディレクトリが削除されたかどうかを確認するには、**dir** *filesystem*: ブート ローダー コマンドを入力します。

関連コマンド

コマンド	説明
dir	指定されたファイル システムのファイルおよびディレクトリのリストを表示します。
mkdir	指定されたファイル システムに 1 つ以上のディレクトリを新規作成します。

set

ブート ローダーまたはスイッチ上で稼動している他のソフトウェアを制御するために使用できる環境変数を設定したり、表示したりするには、**set** ブート ローダー コマンドを使用します。

set *variable value*

構文の説明

variable value

variable および *value* には、次に示すキーワードのいずれかを使用します。

MANUAL_BOOT：スイッチを自動で起動するか、または手動で起動するかを決定します。

有効値は 1、yes、0、および no です。no または 0 に設定されている場合、ブートローダーはシステムを自動的に起動しようとします。それ以外に設定されている場合は、ブート ローダー モードから手動でスイッチを起動する必要があります。

BOOT *filesystem***:/***file-url*：自動起動時にロードおよび実行される実行可能ファイルのセミコロン区切りリストです。

BOOT 環境変数が設定されていない場合、システムは、フラッシュ ファイル システム全体に再帰的な縦型検索を行って、最初に検出された実行可能イメージをロードして実行を試みます。BOOT 環境変数が設定されていても指定されたイメージをロードできない場合は、システムはフラッシュ ファイル システムで最初に見つかったブート ファイルを起動しようとします。

ENABLE_BREAK：コンソール上の Break キーを使用して自動起動プロセスを中断できるかどうかを決定します。

有効値は 1、yes、on、0、no、および off です。1、yes、または on に設定されている場合は、フラッシュ ファイル システムの初期化後にコンソール上で Break キーを押して、自動起動プロセスを中断できます。

HELPER *filesystem***:/***file-url*：ブート ローダーの初期化中に動的にロードされるロード可能ファイルのセミコロン区切りリストです。ヘルパー ファイルは、ブート ローダーの機能を拡張したり、パッチを当てたりします。

PS1 *prompt*：ブート ローダー モードの場合に、コマンドライン プロンプトとして使用される文字列です。

CONFIG_FILE flash:/*file-url*：Cisco IOS がシステム設定の不揮発性コピーの読み書きに使用するファイル名です。

BAUD *rate*：コンソールで使用される速度（ビット / 秒単位）です。コンフィギュレーション ファイルに別の設定が指定されていない限り、Cisco IOS ソフトウェアはブート ローダーからボー レート設定を継承し、この値を引き続き使用します。指定できる範囲は 0 ～ 4294967295 bps です。有効値は、50、75、110、150、300、600、1200、1800、2000、2400、3600、4800、7200、9600、14400、19200、28800、38400、56000、57600、115200、および 128000 です。

最も一般的な値は、300、1200、2400、9600、19200、57600、および 115200 です。

HELPER_CONFIG_FILE *filesystem***:/***file-url*：Cisco IOS ヘルパー イメージで使用されるコンフィギュレーション ファイルの名前です。この名前が設定されていない場合は、CONFIG_FILE 環境変数で指定されたファイルが、ロードされるすべてのバージョンの Cisco IOS（ヘルパー イメージを含む）で使用されます。この変数は、内部開発およびテスト専用です。

デフォルト

環境変数のデフォルト値は、次のとおりです。

MANUAL_BOOT: No (0)

BOOT: ヌル ストリング

ENABLE_BREAK: no（off または 0）（コンソール上で Break キーを押して自動起動プロセスを中断することはできません）

HELPER: デフォルト値はありません（ヘルパー ファイルは自動的にロードされません）。

PS1: switch:

CONFIG_FILE: config.text

BAUD: 9600 bps

HELPER_CONFIG_FILE: デフォルト値はありません（ヘルパー コンフィギュレーション ファイルは指定されません）

SWITCH_NUMBER: 1

SWITCH_PRIORITY: 1

（注）値が設定された環境変数は、各ファイルのフラッシュ ファイル システムに保存されています。これらのファイルの各行に、環境変数名と等号、その後に変数の値が格納されています。このファイルに表示されていない変数には値がありません。表示されていればヌル ストリングであっても値があります。ヌル ストリング（たとえば「 」）に設定されている変数は、値が設定された変数です。多くの環境変数は事前に定義されており、デフォルト値が設定されています。

コマンド モード

ブート ローダー

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

環境変数は大文字と小文字の区別があり、指定どおりに入力する必要があります。

値を持つ環境変数は、フラッシュ ファイル システムの外にあるフラッシュ メモリに保存されます。

通常の環境では、環境変数の設定を変更する必要はありません。

MANUAL_BOOT 環境変数は、**boot manual** 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設定することもできます。

BOOT 環境変数は、**boot system** *filesystem*:/*file-url* 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設定することもできます。

ENABLE_BREAK 環境変数は、**boot enable-break** 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設定することもできます。

HELPER 環境変数は、**boot helper** *filesystem*:/*file-url* 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設定することもできます。

CONFIG_FILE 環境変数は、**boot config-file flash:**/*file-url* 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設定することもできます。

HELPER_CONFIG_FILE 環境変数は、**boot helper-config-file** *filesystem*:/*file-url* 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設定することもできます。

SWITCH_NUMBER 環境変数は、**switch** *current-stack-member-number* **renumber** *new-stack-member-number* 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設定することもできます。

SWITCH_PRIORITY 環境変数は、**switch** *stack-member-number* **priority** *priority-number* 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設定することもできます。

ブート ローダーのプロンプト ストリング（PS1）には、等号（=）を除く、出力可能な文字列を 120 文字まで指定できます。

例

次の例では、ブート ローダーのプロンプトを変更する方法を示します。

```
switch: set PS1 loader:
loader:
```

設定を確認するには、**set** ブート ローダー コマンドを使用します。

関連コマンド

コマンド	説明
unset	1 つ以上の環境変数を元の設定に戻します。

type

1 つ以上のファイルの内容を表示するには、**type** ブート ローダー コマンドを使用します。

type *filesystem***:**/*file-url* ...

構文の説明

*filesystem***:**	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスには **flash:** を使用します。
/*file-url*	表示するファイルのパス（ディレクトリ）および名前です。ファイル名はスペースで区切ります。

コマンド モード

ブート ローダー

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

ファイルのリストを指定した場合は、各ファイルの内容が順に表示されます。

例

次の例では、2 つのファイル内容を表示する方法を示します。

```
switch: type flash:/new-images/info flash:env_vars
version_suffix: image-version
version_directory:image-name
image_name:image-name .bin
ios_image_file_size: 6398464
total_image_file_size: 8133632
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128switch-family
info_end:
BAUD=57600
MANUAL_BOOT=no
```

関連コマンド

コマンド	説明
cat	1 つ以上のファイルの内容を表示します。
more	1 つ以上のファイルの内容を表示します。

unset

1 つ以上の環境変数をリセットするには、**unset** ブート ローダー コマンドを使用します。

unset *variable ...*

構文の説明

variable	*variable* には、次に示すキーワードのいずれかを使用します。 **MANUAL_BOOT**：スイッチを自動で起動するか、または手動で起動するかを決定します。 **BOOT**：自動起動時に、実行可能ファイルのリストをリセットして、ロードおよび実行します。BOOT 環境変数が設定されていない場合、システムは、フラッシュ ファイル システム全体に再帰的な縦型検索を行って、最初に検出された実行可能イメージをロードして実行を試みます。BOOT 環境変数が設定されていても指定されたイメージをロードできない場合は、システムはフラッシュ ファイル システムで最初に見つかったブート ファイルを起動しようとします。 **ENABLE_BREAK**：フラッシュ ファイル システムの初期化後に、コンソール上の Break キーを使用して自動起動プロセスを中断できるかどうかを決定します。 **HELPER**：ブート ローダーの初期化中に動的にロードされるロード可能ファイルのセミコロン区切りリストです。ヘルパー ファイルは、ブート ローダーの機能を拡張したり、パッチを当てたりします。 **PS1**：ブート ローダー モードの場合に、コマンドライン プロンプトとして使用される文字列です。 **CONFIG_FILE**：Cisco IOS がシステム設定の不揮発性コピーの読み書きに使用するファイル名をリセットします。 **BAUD**：コンソールで使用される速度（ビット/秒単位）をリセットします。コンフィギュレーション ファイルに別の設定が指定されていない限り、Cisco IOS ソフトウェアはブート ローダーからボー レート設定を継承し、この値を引き続き使用します。 **HELPER_CONFIG_FILE**：Cisco IOS ヘルパー イメージで使用されるコンフィギュレーション ファイルの名前をリセットします。この名前が設定されていない場合は、CONFIG_FILE 環境変数で指定されたファイルが、ロードされるすべてのバージョンの Cisco IOS（ヘルパー イメージを含む）で使用されます。この変数は、内部開発およびテスト専用です。

コマンド モード

ブート ローダー

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

通常の環境では、環境変数の設定を変更する必要はありません。

MANUAL_BOOT 環境変数は、**no boot manual** 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リセットすることもできます。

BOOT 環境変数は、**no boot system** 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リセットすることもできます。

ENABLE_BREAK 環境変数は、**no boot enable-break** 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リセットすることもできます。

HELPER 環境変数は、**no boot helper** 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リセットすることもできます。

CONFIG_FILE 環境変数は、**no boot config-file** 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リセットすることもできます。

HELPER_CONFIG_FILE 環境変数は、**no boot helper-config-file** 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リセットすることもできます。

ブート ローダーのプロンプト ストリング（PS1）には、等号（=）を除く、出力可能な文字列を 120 文字まで指定できます。

例

次の例では、プロンプト ストリングを元の設定にリセットする方法を示します。

```
switch: unset PS1
switch:
```

関連コマンド

コマンド	説明
set	環境変数を設定または表示します。

version

ブート ローダーのバージョンを表示するには、**version** ブート ローダー コマンドを使用します。

version

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド モード

ブート ローダー

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

例

次の例では、ブート ローダーのバージョンを表示する方法を示します。

```
switch: version
C3750 Boot Loader (C3750-HBOOT-M) Version 12.1(11)AX
Compiled Wed 05-Mar-08 10:11 by engineer
```

APPENDIX **B**

Catalyst 3750 スイッチ デバッグ コマンド

この付録では、Catalyst 3750 スイッチ用に作成または変更された **debug** 特権 EXEC コマンドについて説明します。これらのコマンドは、インターネットワーキングの問題の診断および解決に役立ちます。使用する場合には、必ずシスコのテクニカル サポート担当者の指示に従ってください。

注意 デバッグ出力には、CPU プロセスで高いプライオリティが与えられるため、システムが使用不能になる可能性があります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用するのが最良です。このような時間帯を選んでデバッグを実行すると、**debug** コマンドの処理の負担によってシステム利用が影響を受ける可能性が少なくなります。

debug authentication

インターフェイスの認証設定のデバッグをイネーブルにするには、**debug authentication** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug authentication {**all** | **errors** | **events** | **sync** | **feature** [**all**] [**acct**] [**auth_fail_vlan**] [**auth_policy**] [**autocfg**] [**critical**] [**dhcp**] [**guest_vlan**] [**mab_pm**] [**mda**] [**multi_auth**] [**switch_pm**] [**switch_sync**] [**vlan_assign**] [**voice**] [**webauth**] [**all** | **errors** | **events**]}

no debug authentication {**all** | **errors** | **events** | **sync** | **feature** [**all**] [**acct**] [**auth_fail_vlan**] [**auth_policy**] [**autocfg**] [**critical**] [**dhcp**] [**guest_vlan**] [**mab_pm**] [**mda**] [**multi_auth**] [**switch_pm**] [**switch_sync**] [**vlan_assign**] [**voice**] [**webauth**] [**all** | **errors** | **events**]}

構文の説明

acct	（任意）認証マネージャ アカウンティング情報を表示します。
all	（任意）認証マネージャ デバッグ メッセージをすべて表示します。
auth_fail_vlan	（任意）制限された VLAN の認証マネージャ エラーを表示します。
auth_policy	（任意）認証ポリシー メッセージを表示します。
autocfg	（任意）自動設定認証マネージャ デバッグ メッセージを表示します。
critical	（任意）アクセス不能な認証バイパス メッセージを表示します。 **（注）** アクセス不能な認証バイパス機能は、クリティカル認証または Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）失敗ポリシーとも呼ばれています。
dhcp	（任意）DHCP ダイナミック アドレス対応インターフェイスでの認証マネージャ デバッグ メッセージを表示します。
errors	（任意）認証マネージャ エラー デバッグ メッセージをすべて表示します。
events	（任意）すべての認証マネージャ イベントのデバッグ メッセージ（レジストリおよび各種イベントを含む）を表示します。
feature	（任意）認証マネージャ機能のデバッグ メッセージを表示します。
guest_vlan	（任意）ゲスト VLAN 認証マネージャ メッセージを表示します。
mab_pm	（任意）MAC 認証マネージャ バイパス認証デバッグ メッセージを表示します。
mda	（任意）マルチドメイン認証マネージャ デバッグ メッセージを表示します。
multi_auth	（任意）マルチ認証マネージャ デバッグ認証メッセージを表示します。
switch_pm	（任意）スイッチ ポート マネージャ メッセージを表示します。
switch_sync	（任意）スイッチ、認証サーバ、および接続装置の間の同期メッセージを表示します。
sync	（任意）操作同期認証マネージャ デバッグ メッセージを表示します。
vlan_assign	（任意）VLAN-assignment デバッグ メッセージを表示します。
voice	（任意）音声 VLAN デバッグ メッセージを表示します。
webauth	（任意）Web 認証マネージャ デバッグ メッセージを表示します。

デフォルト

認証デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

undebug authentication コマンドは、**no debug authentication** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。

スタック メンバのデバッグをイネーブルにする場合は、**session switch-number** 特権 EXEC コマンドでスタック マスターからセッションを開始して、スタック メンバのコマンドライン プロンプトで **debug authentication** コマンドを入力できます。また、スタック マスター スイッチ上で **remote command** stack-member-number *LINE* 特権 EXEC コマンドを使用して、スタック メンバのデバッグをイネーブルにすることもできます。

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication violation	新しいデバイスがポートに接続するか、ポートに最大数のデバイスが接続した後で、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

debug auto qos

Automatic Quality of Service（auto-QoS）機能のデバッグをイネーブルにするには、**debug auto qos** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug auto qos

no debug auto qos

構文の説明

このコマンドには、キーワードと引数はありません。

デフォルト

auto-QoS デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。
12.2(18)SE	**debug autoqos** コマンドは、**debug auto qos** コマンドに替わりました。

使用上のガイドライン

auto-QoS がイネーブルのときに自動的に生成される Quality of Service（QoS）の設定を表示するには、auto-QoS をイネーブルにする前にデバッグをイネーブルにします。デバッグをイネーブルするには、**debug auto qos** 特権 EXEC コマンドを入力します。

undebug auto qos コマンドは、**no debug auto qos** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

例

次の例では、auto-QoS がイネーブルの場合に自動的に生成される QoS 設定を表示する方法を示します。

```
Switch# debug auto qos
AutoQoS debugging is on
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# auto qos voip cisco-phone

21:29:41: mls qos map cos-dscp 0 8 16 26 32 46 48 56
21:29:41: mls qos
21:29:42: no mls qos srr-queue input cos-map
21:29:42: no mls qos srr-queue output cos-map
21:29:42: mls qos srr-queue input cos-map queue 1 threshold 3 0
```

```
21:29:42: mls qos srr-queue input cos-map queue 1 threshold 2 1
21:29:42: mls qos srr-queue input cos-map queue 2 threshold 1 2
21:29:42: mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7
21:29:43: mls qos srr-queue input cos-map queue 2 threshold 3 3 5
21:29:43: mls qos srr-queue output cos-map queue 1 threshold 3 5
21:29:43: mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7
21:29:44: mls qos srr-queue output cos-map queue 3 threshold 3 2 4
21:29:44: mls qos srr-queue output cos-map queue 4 threshold 2 1
21:29:44: mls qos srr-queue output cos-map queue 4 threshold 3 0
21:29:44: no mls qos srr-queue input dscp-map
21:29:44: no mls qos srr-queue output dscp-map
21:29:44: mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15
21:29:45: mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7
21:29:45: mls qos srr-queue input dscp-map queue 1 threshold 3 32
21:29:45: mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
21:29:45: mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48
21:29:46: mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56
21:29:46: mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63
21:29:46: mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
21:29:47: mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47
21:29:47: mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47
21:29:47: mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
21:29:47: mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
21:29:48: mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
21:29:48: mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23
21:29:48: mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39
21:29:49: mls qos srr-queue output dscp-map queue 4 threshold 1 8
21:29:49: mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15
21:29:49: mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7
21:29:49: no mls qos srr-queue input priority-queue 1
21:29:49: no mls qos srr-queue input priority-queue 2
21:29:50: mls qos srr-queue input bandwidth 90 10
21:29:50: no mls qos srr-queue input buffers
21:29:50: mls qos queue-set output 1 buffers 10 10 26 54
21:29:50: interface GigabitEthernet2/0/1
21:29:50:  mls qos trust device cisco-phone
21:29:50:  mls qos trust cos
21:29:50:  no queue-set 1
21:29:50:  srr-queue bandwidth shape 10 0 0 0
21:29:50:  srr-queue bandwidth share 10 10 60 20
```

関連コマンド

コマンド	説明
auto qos voip	QoS ドメイン内で Voice over IP（VoIP）の auto-QoS を設定します。
show auto qos	auto-QoS 機能によって生成された初期設定を表示します。
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug backup

Flex Link バックアップ インターフェイスのデバッグをイネーブルにするには、**debug backup** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug backup {**all** | **errors** | **events** | **vlan-load-balancing**}

no debug backup {**all** | **errors** | **events** | **vlan-load-balancing**}

構文の説明

all	バックアップ インターフェイスのデバッグ メッセージをすべて表示します。
errors	バックアップ インターフェイスのエラーまたは例外デバッグ メッセージを表示します。
events	バックアップ インターフェイスのイベント デバッグ メッセージを表示します。
vlan-load-balancing	バックアップ インターフェイスの VLAN ロード バランシングを表示します。

デフォルト

バックアップ インターフェイス デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。
12.2(37)SE	**vlan-load-balancing** キーワードが追加されました。

使用上のガイドライン

undebug backup コマンドは、**no debug backup** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug cisp

Client Information Signalling Protocol（CISP）対応インターフェイス上で、デバッグ メッセージ交換およびイベントをイネーブルにするには、**debug cisp** グローバル コンフィギュレーション コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug cisp [all | errors | events | packets | sync]

no debug cisp [initialization | interface-configuration | rpc]

構文の説明

all	CISP デバッグ メッセージをすべて表示します。
errors	CISP デバッグ メッセージを表示します。
events	CISP イベント デバッグ メッセージを表示します。
packets	CISP パケット デバッグ メッセージを表示します。
sync	CISP 操作同期デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

undebug cisp コマンドは、**no debug cisp** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
cisp enable	Client Information Signalling Protocol（CISP）をイネーブルにします。
dot1x credentials（グローバル コンフィギュレーション）*profile*	プロファイルをサプリカント スイッチに設定します。
show cisp	指定されたインターフェイスの CISP 情報を表示します。

debug cluster

クラスタ固有イベントのデバッグをイネーブルにするには、**debug cluster** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug cluster {**discovery** | **events** | **extended** | **hsrp** | **http** | **ip** [**packet**] | **members** | **nat** | **neighbors** | **platform** | **snmp** | **vqpxy**}

no debug cluster {**discovery** | **events** | **extended** | **hsrp** | **http** | **ip** [**packet**] | **members** | **nat** | **neighbors** | **platform** | **snmp** | **vqpxy**}

構文の説明

discovery	クラスタ ディスカバリ デバッグ メッセージを表示します。
events	クラスタ イベント デバッグ メッセージを表示します。
extended	拡張ディスカバリ デバッグ メッセージを表示します。
hsrp	Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）デバッグ メッセージを表示します。
http	HTTP デバッグ メッセージを表示します。
ip [**packet**]	IP またはトランスポート パケット デバッグ メッセージを表示します。
members	クラスタ メンバ デバッグ メッセージを表示します。
nat	Network Address Translation（NAT; ネットワーク アドレス変換）デバッグ メッセージを表示します。
neighbors	クラスタ ネイバー デバッグ メッセージを表示します。
platform	プラットフォーム特定クラスタ デバッグ メッセージを表示します。
snmp	Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）デバッグ メッセージを表示します。
vqpxy	VLAN Query Protocol（VQP）プロキシ デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドが利用できるのは、クラスタ コマンド スイッチ スタックまたはクラスタ コマンド スイッチに限られます。

undebug cluster コマンドは、**no debug cluster** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプト

で **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。
show cluster candidates	コマンド スイッチ上で入力された場合に候補スイッチのリストを表示します。
show cluster members	コマンド スイッチ上で実行された場合にクラスタ メンバに関する情報を表示します。

debug dot1x

IEEE 802.1x 認証機能のデバッグをイネーブルにするには、**debug dot1x** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug dot1x {**all** | **errors** | **events** | **feature** | **packets** | **registry** | **state-machine**}

no debug dot1x {**all** | **errors** | **events** | **feature** | **packets** | **registry** | **state-machine**}

構文の説明

all	すべての IEEE 802.1x 認証デバッグ メッセージを表示します。
errors	IEEE 802.1x エラー デバッグ メッセージを表示します。
events	IEEE 802.1x イベント デバッグ メッセージを表示します。
feature	IEEE 802.1x 機能のデバッグ メッセージを表示します。
packets	IEEE 802.1x パケット デバッグ メッセージを表示します。
registry	IEEE 802.1x レジストリ呼び出しのデバッグ メッセージを表示します。
state-machine	ステート マシン関連イベント デバッグ メッセージを表示します。

（注）　**redundancy** キーワードは、コマンドラインのヘルプ ストリングには表示されますが、サポートされていません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**authsm**、**backend**、**besm**、**core**、および **reauthsm** キーワードは削除されました。**errors**、**events**、**packets registry**、および **state-machine** キーワードが追加されました。
12.2(25)SEE	**feature** キーワードが追加されました。

使用上のガイドライン

undebug dot1x コマンドは、**no debug dot1x** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show dot1x	スイッチまたは指定されたポートの IEEE 802.1x 統計情報、管理ステータス、および動作ステータスを表示します。

debug dtp

Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）アクティビティのデバッグをイネーブルにするには、**debug dtp** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug dtp {**aggregation** | **all** | **decision** | **events** | **oserrs** | **packets** | **queue** | **states** | **timers**}

no debug dtp {**aggregation** | **all** | **decision** | **events** | **oserrs** | **packets** | **queue** | **states** | **timers**}

構文の説明

aggregation	DTP ユーザ メッセージ アグリゲーション デバッグ メッセージを表示します。
all	すべての DTP デバッグ メッセージを表示します。
decision	DTP 決定テーブル デバッグ メッセージを表示します。
events	DTP イベント デバッグ メッセージを表示します。
oserrs	DTP オペレーティングシステム関連エラー デバッグ メッセージを表示します。
packets	DTP パケット処理デバッグ メッセージを表示します。
queue	DTP パケット キューイング デバッグ メッセージを表示します。
states	DTP ステート遷移デバッグ メッセージを表示します。
timers	DTP タイマー イベント デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug dtp コマンドは、**no debug dtp** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show dtp	スイッチまたは指定されたインターフェイスの DTP 情報を表示します。

debug eap

Extensible Authentication Protocol（EAP）のアクティビティをデバッグするには、**debug eap** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug dot1x {**all** | **authenticator** | **errors** | **events** | **md5** | **packets** | **peer** | **sm**}

no debug dot1x {**all** | **authenticator** | **errors** | **events** | **md5** | **packets** | **peer** | **sm**}

構文の説明

all	EAP デバッグ メッセージをすべて表示します。
authenticator	オーセンティケータ デバッグ メッセージを表示します。
errors	EAP エラー デバッグ メッセージを表示します。
events	EAP イベント デバッグ メッセージを表示します。
md5	EAP-MD5 デバッグ メッセージを表示します。
packets	EAP パケット デバッグ メッセージを表示します。
peer	EAP ピア デバッグ メッセージを表示します。
sm	EAP ステート マシン関連イベント デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

undebug dot1x コマンドは、**no debug dot1x** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show eap	スイッチまたは指定されたポートの EAP のレジストレーション情報およびセッション情報を表示します。

debug etherchannel

EtherChannel/Port Aggregation Protocol（PAgP; ポート集約プロトコル）シムのデバッグをイネーブルにするには、**debug etherchannel** 特権 EXEC コマンドを使用します。このシムは、Port Aggregation Protocol（PAgP）ソフトウェア モジュールとポート マネージャ ソフトウェア モジュール間のインターフェイスとなるソフトウェア モジュールです。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug etherchannel [**all** | **detail** | **error** | **event** | **idb**]

no debug etherchannel [**all** | **detail** | **error** | **event** | **idb**]

構文の説明

all	（任意）EtherChannel デバッグ メッセージをすべて表示します。
detail	（任意）EtherChannel デバッグ メッセージの詳細を表示します。
error	（任意）EtherChannel エラー デバッグ メッセージを表示します。
event	（任意）主な EtherChannel イベント メッセージをデバッグします。
idb	（任意）PAgP インターフェイス記述子ブロック デバッグ メッセージを表示します。

（注）　**linecard** キーワードは、コマンドラインのヘルプ ストリングには表示されますが、サポートされていません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

キーワードを指定しない場合は、すべてのデバッグ メッセージが表示されます。

undebug etherchannel コマンドは、**no debug etherchannel** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show etherchannel	チャネルの EtherChannel 情報を表示します。

debug ilpower

電源コントローラおよび Power over Ethernet（PoE）システムのデバッグをイネーブルにするには、**debug ilpower** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug ilpower {**cdp** | **controller** | **event** | **ha** | **port** | **powerman** | **registries**}

no debug ilpower {**cdp** | **controller** | **event** | **ha** | **port** | **powerman** | **registries**}

構文の説明

cdp	PoE Cisco Discovery Protocol（CDP）デバッグ メッセージを表示します。
controller	PoE コントローラ デバッグ メッセージを表示します。
event	PoE イベント デバッグ メッセージを表示します。
ha	PoE ハイ アベイラビリティ メッセージを表示します。
port	PoE ポート マネージャ デバッグ メッセージを表示します。
powerman	PoE 電力管理デバッグ メッセージを表示します。
registries	PoE レジストリ デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。
12.2(25)SE	**cdp**、**ha**、および **powerman** キーワードが追加されました。

使用上のガイドライン

このコマンドは、PoE 対応スイッチだけでサポートされています。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show controllers power inline	指定した PoE コントローラのレジスタ値を表示します。
show power inline	指定した PoE ポートまたはすべての PoE ポートの電源ステータスを表示します。

debug interface

インターフェイス関連のアクティビティのデバッグをイネーブルにするには、**debug interface** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug interface {*interface-id* | **null** *interface-number* | **port-channel** *port-channel-number* | **vlan** *vlan-id*}

no debug interface {*interface-id* | **null** *interface-number* | **port-channel** *port-channel-number* | **vlan** *vlan-id*}

構文の説明

interface-id	タイプ スイッチ番号 / モジュール番号 / ポート（例：**gigabitethernet 1/0/2**）によって識別される指定された物理ポートのデバッグ メッセージを表示します。
null *interface-number*	ヌル インターフェイスのデバッグ メッセージを表示します。*interface-number* は常に **0** です。
port-channel *port-channel-number*	指定された EtherChannel ポートチャネル インターフェイスのデバッグ メッセージを表示します。*port-channel-number* は 1 ～ 48 です。
vlan *vlan-id*	指定した VLAN のデバッグ メッセージを表示します。指定できる *vlan id* の範囲は 1 ～ 4094 です。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

キーワードを指定しない場合は、すべてのデバッグ メッセージが表示されます。

undebug interface コマンドは、**no debug interface** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show etherchannel	チャネルの EtherChannel 情報を表示します。

debug ip dhcp snooping

DHCP スヌーピングのデバッグをイネーブルにするには、**debug ip dhcp snooping** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug ip dhcp snooping {*mac-address* | **agent** | **event** | **packet**}

no debug ip dhcp snooping {*mac-address* | **agent** | **event** | **packet**}

構文の説明

mac-address	指定された MAC アドレスを持つ DHCP パケットのデバッグ メッセージを表示します。
agent	DHCP スヌーピング エージェントのデバッグ メッセージを表示します。
event	DHCP スヌーピング イベントのデバッグ メッセージを表示します。
packet	DHCP スヌーピングのデバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

undebug ip dhcp snooping コマンドは、**no debug ip dhcp snooping** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug ip verify source packet

IP 送信元ガードのデバッグをイネーブルにするには、**debug ip verify source packet** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug ip verify source packet

no debug ip verify source packet

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

undebug ip verify source packet コマンドは、**no debug ip verify source packet** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug ip igmp filter

Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）フィルタ イベントのデバッグをイネーブルにするには、**debug ip igmp filter** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug ip igmp filter

no debug ip igmp filter

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug ip igmp filter コマンドは、**no debug ip igmp filter** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug ip igmp max-groups

Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）最大グループ イベントのデバッグをイネーブルにするには、**debug ip igmp max-groups** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug ip igmp max-groups

no debug ip igmp max-groups

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug ip igmp max-groups コマンドは、**no debug ip igmp max-groups** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug ip igmp snooping

Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）スヌーピング アクティビティのデバッグをイネーブルにするには、**debug igmp snooping** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug ip igmp snooping [**group** | **management** | **querier** | **router** | **timer**]

no debug ip igmp snooping [**group** | **management** | **querier** | **router** | **timer**]

構文の説明

group	（任意）IGMP スヌーピング グループ アクティビティのデバッグ メッセージを表示します。
management	（任意）IGMP スヌーピング管理アクティビティのデバッグ メッセージを表示します。
querier	（任意）IGMP スヌーピング クエリア デバッグ メッセージを表示します。
router	（任意）IGMP スヌーピング ルータ アクティビティのデバッグ メッセージを表示します。
timer	（任意）IGMP スヌーピング タイマー イベントのデバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(25)SEA	**querier** キーワードが追加されました。

使用上のガイドライン

undebug ip igmp snooping コマンドは、**no debug ip igmp snooping** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
debug platform ip igmp snooping	プラットフォームに依存する IGMP スヌーピング アクティビティに関する情報を表示します。
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug lacp

Link Aggregation Control Protocol（LACP）のアクティビティのデバッグをイネーブルにするには、**debug lacp** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug lacp [**all** | **event** | **fsm** | **misc** | **packet**]

no debug lacp [**all** | **event** | **fsm** | **misc** | **packet**]

構文の説明

all	（任意）LACP デバッグ メッセージをすべて表示します。
event	（任意）LACP イベント デバッグ メッセージを表示します。
fsm	（任意）LACP 有限ステート マシン デバッグ メッセージを表示します。
misc	（任意）各種 LACP デバッグ メッセージを表示します。
packet	（任意）LACP パケット デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

undebug lacp コマンドは、**no debug lacp** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show lacp	LACP チャネル グループ情報を表示します。

debug lldp packets

Link Layer Discovery Protocol（LLDP）のパケットのデバッグをイネーブルにするには、**debug lldp packets** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug lldp packets

no debug lldp packets

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

undebug lldp packets コマンドは、**no debug lldp packets** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug mac-notification

MAC 通知イベントのデバッグをイネーブルにするには、**debug mac-notification** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug mac-notification

no debug mac-notification

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug mac-notification コマンドは、**no debug mac-notification** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show mac address-table notification	すべての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対する MAC アドレス通知情報を表示します。

debug matm

プラットフォーム独立 MAC アドレス管理のデバッグをイネーブルにするには、**debug matm** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug matm

no debug matm

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug matm コマンドは、**no debug matm** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
debug platform matm	プラットフォームに依存する MAC アドレス管理に関する情報を表示します。
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug matm move update

MAC アドレス テーブル移行更新メッセージ処理のデバッグをイネーブルにするには、**debug matm move update** 特権 EXEC コマンドを使用します。

debug matm move update

no debug matm move update

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

undebug matm move update コマンドは、**no debug matm move update** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
mac address-table move update {**receive** | **transmit**}	スイッチに MAC アドレス テーブル移行更新機能を設定します。
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show mac address-table move update	スイッチに MAC アドレス テーブル移行更新情報を表示します。

debug monitor

Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）機能のデバッグをイネーブルにするには、**debug monitor** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug monitor {**all** | **errors** | **idb-update** | **info** | **list** | **notifications** | **platform** | **requests** | **snmp**}

no debug monitor {**all** | **errors** | **idb-update** | **info** | **list** | **notifications** | **platform** | **requests** | **snmp**}

構文の説明

all	すべての SPAN デバッグ メッセージを表示します。
errors	詳細 SPAN エラー デバッグ メッセージを表示します。
idb-update	SPAN Interface Description Block（IDB; インターフェイス デスクリプション ブロック）更新トレース デバッグ メッセージを表示します。
info	SPAN 情報追跡デバッグ メッセージを表示します。
list	SPAN ポートおよび VLAN リスト追跡デバッグ メッセージを表示します。
notifications	SPAN 通知デバッグ メッセージを表示します。
platform	SPAN プラットフォーム追跡デバッグ メッセージを表示します。
requests	SPAN 要求デバッグ メッセージを表示します。
snmp	SPAN および Simple Network Management Protocol（SNMP）追跡デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug monitor コマンドは、**no debug monitor** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show monitor	スイッチ上の SPAN および Remote SPAN（RSPAN）セッションについてのすべての情報を表示します。

debug mvrdbg

Multicast VLAN Registration（MVR）のデバッグをイネーブルにするには、**debug mvrdbg** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug mvrdbg {**all** | **events** | **igmpsn** | **management** | **ports**}

no debug mvrdbg {**all** | **events** | **igmpsn** | **management** | **ports**}

構文の説明

all	MVR アクティビティ デバッグ メッセージをすべて表示します。
events	MVR イベント処理デバッグ メッセージを表示します。
igmpsn	MVR Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）スヌーピング アクティビティ デバッグ メッセージを表示します。
management	MVR 管理アクティビティ デバッグ メッセージを表示します。
ports	MVR ポート デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug mvrdbg コマンドは、**no debug mvrdbg** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show mvr	現在の MVR 設定を表示します。

debug nmsp

スイッチの Network Mobility Services Protocol（NMSP）のデバッグをイネーブルにするには、**debug nmsp** 特権 EXEC コマンドを使用します。このコマンドは、スイッチで暗号化ソフトウェア イメージが実行されている場合にだけ利用できます。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug nmsp {**all** | **connection** | **error** | **event** | **packet** | **rx** | **tx**}

no debug nmsp

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

undebug nmsp コマンドは、**no debug nmsp** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show nmsp	NMSP 情報を表示します。

debug nvram

NVRAM（不揮発性 RAM）のアクティビティのデバッグをイネーブルにするには、**debug nvram** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug nvram

no debug nvram

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug nvram コマンドは、**no debug nvram** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug pagp

Port Aggregation Protocol（PAgP; ポート集約プロトコル）のアクティビティのデバッグをイネーブルにするには、**debug pagp** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug pagp [**all** | **dual-active** | **event** | **fsm** | **misc** | **packet**]

no debug pagp [**all** | **dual-active** | **event** | **fsm** | **misc** | **packet**]

構文の説明

all	（任意）PAgP デバッグ メッセージをすべて表示します。
dual-active	（任意）デュアル アクティブ検出メッセージを表示します。
event	（任意）PAgP イベント デバッグ メッセージを表示します。
fsm	（任意）PAgP 有限ステート マシン デバッグ メッセージを表示します。
misc	（任意）各種 PAgP デバッグ メッセージを表示します。
packet	（任意）PAgP パケット デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(46)SE	**dual-active** キーワードが追加されました。

使用上のガイドライン

undebug pagp コマンドは、**no debug pagp** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show pagp	PAgP チャネル グループ情報を表示します。

debug platform acl

Access Control List（ACL; アクセス コントロール リスト）マネージャのデバッグをイネーブルにするには、**debug platform acl** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform acl {**all** | **exit** | **label** | **main** | **racl** | **stack** | **vacl** | **vlmap** | **warn**}

no debug platform acl {**all** | **exit** | **label** | **main** | **racl** | **stack** | **vacl** | **vlmap** | **warn**}

構文の説明

all	ACL マネージャ デバッグ メッセージをすべて表示します。
exit	ACL 終了関連デバッグ メッセージを表示します。
label	ACL ラベル関連デバッグ メッセージを表示します。
main	主な、または重要な ACL デバッグ メッセージを表示します。
racl	ルータ ACL 関連デバッグ メッセージを表示します。
stack	ACL スタック関連デバッグ メッセージを表示します。
vacl	VLAN ACL 関連デバッグ メッセージを表示します。
vlmap	ACL VLAN マップ関連デバッグ メッセージを表示します。
warn	ACL 警告関連デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform acl コマンドは、**no debug platform acl** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform backup interface

Flex Link プラットフォーム バックアップ インターフェイスのデバッグをイネーブルにするには、**debug platform backup interface** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform backup interface

no debug platform backup interface

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

プラットフォーム バックアップ インターフェイス デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

undebug platform backup interface コマンドは、**no debug platform backup interface** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform cisp

Client Information Signalling Protocol（CISP）対応インターフェイスが 1 つ以上あるスイッチのプラットフォーム レベル デバッグをイネーブルにするには、**debug platform cisp** グローバル コンフィギュレーション コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform cisp [initialization | interface-configuration | rpc]

no debug platform cisp [initialization | interface-configuration | rpc]

構文の説明

initialization	CISP 初期化シーケンスのデバッグをイネーブルにします。
interface-configuration	CISP 設定のデバッグをイネーブルにします。
rpc	CISP RPC 要求のデバッグをイネーブルにします。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

undebug platform cisp コマンドは、**no debug platform cisp** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session switch-number** 特権 EXEC コマンドでスタック マスターからセッションを開始して、スタック メンバのコマンドライン プロンプトで debug コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command stack-member-number** <*line*> 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
cisp enable	Client Information Signalling Protocol（CISP）をイネーブルにします。
dot1x credentials（グローバル コンフィギュレーション）*profile*	プロファイルをサプリカント スイッチに設定します。
show cisp	指定されたインターフェイスの CISP 情報を表示します。

debug platform cli-redirection main

主要（重要）な Command-Line Interface（CLI; コマンドライン インターフェイス）リダイレクション イベントのデバッグをイネーブルにするには、**debug platform cli-redirection main** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform cli-redirection main

no debug platform cli-redirection main

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform cli-redirection main コマンドは、**no debug platform cli-redirection main** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform configuration

スタック全体のコンフィギュレーション ファイル アクティビティのデバッグをイネーブルにするには、**debug platform configuration** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform configuration {**all** | **reception** | **transmission**}

no debug platform configuration {**all** | **reception** | **transmission**}

構文の説明

all	スタック全体のすべてのコンフィギュレーション ファイルの送受信イベントのデバッグ メッセージを表示します。
reception	他のスタック メンバからのコンフィギュレーション ファイル受信のデバッグ メッセージを表示します。
transmission	他のスタック メンバへのコンフィギュレーション ファイル送信のデバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform configuration コマンドは、**no debug platform configuration** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform cpu-queues

プラットフォーム CPU 受信キューのデバッグをイネーブルにするには、**debug platform cpu-queues** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform cpu-queues {broadcast-q | cbt-to-spt-q | cpuhub-q | host-q | icmp-q | igmp-snooping-q | layer2-protocol-q | logging-q | remote-console-q | routing-protocol-q | rpffail-q | software-fwd-q | stp-q}

no debug platform cpu-queues {broadcast-q | cbt-to-spt-q | cpuhub-q | host-q | icmp-q | igmp-snooping-q | layer2-protocol-q | logging-q | remote-console-q | routing-protocol-q | rpffail-q | software-fwd-q | stp-q}

構文の説明

broadcast-q	ブロードキャスト キューによって受信されたパケットに関するデバッグ メッセージを表示します。
cbt-to-spt-q	core-based tree to shortest-path tree（cbt-to-spt）キューによって受信されたパケットに関するデバッグ メッセージを表示します。
cpuhub-q	CPU ハートビート キューによって受信されたパケットに関するデバッグ メッセージを表示します。
host-q	ホスト キューによって受信されたパケットに関するデバッグ メッセージを表示します。
icmp-q	Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）キューによって受信されたパケットに関するデバッグ メッセージを表示します。
igmp-snooping-q	Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）スヌーピング キューによって受信されたパケットに関するデバッグ メッセージを表示します。
layer2-protocol-q	レイヤ 2 プロトコル キューによって受信されたパケットに関するデバッグ メッセージを表示します。
logging-q	ロギング キューによって受信されたパケットに関するデバッグ メッセージを表示します。
remote-console-q	リモート コンソール キューによって受信されたパケットに関するデバッグ メッセージを表示します。
routing-protocol-q	ルーティング プロトコル キューによって受信されたパケットに関するデバッグ メッセージを表示します。
rpffail-q	Reverse Path Forwarding（RPF）障害キューによって受信されたパケットに関するデバッグ メッセージを表示します。
software-fwd-q	ソフトウェア フォワーディング キューによって受信されたパケットをデバッグします。
stp-q	Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）キューによって受信されたパケットをデバッグします。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform cpu-queues コマンドは、**no debug platform cpu-queues** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform device-manager

プラットフォームに依存するデバイス マネージャのデバッグをイネーブルにするには、**debug platform device-manager** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform device-manager {**all** | **device-info** | **poll** | **port-download** | **trace**}

no debug platform device-manager {**all** | **device-info** | **poll** | **port-download** | **trace**}

構文の説明

all	プラットフォーム デバイス マネージャ デバッグ メッセージをすべて表示します。
device-info	プラットフォーム デバイス マネージャ デバイス構造デバッグ メッセージを表示します。
poll	プラットフォーム デバイス マネージャ 1 セカンド ポール デバッグ メッセージを表示します。
port-download	デバイス マネージャ Remote Procedure Call（RPC; リモート プロシージャ コール）使用状況デバッグ メッセージを表示します。
trace	プラットフォーム デバイス マネージャ機能の入口と出口のデバッグ メッセージを追跡します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform device-manager コマンドは、**no debug platform device-manager** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform dot1x

スタック関連 IEEE 802.1x イベントのデバッグをイネーブルにするには、**debug platform dot1x** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform dot1x {**initialization** | **interface-configuration** | **rpc**}

no debug platform dot1x {**initialization** | **interface-configuration** | **rpc**}

構文の説明

initialization	IEEE 802.1x 認証初期化シーケンス デバッグ メッセージを表示します。
interface-configuration	IEEE 802.1x インターフェイス コンフィギュレーション関連デバッグ メッセージを表示します。
rpc	IEEE 802.1x Remote Procedure Call（RPC）要求デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform dot1x コマンドは、**no debug platform dot1x** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform etherchannel

プラットフォームに依存する EtherChannel イベントのデバッグをイネーブルにするには、**debug platform etherchannel** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform etherchannel {**init** | **link-up** | **rpc** | **warnings**}

no debug platform etherchannel {**init** | **link-up** | **rpc** | **warnings**}

構文の説明

init	EtherChannel モジュール初期化デバッグ メッセージを表示します。
link-up	EtherChannel リンクアップおよびリンクダウンに関連したデバッグ メッセージを表示します。
rpc	EtherChannel Remote Procedure Call（RPC）デバッグ メッセージを表示します。
warnings	EtherChannel 警告デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform etherchannel コマンドは、**no debug platform etherchannel** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform fallback-bridging

プラットフォームに依存するフォールバック ブリッジング マネージャのデバッグをイネーブルにするには、**debug platform fallback-bridging** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform fallback-bridging [**error** | **retry** | **rpc** {**events** | **messages**}]

no debug platform fallback-bridging [**error** | **retry** | **rpc** {**events** | **messages**}]

構文の説明

error	（任意）フォールバック ブリッジング マネージャ エラー条件メッセージを表示します。
retry	（任意）フォールバック ブリッジング マネージャ リトライ メッセージを表示します。
rpc {**events** | **messages**}	（任意）フォールバック ブリッジング デバッグ情報を表示します。キーワードの意味は次のとおりです。 • **events** : Remote Procedure Call（RPC）イベントを表示します。 • **messages** : RPC メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

キーワードを指定しない場合、すべてのフォールバック ブリッジング マネージャ デバッグ メッセージが表示されます。

undebug platform fallback-bridging コマンドは、**no debug platform fallback-bridging** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform forw-tcam

フォワーディング Ternary CAM（TCAM）マネージャのデバッグをイネーブルにするには、**debug platform forw-tcam** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform forw-tcam [**adjustment** | **allocate** | **audit** | **error** | **move** | **read** | **write**]

no debug platform forw-tcam [**adjustment** | **allocate** | **audit** | **error** | **move** | **read** | **write**]

構文の説明

adjustment	（任意）TCAM マネージャ調整デバッグ メッセージを表示します。
allocate	（任意）TCAM マネージャ割り当てデバッグ メッセージを表示します。
audit	（任意）TCAM マネージャ監査メッセージを表示します。
error	（任意）TCAM マネージャ エラー メッセージを表示します。
move	（任意）TCAM マネージャ移行メッセージを表示します。
read	（任意）TCAM マネージャ読み込みメッセージを表示します。
write	（任意）TCAM マネージャ書き込みメッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

キーワードが指定されない場合、転送 TCAM マネージャ デバッグ メッセージがすべて表示されます。

undebug platform forw-tcam コマンドは、**no debug platform forw-tcam** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform frontend-controller

フロントエンド コントローラ アクティビティのデバッグをイネーブルにするには、**debug platform frontend-controller** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform frontend-controller {all | image | led | manager | poe | register | thermal}

no debug platform frontend-controller {all | image | led | manager | poe | register | thermal}

構文の説明

all	フロントエンド コントローラのデバッグ メッセージをすべて表示します。
image	Image Manager デバッグ メッセージを表示します。
led	LED デバッグ メッセージを表示します。
manager	フロントエンド コントローラ マネージャ デバッグ メッセージを表示します。
poe	Power over Ethernet（PoE）デバッグ メッセージを表示します。
register	Register Access デバッグ メッセージを表示します。
thermal	温度デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(20)SE3	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、PoE スイッチだけでサポートされています。

undebug platform frontend-controller コマンドは、**no debug platform frontend-controller** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show platform frontend-controller	フロントエンド コントローラ マネージャとその従属アプリケーションのカウンタおよびステータス情報を表示します。また、フロントエンド コントローラのハードウェアおよびソフトウェア情報を表示します。
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform ip arp inspection

ダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査イベントをデバッグするには、**debug platform ip arp inspection** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform ip arp inspection {**all** | **error** | **event** | **packet** | **rpc**}

no debug platform ip arp inspection {**all** | **error** | **event** | **packet** | **rpc**}

構文の説明

all	すべてのダイナミック ARP 検査デバッグ メッセージを表示します。
error	ダイナミック ARP 検査エラー デバッグ メッセージを表示します。
event	ダイナミック ARP 検査イベント デバッグ メッセージを表示します。
packet	ダイナミック ARP 検査パケット関連デバッグ メッセージを表示します。
rpc	ダイナミック ARP 検査 Remote Procedure Call（RPC）要求デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

undebug platform ip arp inspection コマンドは、**no debug platform ip arp inspection** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show inventory	ダイナミック ARP 検査の設定および動作ステートを表示します。
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform ip dhcp

DHCP イベントをデバッグするには、**debug platform ip dhcp** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform ip dhcp [**all** | **error** | **event** | **packet** | **rpc**]

no debug platform ip dhcp [**all** | **error** | **event** | **packet** | **rpc**]

構文の説明

all	（任意）DHCP デバッグ メッセージをすべて表示します。
error	（任意）DHCP エラー デバッグ メッセージを表示します。
event	（任意）DHCP イベント デバッグ メッセージを表示します。
packet	（任意）DHCP パケット関連デバッグ メッセージを表示します。
rpc	（任意）DHCP Remote Procedure Call（RPC）要求デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(19)EA1	このコマンドが追加されました。

使用上のガイドライン

undebug platform ip dhcp コマンドは、**no debug platform ip dhcp** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform ip igmp snooping

プラットフォーム依存型 Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）スヌーピングのデバッグをイネーブルにするには、**debug platform ip igmp snooping** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform ip igmp snooping {**all** | **di** | **error** | **event** | **group** | **mgmt** | **pak** | **retry** | **rpc** | **warn**}

debug platform ip igmp snooping pak {*ip-address* | **error** | **ipopt** | **leave**| **query** | **report** | **rx** | **svi** | **tx**}

debug platform ip igmp snooping rpc [**cfg** |**l3mm** | **misc** | **vlan**]

no debug platform ip igmp snooping {**all** | **di** | **error** | **event** | **group** | **mgmt** | **pak** | **retry** | **rpc** | **warn**}

構文の説明

all	すべての IGMP スヌーピング デバッグ メッセージを表示します。
di	IGMP スヌーピング宛先インデックス（di）調整 Remote Procedure Call（RPC）デバッグ メッセージを表示します。
error	IGMP スヌーピング エラー メッセージを表示します。
event	IGMP スヌーピング イベント デバッグ メッセージを表示します。
group	IGMP スヌーピング グループ デバッグ メッセージを表示します。
mgmt	IGMP スヌーピング管理デバッグ メッセージを表示します。
pak {*ip-address* | **error** | **ipopt** | **leave** | **query** | **report** | **rx** | **svi** | **tx**}	IGMP スヌーピング パケット イベント デバッグ メッセージを表示します。キーワードの意味は次のとおりです。 • *ip-address* : IGMP グループの IP アドレス • **error** : IGMP スヌーピング パケット エラー デバッグ メッセージを表示します。 • **ipopt** : IGMP スヌーピング IP ブリッジング オプション デバッグ メッセージを表示します。 • **leave** : IGMP スヌーピング脱退デバッグ メッセージを表示します。 • **query** : IGMP スヌーピング クエリー デバッグ メッセージを表示します。 • **report** : IGMP スヌーピング レポート デバッグ メッセージを表示します。 • **rx** : IGMP スヌーピング受信パケット デバッグ メッセージを表示します。 • **svi** : IGMP スヌーピング Switched Virtual Interface（SVI）パケット デバッグ メッセージを表示します。 • **tx** : IGMP スヌーピング送信パケット デバッグ メッセージを表示します。
retry	IGMP スヌーピング リトライ デバッグ メッセージを表示します。

rpc [**cfg** | **l3mm** | **misc** | **vlan**]	IGMP スヌーピング Remote Procedure Call（RPC）イベント デバッグ メッセージを表示します。キーワードの意味は次のとおりです。 • **cfg**：（任意）IGMP スヌーピング RPC デバッグ メッセージを表示します。 • **l3mm**：（任意）IGMP スヌーピング レイヤ 3 マルチキャスト ルータ グループ RPC デバッグ メッセージを表示します。 • **misc**：（任意）IGMP スヌーピングのその他の RPC デバッグ メッセージを表示します。 • **vlan**：（任意）IGMP スヌーピング VLAN アサート RPC デバッグ メッセージ
warn	IGMP スヌーピング警告メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform ip igmp snooping コマンドは、**no debug platform ip igmp snooping** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
debug ip igmp snooping	プラットフォーム独立 IGMP スヌーピング アクティビティに関する情報を表示します。
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform ip multicast

IP マルチキャスト ルーティングのデバッグをイネーブルにするには、**debug platform ip multicast** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform ip multicast {all | mdb | mdfs-rp-retry | midb | mroute-rp | resources | retry | rpf-throttle | snoop-events | software-forward | swidb-events | vlan-locks}

no debug platform ip multicast {all | mdb | mdfs-rp-retry | midb | mroute-rp | resources | retry | rpf-throttle | snoop-events | software-forward | swidb-events | vlan-locks}

構文の説明

all	すべてのプラットフォームの IP マルチキャスト イベント デバッグ メッセージを表示します。 （注）　このコマンドを使用すると、スイッチのパフォーマンスが悪化する可能性があります。
mdb	Multicast Distributed Fast Switching（MDFS）の Multicast Descriptor Block（MDB）イベントの IP マルチキャスト デバッグ メッセージを表示します。
mdfs-rp-retry	IP マルチキャスト MDFS の Randezvous Point（RP; ランデブー ポイント）のリトライ イベント デバッグ メッセージを表示します。
midb	IP マルチキャスト MDFS の Multicast Interface Descriptor Block（MIDB）のデバッグ メッセージを表示します。
mroute-rp	IP マルチキャスト RP イベントのデバッグ メッセージを表示します。
resources	IP マルチキャスト ハードウェア リソースのデバッグ メッセージを表示します。
retry	IP マルチキャスト リトライ処理イベントのデバッグ メッセージを表示します。
rpf-throttle	IP マルチキャストの Reverse Path Forwarding（RPF）スロットル イベントのデバッグ メッセージを表示します。
snoop-events	IP マルチキャスト IGMP スヌーピング イベントのデバッグ メッセージを表示します。
software-forward	IP マルチキャスト ソフトウェア転送イベントのデバッグ メッセージを表示します。
swidb-events	IP マルチキャスト MDFS の Software Interface Descriptor Block（SWIDB）またはグローバル イベントのデバッグ メッセージを表示します。
vlan-locks	IP マルチキャスト VLAN ロックおよびロック解除イベントのデバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform ip multicast コマンドは、**no debug platform ip multicast** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform ip source-guard

IP 送信元ガード イベントをデバッグするには、**debug platform ip source-guard** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform ip source-guard {**all** | **error** | **event**}

no debug platform ip source-guard {**all** | **error** | **event** }

構文の説明

all	すべての IP 送信元ガード プラットフォーム デバッグ メッセージを表示します。
error	IP 送信元ガード プラットフォーム エラー デバッグ メッセージを表示します。
event	IP 送信元ガード プラットフォーム イベント デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

undebug platform ip source-guard コマンドは、**no debug platform ip source-guard** コマンドと同じです。

関連コマンド

コマンド	説明
show ip verify source	IP 送信元ガードの設定を表示します。
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform ip unicast

プラットフォームに依存する IP ユニキャスト ルーティングのデバッグをイネーブルにするには、**debug platform ip unicast** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform ip unicast {adjacency | all | arp | dhcp | errors | events | interface | mpath | registries | retry | route | rpc | standby | statistics}

no debug platform ip unicast {adjacency | all | arp | dhcp | errors | events | interface | mpath | registries | retry | route | rpc | standby | statistics}

構文の説明

adjacency	IP ユニキャスト ルーティング隣接プログラミング イベントのデバッグ メッセージを表示します。
all	すべてのプラットフォームの IP ユニキャスト ルーティングのデバッグ メッセージを表示します。 **（注）** このコマンドを使用すると、スイッチのパフォーマンスが悪化する可能性があります。
arp	IP ユニキャスト ルーティングの Address Resolution Protocol（ARP; アドレス解決プロトコル）および ARP スロットリングのデバッグ メッセージを表示します。
dhcp	IP ユニキャスト ルーティング DHCP ダイナミック アドレス関連イベントのデバッグ メッセージを表示します。
errors	すべての IP ユニキャスト ルーティング エラーのデバッグ メッセージ（リソース割り当てエラーを含む）を表示します。
events	すべての IP ユニキャスト ルーティング イベントのデバッグ メッセージ（レジストリおよび各種イベントを含む）を表示します。
interface	IP ユニキャスト ルーティング インターフェイス イベントのデバッグ メッセージを表示します。
mpath	IP ユニキャスト ルーティング マルチパス隣接プログラミング イベントのデバッグ メッセージ（等価または不等価コスト ルーティングの実行時に発生）を表示します。
registries	IP ユニキャスト ルーティング Forwarding Information Database（FIB; 転送情報ベース）、隣接の追加、更新、および削除レジストリ イベントのデバッグ メッセージを表示します。
retry	Ternary CAM（TCAM）の割り当てエラーの発生した IP ユニキャスト ルーティング プログラム FIB のデバッグ メッセージを表示します。
route	IP ユニキャスト ルーティング FIB TCAM プログラミング イベントのデバッグ メッセージを表示します。
rpc	IP ユニキャスト ルーティング レイヤ 3 ユニキャスト Remote Procedure Call（RPC）相互作用のデバッグ メッセージを表示します。
standby	Hot Standby Routing Protocol（HSRP）の問題発生時のトラブルシューティングに役立つ、IP ユニキャスト ルーティング スタンバイ イベントのデバッグ メッセージを表示します。
statistics	IP ユニキャスト ルーティング統計情報収集関連イベントのデバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform ip unicast コマンドは、**no debug platform ip unicast** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform ip wccp

Web Cache Communication Protocol（WCCP）のデバッグをイネーブルにするには、**debug platform ip wccp** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform ip wccp {**acl** | **event** | **odm** | **trace**}

no debug platform ip wccp {**acl** | **event** | **odm** | **trace**}

（注）　このコマンドは、スイッチが IP サービス イメージを実行している場合だけ使用可能です。

構文の説明

acl	WCCP Access Control List（ACL; アクセス コントロール リスト）を表示します。
event	WCCP イベント デバッグ メッセージを表示します。
odm	WCCP OD マージ VMR を表示します。
trace	WCCP 実行をトレースします。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(37)SE	このコマンドが追加されました。

使用上のガイドライン

undebug platform ip wccp コマンドは、**no debug platform ip wccp** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform ipc

プラットフォーム依存 Interprocess Communication（IPC; プロセス間通信）プロトコルのデバッグをイネーブルにするには、**debug platform ipc** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform ipc {**all** | **init** | **receive** | **send** | **trace**}

no debug platform {**all** | **init** | **receive** | **send** | **trace**}

構文の説明

all	すべてのプラットフォーム IPC デバッグ メッセージを表示します。 （注）　このコマンドを使用すると、スイッチのパフォーマンスが悪化する可能性があります。
init	IPC 初期化関連デバッグ メッセージを表示します。
receive	IPC パケットがスイッチで受信されるたびに IPC 追跡を表示します。
send	IPC パケットをスイッチが送信するたびに IPC 追跡を表示します。
trace	IPC 機能の実行に従いコード パスを追跡する IPC 追跡デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform ipc コマンドは、**no debug platform ipc** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform led

Light-Emitting Diode（LED）動作のデバッグをイネーブルにするには、**debug platform led** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform led {**generic** | **signal** | **stack**}

no debug platform led {**generic** | **signal** | **stack**}

構文の説明

generic	LED 総称アクション デバッグ メッセージを表示します。
signal	LED 信号ビット マップ デバッグ メッセージを表示します。
stack	LED スタック アクション デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform led コマンドは、**no debug platform led** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform matm

プラットフォームに依存する MAC アドレス管理のデバッグをイネーブルにするには、**debug platform matm** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform matm {**aging** | **all** | **ec-aging** | **errors** | **learning** | **rpc** | **secure-address** | **warnings**}

no debug platform matm {**aging** | **all** | **ec-aging** | **errors** | **learning** | **rpc** | **secure-address** | **warnings**}

構文の説明

aging	MAC アドレス エージング デバッグ メッセージを表示します。
all	すべてのプラットフォーム MAC アドレス管理イベント デバッグ メッセージを表示します。
ec-aging	EtherChannel アドレス エージング関連デバッグ メッセージを表示します。
errors	MAC アドレス管理エラー メッセージを表示します。
learning	MAC アドレス管理アドレス学習デバッグ メッセージを表示します。
rpc	MAC アドレス管理 Remote Procedure Call（RPC）関連デバッグ メッセージを表示します。
secure-address	MAC アドレス管理セキュア アドレス学習デバッグ メッセージを表示します。
warning	MAC アドレス管理警告メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform matm コマンドは、**no debug platform matm** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
debug matm	プラットフォーム独立 MAC アドレス管理に関する情報を表示します。
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform messaging application

アプリケーション メッセージング アクティビティのデバッグをイネーブルにするには、**debug platform messaging application** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform messaging application {all | badpak | cleanup | events | memerr | messages | stackchg | usererr}

no debug platform messaging application {all | badpak | cleanup | events | memerr | messages | stackchg | usererr}

構文の説明

all	すべてのアプリケーション メッセージング デバッグ メッセージを表示します。
badpak	不良パケット デバッグ メッセージを表示します。
cleanup	クリーンアップ デバッグ メッセージを表示します。
events	イベント デバッグ メッセージを表示します。
memerr	メモリ エラー デバッグ メッセージを表示します。
messages	アプリケーション メッセージング デバッグ メッセージを表示します。
stackchg	スタック変更デバッグ メッセージを表示します。
usererr	ユーザ エラー デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform messaging application コマンドは、**no debug platform messaging application** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform phy

PHY（物理サブレイヤ）ドライバ情報のデバッグをイネーブルにするには、**debug platform phy** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform phy {**automdix** | **cablediag** | **dual-purpose** | **flcd** {**configure** | **ipc** | **iter** | **trace**} | **flowcontrol** | **forced** | **init-seq** | **link-status** | **read** | **sfp** | **show-controller** | **speed** | **write** | **xenpak**}

no debug platform phy {**automdix** | **cablediag** | **dual-purpose** | **flcd** {**configure** | **ipc** | **iter** | **trace**} | **flowcontrol** | **forced** | **init-seq** | **link-status** | **read** | **sfp** | **show-controller** | **speed** | **write** | **xenpak**}

構文の説明

automdix	PHY Automatic Medium-Dependent Interface Crossover（Auto-MDIX）デバッグ メッセージを表示します。
cablediag	PHY ケーブル診断デバッグ メッセージを表示します。
dual-purpose	PHY 兼用イベント デバッグ メッセージを表示します。
flcd {**configure** | **ipc** | **iter** | **trace**}	PHY FLCD デバッグ メッセージを表示します。キーワードの意味は次のとおりです。 • **configure**：PHY 設定デバッグ メッセージを表示します。 • **ipc**：Interprocess Communication（IPC; プロセス間通信）デバッグ メッセージを表示します。 • **iter**：iter デバッグ メッセージを表示します。 • **trace**：追跡デバッグ メッセージを表示します。
flowcontrol	PHY フロー制御デバッグ メッセージを表示します。
forced	PHY 強制モード デバッグ メッセージを表示します。
init-seq	PHY 初期化シーケンス デバッグ メッセージを表示します。
link-status	PHY リンクステータス デバッグ メッセージを表示します。
read	PHY 読み取りデバッグ メッセージを表示します。
sfp	PHY Small Form-factor Pluggable（SFP; 着脱可能小型フォーム ファクタ）モジュール デバッグ メッセージを表示します。
show-controller	PHY show-controller デバッグ メッセージを表示します。
speed	PHY 速度変更デバッグ メッセージを表示します。
write	PHY 書き込みデバッグ メッセージを表示します。
xenpak	PHY XENPAK デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**automdix** キーワードが追加されました。

使用上のガイドライン

undebug platform phy コマンドは、**no debug platform phy** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform pm

プラットフォームに依存するポート マネージャ ソフトウェア モジュールのデバッグをイネーブルにするには、**debug platform pm** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform pm {**all** | **counters** | **errdisable** | **etherchnl** | **exceptions** | **hpm-events** | **idb-events** | **if-numbers** | **ios-events** | **link-status** | **platform** | **pm-events** | **pm-span** | **pm-vectors** [**detail**] | **rpc** [**general** | **oper-info** | **state** | **vectors** | **vp-events**] | **soutput-vectors** | **stack-manager** | **sync** | **vlans**}

no debug platform pm {**all** | **counters** | **errdisable** | **etherchnl** | **exceptions** | **hpm-events** | **idb-events** | **if-numbers** | **ios-events** | **link-status** | **platform** | **pm-events** | **pm-span** | **pm-vectors** [**detail**] | **rpc** [**general** | **oper-info** | **state** | **vectors** | **vp-events**] | **soutput-vectors** | **stack-manager** | **sync** | **vlans**}

構文の説明

all	すべてのポート マネージャ デバッグ メッセージを表示します。
counters	Remote Procedure Call（RPC）デバッグ メッセージのカウンタを表示します。
errdisable	errdisable 関連イベント デバッグ メッセージを表示します。
etherchnl	EtherChannel 関連イベント デバッグ メッセージを表示します。
exceptions	システム例外デバッグ メッセージを表示します。
hpm-events	プラットフォーム ポート マネージャ イベント デバッグ メッセージを表示します。
idb-events	Interface Descriptor Block（IDB）関連イベント デバッグ メッセージを表示します。
if-numbers	インターフェイス番号トランスレーション イベント デバッグ メッセージを表示します。
ios-events	Cisco IOS イベント デバッグ メッセージを表示します。
link-status	インターフェイス リンク検出イベント デバッグ メッセージを表示します。
platform	ポート マネージャ機能イベント デバッグ メッセージを表示します。
pm-events	ポート マネージャ イベント デバッグ メッセージ を表示します。
pm-span	ポート マネージャ Switched Port Analyzer（SPAN）関連イベント デバッグ メッセージを表示します。
pm-vectors [**detail**]	ポート マネージャ ベクタ関連イベント デバッグ メッセージを表示します。キーワードの意味は次のとおりです。 • **detail**：ベクタ機能詳細を表示します。
rpc [**general** | **oper-info** | **state** | **vectors** | **vp-events**]	RPC 関連イベント デバッグ メッセージを表示します。キーワードの意味は次のとおりです。 • **general**：（任意）RPC 一般イベントを表示します。 • **oper-info**：（任意）操作および情報関連 RPC メッセージを表示します。 • **state**：（任意）管理および操作関連 RPC メッセージを表示します。 • **vectors**：（任意）ベクタ関連 RPC メッセージを表示します。 • **vp-events**：（任意）仮想ポート関連イベント RPC メッセージを表示します。

soutput-vectors	IDB 出力ベクタ イベント デバッグ メッセージを表示します。
stack-manager	スタック マネージャ関連イベント デバッグ メッセージを表示します。
sync	操作同期および VLAN ラインステート イベント デバッグ メッセージを表示します。
vlans	VLAN 作成および削除イベント デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform pm コマンドは、**no debug platform pm** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform port-asic

ポート Application-Specific Integrated Circuit（ASIC; 特定用途向け集積回路）ドライバのデバッグをイネーブルにするには、**debug platform port-asic** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform port-asic {interrupt | periodic | read | stack | write}

no debug platform port-asic {interrupt | periodic | read | stack | write}

構文の説明

interrupt	ポート ASIC 割り込み関連機能デバッグ メッセージを表示します。
periodic	ポート ASIC 定期機能コール デバッグ メッセージを表示します。
read	ポート ASIC 読み取りデバッグ メッセージを表示します。
stack	スタック関連機能デバッグ メッセージを表示します。
write	ポート ASIC 書き込みデバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform port-asic コマンドは、**no debug platform port-asic** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform port-security

プラットフォームに依存するポート セキュリティ情報のデバッグをイネーブルにするには、**debug platform port-security** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform port-security {**add** | **aging** | **all** | **delete** | **errors** | **rpc** | **warnings**}

no debug platform port-security {**add** | **aging** | **all** | **delete** | **errors** | **rpc** | **warnings**}

構文の説明

add	セキュア アドレス追加デバッグ メッセージを表示します。
aging	セキュア アドレス エージング デバッグ メッセージを表示します。
all	すべてのポート セキュリティ デバッグ メッセージを表示します。
delete	セキュア アドレス削除デバッグ メッセージを表示します。
errors	ポート セキュリティ エラー デバッグ メッセージを表示します。
rpc	Remote Procedure Call（RPC）デバッグ メッセージを表示します。
warnings	警告デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform port-security コマンドは、**no debug platform port-security** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform qos-acl-tcam

Quality of Service（QoS）および Access Control List（ACL; アクセス コントロール リスト）Ternary CAM（TCAM）マネージャ ソフトウェアのデバッグをイネーブルにするには、**debug platform qos-acl-tcam** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform qos-acl-tcam {**all** | **ctcam** | **errors** | **labels** | **mask** | **rpc** | **tcam**}

no debug platform qos-acl-tcam {**all** | **ctcam** | **errors** | **labels** | **mask** | **rpc** | **tcam**}

構文の説明

all	すべての QoS および ACL TCAM（QATM）マネージャ デバッグ メッセージを表示します。
ctcam	Cisco TCAM（CTCAM）関連イベント デバッグ メッセージを表示します。
errors	QATM エラー関連イベント デバッグ メッセージを表示します。
labels	QATM ラベル関連イベント デバッグ メッセージを表示します。
mask	QATM マスク関連イベント デバッグ メッセージを表示します。
rpc	QATM Remote Procedure Call（RPC）関連イベント デバッグ メッセージを表示します。
tcam	QATM TCAM 関連イベント デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform qos-acl-tcam コマンドは、**no debug platform qos-acl-tcam** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform remote-commands

リモート コマンドのデバッグをイネーブルにするには、**debug platform remote-commands** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform remote-commands

no debug platform remote-commands

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform remote-commands コマンドは、**no debug platform remote-commands** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform resource-manager

リソース マネージャ ソフトウェアのデバッグをイネーブルにするには、**debug platform resource-manager** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform resource-manager {**all** | **dm** | **erd** | **errors** | **madmed** | **sd** | **stats** | **vld**}

no debug platform resource-manager {**all** | **dm** | **erd** | **errors** | **madmed** | **sd** | **stats** | **vld**}

構文の説明

all	すべてのリソース マネージャ デバッグ メッセージを表示します。
dm	宛先マップ デバッグ メッセージを表示します。
erd	等価コスト ルート記述子テーブル デバッグ メッセージを表示します。
errors	エラー デバッグ メッセージを表示します。
madmed	MAC アドレス記述子テーブルおよびマルチエクスパンション記述子テーブル デバッグ メッセージを表示します。
sd	ステーション記述子テーブル デバッグ メッセージを表示します。
stats	統計デバッグ メッセージを表示します。
vld	VLAN リスト記述子デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform resource-manager コマンドは、**no debug platform resource-manager** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform snmp

プラットフォームに依存する Simple Network Management Protocol（SNMP）ソフトウェアのデバッグをイネーブルにするには、**debug platform snmp** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform snmp

no debug platform snmp

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform snmp コマンドは、**no debug platform snmp** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform span

プラットフォームに依存する Switched Port Analyzer（SPAN）ソフトウェアのデバッグをイネーブルにするには、**debug platform span** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform span

no debug platform span

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform span コマンドは、**no debug platform span** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform stack-manager

スタック マネージャ ソフトウェアのデバッグをイネーブルにするには、**debug platform stack-manager** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform stack-manager {all | rpc | sdp | sim | ssm | trace}

no debug platform stack-manager {all | rpc | sdp | sim | ssm | trace}

構文の説明

all	すべてのスタック マネージャ デバッグ メッセージを表示します。
rpc	スタック マネージャ Remote Procedure Call（RPC）使用状況デバッグ メッセージを表示します。
sdp	Stack Discovery Protocol（SDP）デバッグ メッセージを表示します。
sim	スタック情報モジュール デバッグ メッセージを表示します。
ssm	スタック ステートマシン デバッグ メッセージを表示します。
trace	スタック マネージャの入口と出口のデバッグ メッセージを追跡します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform stack-manager コマンドは、**no debug platform stack-manager** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform supervisor-asic

スーパーバイザ Application-Specific Integrated Circuit（ASIC; 特定用途向け集積回路）のデバッグをイネーブルにするには、**debug platform supervisor-asic** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform supervisor-asic {**all** | **errors** | **receive** | **send**}

no debug platform supervisor-asic {**all** | **errors** | **receive** | **send**}

構文の説明

all	すべてのスーパーバイザ ASIC イベント デバッグ メッセージを表示します。
errors	スーパーバイザ ASIC エラー デバッグ メッセージを表示します。
receive	スーパーバイザ ASIC 受信デバッグ メッセージを表示します。
send	スーパーバイザ ASIC 送信デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform supervisor-asic コマンドは、**no debug platform supervisor-asic** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform sw-bridge

ソフトウェア ブリッジング機能のデバッグをイネーブルにするには、**debug platform sw-bridge** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform sw-bridge {**broadcast** | **control** | **multicast** | **packet** | **unicast**}

no debug platform sw-bridge {**broadcast** | **control** | **multicast** | **packet** | **unicast**}

構文の説明

broadcast	ブロードキャスト データ デバッグ メッセージを表示します。
control	プロトコル パケット デバッグ メッセージを表示します。
multicast	マルチキャスト データ デバッグ メッセージを表示します。
packet	送受信データ デバッグ メッセージを表示します。
unicast	ユニキャスト データ デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform sw-bridge コマンドは、**no debug platform sw-bridge** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform tcam

Ternary CAM（TCAM）アクセスおよびルックアップのデバッグをイネーブルにするには、**debug platform tcam** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform tcam {**log** | **read** | **search** | **write**}

debug platform tcam log l2 {**acl** {**input** | **output**} | **local** | **qos**}

debug platform tcam log l3 {**acl** {**input** | **output**} | **ipv6** {**acl** {**input** | **output**} | **local** | **qos** | **secondary**} | **local** | **qos** | **secondary**}

debug platform tcam read {**reg** | **ssram** | **tcam**}

debug platform tcam search

debug platform tcam write {**forw-ram** | **reg** | **tcam**}

no debug platform tcam {**log** | **read** | **search** | **write**}

no debug platform tcam log l2 {**acl** {**input** | **output**} | **local** | **qos**}

no debug platform tcam log l3 {**acl** {**input** | **output**} | **ipv6** {**acl** {**input** | **output**} | **local** | **qos** | **secondary**} | **local** | **qos** | **secondary**}

no debug platform tcam read {**reg** | **ssram** | **tcam**}

no debug platform tcam search

no debug platform tcam write {**forw-ram** | **reg** | **tcam**}

構文の説明

log l2 {**acl** {**input** | **output**} | **local** | **qos**}	レイヤ 2 フィールド ベース CAM ルックアップ タイプ デバッグ メッセージを表示します。キーワードの意味は次のとおりです。 • **acl** {**input** | **output**}：入力または出力 ACL ルックアップ デバッグ メッセージを表示します。 • **local**：ローカル フォワーディング ルックアップ デバッグ メッセージを表示します。 • **qos**：分類および Quality of Service（QoS）ルックアップ デバッグ メッセージを表示します。

l3 {**acl** {**input** | **output**} | **ipv6** {**acl** {**input** | **output**} | **local** | **qos** | **secondary**} | **local** | **qos** | **secondary**}	レイヤ 3 フィールド ベース CAM ルックアップ タイプ デバッグ メッセージを表示します。キーワードの意味は次のとおりです。 • **acl** {**input** | **output**}：入力または出力 ACL ルックアップ デバッグ メッセージを表示します。 • **ipv6** {**acl** {**input** | **output**} | **local** | **qos** | **secondary**}：IPv6 ベース ルックアップ デバッグ メッセージを表示します。オプションには、入力または出力 ACL ルックアップ、ローカル フォワーディング ルックアップ、および QoS ルックアップ、またはセカンダリ フォワーディング ルックアップ デバッグ メッセージの表示が含まれます。 • **local**：ローカル フォワーディング ルックアップ デバッグ メッセージを表示します。 • **qos**：分類および Quality of Service（QoS）ルックアップ デバッグ メッセージを表示します。 • **secondary**：セカンダリ フォワーディング ルックアップ デバッグ メッセージを表示します。
read {**reg** | **ssram** | **tcam**}	TCAM 読み取りデバッグ メッセージを表示します。キーワードの意味は次のとおりです。 • **reg**：TCAM レジスタ読み取りデバッグ メッセージを表示します。 • **ssram**：Synchronous Static RAM（SSRAM）読み取りデバッグ メッセージを表示します。 • **tcam**：TCAM 読み取りデバッグ メッセージを表示します。
search	スーパーバイザ主導 TCAM サーチ結果デバッグ メッセージを表示します。
write {**forw-ram** | **reg** | **tcam**}	TCAM 書き込みデバッグ メッセージを表示します。キーワードの意味は次のとおりです。 **forw-ram**：フォワーディング RAM 書き込みデバッグ メッセージを表示します。 **reg**：TCAM レジスタ書き込みデバッグ メッセージを表示します。 **tcam**：TCAM 書き込みデバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform tcam コマンドは、**no debug platform tcam** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform udld

プラットフォームに依存する Unidirectional Link Detection（UDLD; 単方向リンク検出）ソフトウェアのデバッグをイネーブルにするには、**debug platform udld** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform udld [**all** | **error** | **rpc** {**events** | **messages**}]

no debug platform udld [**all** | **error** | **rpc** {**events** | **messages**}]

構文の説明

all	（任意）UDLD デバッグ メッセージをすべて表示します。
error	（任意）エラー条件デバッグ メッセージを表示します。
rpc {**events** | **messages**}	（任意）UDLD Remote Procedure Call（RPC）デバッグ メッセージを表示します。キーワードの意味は次のとおりです。 • **events** : UDLD RPC イベントを表示します。 • **messages** : UDLD RPC メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform udld コマンドは、**no debug platform udld** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform vlan

VLAN マネージャ ソフトウェアのデバッグをイネーブルにするには、**debug platform vlan** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform vlan {**errors** | **mvid** | **rpc**}

no debug platform vlan {**errors** | **mvid** | **rpc**}

構文の説明

errors	VLAN エラー デバッグ メッセージを表示します。
mvid	マッピングされた VLAN ID の割り当ておよびフリー デバッグ メッセージを表示します。
rpc	Remote Procedure Call（RPC）デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug platform vlan コマンドは、**no debug platform vlan** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug pm

Port Manager（PM; ポート マネージャ）アクティビティのデバッグをイネーブルにするには、**debug pm** 特権 EXEC コマンドを使用します。PM は、すべての論理および物理インターフェイスを制御するステート マシンです。VLAN や UniDirectional Link Detection（UDLD; 単一方向リンク検出）などを含むすべての機能は、ポート マネージャと連携して、スイッチに機能を提供します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug pm {all | assert | card | etherchnl | hatable | messages | port | redundancy | registry | sm | span | split | vlan | vp}

no debug pm {all | assert | card | etherchnl | hatable | messages | port | redundancy | registry | sm | span | split | vlan | vp}

構文の説明

all	すべての PM デバッグ メッセージを表示します。
assert	アサート デバッグ メッセージを表示します。
card	ラインカード関連イベント デバッグ メッセージを表示します。
etherchnl	EtherChannel 関連イベント デバッグ メッセージを表示します。
hatable	Host Access Table イベント デバッグ メッセージを表示します。
messages	PM デバッグ メッセージを表示します。
port	ポート関連イベント デバッグ メッセージを表示します。
redundancy	冗長デバッグ メッセージを表示します。
registry	PM レジストリ呼び出しデバッグ メッセージを表示します。
sm	ステート マシン関連イベント デバッグ メッセージを表示します。
span	スパニング ツリー関連イベント デバッグ メッセージを表示します。
split	スプリットプロセッサ デバッグ メッセージを表示します。
vlan	VLAN 関連イベント デバッグ メッセージを表示します。
vp	仮想ポート関連イベント デバッグ メッセージを表示します。

（注）　**scp** および **pvlan** キーワードはコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**hatable** キーワードが追加されました。

使用上のガイドライン

undebug pm コマンドは、**no debug pm** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug port-security

ポート セキュリティ サブシステムの割り当ておよびステートのデバッグをイネーブルにするには、**debug port-security** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug port-security

no debug port-security

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug port-security コマンドは、**no debug port-security** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show port-security	インターフェイスまたはスイッチのポート セキュリティ設定を表示します。

debug qos-manager

Quality of Service（QoS）マネージャ ソフトウェアのデバッグをイネーブルにするには、**debug qos-manager** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug qos-manager {**all** | **event** | **verbose**}

no debug qos-manager {**all** | **event** | **verbose**}

構文の説明

all	すべての QoS マネージャ デバッグ メッセージを表示します。
event	QoS マネージャ関連イベント デバッグ メッセージを表示します。
verbose	QoS マネージャ詳細デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug qos-manager コマンドは、**no debug qos-manager** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug spanning-tree

スパニング ツリーのアクティビティのデバッグをイネーブルにするには、**debug spanning-tree** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug spanning-tree {**all** | **backbonefast** | **bpdu** | **bpdu-opt** | **config** | **csuf/csrt** | **etherchannel** | **events** | **exceptions** | **general** | **mstp** | **pvst+** | **root** | **snmp** | **switch** | **synchronization** | **uplinkfast**}

no debug spanning-tree {**all** | **backbonefast** | **bpdu** | **bpdu-opt** | **config** | **csuf/csrt** | **etherchannel** | **events** | **exceptions** | **general** | **mstp** | **pvst+** | **root** | **snmp** | **switch** | **synchronization** | **uplinkfast**}

構文の説明

all	スパニング ツリーのデバッグ メッセージをすべて表示します。
backbonefast	BackboneFast イベント デバッグ メッセージを表示します。
bpdu	スパニング ツリー UniDirectional Link Detection（UDLD; 単一方向リンク検出）デバッグ メッセージを表示します。
bpdu-opt	最適化された BPDU 処理デバッグ メッセージを表示します。
config	スパニング ツリー設定変更デバッグ メッセージを表示します。
csuf/csrt	クロススタック UplinkFast およびクロススタック高速遷移アクティビティ デバッグ メッセージを表示します。
etherchannel	EtherChannel サポート デバッグ メッセージを表示します。
events	スパニング ツリー トポロジ イベント デバッグ メッセージを表示します。
exceptions	スパニング ツリー例外デバッグ メッセージを表示します。
general	一般的なスパニング ツリー アクティビティ デバッグ メッセージを表示します。
mstp	Multiple Spanning-Tree Protocol（MSTP）イベントをデバッグします。
pvst+	Per-VLAN Spanning-Tree Plus（PVST+）イベント デバッグ メッセージを表示します。
root	スパニング ツリー ルート イベント デバッグ メッセージを表示します。
snmp	スパニング ツリー Simple Network Management Protocol（SNMP）処理デバッグ メッセージを表示します。
synchronization	スパニング ツリー同期イベント デバッグ メッセージを表示します。
switch	スイッチ シム コマンド デバッグ メッセージを表示します。このシムは、一般的な Spanning-Tree Protocol（STP）コードと、各スイッチ プラットフォーム固有コードとの間のインターフェイスとなるソフトウェア モジュールです。
uplinkfast	UplinkFast イベント デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**mstp** および **csuf/csrt** キーワードが追加されました。

使用上のガイドライン

undebug spanning-tree コマンドは、**no debug spanning-tree** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show spanning-tree	スパニング ツリー ステート情報を表示します。

debug spanning-tree backbonefast

スパニング ツリー BackboneFast イベントのデバッグをイネーブルにするには、**debug spanning-tree backbonefast** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug spanning-tree backbonefast [**detail** | **exceptions**]

no debug spanning-tree backbonefast [**detail** | **exceptions**]

構文の説明

detail	（任意）BackboneFast デバッグ メッセージの詳細を表示します。
exceptions	（任意）スパニング ツリー BackboneFast 例外のデバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug spanning-tree backbonefast コマンドは、**no debug spanning-tree backbonefast** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show spanning-tree	スパニング ツリー ステート情報を表示します。

debug spanning-tree bpdu

送受信されたスパニング ツリー UniDirectional Link Detection（UDLD; 単一方向リンク検出）のデバッグをイネーブルにするには、**debug spanning-tree bpdu** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug spanning-tree bpdu [**receive** | **transmit**]

no debug spanning-tree bpdu [**receive** | **transmit**]

構文の説明

receive	（任意）受信 BPDU 用非最適化パスのデバッグ メッセージを表示します。
transmit	（任意）送信された BPDU デバッグ メッセージについて、最適化されないパスを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug spanning-tree bpdu コマンドは、**no debug spanning-tree bpdu** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show spanning-tree	スパニング ツリー ステート情報を表示します。

debug spanning-tree bpdu-opt

最適化されたスパニング ツリー UniDirectional Link Detection（UDLD; 単一方向リンク検出）処理のデバッグをイネーブルにするには、**debug spanning-tree bpdu-opt** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug spanning-tree bpdu-opt [**detail** | **packet**]

no debug spanning-tree bpdu-opt [**detail** | **packet**]

構文の説明

detail	（任意）最適化された BPDU 処理デバッグ メッセージの詳細を表示します。
packet	（任意）パケット レベルの最適化された BPDU 処理デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug spanning-tree bpdu-opt コマンドは、**no debug spanning-tree bpdu-opt** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show spanning-tree	スパニング ツリー ステート情報を表示します。

debug spanning-tree mstp

Multiple Spanning-Tree Protocol（MSTP）ソフトウェアのデバッグをイネーブルにするには、**debug spanning-tree mstp** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug spanning-tree mstp {all | boundary | bpdu-rx | bpdu-tx | errors | flush | init | migration | pm | proposals | region | roles | sanity_check | sync | tc | timers}

no debug spanning-tree mstp {all | boundary | bpdu-rx | bpdu-tx | errors | flush | init | migration | pm | proposals | region | roles | sanity_check | sync | tc | timers}

構文の説明

all	デバッグ メッセージをすべてイネーブルにします。
boundary	次に示す境界上でのフラグ変更をデバッグします。 • Multiple Spanning-Tree（MST）リージョンと、Rapid Spanning-Tree Protocol（RSTP）が稼動する単一のスパニング ツリー リージョンとの境界 • MST リージョンと、802.1D が稼動する単一のスパニング ツリー リージョンとの境界 • MST リージョンと、設定が異なる別の MST リージョンとの境界
bpdu-rx	受信した MST UniDirectional Link Detection（UDLD; 単一方向リンク検出）をデバッグします。
bpdu-tx	送信された MST BPDU をデバッグします。
errors	MSTP エラーをデバッグします。
flush	ポート フラッシュ メカニズムをデバッグします。
init	MSTP データ構造の初期化をデバッグします。
migration	プロトコル移行ステート マシンをデバッグします。
pm	MSTP ポート マネージャ イベントをデバッグします。
proposals	指定スイッチとルート スイッチ間のハンドシェイク メッセージをデバッグします。
region	Switch Processor（SP; スイッチ プロセッサ）と Route Processor（RP; ルート プロセッサ）間のリージョン同期をデバッグします。
roles	MSTP のロールをデバッグします。
sanity_check	受信した BPDU の正常性確認メッセージをデバッグします。
sync	ポート同期イベントをデバッグします。
tc	トポロジ変更通知イベントをデバッグします。
timers	開始、停止、および期限切れイベントの MSTP タイマーをデバッグします。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

undebug spanning-tree mstp コマンドは、**no debug spanning-tree mstp** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show spanning-tree	スパニング ツリー ステート情報を表示します。

debug spanning-tree switch

Spanning-Tree Protocol（STP）ソフトウェア モジュールとポート マネージャ ソフトウェア モジュール間のソフトウェア インターフェイスのデバッグをイネーブルにするには、**debug spanning-tree switch** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug spanning-tree switch {all | errors | flush | general | helper | pm | rx {decode | errors | interrupt | process} | state | tx [decode] | uplinkfast}

no debug spanning-tree switch {all | errors | flush | general | helper | pm | rx {decode | errors | interrupt | process} | state | tx [decode] | uplinkfast}

構文の説明

all	スパニング ツリー スイッチのデバッグ メッセージをすべて表示します。
errors	スパニング ツリー ソフトウェア モジュールとポート マネージャ ソフトウェア モジュール間のインターフェイスに関するデバッグ メッセージを表示します。
flush	シム フラッシュ動作に関するデバッグ メッセージを表示します。
general	一般イベント デバッグ メッセージを表示します。
helper	スパニング ツリー ヘルパー タスク デバッグ メッセージを表示します。ヘルパー タスクは大容量スパニング ツリー更新を処理します。
pm	ポート マネージャ イベント デバッグ メッセージを表示します。
rx	受信した UniDirectional Link Detection（UDLD; 単一方向リンク検出）処理のデバッグ メッセージを表示します。キーワードの意味は次のとおりです。 • **decode**：デコード済み受信パケットを表示します。 • **errors**：受信エラー デバッグ メッセージを表示します。 • **interrupt**：Interrupt Service Request（ISR）デバッグ メッセージを表示します。 • **process**：処理受信 BPDU デバッグ メッセージを表示します。
state	スパニング ツリー ポート ステート変更デバッグ メッセージを表示します。
tx [decode]	送信された BPDU 処理デバッグ メッセージを表示します。キーワードの意味は次のとおりです。 • **decode**：（任意）デコードされた送信パケットを表示します。
uplinkfast	UplinkFast パケット送信デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.1(14)EA1	**flush** および **uplinkfast** キーワードが追加されました。

使用上のガイドライン

undebug spanning-tree switch コマンドは、**no debug spanning-tree switch** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show spanning-tree	スパニング ツリー ステート情報を表示します。

debug spanning-tree uplinkfast

スパニング ツリー UplinkFast イベントのデバッグをイネーブルにするには、**debug spanning-tree uplinkfast** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug spanning-tree uplinkfast [**exceptions**]

no debug spanning-tree uplinkfast [**exceptions**]

構文の説明

exceptions	（任意）スパニング ツリー UplinkFast 例外のデバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug spanning-tree uplinkfast コマンドは、**no debug spanning-tree uplinkfast** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show spanning-tree	スパニング ツリー ステート情報を表示します。

debug sw-vlan

VLAN マネージャのアクティビティのデバッグをイネーブルにするには、**debug sw-vlan** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug sw-vlan {badpmcookies | cfg-vlan {bootup | cli} | events | ifs | management | mapping | notification | packets | redundancy | registries | vtp}

no debug sw-vlan {badpmcookies | cfg-vlan {bootup | cli} | events | ifs | management | mapping | notification | packets | redundancy | registries | vtp}

構文の説明

badpmcookies	不良ポート マネージャ クッキーの VLAN マネージャ インシデントに関するデバッグ メッセージを表示します。
cfg-vlan {bootup | cli}	config-vlan デバッグ メッセージを表示します。キーワードの意味は次のとおりです。 • **bootup**：スイッチがブートアップするときにメッセージを表示します。 • **cli**：Command-Line Interface（CLI）が config-vlan モードである場合のメッセージを表示します。
events	VLAN マネージャ イベントのデバッグ メッセージを表示します。
ifs	**debug sw-vlan ifs** コマンドを参照してください。
management	内部 VLAN の VLAN マネージャ管理のデバッグ メッセージを表示します。
mapping	VLAN マッピングのデバッグ メッセージを表示します。
notification	**debug sw-vlan notification** コマンドを参照してください。
packets	パケット処理およびカプセル化プロセスのデバッグ メッセージを表示します。
redundancy	VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）VLAN 冗長性のデバッグ メッセージを表示します。
registries	VLAN マネージャ レジストリのデバッグ メッセージを表示します。
vtp	**debug sw-vlan vtp** コマンドを参照してください。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug sw-vlan コマンドは、**no debug sw-vlan** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプト

で **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show vlan	管理ドメインに設定されたすべての VLAN または特定の VLAN（VLAN 名または ID を指定した場合）のパラメータを表示します。
show vtp	VTP 管理ドメイン、ステータス、およびカウンタに関する一般情報を表示します。

debug sw-vlan ifs

VLAN マネージャ IOS File System（IFS）エラー テストのデバッグをイネーブルにするには、**debug sw-vlan ifs** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug sw-vlan ifs {**open** {**read** | **write**} | **read** {**1** | **2** | **3** | **4**} | **write**}

no debug sw-vlan ifs {**open** {**read** | **write**} | **read** {**1** | **2** | **3** | **4**} | **write**}

構文の説明

open {**read** | **write**}	VLAN マネージャ IFS ファイルオープン操作デバッグ メッセージを表示します。キーワードの意味は次のとおりです。 • **read** : VLAN マネージャ IFS ファイル読み取り動作のデバッグ メッセージを表示します。 • **write** : VLAN マネージャ IFS ファイル書き込み操作デバッグ メッセージを表示します。
read {**1** | **2** | **3** | **4**}	指定されたエラー テスト（1、2、3、または 4）に関するファイル読み取り動作のデバッグ メッセージを表示します。
write	ファイル書き込み動作のデバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug sw-vlan ifs コマンドは、**no debug sw-vlan ifs** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

ファイルの読み取り処理に処理 **1** を選択すると、ヘッダー検証ワードおよびファイル バージョン番号が格納されたファイル ヘッダーが読み込まれます。処理 **2** を指定すると、ドメインおよび VLAN 情報の大部分が格納されたファイル本体が読み取られます。処理 **3** を指定すると、Type Length Version（TLV）記述子構造が読み取られます。処理 **4** を指定すると、TLV データが読み取られます。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show vlan	管理ドメインに設定されたすべての VLAN または特定の VLAN（VLAN 名または ID を指定した場合）のパラメータを表示します。

debug sw-vlan notification

Inter-Link Switch（ISL; スイッチ間リンク）VLAN ID のアクティブ化および非アクティブ化のデバッグをイネーブルにするには、**debug sw-vlan notification** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug sw-vlan notification {accfwdchange | allowedvlancfgchange | fwdchange | linkchange | modechange | pruningcfgchange | statechange}

no debug sw-vlan notification {accfwdchange | allowedvlancfgchange | fwdchange | linkchange | modechange | pruningcfgchange | statechange}

構文の説明

accfwdchange	集約アクセス インターフェイス スパニング ツリー転送変更に関する VLAN マネージャ通知のデバッグ メッセージを表示します。
allowedvlancfgchange	許可 VLAN の設定変更に関する VLAN マネージャ通知のデバッグ メッセージを表示します。
fwdchange	スパニング ツリー転送変更に関する VLAN マネージャ通知のデバッグ メッセージを表示します。
linkchange	インターフェイス リンクステート変更の VLAN マネージャ通知のデバッグ メッセージを表示します。
modechange	インターフェイス モード変更の VLAN マネージャ通知のデバッグ メッセージを表示します。
pruningcfgchange	プルーニング設定変更の VLAN マネージャ通知のデバッグ メッセージを表示します。
statechange	インターフェイス ステート変更の VLAN マネージャ通知のデバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug sw-vlan notification コマンドは、**no debug sw-vlan notification** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show vlan	管理ドメインに設定されたすべての VLAN または特定の VLAN（VLAN 名または ID を指定した場合）のパラメータを表示します。

debug sw-vlan vtp

VLAN Trunking Protocol（VTP）コードのデバッグをイネーブルにするには、**debug sw-vlan vtp** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug sw-vlan vtp {**events** | **packets** | **pruning** [**packets** | **xmit**] | **redundancy** | **xmit**}

no debug sw-vlan vtp {**events** | **packets** | **pruning** | **redundancy** | **xmit**}

構文の説明

events	汎用の論理フローのデバッグ メッセージおよび VTP コード内の VTP_LOG_RUNTIME マクロによって生成された VTP メッセージの詳細を表示します。
packets	IOS VTP プラットフォーム依存層から VTP コードに渡されたすべての着信 VTP パケット（プルーニング パケットを除く）の内容のデバッグ メッセージを表示します。
pruning [**packets** | **xmit**]	VTP コードのプルーニング セグメントによって生成されるデバッグ メッセージを表示します。キーワードの意味は次のとおりです。 • **packets** :（任意）IOS VTP プラットフォーム依存層から VTP コードに渡されたすべての着信 VTP プルーニング パケットの内容のデバッグ メッセージを表示します。 • **xmit** :（任意）VTP コードが IOS VTP プラットフォーム依存層に送信するように要求したすべての発信 VTP パケットの内容のデバッグ メッセージを表示します。
redundancy	VTP 冗長性のデバッグ メッセージを表示します。
xmit	VTP コードが IOS VTP プラットフォーム依存層に送信するように要求したすべての発信 VTP パケット（プルーニング パケットを除く）の内容のデバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug sw-vlan vtp コマンドは、**no debug sw-vlan vtp** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

pruning キーワードの後にパラメータを指定しない場合は、VTP プルーニング デバッグ メッセージが表示されます。これらのメッセージは、VTP プルーニング コード内の VTP_PRUNING_LOG_NOTICE、VTP_PRUNING_LOG_INFO、VTP_PRUNING_LOG_DEBUG、VTP_PRUNING_LOG_ALERT、および VTP_PRUNING_LOG_WARNING マクロによって生成されます。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show vtp	VTP 管理ドメイン、ステータス、およびカウンタに関する一般情報を表示します。

debug udld

UniDirectional Link Detection（UDLD; 単一方向リンク検出）機能のデバッグをイネーブルにするには、**debug udld** 特権 EXEC コマンドを使用します。UDLD デバッ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。

debug udld {**events** | **packets** | **registries**}

no debug udld {**events** | **packets** | **registries**}

構文の説明

events	UDLD プロセス イベントが発生したときのデバッグ メッセージを表示します。
packets	UDLD プロセスがパケット キューからパケットを受信し、UDLD プロトコル コードの要求に応答してそれらを送信するときに、このプロセスのデバッグ メッセージを表示します。
registries	UDLD プロセスが UDLD プロセスに依存するモジュールおよびその他のフィーチャ モジュールからのレジストリ コールを処理するときに、このプロセスのデバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug udld コマンドは、**no debug udld** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

debug udld events を入力すると、次に示すデバッグ メッセージが表示されます。

- 一般的な UDLD プログラム論理フロー
- ステート マシンのステート変更
- errdisable ステートの設定および消去のプログラム アクション
- ネイバー キャッシュの追加および削除
- コンフィギュレーション コマンドの処理
- リンクアップおよびリンクダウン通知処理

debug udld packets を入力すると、次に示すデバッグ メッセージが表示されます。

- 着信パケット受信時の一般的なパケット処理プログラム フロー
- 受信したパケットをパケット受信コードで調べるときの、各パケットの内容の識別情報（Type Length Version（TLV）など）
- パケット送信の試行内容およびその成果

debug udld registries を入力すると、次に示すカテゴリのデバッグ メッセージが表示されます。

- サブブロックの作成
- ファイバポート ステータスの変更
- ポート マネージャ ソフトウェアからのステート変更通知情報
- MAC アドレス レジストリ コール

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show udld	すべてのポートまたは指定されたポートの UDLD の管理ステータスおよび動作ステータスを表示します。

debug vqpc

VLAN Query Protocol（VQP）クライアントのデバッグをイネーブルにするには、**debug vqpc** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug vqpc [**all** | **cli** | **events** | **learn** | **packet**]

no debug vqpc [**all** | **cli** | **events** | **learn** | **packet**]

構文の説明

all	（任意）VQP クライアント デバッグ メッセージをすべて表示します。
cli	（任意）VQP クライアント Command-Line Interface（CLI; コマンドライン インターフェイス）デバッグ メッセージを表示します。
events	（任意）VQP クライアント イベント デバッグ メッセージを表示します。
learn	（任意）VQP クライアント アドレス学習デバッグ メッセージを表示します。
packet	（任意）VQP クライアント パケット情報デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

undebug vqpc コマンドは、**no debug vqpc** コマンドと同じです。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform wireless-controller

Catalyst 3750G Integrated Wireless LAN Controller スイッチの内部ワイヤレス LAN コントローラのデバッグをイネーブルにするには、**debug platform wireless-controller** 特権 EXEC コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug platform wireless-controller {**all** | **packets** | **session** | **sm** | **wcp**}

no debug platform wireless-controller {**all** | **packets** | **session** | **sm** | **wcp**}

構文の説明

all	ワイヤレス コントローラ デバッグ メッセージをすべて表示します。
packets	Wireless LAN Control Protocol（WCP; ワイヤレス LAN 制御プロトコル）パケットのデバッグ メッセージを表示します。
session	ワイヤレス コントローラ セッション デバッグ メッセージを表示します。
sm	ワイヤレス コントローラ ステート マシン デバッグ メッセージを表示します。
wcp	WCP デバッグ メッセージをすべて表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(25)FZ	このコマンドが追加されました。

使用上のガイドライン

undebug platform wireless-controller コマンドは、**no debug platform wireless-controller** コマンドと同じです。

このコマンドは、Catalyst 3750G Wireless LAN Controller スイッチだけに適用されます。

デバッグをイネーブルにすると、スタック マスターだけでデバッグがイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでスタック マスターからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、スタック マスター スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用します。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show platform wireless-controller	内部ワイヤレス コントローラに関する情報を表示します。

APPENDIX C

Catalyst 3750 スイッチ Show Platform コマンド

この付録では、Catalyst 3750 スイッチ用に作成または変更された **show platform** 特権 EXEC コマンドについて説明します。これらのコマンドは、インターネットワーキングの問題の診断および解決に役立つ情報を表示します。使用する場合には、必ずシスコのテクニカル サポート担当者の指示に従ってください。

show platform acl

プラットフォームに依存する Access Control List（ACL; アクセス コントロール リスト）マネージャ情報を表示するには、**show platform acl** 特権 EXEC コマンドを使用します。

show platform acl {**interface** *interface-id* | **label** *label-number* [**detail**] | **statistics** *asic-number* | **usage** *asic-number* [**summary**] | **vlan** *vlan-id*} [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface *interface-id*	指定されたインターフェイスについて、インターフェイス単位の ACL マネージャ情報を表示します。このインターフェイスには物理インターフェイスまたは VLAN を指定できます。
label *label-number* [**detail**]	ラベル単位の ACL マネージャ情報を表示します。*label-number* に指定できる範囲は 0 ～ 255 です。キーワードの意味は次のとおりです。 • **detail**：（任意）ACL マネージャ ラベル情報の詳細を表示します。
statistics *asic-number*	ASIC 単位の ACL マネージャ情報を表示します。*asic-number* に指定できる範囲は、0 または 1 のいずれかのポート ASIC 番号です。
usage *asic-number* [**summary**]	ASIC 単位の ACL 使用状況情報を表示します。キーワードの意味は次のとおりです。 • **summary**：（任意）使用状況情報の概要を表示します。
vlan *vlan-id*	VLAN 単位の ACL マネージャ情報を表示します。*vlan-id* に指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform backup interface

Flex Link 設定で使用されるプラットフォーム依存型バックアップ情報を表示するには、**show platform backup interface** 特権 EXEC コマンドを使用します。

show platform backup interface [*interface-id* | **dummyQ**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface-id	（任意）すべての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対するバックアップ情報を表示します。このインターフェイスには物理インターフェイスまたはポート チャネルを指定できます。
dummyQ	（任意）ダミー キュー情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(20)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform configuration

プラットフォームに依存するコンフィギュレーション マネージャ関連情報を表示するには、**show platform configuration** 特権 EXEC コマンドを使用します。

show platform configuration {**config-output** | **default** | **running** | **startup**} [| {**begin** | **exclude** | **include**} ***expression***]

構文の説明

config-output	最後の自動設定アプリケーションの出力を表示します。
default	システムがデフォルト設定を実行しているかどうかを表示します。
running	ローカル スイッチのバックアップ実行コンフィギュレーションのスナップショットを表示します。
startup	ローカル スイッチのバックアップ スタートアップ コンフィギュレーションのスナップショットを表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform etherchannel

プラットフォームに依存する EtherChannel 情報を表示するには、**show platform etherchannel** 特権 EXEC コマンドを使用します。

show platform etherchannel {**flags** | **time-stamps**} [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

flags	EtherChannel ポート フラグを表示します。
time-stamps	EtherChannel タイム スタンプを表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform forward

ハードウェアが指定されたパラメータと一致するフレームを転送する方法を指定するには、インターフェイスの **show platform forward** 特権 EXEC コマンドを使用します。

show platform forward *interface-id* [**vlan** *vlan-id*] *src-mac dst-mac* [*l3protocol-id*] [**ipv6** | **sap** | **snap**] [**cos** *cos*] [**ip** *src-ip dst-ip* [**frag** *field*] [**dscp** *dscp*] {*l4protocol-id* | **icmp** *icmp-type icmp-code* | **igmp** *igmp-version igmp-type* | **sctp** *src-port dst-port* | **tcp** *src-port dst-port flags* | **udp** *src-port dst-port*]} [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

interface-id	パケットがスイッチに着信するポートとなる入力物理インターフェイス。
vlan *vlan-id*	（任意）入力 VLAN ID。指定できる範囲は 1 ～ 4094 です。この値が指定されず、入力インターフェイスがルーテッド ポートでない場合、デフォルトは 1 です。
src-mac	48 ビット送信元 MAC アドレス。
dst-mac	48 ビット宛先 MAC アドレス。
l3protocol-id	（任意）パケットで使用されるレイヤ 3 プロトコル。指定できる範囲は 0 ～ 65535 です。
ipv6	（任意）IPv6 フレーム。
sap	（任意）Service Access Point（SAP; サービス アクセス ポイント）カプセル化タイプ
snap	（任意）Subnetwork Access Protocol（SNAP; サブネットワーク アクセス プロトコル）カプセル化タイプ
cos *cos*	（任意）フレームの Class of Service（CoS; サービス クラス）値。指定できる範囲は 0 ～ 7 です。
ip *src-ip dst-ip*	（任意、ただし IP パケットの場合は必須）ドット付き 10 進表記の送信元および宛先 IP アドレス。
frag *field*	（任意）フラグメント IP パケットの IP フラグメント フィールド。指定できる範囲は 0 ～ 65535 です。
dscp *dscp*	（任意）IP ヘッダーの Differentiated Service Code Point（DSCP）フィールド。指定できる範囲は 0 ～ 63 です。
l4protocol-id	IP ヘッダーのレイヤ 4 プロトコル フィールドの数値。指定できる範囲は 0 ～ 255 です。たとえば、47 は Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）であり、89 は Open Shortest Path First（OSPF）です。プロトコルが TCP、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）、または Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）である場合、数値の代わりに適切なキーワードを使用する必要があります。
icmp *icmp-type icmp-code*	ICMP パラメータ。*icmp-type* および *icmp-code* に指定できる範囲は 0 ～ 255 です。
igmp *igmp-version igmp-type*	IGMP パラメータ。指定できる範囲は、*igmp-version* は 1 ～ 15、*igmp-type* は 0 ～ 15 です。
sctp *src-port dst-port*	Stream Control Transmission Protocol（SCTP）パラメータ。SCTP 送信元および宛先ポートに指定できる範囲は 0 ～ 65535 です。

tcp *src-port dst-port flags*	TCP パラメータ：TCP 送信元ポート、宛先ポート、ヘッダーの TCP フラグ バイトの数値。*src-port* および *dst-port* に指定できる範囲は 0 ～ 65535 です。指定できるフラグ範囲は 0 ～ 1024 です。
udp *src-port dst-port*	UDP パラメータ。*src-port* および *dst-port* に指定できる範囲は 0 ～ 65535 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(25)SEB	**ipv6** キーワードが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

show platform forward コマンドの出力表示およびその例の意味については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Troubleshooting」の章を参照してください。

show platform frontend-controller

フロントエンド コントローラ マネージャとその従属アプリケーションのカウンタおよびステータス情報、およびフロントエンド コントローラのハードウェアおよびソフトウェア情報を表示するには、**show platform frontend-controller** 特権 EXEC コマンドを使用します。

show platform frontend-controller {**buffer** | **generic** | **manager** *number* | **subordinate** *number* | **version** *number*} [| {**begin** | **exclude** | **include**} *expression*]

（注）　このコマンドは、Catalyst 3750G-48TS、3750G-48PS、3750G-24TS-1U、および 3750G-24PS スイッチでだけサポートされます。

構文の説明

buffer	マネージャから従属アプリケーションに送信された最後の 1024 バイトを表示します。または、従属アプリケーションからマネージャに送信された最後の 1024 バイトを表示します。
generic	マネージャまたは従属アプリケーションに限定的に適用されるわけではない一般的なカウンタを表示します。
manager *number*	*number* で指定されたマネージャおよび従属アプリケーションのカウンタを表示します。*number* の範囲については、「使用上のガイドライン」を参照してください。
subordinate *number*	*number* で指定された従属アプリケーションの従属ステータスおよびカウンタを表示します。*number* の範囲については、「使用上のガイドライン」を参照してください。
version *number*	*number* で指定された従属ステータスのハードウェアおよびソフトウェアバージョン情報を表示します。*number* の範囲については、「使用上のガイドライン」を参照してください。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(20)SE3	このコマンドが追加されました。

使用上のガイドライン

Catalyst 3750G-48TS および 3750G-48PS スイッチでは、指定できる下位番号の範囲は 0 ～ 2 です。

Catalyst 3750G-24TS-1U および 3750G-24PS スイッチでは、指定できる下位番号の範囲は 0 ～ 1 です。

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform ip igmp snooping

プラットフォームに依存する Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）スヌーピング情報を表示するには、**show platform ip igmp snooping** 特権 EXEC コマンドを使用します。

show platform ip igmp snooping {**all** | **control** [**di**] | **counters** | **flood** [**vlan** *vlan-id*] | **group** *ip-address* | **hardware** | **retry** [**count** | **local** [**count**] | **remote** [**count**]]} [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

all	すべての IGMP スヌーピング プラットフォーム IP マルチキャスト情報を表示します。
control [**di**]	IGMP スヌーピング コントロール エントリを表示します。キーワードの意味は次のとおりです。 • **di**：（任意）IGMP スヌーピング コントロール宛先インデックス エントリを表示します。
counters	IGMP スヌーピング カウンタを表示します。
flood [**vlan** *vlan-id*]	IGMP スヌーピング フラッディング情報を表示します。キーワードの意味は次のとおりです。 • **vlan** *vlan-id*：（任意）指定された VLAN のフラッディング情報を表示します。指定できる範囲は 1 ～ 4094 です。
group *ip-address*	IGMP スヌーピング マルチキャスト グループ情報を表示します。ここで、*ip-address* はグループの IP アドレスです。
hardware	ハードウェアにロードされた IGMP スヌーピング情報を表示します。
retry [**count** | **local** [**count**]	IGMP スヌーピング再試行情報を表示します。キーワードの意味は次のとおりです。 • **count**：（任意）再試行回数だけを表示します。 • **local**：（任意）ローカル再試行エントリを表示します。
remote [**count**]	リモート エントリを表示します。キーワードの意味は次のとおりです。 • **count**：（任意）リモート カウントだけを表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform ip multicast

プラットフォームに依存する IP マルチキャスト テーブルおよび他の情報を表示するには、**show platform ip multicast** 特権 EXEC コマンドを使用します。

show platform ip multicast {**acl-full-info**| **counters** | **groups** | **hardware** [**detail**] | **interfaces** | **locks** | **mdfs-routes** | **mroute-retry** | **retry** | **vrf** | **trace**} [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

acl-full-info	IP マルチキャスト ルーティング Access Control List（ACL; アクセス コントロール リスト）情報、特にハードウェアで出力のルータ ACL が適用されない発信 VLAN の数を表示します。
counters	IP マルチキャスト カウンタと統計を表示します。
groups	グループごとの IP マルチキャスト ルータを表示します。
hardware [**detail**]	ハードウェアにロードされた IP マルチキャスト ルートを表示します。任意の **detail** キーワードは、宛先インデックスおよびルート インデックスのポート メンバ を表示するために使用します。
interfaces	IP マルチキャスト インターフェイスを表示します。
locks	IP マルチキャスト宛先インデックス ロックを表示します。
mdfs-routes	Multicast Distributed Fast Switching（MDFS）IP マルチキャスト ルートを表示します。
mroute-retry	IP マルチキャスト ルート リトライ キューを表示します。
retry	リトライ キューの IP マルチキャスト ルートを表示します。
vrf	VPN ルーティングおよび転送インスタンスを表示します。
trace	IP マルチキャスト トレース バッファを表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(40)SE	**vrf** キーワードが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform ip unicast

プラットフォームに依存する IP ユニキャスト ルーティング情報を表示するには、**show platform ip unicast** 特権 EXEC コマンドを使用します。

show platform ip unicast {**adjacency** | **cef-idb** | **counts** | **dhcp** | **failed** {**adjacency** | **arp** [*A.B.C.D*] | **route**} | **loadbalance** | **mpaths** | **proxy** | **route** | **standby** | **statistics** | **table** | **trace**} [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

adjacency	プラットフォーム隣接データベースを表示します。
cef-idb	Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）インターフェイス記述子ブロックに対応するプラットフォーム情報を表示します。
counts	レイヤ 3 ユニキャスト データベースのカウントを表示します。
dhcp	DHCP システム ダイナミック アドレスを表示します。
failed {**adjacency** | **arp** [*A.B.C.D*] | **route**}	ハードウェア リソース障害を表示します。キーワードの意味は次のとおりです。 • **adjacency**：ハードウェアでのプログラミングに失敗した隣接エントリを表示します。 • **arp**：障害および再試行による Address Resolution Protocol（ARP; アドレス解決プロトコル）削除を表示します。 • *A.B.C.D*：（任意）表示する ARP エントリのプレフィクス。 • **route**：ハードウェアでプログラミングされなかったルート エントリを表示します。
loadbalance	プラットフォーム ロードバランス データベースを表示します。
mpaths	レイヤ 3 ユニキャスト ルーティング マルチパス隣接データベースを表示します。
proxy	プラットフォーム プロキシ ARP データベースを表示します。
route	プラットフォーム ルート データベースを表示します。
standby	プラットフォーム スタンバイ情報を表示します。
statistics	レイヤ 3 ユニキャスト ルーティング累積統計を表示します。
table	プラットフォーム IP version 4（IPv4）情報を表示します。
trace	プラットフォーム イベント トレース ログを表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

（注）　**proxy** および **table** キーワードは、コマンドラインのヘルプ ストリングには表示されますが、サポートされていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform ip unicast vrf compaction

圧縮要求キューおよび圧縮ステータスを表示するには、**show platform ip unicast vrf compaction** 特権 EXEC コマンドを使用します。

show platform ip unicast vrf compaction [| {begin | exclude | include} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(25)SEC	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

show platform ip unicast vrf tcam-label

PBR および VRF-Lite ラベルと、PBR で使用されているラベルの数を表示するには、**show platform ip unicast vrf tcam-label** 特権 EXEC コマンドを使用します。

show platform ip unicast vrf tcam-label [| {begin | exclude | include} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(25)SEC	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

show platform ip wccp

プラットフォームに依存する Web Cache Communication Protocol（WCCP）の情報を表示するには、**show platform ip wccp** 特権 EXEC コマンドを使用します。

show platform ip wccp {**detail** | **label**} [| {**begin** | **exclude** | **include**} *expression*]

（注）　このコマンドは、スイッチが IP サービス イメージを実行している場合だけ使用可能です。

構文の説明

detail	プラットフォーム WCCP の詳細を表示します。
label	プラットフォーム WCCP のラベルを表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(37)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude outpu**t と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform ipc trace

プラットフォーム依存 Interprocess Communication（IPC; プロセス間通信）プロトコル追跡ログ情報を表示するには、**show platform ipc trace** 特権 EXEC コマンドを使用します。

show platform ipc trace [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform ipv6 unicast

プラットフォームに依存する IPv6 ユニキャスト ルーティング情報を表示するには、**show platform ipv6 unicast** 特権 EXEC コマンドを使用します。このコマンドは、スタックが IP サービス イメージを稼動している場合にだけ利用できます。

show platform ipv6 unicast {**adjacency** [*ipv6-prefix*] | **backwalk** {**adjacency** | **loadbalance**} | **compress** *ipv6-prefix/prefix length* | **interface** | **loadbalance** | **mpath** | **retry** {**adjacency** | **route**} | **route** [*ipv6-prefix/prefix length* | **tcam**] [**detail**] | **statistics** | **table** [**detail**] | **trace**}
[| {**begin** | **exclude** | **include**} *expression*]

構文の説明

adjacency	スイッチまたは指定された IPv6 ネットワークの IPv6 隣接情報を表示します。
ipv6-prefix	（任意）表示する IPv6 ネットワーク。この引数には RFC2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。
backwalk {**adjacency** | **loadbalance**}	IPv6 バックウォーク情報を表示します。 • **adjacency**：隣接バックウォーク情報を表示します。 • **loadbalance**：バックウォーク ロードバランス情報を表示します。
compress *ipv6-prefix/prefix length*	IPv6 プレフィクス圧縮情報を表示します。 • *ipv6-prefix*：IPv6 ネットワークです。 • */prefix length*：IPv6 ネットワーク プレフィクスの長さです。アドレスの上位何ビットがプレフィクス（アドレスのネットワーク部）であるかを示す、0 ～ 128 の 10 進値。スラッシュ記号を 10 進値の前に付ける必要があります。
interface	IPv6 インターフェイス情報を表示します。
loadbalance	IPv6 ロードバランス情報を表示します。
mpath	IPv6 マルチパス情報を表示します。
retry {**adjacency** | **route**}	IPv6 リトライ情報を表示します。 • **adjacency**：IPv6 隣接リトライ情報を表示します。 • **route**：IPv6 ルート リトライ情報を表示します。
route	IPv6 ルート情報を表示します。
tcam	（任意）IPv6 TCAM ルート テーブル情報を表示します。
detail	（任意）IPv6 ルート情報の詳細を表示します。
statistics	IPv6 累積統計を表示します。
table	IPv6 ユニキャスト テーブル情報を表示します。
trace	IPv6 ユニキャスト トレースを表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(25)SEA	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude outpu**t と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform layer4op

プラットフォームに依存するレイヤ 4 演算子情報を表示するには、**show platform layer4op** 特権 EXEC コマンドを使用します。

show platform layer4op {**acl** | **pacl** [*port-asic*] | **qos** [*port-asic*]} {**and-or** | **map** | **or-and** | **vcu**} [|{**begin** | **exclude** | **include**} *expression*]

構文の説明

acl	Access Control List（ACL; アクセス コントロール リスト）レイヤ 4 演算子情報を表示します。
pacl [*port-asic*]	ポート ACL レイヤ 4 演算子情報を表示します。キーワードの意味は次のとおりです。 • *port-asic*：（任意）ポート ASIC 番号を表示します。
qos [*port-asic*]	Quality of Service（QoS）レイヤ 4 演算子情報を表示します。キーワードの意味は次のとおりです。 • *port-asic*：（任意）QoS ポート ASIC 番号を表示します。
and-or	AND-OR レジスタ情報を表示します。
map	選択マップ情報を表示します。
or-and	OR-AND レジスタ情報を表示します。
vcu	Value Compare Unit（VCU）レジスタ情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform mac-address-table

プラットフォームに依存する MAC アドレス テーブル情報を表示するには、**show platform mac-address-table** 特権 EXEC コマンドを使用します。

show platform mac-address-table [**aging-array** | **hash-table** | **mac-address** *mac-address*] [**vlan** *vlan-id*]] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

aging-array	（任意）MAC アドレス テーブル エージング アレイを表示します。
hash-table	（任意）MAC アドレス テーブル ハッシュ テーブルを表示します。
mac-address *mac-address*	（任意）MAC アドレス テーブル MAC アドレス情報を表示します。ここで、*mac-address* は 48 ビット ハードウェア アドレスです。
vlan *vlan-id*	（任意）指定された VLAN の情報を表示します。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform messaging

プラットフォームに依存するアプリケーションおよびパフォーマンス メッセージ情報を表示するには、**show platform messaging** 特権 EXEC コマンドを使用します。

show platform messaging {**application** [**incoming** | **outgoing** | **summary**] | **hiperf** [*class-number*]} [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

application [**incoming** | **outgoing** | **summary**]	アプリケーション メッセージ情報を表示します。キーワードの意味は次のとおりです。 • **incoming**：（任意）着信アプリケーション メッセージング要求に関する情報だけを表示します。 • **outgoing**：（任意）発信アプリケーション メッセージング要求に関する情報だけを表示します。 • **summary**：（任意）アプリケーション メッセージング要求すべてに関するサマリー情報を表示します。
hiperf [*class-number*]	発信するハイパフォーマンス メッセージ情報を表示します。特定のクラス番号のハイパフォーマンス メッセージについての情報を表示するには、*class-number* オプションを指定します。指定できる範囲は 0 ～ 36 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude outpu**t と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform monitor

プラットフォームに依存する Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）情報を表示するには、**show platform monitor** 特権 EXEC コマンドを使用します。

show platform monitor [**session** *session-number*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

session *session-number*	（任意）指定された SPAN セッションの SPAN 情報を表示します。指定できる範囲は 1 ～ 66 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform mvr table

プラットフォームに依存する Multicast VLAN Registration（MVR; マルチキャスト VLAN レジストレーション）Multi-Expansion Descriptor（MED）グループ マッピング テーブルを表示するには、**show platform mvr table** 特権 EXEC コマンドを使用します。

show platform mvr table [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude outpu**t と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform pm

プラットフォームに依存するポート マネージャ情報を表示するには、**show platform pm** 特権 EXEC コマンドを使用します。

show platform pm {**counters** | **group-masks** | **idbs** {**active-idbs** | **deleted-idbs**} | **if-numbers** | **link-status** | **platform-block** | **port-info** *interface-id* | **stack-view** | **vlan** {**info** | **line-state**}
[| {**begin** | **exclude** | **include**} *expression*]

構文の説明

counters	モジュール カウンタ情報を表示します。
group-masks	EtherChannel グループ マスク情報を表示します。
idbs {**active-idbs** | **deleted-idbs**}	Interface Data Block（IDB）情報を表示します。キーワードの意味は次のとおりです。 • **active-idbs**：アクティブ IDB 情報を表示します。 • **deleted-idbs**：削除または漏えいされた IDB 情報を表示します。
if-numbers	インターフェイス番号情報を表示します。
link-status	ローカル ポート リンク ステータス情報を表示します。
platform-block	プラットフォーム ポート ブロック情報を表示します。
port-info *interface-id*	指定されたインターフェイスのポート管理フィールドおよび動作フィールドを表示します。
stack-view	スタックのステータス情報を表示します。
vlan {**info** | **line-state**}	プラットフォーム VLAN 情報を表示します。キーワードの意味は次のとおりです。 • **info**：アクティブ VLAN の情報を表示します。 • **line-state**：ラインステート情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform port-asic

プラットフォームに依存するポート ASIC レジスタ情報を表示するには、**show platform port-asic** 特権 EXEC コマンドを使用します。

show platform port-asic {**cpu-queue-map-table** [**asic** *number* | **port** *number* [**asic** *number*]] |
dest-map index *number* |
etherchannel-info [**asic** *number* | **port** *number* [**asic** *number*]] |
exception [**asic** *number* | **port** *number* [**asic** *number*]] |
global-status [**asic** *number* | **port** *number* [**asic** *number*]] |
learning [**asic** *number* | **port** *number* [**asic** *number*]] |
mac-info [**asic** *number* | **port** *number* [**asic** *number*]] |
mvid [**asic** *number*] |
packet-info-ram [**asic** *number* | **index** *number* [**asic** *number*]] |
port-info [**asic** *number* | **port** *number* [**asic** *number*]] |
prog-parser [**asic** *number* | **port** *number* [**asic** *number*]] |
receive {**buffer-queue** | **port-fifo** | **supervisor-sram**} [**asic** *number* | **port** *number* [**asic** *number*]] |
span [*vlan-id* [**asic** *number*] | [**asic** *number*]
stack {**control** | **dest-map** | **learning** | **messages** | **mvid** | **prog-parser** | **span** | **stats** [**asic** *number* | **port** *number* [**asic** *number*]}
stats {**drop** | **enqueue** | **miscellaneous** | **supervisor**} [**asic** *number* | **port** *number* [**asic** *number*]] |
transmit {**port-fifo** | **queue** | **supervisor-sram**} [**asic** *number* | **port** *number* [**asic** *number*]]
vct [**asic** *number* | **port** *number* [**asic** *number*]]
version}
[| {**begin** | **exclude** | **include**} *expression*]

構文の説明

cpu-queue-map-table [**asic** *number* | **port** *number* [**asic** *number*]]	CPU キュー マップ テーブル エントリを表示します。キーワードの意味は次のとおりです。 • **asic** *number* :（任意）指定された ASIC の情報を表示します。指定できる範囲は 0 ～ 1 です。 • **port** *number* :（任意）指定されたポートおよび ASIC 番号の情報を表示します。指定できる範囲は 0 ～ 27 です。
dest-map index *number*	指定されたインデックスの宛先マップ情報を表示します。指定できる範囲は 0 ～ 65535 です。
etherchannel-info [**asic** *number* | **port** *number* [**asic** *number*]]	EtherChannel 情報レジスタの内容を表示します。キーワードの意味は次のとおりです。 • **asic** *number* :（任意）指定された ASIC の情報を表示します。指定できる範囲は 0 ～ 1 です。 • **port** *number* :（任意）指定されたポートおよび ASIC 番号の情報を表示します。指定できる範囲は 0 ～ 27 です。0 はスーパーバイザで、1 ～ 25 はポートを示します。

exception [**asic** *number* | **port** *number* [**asic** *number*]]	例外インデックス レジスタ情報を表示します。キーワードの意味は次のとおりです。 • **asic** *number*：（任意）指定された ASIC の情報を表示します。指定できる範囲は 0 ～ 1 です。 • **port** *number*：（任意）指定されたポートおよび ASIC 番号の情報を表示します。指定できる範囲は 0 ～ 27 です。0 はスーパーバイザで、1 ～ 25 はポートを示します。
global-status [**asic** *number* | **port** *number* [**asic** *number*]]	グローバルおよび中断ステータスを表示します。キーワードの意味は次のとおりです。 • **asic** *number*：（任意）指定された ASIC の情報を表示します。指定できる範囲は 0 ～ 1 です。 • **port** *number*：（任意）指定されたポートおよび ASIC 番号の情報を表示します。指定できる範囲は 0 ～ 27 です。0 はスーパーバイザで、1 ～ 25 はポートを示します。
learning [**asic** *number* | **port** *number* [**asic** *number*]]	学習キャッシュ内のエントリを表示します。キーワードの意味は次のとおりです。 • **asic** *number*：（任意）指定された ASIC の情報を表示します。指定できる範囲は 0 ～ 1 です。 • **port** *number*：（任意）指定されたポートおよび ASIC 番号の情報を表示します。指定できる範囲は 0 ～ 27 です。0 はスーパーバイザで、1 ～ 25 はポートを示します。
mac-info [**asic** *number* | **port** *number* [**asic** *number*]]	MAC 情報レジスタの内容を表示します。キーワードの意味は次のとおりです。 • **asic** *number*：（任意）指定された ASIC の情報を表示します。指定できる範囲は 0 ～ 1 です。 • **port** *number*：（任意）指定されたポートおよび ASIC 番号の情報を表示します。指定できる範囲は 0 ～ 27 です。0 はスーパーバイザで、1 ～ 25 はポートを示します。
mvid [**asic** *number*]	マッピングされた VLAN ID テーブルを表示します。キーワードの意味は次のとおりです。 • **asic** *number*：（任意）指定された ASIC の情報を表示します。指定できる範囲は 0 ～ 1 です。
packet-info-ram [**asic** *number* | **index** *number* [**asic** *number*]]	パケット情報 RAM を表示します。キーワードの意味は次のとおりです。 • **asic** *number*：（任意）指定された ASIC の情報を表示します。指定できる範囲は 0 ～ 1 です。 • **index** *number*：（任意）指定されたパケット RAM インデックス番号および ASIC 番号の情報を表示します。指定できる範囲は 0 ～ 63 です。
port-info [**asic** *number* | **port** *number* [**asic** *number*]]	ポート情報レジスタ値を表示します。キーワードの意味は次のとおりです。 • **asic** *number*：（任意）指定された ASIC の情報を表示します。指定できる範囲は 0 ～ 1 です。 • **port** *number*：（任意）指定されたポートおよび ASIC 番号の情報を表示します。指定できる範囲は 0 ～ 27 です。0 はスーパーバイザで、1 ～ 25 はポートを示します。

prog-parser [**asic** *number* | **port** *number* [**asic** *number*]]	プログラマブル パーサー テーブルを表示します。キーワードの意味は次のとおりです。 • **asic** *number*：（任意）指定された ASIC の情報を表示します。指定できる範囲は 0 ～ 1 です。 • **port** *number*：（任意）指定されたポートおよび ASIC 番号の情報を表示します。指定できる範囲は 0 ～ 27 です。0 はスーパーバイザで、1 ～ 25 はポートを示します。
receive {**buffer-queue** | **port-fifo** | **supervisor-sram**} [**asic** *number* | **port** *number* [**asic** *number*]]	受信情報を表示します。キーワードの意味は次のとおりです。 • **buffer-queue**：バッファ キュー情報を表示します。 • **port-fifo**：ポート FIFO 情報を表示します。 • **supervisor-sram**：スーパーバイザ Static RAM（SRAM）情報を表示します。 • **asic** *number*：（任意）指定された ASIC の情報を表示します。指定できる範囲は 0 ～ 1 です。 • **port** *number*：（任意）指定されたポートおよび ASIC 番号の情報を表示します。指定できる範囲は 0 ～ 27 です。0 はスーパーバイザで、1 ～ 25 はポートを示します。
span [*vlan-id* | **asic** *number*]	Switched Port Analyzer（SPAN）関連情報を表示します。キーワードの意味は次のとおりです。 • *vlan-id*：（任意）指定された VLAN の情報を表示します。指定できる範囲は 0 ～ 1023 です。 • **asic** *number*：（任意）指定された ASIC の情報を表示します。指定できる範囲は 0 ～ 1 です。
stack {**control** | **dest-map** | **learning** | **messages** | **mvid** | **prog-parser** | **span** | **stats** [**asic** *number* | **port** *number* [**asic** *number*]}	スタック関連情報を表示します。キーワードの意味は次のとおりです。 • **control**：スタック制御ステータス レジスタ情報を表示します。 • **dest-map**：宛先マップ情報を表示します。 • **learning**：学習キャッシュ内のエントリを表示します。 • **messages**：スタック メッセージ レジスタ情報を表示します。 • **mvid**：マッピングされた VLAN ID テーブルのエントリを表示します。 • **prog-parser**：プログラマブル パーサー テーブルを表示します。 • **span**：SPAN 関連情報を表示します。 • **stats**：ポート ASIC の未処理の統計を表示します。 • **asic** *number*：（任意）指定された ASIC の情報を表示します。指定できる範囲は 0 ～ 1 です。 （注）　**port** *number*：（任意）指定されたポートおよび ASIC 番号の情報を表示します。指定できる範囲は 0 ～ 27 です。0 はスーパーバイザで、1 ～ 25 はポートを示します。

stats {**drop** | **enqueue** | **miscellaneous** | **supervisor**} [**asic** *number* | **port** *number* [**asic** *number*]]	ポート ASIC の未処理の統計を表示します。キーワードの意味は次のとおりです。 • **drop**：ドロップ統計情報を表示します。 • **enqueue**：エンキュー統計情報を表示します。 • **miscellaneous**：各種統計情報を表示します。 • **supervisor**：スーパーバイザ統計情報を表示します。 • **asic** *number*：（任意）指定された ASIC の情報を表示します。指定できる範囲は 0 ～ 1 です。 • **port** *number*：（任意）指定されたポートおよび ASIC 番号の情報を表示します。指定できる範囲は 0 ～ 27 です。0 はスーパーバイザで、1 ～ 25 はポートを示します。
transmit {**port-fifo** | **queue** | **supervisor-sram**} [**asic** *number* | **port** *number* [**asic** *number*]]	送信情報を表示します。キーワードの意味は次のとおりです。 • **port-fifo**：ポート FIFO 情報レジスタの内容を表示します。 • **queue**：キュー情報レジスタの内容を表示します。 • **supervisor-sram**：スーパーバイザ SRAM 情報を表示します。 • **asic** *number*：（任意）指定された ASIC の情報を表示します。指定できる範囲は 0 ～ 1 です。 • **port** *number*：（任意）指定されたポートおよび ASIC 番号の情報を表示します。指定できる範囲は 0 ～ 27 です。0 はスーパーバイザで、1 ～ 25 はポートを示します。
vct [**asic** *number* | **port** *number* [**asic** *number*]]	指定された ASIC または指定されたポートおよび ASIC の VLAN 圧縮テーブル エントリを表示します。キーワードの意味は次のとおりです。 • **asic** *number*：（任意）指定された ASIC の情報を表示します。指定できる範囲は 0 ～ 1 です。 • **port** *number*：（任意）指定されたポートおよび ASIC 番号の情報を表示します。指定できる範囲は 0 ～ 27 です。0 はスーパーバイザで、1 ～ 25 はポートを示します。
version	ポート ASIC のバージョンおよびデバイス タイプ情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform port-security

プラットフォームに依存するポート セキュリティ情報を表示するには、**show platform port-security** 特権 EXEC コマンドを使用します。

show platform port-security [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform qos

プラットフォームに依存する Quality of Service（QoS）情報を表示するには、**show platform qos** 特権 EXEC コマンドを使用します。

show platform qos {**label asic** *number* | **policer** {**parameters asic** *number* | **port alloc** *number* **asic** *number*}} [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

label asic *number*	指定された ASIC の QoS ラベル マップを表示します。 （任意）**asic** *number* に指定できる範囲は 0 ～ 1 です。
policer {**parameters asic** *number* | **port alloc** *number* **asic** *number*}	ポリサー情報を表示します。キーワードの意味は次のとおりです。 • **parameters asic** *number* : 指定された ASIC のパラメータ情報を表示します。指定できる範囲は 0 ～ 1 です。 • **port alloc** *number* **asic** *number*:指定されたポートおよび ASIC のポート割り当て情報を表示します。ポート割り当てに指定できる範囲は 0 ～ 25 です。ASIC に指定できる範囲は 0 ～ 1 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform resource-manager

プラットフォームに依存するリソース マネージャ情報を表示するには、**show platform resource-manager** 特権 EXEC コマンドを使用します。

show platform resource-manager {**dm** [**index** *number*] | **erd** [**index** *number*] | **mad** [**index** *number*] | **med** [**index** *number*] | **mod** | **msm** {**hash-table** [**vlan** *vlan-id*] | **mac-address** *mac-address* [**vlan** *vlan-id*]} | **sd** [**index** *number*] | **vld** [**index** *number*]} [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

dm [**index** *number*]	宛先マップを表示します。キーワードの意味は次のとおりです。 • **index** *number*：（任意）指定されたインデックスを表示します。指定できる範囲は 0 ～ 65535 です。
erd [**index** *number*]	指定されたインデックスの等価コスト ルート記述子テーブルを表示します。キーワードの意味は次のとおりです。 • **index** *number*：（任意）指定されたインデックスを表示します。指定できる範囲は 0 ～ 65535 です。
mad [**index** *number*]	指定されたインデックスの MAC アドレス記述子テーブルを表示します。キーワードの意味は次のとおりです。 • **index** *number*：（任意）指定されたインデックスを表示します。指定できる範囲は 0 ～ 65535 です。
med [**index** *number*]	指定されたインデックスのマルチエクスパンション記述子テーブルを表示します。キーワードの意味は次のとおりです。 • **index** *number*：（任意）指定されたインデックスを表示します。指定できる範囲は 0 ～ 65535 です。
mod	リソースマネージャ モジュール情報を表示します。
msm {**hash-table** [**vlan** *vlan-id*] | **mac-address** *mac-address* [**vlan** *vlan-id*]}	MAC アドレス記述子テーブルおよびステーション記述子テーブル情報を表示します。キーワードの意味は次のとおりです。 • **hash-table** [**vlan** *vlan-id*]：すべての VLAN または指定された VLAN のハッシュ テーブルを表示します。指定できる範囲は 1 ～ 4094 です。 • **mac-address** *mac-address* [**vlan** *vlan-id*]：すべての VLAN または指定された VLAN に対する 48 ビット ハードウェア アドレスで表される指定された MAC アドレスの MAC アドレス記述子テーブルを表示します。指定できる範囲は 1 ～ 4094 です。
sd [**index** *number*]	指定されたインデックスのステーション記述子テーブルを表示します。キーワードの意味は次のとおりです。 • **index** *number*：（任意）指定されたインデックスを表示します。指定できる範囲は 0 ～ 65535 です。
vld [**index** *number*]	指定されたインデックスの VLAN リスト記述子テーブルを表示します。キーワードの意味は次のとおりです。 • **index** *number*：（任意）指定されたインデックスを表示します。指定できる範囲は 0 ～ 65535 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。

| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform snmp counters

プラットフォームに依存する Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）カウンタ情報を表示するには、**show platform snmp counters** 特権 EXEC コマンドを使用します。

show platform snmp counters [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform spanning-tree

プラットフォームに依存するスパニング ツリー情報を表示するには、**show platform spanning-tree** 特権 EXEC コマンドを使用します。

show platform spanning-tree synchronization [**detail** | **vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

synchronization [**detail** | **vlan** *vlan-id*]	スパニング ツリー ステート同期情報を表示します。キーワードの意味は次のとおりです。 • **detail**：（任意）スパニング ツリー情報の詳細を表示します。 • **vlan** *vlan-id*：（任意）指定された VLAN の VLAN スイッチ スパニング ツリー情報を表示します。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform stp-instance

プラットフォームに依存するスパニング ツリー インスタンス情報を表示するには、**show platform stp-instance** 特権 EXEC コマンドを使用します。

show platform stp-instance *vlan-id* [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

vlan-id	指定された VLAN のスパニング ツリー インスタンス情報を表示します。指定できる範囲は 1 ～ 4094 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform stack manager

プラットフォームに依存するスタック情報を表示するには、**show platform stack-manager** 特権 EXEC コマンドを使用します。

show platform stack manager {**all** | **counters** | **trace** [**sdp** [**reverse**] | **state** [**reverse**]]} [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

all	スイッチ スタック全体の情報をすべて表示します。
counters	スタック マネージャ カウンタを表示します。
trace [**sdp** [**reverse**]]	追跡情報を表示します。キーワードの意味は次のとおりです。 • **sdp**：（任意）Stack Discovery Protocol（SDP; スタック ディスカバリ プロトコル）情報を表示します。 • **reverse**：（任意）追跡情報を逆順に（最新の情報から順にさかのぼって）表示します。
trace [**state** [**reverse**]]	追跡情報を表示します。キーワードの意味は次のとおりです。 • **state**：（任意）スタック ステート マシン情報を表示します。 • **reverse**：（任意）追跡情報を逆順に（最新の情報から順にさかのぼって）表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(50)SE	このコマンドの構文が **show platform stack-manager** から **show platform stack manager** に変更されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

スイッチ スタックのサマリー情報に表示されるステートは次のとおりです。

- Waiting：スイッチは起動中で、スタック内にある他のスイッチからの通信を待っています。スイッチはまだスタック マスターであるかどうかを判別していません。

  スタック マスター選出に参加していないスタック メンバは、スタック マスターが選出され準備ができるまで Waiting ステートのままです。

- Initializing：スイッチがスタック マスター ステータスを判別しました。スイッチがスタック マスターでない場合、このスイッチはスタック マスターからシステム レベルおよびインターフェイス レベルの設定を受信してロードしています。
- Ready：メンバがシステム レベルおよびインターフェイス レベルの設定のロードを完了し、トラフィックを転送できるようになっています。
- Master Re-Init：マスターの再選出で、異なるメンバがマスターに選出された直後のステート。新しいマスターがその設定を再初期化しています。このステートは、新しいマスターだけに適用されます。
- Ver Mismatch：Version-Mismatch モードのスイッチ。Version-Mismatch モードは、スタックに加入しているスイッチに、マスターとは異なるスタック プロトコル マイナー バージョン番号がある状態です。

スタック メンバ（スタック マスターを含む）の代表的なステート遷移は、Waiting -> Initializing -> Ready です。

マスター選出後のスタック マスターになるスタック メンバの代表的なステート遷移は、Ready -> Master Re-Init -> Ready です。

Version Mismatch モードのスタック メンバの代表的なステート遷移は、Waiting -> Ver Mismatch です。

show platform stack ports

プラットフォームに依存するスタック情報を表示するには、**show platform stack ports** 特権 EXEC コマンドを使用します。

show platform stack ports {**buffer** | **history**}[| {**begin** | **exclude** | **include**} *expression*]

構文の説明

buffer	StackWise ポート リンクおよび sync ステート イベントを表示します。
history	StackWise ポート履歴を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show platform stack port buffer** コマンドの出力を示します。

```
Switch# show platform stack ports buffer
              Stack Debug Event Data Trace
==============================================================
Event type LINK: Link status change
Event type RAC: RAC changes to Not OK
Event type SYNC: Sync changes to Not OK
==============================================================

  Event    Stack           Stack PCS Info              Ctrl-Status  Loopback   Cable
  Count    Port                                                     IOS / HW   length
=========  =====  ====================================  ===========  ========  ========
Event type: LINK OK Stack Port 1
0000000011   1    FF08FF00 860302A5 AA55FFFF FFFFFFFF   1CE61CE6     Yes/Yes  No cable
0000000011   2    FF08FF00 86031805 55AAFFFF FFFFFFFF   1CE61CE6     Yes/Yes  No cable
Event type: LINK OK Stack Port 2
0000000012   1    FF08FF00 860302A5 AA55FFFF FFFFFFFF   1CE61CE6     Yes/Yes  No cable
0000000012   2    FF08FF00 86031805 55AAFFFF FFFFFFFF   1CE61CE6     Yes/Yes  No cable
Event type: RAC
0000000013   1    FF08FF00 860302A5 AA55FFFF FFFFFFFF   1CE61CE6     Yes/Yes  No cable
0000000013   2    FF08FF00 86031805 55AAFFFF FFFFFFFF   1CE61CE6     Yes/Yes  No cable
```

次の例では、**show platform stack ports history** コマンドの出力を示します。

```
Switch# show platform stack ports history
Switch#/   Lost Sync   # times Link   # Changes
  Port#      Events        Not OK      To LinkOK
---------  -----------  ------------  ----------
  1/1               0             0           0
  1/2               3             4           3
  2/1               3             4           3
  2/2               0             0           0
  3/1               0             0           0
  3/2               0             0           0
```

show platform tb

スタック マスターを新しいスタック マスターに変更している間に、プラットフォーム依存の信頼性のある境界情報を表示するには、**show platform tb** 特権 EXEC コマンドを使用します。

show platform tb [| {begin | exclude | include} *expression*]

構文の説明

| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、**show platform tb** コマンドの出力を示します。

```
Switch# show platform tb
Print TB sub-block information
(Fa1/0/2) device:(Cisco phone)
/* current interfaces with TB enabled, and the trust device type */

Current master switch:(Yes)
/* Is this switch the current master switch?*/

New elected master   :(No)
/* Is the master switch-over occurred and this is the new master switch?*/

Master ready         :(No)
/* Is the Master switch in ready state?*/

HULC TB process on   :(No)
/* Is the TB platform process currently running?*/

CDP stable timer ON  :(No)(360 secs)
/* Is the CDP stable timer running?After the CDP stable timer expired, CDP neighbors of
all the TB enabled interfaces will be verified to make sure the replacement of IP phone
and PC did not happen during the master switch-over.*/

Print TB residue trust ports information
/* The interfaces with TB enabled right before master switch-over.*/
```

```
Print port CDP neighbor information
/* Is the CDP message still received after switch-over?*/

HULC TB is not detecting CDP events
/* Currently, this switch is not detecting any CDP event.*/
```

show platform tcam

プラットフォームに依存する Ternary Content Addressable Memory（TCAM）ドライバ情報を表示するには、**show platform tcam** 特権 EXEC コマンドを使用します。

show platform tcam {**errors** | **handle** *number* | **log-results** | **table** {**acl** | **all** | **equal-cost-route** | **ipv6** {**acl** | **qos** | **secondary**} **local** | **mac-address** | **multicast-expansion** | **qos** | **secondary** | **show platform tcam table equal-cost-route** [**asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [| {**begin** | **exclude** | **include**} *expression*]**station** | **vlan-list**} | **usage**} [**asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [| {**begin** | **exclude** | **include**} *expression*]

show platform tcam table acl [**asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [| {**begin** | **exclude** | **include**} *expression*]

show platform tcam table all [**asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [| {**begin** | **exclude** | **include**} *expression*]

show platform tcam table ipv6 {**acl** | **qos** | **secondary**} [**asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [| {**begin** | **exclude** | **include**} *expression*]

show platform tcam table local [**asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [| {**begin** | **exclude** | **include**} *expression*]

show platform tcam table mac-address [**asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [| {**begin** | **exclude** | **include**} *expression*]

show platform tcam table multicast-expansion [**asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [| {**begin** | **exclude** | **include**} *expression*]

show platform tcam table qos [**asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [| {**begin** | **exclude** | **include**} *expression*]

show platform tcam table secondary [**asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [| {**begin** | **exclude** | **include**} *expression*]

show platform tcam table station [**asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [| {**begin** | **exclude** | **include**} *expression*]

show platform tcam table vlan-list [[**asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

errors	Hulc Quality of Service（QoS）/Access Control List（ACL; アクセス コントロール リスト）TCAM Manager（HQATM）、Hulc Forwarding TCAM Manager（HFTM）、および TCAM で割り当てられていないスペース内での TCAM メモリ整合性検査エラーを表示します。
handle *number*	TCAM ハンドルを表示します。指定できる範囲は 0 ～ 4294967295 です。
log-results	TCAM ログ結果を表示します。
table {**acl** | **all** | **equal-cost-route** | **ipv6** {**acl** | **qos** | **secondary**} **local** | **mac-address** | **multicast-expansion** | **qos** | **secondary** | **station** | **vlan-list**}	ルックアップおよび転送テーブル情報を表示します。キーワードの意味は次のとおりです。 • **acl**：Access Control List（ACL; アクセス コントロール リスト）テーブルを表示します。 • **all**：すべての TCAM テーブルを表示します。 • **equal-cost-route**：等価コスト ルート テーブルを表示します。 • **ipv6**：IPv6 情報を表示します。 – **acl**：IPv6 ACL テーブル情報を表示します。 – **qos**：IPv6 QoS テーブル情報を表示します。 – **secondary**：IPv6 セカンダリ テーブル情報を表示します。 • **local**：ローカル テーブルを表示します。 • **mac-address**：MAC アドレス テーブルを表示します。 • **multicast-expansion**：IPv6 マルチキャスト拡張テーブルを表示します。 • **qos**：QoS テーブルを表示します。 • **secondary**：セカンダリ テーブルを表示します。 • **station**：ステーション テーブルを表示します。 • **vlan-list**：VLAN リスト テーブルを表示します。
usage	CAM（連想メモリ）および転送テーブル使用状況を表示します。
[[**asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]]	情報を表示します。キーワードの意味は次のとおりです。 • **asic** *number*：指定された ASIC のデバイス ID の情報を表示します。指定できる範囲は 0 ～ 15 です。 • **detail** [**invalid**]：（任意）有効または無効の詳細を表示します。 • **index** *number*：（任意）指定された TCAM テーブル インデックスの情報を表示します。指定できる範囲は 0 ～ 32768 です。 • **num** *number*：（任意）指定された TCAM テーブル番号の情報を表示します。指定できる範囲は 0 ～ 32768 です。
| **begin**	（任意）*expression* と一致する行から表示を開始します。
| **exclude**	（任意）*expression* と一致する行を表示から除外します。

| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

（注）　**usage** キーワードは、コマンドラインのヘルプ ストリングには表示されますが、サポートされていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。
12.2(55)SE	**errors** キーワー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、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform vlan

プラットフォームに依存する VLAN 情報を表示するには、**show platform vlan** 特権 EXEC コマンドを使用します。

show platform vlan {**misc** | **mvid** | **prune** | **refcount** | **rpc** {**receive** | **transmit**}} [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

misc	各種 VLAN モジュール情報を表示します。
mvid	Mapped VLAN ID（MVID）割り当て情報を表示します。
prune	スタック プルーニング データベースを表示します。
refcount	VLAN ロック モジュールについてのリファレンス カウントを表示します。
rpc {**receive** | **transmit**}	Remote Procedure Call（RPC; リモート プロシージャ コール）メッセージを表示します。キーワードの意味は次のとおりです。 • **receive**：受信した情報を表示します。 • **transmit**：送信した情報を表示します。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

show platform wireless-controller

Catalyst 3750G Integrated Wireless LAN Controller スイッチの内部ワイヤレス コントローラに関する情報を表示するには、**show platform wireless-controller** 特権 EXEC コマンドを使用します。

show platform wireless-controller [**management-info** | **status** | **summary**]
[*switch-number*]
[| {**begin** | **exclude** | **include**} *expression*]

構文の説明

management-info	（任意）ワイヤレス コントローラの管理インターフェイスに関する情報を表示します。
status	（任意）ワイヤレス コントローラ ステータス情報を表示します。
summary	（任意）ワイヤレス コントローラ サマリー情報を表示します。
switch-number	（任意）指定されたスタック メンバのワイヤレス コントローラ情報を表示します。指定できる範囲は 1 ～ 9 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(25)FZ	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

Integrated Wireless LAN Controller を内蔵したスタックにおけるスイッチのスタック番号を判別するには、**show platform wireless-controller** コマンドを入力します。このコマンドの出力では、コントローラにアクセスし、コントローラを設定するために使用するコントローラの MAC アドレスと IP アドレスも表示します。

このコマンドは、Catalyst 3750G Wireless Controller スイッチだけに適用されます。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

例

次の例では、キーワードを指定しない場合の **show platform wireless-controller** 特権 EXEC コマンドの出力を示します。

```
Switch# show platform wireless-controller
Wireless Controller in Switch 2
Operational Status of the Controller : operational
Service VLAN                         : 4095
```

```
Service Port Mac Address             : 000b.8540.3783
Service IP Address                   : 127.0.1.2
Management IP Address                : 22.2.2.2
Management VLAN                      : 7
Software Version                     : 3.3.0.3
Keepalive Version(controller/switch) : 1/1
Keepalives Missed                    : 0
Controller accepts http/https        : 0/1
Controller's Status Line             : up
Watchdog resets of Controller        : 0
Controller resets total              : 0
Unacknowledged control messages      : 0

Wireless Controller in Switch 3
Operational Status of the Controller : operational
Service VLAN                         : 4095
Service Port Mac Address             : 000b.8540.33e3
Service IP Address                   : 127.0.1.3
Management IP Address                : 8.8.8.8
Management VLAN                      : 8
Software Version                     : 3.3.0.3
Keepalive Version(controller/switch) : 1/1
Keepalives Missed                    : 0
Controller accepts http/https        : 0/1
Controller's Status Line             : up
Watchdog resets of Controller        : 0
Controller resets total              : 0
Unacknowledged control messages      : 0
```

次の例では、**show platform wireless-controller management-info** コマンドの出力を示します。

```
Switch# show platform wireless-controller management-info
sw vlan ip                gateway         http https mac            version
2  7    22.2.2.2/24       22.2.2.1        0    1     000b.8540.3783 3.3.0.3
3  8    8.8.8.8/24        8.8.8.1         0    1     000b.8540.33e3 3.3.0.3
```

次の例では、**show platform wireless-controller status** コマンドの出力を示します。

```
Switch# show platform wireless-controller status 1
Switch  Service IP      Management IP   SW Version      Status
------+---------------+---------------+---------------+-------
 2      127.0.1.2       22.2.2.2        3.3.0.3         operational
 3      127.0.1.3       8.8.8.8         3.3.0.3         operational
```

次の例では、**show platform wireless-controller summary** コマンドの出力を示します。

```
Switch# show platform wireless-controller summary
Switch  Status  State
2       up      operational
3       up      operational
```

APPENDIX D

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 pipe コマンドは、Henry Spencer の正規表現ライブラリ（regex）を使用しています。このライブラリの最新版は、ライブラリの旧バージョンとの互換性を保つために Catalyst オペレーティング システム ソフトウェアで若干修正されています。

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.

INDEX

A

aaa accounting dot1x コマンド 2-1

aaa authentication dot1x コマンド 2-3, 2-857

aaa authorization network コマンド 2-5, 2-24, 2-30, 2-32, 2-34, 2-36, 2-38, 2-150, 2-320, 2-495, B-7, B-35

AAA 方式 2-3, 2-857

access ports 2-813

ACE 2-134, 2-417

ACL

- deny コマンド 2-132
- IP 2-205
- 許可 2-415
- 照合 2-336
- 非 IP プロトコル対応 2-324
- 表示 2-476
- レイヤ 2 インターフェイス上 2-205

action コマンド 2-6

archive copy-sw コマンド 2-8

archive download-sw コマンド 2-11

archive tar コマンド 2-15

archive upload-sw コマンド 2-18

arp access-list コマンド 2-20

authentication command bounce-port ignore 2-22

authentication command disable-port ignore 2-23

authentication control-direction コマンド 2-24

authentication event コマンド 2-26

authentication fallback コマンド 2-30

authentication host-mode コマンド 2-32

authentication mac-move permit コマンド 2-34

authentication open コマンド 2-36

authentication order コマンド 2-38

authentication periodic コマンド 2-40

authentication port-control コマンド 2-42

authentication priority コマンド 2-44

authentication timer コマンド 2-46

authentication violation コマンド 2-48

auth-fail max-attempts コマンド

- 「dot1x auth-fail max-attempts コマンド」を参照

auth-fail vlan

- 「dot1x auth-fail vlan」を参照

auth open コマンド 2-36

auth order コマンド 2-38

auth timer コマンド 2-46

auto qos classify コマンド 2-50

auto qos trust コマンド 2-53

auto qos voip コマンド 2-56

B

BackboneFast、STP 用 2-729

boot auto-copy-sw コマンド 2-62

boot auto-download-sw コマンド 2-63

boot config-file コマンド 2-66

boot enable-break コマンド 2-67

boot helper-config file コマンド 2-69

boot helper コマンド 2-68

boot manual コマンド 2-70

boot private-config-file コマンド 2-71

boot system コマンド 2-72

boot（ブート ローダー）コマンド A-2

BPDU ガード、スパニング ツリー用 2-732, 2-767

BPDU フィルタリング、スパニング ツリー用 2-730, 2-767

C

Catalyst 3750G Integrated Wireless LAN Controller スイッチ 2-467
cat（ブート ローダー）コマンド A-4
CDP、プロトコル トンネリングのイネーブル化 2-300
channel-group コマンド 2-75
channel-protocol コマンド 2-79
Cisco SoftPhone
　auto-QoS の設定 2-56
　送信されたパケットを信頼する 2-375
CISP
　「Client Information Signalling Protocol」を参照
　debug platform cisp コマンド B-35
cisp enable コマンド 2-80
class-map コマンド 2-84
class コマンド 2-81
clear dot1x コマンド 2-86
clear eap sessions コマンド 2-87
clear errdisable interface 2-88
clear ip arp inspection log コマンド 2-89
clear ip arp inspection statistics コマンド 2-90
clear ipc コマンド 2-93
clear ip dhcp snooping database コマンド 2-91
clear ipv6 dhcp conflict コマンド 2-94
clear l2protocol-tunnel counters コマンド 2-95
clear lacp コマンド 2-96
clear mac address-table コマンド 2-97, 2-99
clear nmsp statistics コマンド 2-100
clear pagp コマンド 2-101
clear port-security コマンド 2-102
clear spanning-tree counters コマンド 2-104
clear spanning-tree detected-protocols コマンド 2-105
clear vmps statistics コマンド 2-106
clear vtp counters コマンド 2-107
Client Information Signalling Protocol 2-80, 2-150, 2-495, B-7, B-35
cluster commander-address コマンド 2-108
cluster discovery hop-count コマンド 2-110
cluster enable コマンド 2-111
cluster holdtime コマンド 2-112
cluster member コマンド 2-113
cluster outside-interface コマンド 2-115
cluster run コマンド 2-116
cluster standby-group コマンド 2-117
cluster timer コマンド 2-119
copy（ブート ローダー）コマンド A-5
CoS
　着信値の上書き 2-345
　着信パケットへのデフォルト値の割り当て 2-345
　レイヤ 2 プロトコル パケットへの割り当て 2-304
CoS/DSCP マップ 2-349
CPU ASIC 統計、表示 2-503
crashinfo ファイル 2-194

D

debug authentication B-2
debug auto qos コマンド B-4
debug backup コマンド B-6
debug cisp コマンド B-7
debug cluster コマンド B-8
debug dot1x コマンド B-10
debug dtp コマンド B-12
debug eap コマンド B-13
debug etherchannel コマンド B-14
debug ilpower コマンド B-15
debug interface コマンド B-16
debug ip dhcp snooping コマンド B-17
debug ip igmp filter コマンド B-19
debug ip igmp max-groups コマンド B-20
debug ip igmp snooping コマンド B-21
debug ip verify source packet コマンド B-18
debug lacp コマンド B-22
debug lldp packets コマンド B-23
debug mac-notification コマンド B-24
debug matm move update コマンド B-26
debug matm コマンド B-25

debug monitor コマンド B-27
debug mvrdbg コマンド B-29
debug nmsp コマンド B-30
debug nvram コマンド B-31
debug pagp コマンド B-32
debug platform acl コマンド B-33
debug platform backup interface コマンド B-34
debug platform cisp コマンド B-35
debug platform cli-redirection main コマンド B-36
debug platform configuration コマンド B-37, B-45
debug platform cpu-queues コマンド B-38
debug platform device-manager コマンド B-40
debug platform dot1x コマンド B-41
debug platform etherchannel コマンド B-42
debug platform fallback-bridging コマンド B-43
debug platform forw-tcam コマンド B-44
debug platform ip arp inspection コマンド B-46
debug platform ipc コマンド B-56
debug platform ip dhcp コマンド B-47
debug platform ip igmp snooping コマンド B-48
debug platform ip multicast コマンド B-50
debug platform ip source-guard コマンド B-52
debug platform ip unicast コマンド B-53
debug platform ip wccp コマンド B-55
debug platform led コマンド B-57
debug platform matm コマンド B-58
debug platform messaging application コマンド B-59
debug platform phy コマンド B-60
debug platform pm コマンド B-62
debug platform port-asic コマンド B-64
debug platform port-security コマンド B-65
debug platform qos-acl-tcam コマンド B-66
debug platform remote-commands コマンド B-67
debug platform resource-manager コマンド B-68
debug platform snmp コマンド B-69
debug platform span コマンド B-70
debug platform stack-manager コマンド B-71
debug platform supervisor-asic コマンド B-72
debug platform sw-bridge コマンド B-73
debug platform tcam コマンド B-74
debug platform udld コマンド B-77
debug platform vlan コマンド B-78
debug platform wireless-controller B-104
debug pm コマンド B-79
debug port-security コマンド B-81
debug qos-manager コマンド B-82
debug spanning-tree backbonefast コマンド B-85
debug spanning-tree bpdu-opt コマンド B-87
debug spanning-tree bpdu コマンド B-86
debug spanning-tree mstp コマンド B-88
debug spanning-tree switch コマンド B-90
debug spanning-tree uplinkfast コマンド B-92
debug spanning-tree コマンド B-83
debug sw-vlan ifs コマンド B-95
debug sw-vlan notification コマンド B-97
debug sw-vlan vtp コマンド B-99
debug sw-vlan コマンド B-93
debug udld コマンド B-101
debug vqpc コマンド B-103
define interface-range コマンド 2-120
delete コマンド 2-122
delete（ブート ローダー）コマンド A-6
deny（ARP アクセスリスト コンフィギュレーション）コマンド 2-124
deny（IPv6）コマンド 2-126
deny コマンド 2-132
DHCP スヌーピング
　イネーブル化
　　VLAN 上 2-241
　　インターフェイス上で信頼 2-239
　　オプション 82 2-233, 2-235
　エッジ スイッチからの信頼できないパケットの受け入れ 2-235
　エラー回復タイマー 2-191
　レート制限 2-238
DHCP スヌーピング バインディング データベース
　エージェント統計情報のクリア 2-91
　更新 2-453

データベース エージェント、設定 2-231
バインディング
削除 2-229
追加 2-229
表示 2-570
バインディング ファイル、設定 2-231
表示
データベースエージェント ステータス 2-572, 2-574
バインディング エントリ 2-570
dir（ブート ローダー）コマンド A-7
dot1x auth-fail max-attempts コマンド 2-144
dot1x auth-fail vlan 2-146
dot1x control-direction コマンド 2-148
dot1x credentials（グローバル コンフィギュレーション）コマンド 2-150
dot1x critical インターフェイス コンフィギュレーション コマンド 2-153
dot1x critical グローバル コンフィギュレーション コマンド 2-151
dot1x default コマンド 2-155
dot1x fallback コマンド 2-156
dot1x guest-vlan コマンド 2-157
dot1x host-mode コマンド 2-160
dot1x initialize コマンド 2-162
dot1x mac-auth-bypass コマンド 2-163
dot1x max-reauth-req コマンド 2-165
dot1x max-req コマンド 2-167
dot1x multiple-hosts コマンド 2-168
dot1x pae コマンド 2-169
dot1x port-control コマンド 2-170
dot1x re-authenticate コマンド 2-172
dot1x re-authentication コマンド 2-173
dot1x reauthentication コマンド 2-174
dot1x supplicant force-multicast コマンド 2-175
dot1x test eapol-capable コマンド 2-176
dot1x test timeout コマンド 2-177
dot1x timeout コマンド 2-178
dot1x violation-mode コマンド 2-181
dot1x コマンド 2-142
DSCP/CoS マップ 2-349
DSCP/DSCP 変換マップ 2-349
DTP 2-814
DTP ネゴシエーション 2-818
DTP フラップ
エラー回復タイマー 2-191
エラー検出 2-185
dual-purpose アップリンク ポート
設定可能なオプションの表示 2-554
duplex コマンド 2-182
dynamic auto VLAN メンバシップ モード 2-813
dynamic desirable VLAN メンバシップ モード 2-813
Dynamic Host Configuration Protocol（DHCP）
「DHCP スヌーピング」を参照
Dynamic Trunking Protocol（ダイナミック トランキング プロトコル）
「DTP」を参照

E

EAP-Request/Identity フレーム
再送信するまでの時間 2-178
送信する最高回数 2-167
encapsulation methods 2-833
epm access-control open 2-184
errdisable detect cause small-frame コマンド 2-188
errdisable detect cause コマンド 2-185
errdisable recovery cause small-frame 2-190
errdisable recovery コマンド 2-191
errdisable インターフェイス、表示 2-551
errdisable 検出 2-185
EtherChannel
EtherChannel/PAgP のデバッグ、表示 B-14
LACP
channel-group 情報のクリア 2-96
システム プライオリティ 2-307
デバッグ メッセージ、表示 B-22
表示 2-610
プロトコルの制限 2-79

ホットスタンバイ ポートのポート プライオリティ 2-305
モード 2-75
PAgP
channel-group 情報のクリア 2-101
エラー回復タイマー 2-191
エラー検出 2-185
学習方式 2-403
集約ポート ラーナー 2-403
送信トラフィックのインターフェイスのプライオリティ 2-405
デバッグ メッセージ、表示 B-32
表示 2-668
物理ポート ラーナー 2-403
モード 2-75
イーサネット インターフェイスのチャネル グループへの割り当て 2-75
インターフェイス情報、表示 2-551
表示 2-542
負荷分散方式 2-425
プラットフォーム特定イベントのデバッグ、表示 B-42
ポート チャネル論理インターフェイスの作成 2-199
レイヤ 2 プロトコル トンネリングのイネーブル化
LACP 2-301
PAgP 2-301
UDLD 2-301
exception crashinfo コマンド 2-194

F

fallback profile コマンド 2-195
flash_init（ブート ローダー）コマンド A-9
Flex Link
設定 2-806
表示 2-552
優先 VLAN の設定 2-809
flowcontrol コマンド 2-197
format（ブート ローダー）コマンド A-10
fsck（ブート ローダー）コマンド A-11

H

help（ブート ローダー）コマンド A-12
Hot Standby Router Protocol（ホットスタンバイ ルータ プロトコル）
「HSRP」を参照
HSRP
HSRP グループのクラスタへのバインド 2-117
スタンバイ グループ 2-117

I

IEEE 802.1Q トランク ポートおよびネイティブ VLAN 2-863
IEEE 802.1Q トンネル ポート
制限 2-814
設定 2-813
表示 2-522
IEEE 802.1x
違反エラーの回復 2-191
スイッチポート モード 2-815
「ポートベースの認証」も参照
IEEE 802.1x ポート ベース認証
ゲスト VLAN のサプリカントのイネーブル化 2-145, 2-156, 2-196
IGMP グループ、最大値の設定 2-245
IGMP 最大グループ、デバッグ B-20
IGMP スヌーピング
querier 2-253
イネーブル化 2-249
インターフェイスのトポロジ変更通知動作 2-259
クエリー要求 2-257
グループのスタティック メンバーとしてのポートの追加 2-263
スイッチのトポロジ変更通知動作 2-257
設定可能脱退タイマーのイネーブル化 2-251
即時脱退機能のイネーブル化 2-260
表示 2-578, 2-583, 2-585

フラッディング クエリー カウント 2-257
マルチキャスト テーブル 2-581
レポート抑制 2-255
IGMP フィルタ
適用 2-244
デバッグ メッセージ、表示 B-19
IGMP プロファイル
作成 2-247
表示 2-577
interface port-channel コマンド 2-199
interface range コマンド 2-201
interface vlan コマンド 2-203
Internet Group Management Protocol（インターネット グループ管理プロトコル）
「IGMP」を参照
ip access-group コマンド 2-205
ip address コマンド 2-208
ip admission name proxy http コマンド 2-211
ip admission コマンド 2-210
ip arp inspection filter vlan コマンド 2-213
ip arp inspection limit コマンド 2-215
ip arp inspection log-buffer コマンド 2-217
ip arp inspection trust コマンド 2-219
ip arp inspection validate コマンド 2-220
ip arp inspection vlan logging コマンド 2-223
ip arp inspection vlan コマンド 2-222
ip device tracking probe コマンド 2-225
ip device tracking コマンド 2-227
ip dhcp snooping binding コマンド 2-229
ip dhcp snooping database コマンド 2-231
ip dhcp snooping information option allow-untrusted コマンド 2-235
ip dhcp snooping information option format remote-id コマンド 2-237
ip dhcp snooping information option コマンド 2-233
ip dhcp snooping limit rate コマンド 2-238
ip dhcp snooping trust コマンド 2-239
ip dhcp snooping verify コマンド 2-240
ip dhcp snooping vlan information option format-type circuit-id string コマンド 2-242
ip dhcp snooping vlan コマンド 2-241
ip dhcp snooping コマンド 2-228
IP DHCP スヌーピング
「DHCP スヌーピング」を参照
ip igmp filter コマンド 2-244
ip igmp max-groups コマンド 2-245, 2-269, 2-271
ip igmp profile コマンド 2-247
ip igmp snooping last-member-query-interval コマンド 2-251
ip igmp snooping querier コマンド 2-253
ip igmp snooping report-suppression コマンド 2-255
ip igmp snooping tcn flood コマンド 2-259
ip igmp snooping tcn コマンド 2-257
ip igmp snooping vlan immediate-leave コマンド 2-260
ip igmp snooping vlan mrouter コマンド 2-261
ip igmp snooping vlan static コマンド 2-263
ip igmp snooping コマンド 2-249
IP Phone
auto-QoS の設定 2-56
送信されたパケットを信頼する 2-375
IP Precedence/DSCP マップ 2-349
ip snap forwarding コマンド 2-265
ip source binding コマンド 2-266
ip ssh コマンド 2-268
ipv6 access-list コマンド 2-275
ipv6 address dhcp コマンド 2-278
ipv6 dhcp client request vendor コマンド 2-279
ipv6 dhcp ping packets コマンド 2-280
ipv6 dhcp pool コマンド 2-281
ipv6 dhcp server コマンド 2-283
ipv6 mld snooping last-listener-query count コマンド 2-287
ipv6 mld snooping last-listener-query-interval コマンド 2-289
ipv6 mld snooping listener-message-suppression コマンド 2-291
ipv6 mld snooping robustness-variable コマンド 2-292
ipv6 mld snooping tcn コマンド 2-294
ipv6 mld snooping vlan コマンド 2-296
ipv6 mld snooping コマンド 2-285

IPv6 SDM テンプレート 2-457
ipv6 traffic-filter コマンド 2-298
IPv6 アクセス リスト、拒否条件 2-126
ip verify source コマンド 2-273
IP アドレス、設定 2-208
IP アドレスの照合 2-336
IP 送信元ガード
　スタティック IP 送信元バインディング 2-266
　ディセーブル化 2-273
　表示
　　設定 2-588
　　ダイナミック バインディング エントリのみ 2-570
　　バインディング エントリ 2-587
IP マルチキャスト アドレス 2-384

L

l2protocol-tunnel cos コマンド 2-304
l2protocol-tunnel コマンド 2-300
LACP
　「EtherChannel」を参照
lacp port-priority コマンド 2-305
lacp system-priority コマンド 2-307
Layer 2 モード、イネーブル化 2-800
Layer 3 モード、イネーブル化 2-800
Link Aggregation Control Protocol
　「EtherChannel」を参照
link state group コマンド 2-309
link state track コマンド 2-311
location（インターフェイス コンフィギュレーション）コマンド 2-314
location（グローバル コンフィギュレーション）コマンド 2-312
logging event power-inline-status コマンド 2-317
logging event コマンド 2-316
logging file コマンド 2-318

M

mab request format attribute 32 コマンド 2-320
mac access-group コマンド 2-322
mac access-list extended コマンド 2-324
mac address-table aging-time 2-322, 2-336
mac address-table aging-time コマンド 2-326
mac address-table learning コマンド 2-327
mac address-table move update コマンド 2-329
mac address-table notification コマンド 2-331
mac address-table static drop コマンド 2-334
mac address-table static コマンド 2-333
MAC アクセス リスト 2-132
MAC アクセス リスト コンフィギュレーション モード 2-324
MAC アドレス
　MACアドレス通知トラップのイネーブル化 2-331
　MAC アドレステーブル移行更新のイネーブル化 2-329
　VLAN ごとの MAC アドレス学習のディセーブル化 2-327
　固定スタック 2-787
　照合 2-336
　スタティック
　　インターフェイス上でドロップ 2-334
　　追加および削除 2-333
　　表示 2-638
　テーブル 2-623
　動的
　　エージング タイム 2-326
　　削除 2-97
　　表示 2-629
　表示
　　MAC アドレステーブル移行更新 2-634
　　VLAN 単位 2-640
　　VLAN のアドレス数 2-627
　　インターフェイス単位 2-631
　　エージング タイム 2-625
　　スタティック 2-638

スタティック エントリおよびダイナミック エントリ 2-621
すべて 2-623
通知設定 2-633, 2-636
動的 2-629
MAC アドレス グループ、表示 2-620
MAC アドレス通知、デバッグ B-24
match（アクセス マップ コンフィギュレーション）コマンド 2-336
match（クラスマップ コンフィギュレーション）コマンド 2-338
Maximum Transmission Unit（最大伝送ユニット）
「MTU」を参照
mdix auto コマンド 2-340
memory（ブート ローダー）コマンド A-13
mkdir（ブート ローダー）コマンド A-15
MLD スヌーピング
イネーブル化 2-285
クエリーの設定 2-287, 2-289
設定 2-291, 2-292
トポロジ変更通知の設定 2-294
表示 2-597, 2-599, 2-601, 2-603
mls qos aggregate-policer コマンド 2-343
mls qos cos コマンド 2-345
mls qos dscp-mutation コマンド 2-347
mls qos map コマンド 2-349
mls qos queue-set output buffers コマンド 2-353
mls qos queue-set output threshold コマンド 2-355
mls qos rewrite ip dscp コマンド 2-357
mls qos srr-queue input bandwidth コマンド 2-359
mls qos srr-queue input buffers コマンド 2-361
mls qos srr-queue input cos-map コマンド 2-363
mls qos srr-queue input dscp-map コマンド 2-365
mls qos srr-queue input priority-queue コマンド 2-367
mls qos srr-queue input threshold コマンド 2-369
mls qos srr-queue output cos-map コマンド 2-371
mls qos srr-queue output dscp-map コマンド 2-373
mls qos trust コマンド 2-375
mls qos vlan-based コマンド 2-378
mls qos コマンド 2-341
Mode ボタン、パスワード回復 2-462
monitor session コマンド 2-379
more（ブート ローダー）コマンド A-16
MSTP
MST リージョン
MST コンフィギュレーション モード 2-748
VLAN とインスタンス間のマッピング 2-748
現在または保留中の構成の表示 2-748
コンフィギュレーション リビジョン番号 2-748
設定名 2-748
表示 2-682
変更の中止 2-748
変更の適用 2-748
ステート情報の表示 2-681
ステート変更
BPDU ガードのイネーブル化 2-732, 2-767
BPDU フィルタリングのイネーブル化 2-730, 2-767
PortFast 対応ポートのシャットダウン 2-767
Port Fast のイネーブル化 2-767, 2-770
転送遅延時間 2-752
フォワーディング ステートへの高速移行 2-742
ブロッキング ステートからフォワーディング ステートへ 2-770
リスニングおよびラーニング ステートの期間 2-752
相互運用 2-105
パス コスト 2-750
表示 2-682
プロトコル移行プロセスの再開 2-105
プロトコル モード 2-746
リンク タイプ 2-742
ルート スイッチ
BPDU ドロップまでの最大ホップ数 2-757
BPDU メッセージの間隔 2-755
hello BPDU メッセージの間隔 2-753, 2-763
hello タイム 2-753, 2-763
拡張システム ID の影響 2-738

スイッチのプライオリティ 2-762
選択に関するポート プライオリティ 2-759
プライマリまたはセカンダリ 2-763
有効期限 2-755
ルート ポート
指定ポートの制限 2-740
ルート ガード 2-740
ルートとなるポートの制限 2-740
ループ ガード 2-740
MTU
グローバル設定の表示 2-694
サイズの設定 2-842
Multicase Listener Discovery
「MLD」を参照
Multicast Listener Discovery
「MLD」を参照
Multicast VLAN、MVR 2-385
Multicast VLAN Registration
「MVR」を参照
Multiple Spanning Tree Protocol
「MSTP」を参照
MVR
アドレスのエイリアス 2-385
インターフェイス情報の表示 2-660
インターフェイスの設定 2-387
設定 2-384
デバッグ メッセージ、表示 B-29
表示 2-658
メンバー、表示 2-662
mvr vlan group コマンド 2-388
mvr（インターフェイス コンフィギュレーション）コマンド 2-387
mvr（グローバル コンフィギュレーション）コマンド 2-384

N

Network Admission Control Software Configuration Guide 2-210, 2-212
network-policy profile（ネットワークポリシー コンフィギュレーション）コマンド 2-393
network-policy（グローバル コンフィギュレーション）コマンド 2-391
network-policy コマンド 2-390
nmsp attachment suppress コマンド 2-397
nmsp コマンド 2-395
no authentication logging verbose 2-398
no dot1x logging verbose 2-399
no mab logging verbose 2-400
nonegotiate、速度 2-779
non-stop forwarding 2-401
nsf コマンド 2-401

P

PAgP
「EtherChannel」を参照
pagp learn-method コマンド 2-403
pagp port-priority コマンド 2-405
permit（ARP アクセス リスト コンフィギュレーション）コマンド 2-407
permit（IPv6）コマンド 2-409
permit（MAC アクセス リスト コンフィギュレーション）コマンド 2-415
Per-VLAN Spanning-Tree Plus
「STP」を参照
PID、表示 2-564
PIM-DVMRP、マルチキャスト ルータ学習方式 2-261
PoE
コントローラ レジスタ値の表示 2-513
状態のロギング 2-317
電力管理情報の表示 2-674
電力管理モードの設定 2-426
電力設定 2-429
police aggregate コマンド 2-420
police コマンド 2-418
policy-map コマンド 2-422
Port Aggregation Protocol
「EtherChannel」を参照

port-channel load-balance コマンド 2-425
PortFast、スパニング ツリー用 2-770
power inline consumption コマンド 2-429
power inline コマンド 2-426
Power over Ethernet
「PoE」を参照
power rps コマンド（ユーザ EXEC） 2-431
priority-queue コマンド 2-434
private-vlan mapping コマンド 2-439
private-vlan コマンド 2-436
PVST+
「STP」を参照

Q

QoS
auto-QoS
設定 2-56
デバッグ メッセージ、表示 B-4
表示 2-485
auto-QoS trust
設定 2-53
DSCP 透過 2-357
DSCP の信頼できるポート
DSCP/DSCP 変換マップの定義 2-349
DSCP/DSCP 変換マップの適用 2-347
IP Phone の信頼される境界 2-375
VLAN ベース 2-378
イネーブル化 2-341
キュー、緊急キューのイネーブル化 2-434
クラス マップ
一致基準の定義 2-338
作成 2-84
表示 2-496
出力キュー
CoS 出力キューのしきい値マップの定義 2-371
CoS 出力キューのしきい値マップの表示 2-650
CoS 値のキューおよびしきい値へのマッピング 2-371
DSCP出力キューしきい値マップの定義 2-373
DSCP 出力キューのしきい値マップの表示 2-650
DSCP 値のキューおよびしきい値へのマッピング 2-373
WTD しきい値の設定 2-355
キューイングの方針の表示 2-646
キューセットの表示 2-653
最大および予約済みメモリ割り当ての設定 2-355
帯域幅共有とスケジューリングの有効化 2-785
帯域幅シェーピングとスケジューリングの有効化 2-783
バッファの割り当て 2-353
バッファ割り当ての表示 2-646
ポートでの最大出力の制限 2-781
ポートのキューセットへのマッピング 2-441
設定情報の表示 2-485, 2-642
着信パケットの CoS 値の定義 2-345
統計情報
キューに入れられた、または削除されたパケット 2-646
送受信した CoS 値 2-646
送受信した DSCP 値 2-646
プロファイル内外のパケット 2-646
入力キュー
CoS 値のキューおよびしきい値へのマッピング 2-363
CoS 入力キューのしきい値マップの定義 2-363
CoS 入力キューのしきい値マップの表示 2-650
DSCP 値のキューおよびしきい値へのマッピング 2-365
DSCP入力キューしきい値マップの定義 2-365
DSCP 入力キューのしきい値マップの表示 2-650
SRR スケジューリングの重みの割り当て 2-359
WTD しきい値の設定 2-369

キューイングの方針の表示 2-646
設定の表示 2-644
バッファの割り当て 2-361
バッファ割り当ての表示 2-646
プライオリティ キューのイネーブル化 2-367
ポートの信頼状態 2-375
ポリシー マップ
DSCP 値または IP precedence 値の設定 2-469
インターフェイスへの適用 2-464, 2-471
階層 2-423
作成 2-422
集約ポリサーの適用 2-420
信頼状態 2-850
トラフィックの分類 2-81
ポリサーの定義 2-343, 2-418
ポリサーの表示 2-643
ポリシー マップの表示 2-670
ポリシング設定 DSCP マップ 2-349
マップ
定義 2-349, 2-363, 2-365, 2-371, 2-373
表示 2-650
QoS のポートの信頼状態 2-375
Quality of Service
「QoS」を参照
queue-set コマンド 2-441

R

radius-server dead-criteria コマンド 2-442
radius-server host コマンド 2-444
Rapid Per-VLAN Spanning-Tree Plus
「STP」を参照
Rapid PVST+
「STP」を参照
rcommand コマンド 2-446
Redundant Power Supply
「RPS」を参照
reload コマンド 2-448
remote-span コマンド 2-451
Remote Switched Port Analyzer（リモート スイッチド ポート アナライザ）
「RSPAN」を参照
remote コマンド 2-450
rename（ブート ローダー）コマンド A-17
renew ip dhcp snooping database コマンド 2-453
reset（ブート ローダー）コマンド A-18
rmdir（ブート ローダー）コマンド A-19
rmon collection stats コマンド 2-456
RPS 2300
管理 2-431
設定 2-431
RSPAN
remote-span コマンド 2-451
RSPAN トラフィックのフィルタリング 2-379
セッション
表示 2-656
設定 2-379
表示 2-656

S

sdm prefer コマンド 2-457
SDM テンプレート
許容されるリソース 2-459
スタッキング 2-458
デュアル IPv4 および IPv6 2-457
表示 2-677
SDM ミスマッチ モード 2-458, 2-690
service password-recovery コマンド 2-462
service-policy コマンド 2-464
session コマンド 2-467
setup express コマンド 2-474
setup コマンド 2-471
set コマンド 2-469
set（ブート ローダー）コマンド A-20
show access-lists コマンド 2-476
show archive status コマンド 2-479
show arp access-list コマンド 2-480

show authentication コマンド 2-481
show auto qos コマンド 2-485
show boot コマンド 2-489
show cable-diagnostics tdr コマンド 2-491
show cisp コマンド 2-495
show class-map コマンド 2-496
show cluster candidates コマンド 2-499
show cluster members コマンド 2-501
show cluster コマンド 2-497
show controllers cpu-interface コマンド 2-503
show controllers ethernet-controller コマンド 2-505
show controllers power inline コマンド 2-513
show controllers tcam コマンド 2-515
show controller utilization コマンド 2-517
show dot1q-tunnel コマンド 2-522
show dot1x コマンド 2-523
show dtp 2-527
show eap コマンド 2-529
show env コマンド 2-532
show errdisable detect コマンド 2-536
show errdisable flap-values コマンド 2-538
show errdisable recovery コマンド 2-540
show etherchannel コマンド 2-542
show fallback profile コマンド 2-545
show flowcontrol コマンド 2-547
show idprom コマンド 2-549
show interfaces counters コマンド 2-561
show interfaces コマンド 2-551
show inventory コマンド 2-564
show ip arp inspection コマンド 2-565
show ipc コマンド 2-590
show ip dhcp snooping binding コマンド 2-570
show ip dhcp snooping database コマンド 2-572, 2-574
show ip dhcp snooping コマンド 2-569
show ip igmp profile コマンド 2-577
show ip igmp snooping address コマンド 2-599
show ip igmp snooping groups コマンド 2-581
show ip igmp snooping mrouter コマンド 2-583, 2-601
show ip igmp snooping querier コマンド 2-585, 2-603
show ip igmp snooping コマンド 2-578, 2-597
show ip source binding コマンド 2-587
show ipv6 access-list コマンド 2-594
show ipv6 dhcp conflict コマンド 2-596
show ipv6 route updated 2-605
show ip verify source コマンド 2-588
show l2protocol-tunnel コマンド 2-607
show lacp コマンド 2-610
show link state group コマンド 2-618
show lldp コマンド 2-614
show location 2-615
show mac access-group コマンド 2-620
show mac address-table address コマンド 2-623
show mac address-table aging time コマンド 2-625
show mac address-table count コマンド 2-627
show mac address-table dynamic コマンド 2-629
show mac address-table interface コマンド 2-631
show mac address-table learning コマンド 2-633
show mac address-table move update コマンド 2-634
show mac address-table notification コマンド 2-99, 2-636, B-26
show mac address-table static コマンド 2-638
show mac address-table vlan コマンド 2-640
show mac address-table コマンド 2-621
show mls qos aggregate-policer コマンド 2-643
show mls qos input-queue コマンド 2-644
show mls qos interface コマンド 2-646
show mls qos maps コマンド 2-650
show mls qos queue-set コマンド 2-653
show mls qos vlan コマンド 2-655
show mls qos コマンド 2-642
show monitor コマンド 2-656
show mvr interface コマンド 2-660
show mvr members コマンド 2-662
show mvr コマンド 2-658
show network-policy profile コマンド 2-664
show nmsp コマンド 2-665
show pagp コマンド 2-668
show platform acl コマンド C-2

show platform backup interface コマンド C-3
show platform configuration コマンド C-4
show platform etherchannel コマンド C-5
show platform forward コマンド C-6
show platform frontend-controller コマンド C-8
show platform igmp snooping コマンド C-9
show platform ipc trace コマンド C-17
show platform ip multicast コマンド C-11
show platform ip unicast コマンド C-12
show platform ipv6 unicast コマンド C-18
show platform ip wccp コマンド C-16
show platform layer4op コマンド C-20
show platform mac-address-table コマンド C-21
show platform messaging コマンド C-22
show platform monitor コマンド C-23
show platform mvr table コマンド C-24
show platform pm コマンド C-25
show platform port-asic コマンド C-26
show platform port-security コマンド C-30
show platform qos コマンド C-31
show platform resource-manager コマンド C-32
show platform snmp counters コマンド C-34
show platform spanning-tree コマンド C-35
show platform stack manager コマンド C-37
show platform stp-instance コマンド C-36
show platform tb コマンド C-41
show platform tcam コマンド C-43
show platform vlan コマンド C-46
show policy-map コマンド 2-670
show port security コマンド 2-671
show power inline コマンド 2-674
show sdm prefer コマンド 2-677
show setup express コマンド 2-680
show spanning-tree コマンド 2-681
show storm-control コマンド 2-687
show switch コマンド 2-689
show system mtu コマンド 2-694
show trust コマンド 2-850
show udld コマンド 2-695
show version コマンド 2-698
show vlan access-map コマンド 2-705
show vlan filter コマンド 2-706
show vlan コマンド 2-700
show vlan コマンド、フィールド 2-702
show vmps コマンド 2-707
show vtp コマンド 2-709
shutdown vlan コマンド 2-715
shutdown コマンド 2-714
small violation-rate コマンド 2-716
snmp-server enable traps コマンド 2-718
snmp-server host コマンド 2-723
snmp trap mac-notification change コマンド 2-727
SNMP 通知、送信のイネーブル 2-718
SNMP トラップ
　MAC アドレス通知機能のイネーブル化 2-331
　MACアドレス通知トラップのイネーブル化 2-727
　送信のイネーブル化 2-718
SNMP ホスト、指定 2-723
SoftPhone
　「Cisco SoftPhone」を参照
SPAN
　SPAN トラフィックのフィルタリング 2-379
　セッション
　　インターフェイスへの追加 2-379
　　新規に開始 2-379
　　表示 2-656
　設定 2-379
　デバッグ メッセージ、表示 B-27
　表示 2-656
spanning-tree backbonefast コマンド 2-729
spanning-tree bpdufilter コマンド 2-730
spanning-tree bpduguard コマンド 2-732
spanning-tree cost コマンド 2-734
spanning-tree etherchannel コマンド 2-736
spanning-tree extend system-id コマンド 2-738
spanning-tree guard コマンド 2-740
spanning-tree link-type コマンド 2-742
spanning-tree loopguard default コマンド 2-744

spanning-tree mode コマンド 2-746
spanning-tree mst configuration コマンド 2-748
spanning-tree mst cost コマンド 2-750
spanning-tree mst forward-time コマンド 2-752
spanning-tree mst hello-time コマンド 2-753
spanning-tree mst max-age コマンド 2-755
spanning-tree mst max-hops コマンド 2-757
spanning-tree mst port-priority コマンド 2-759
spanning-tree mst pre-standard コマンド 2-761
spanning-tree mst priority コマンド 2-762
spanning-tree mst root コマンド 2-763
spanning-tree portfast（インターフェイス コンフィギュレーション）コマンド 2-770
spanning-tree portfast（グローバル コンフィギュレーション）コマンド 2-767
spanning-tree port-priority コマンド 2-765
Spanning Tree Protocol（スパニング ツリー プロトコル）
「STP」を参照
spanning-tree transmit hold-count コマンド 2-773
spanning-tree uplinkfast コマンド 2-774
spanning-tree vlan コマンド 2-776
speed コマンド 2-779
srr-queue bandwidth limit コマンド 2-781
srr-queue bandwidth share コマンド 2-785
SSH、バージョンの設定 2-268
stack-mac persistent timer コマンド 2-787
storm-control コマンド 2-790
STP
BackboneFast 2-729
EtherChannel の設定矛盾 2-736
VLAN オプション 2-762, 2-776
カウンタ、クリア 2-104
拡張システム ID 2-738
間接リンク障害の検出 2-729
ステート情報の表示 2-681
ステート変更
BPDU ガードのイネーブル化 2-732, 2-767
BPDU フィルタリングのイネーブル化 2-730, 2-767
PortFast 対応ポートのシャットダウン 2-767
Port Fast のイネーブル化 2-767, 2-770
エラー ステートから回復するタイマーのイネーブル化 2-191
転送遅延時間 2-776
ブロッキング ステートからフォワーディング ステートへ 2-770
リスニングおよびラーニング ステートの期間 2-776
デバッグ メッセージ、表示
BackboneFast イベント B-85
MSTP B-88
UplinkFast B-92
最適化された BPDU 処理 B-87
スイッチ シム B-90
スパニングツリーのアクティビティ B-83
送受信された BPDU B-86
パス コスト 2-734
プロトコル トンネリングのイネーブル化 2-300
プロトコル モード 2-746
ルート スイッチ
BPDU メッセージの間隔 2-776
hello BPDU メッセージの間隔 2-776
hello タイム 2-776
拡張システム ID の影響 2-738, 2-777
スイッチのプライオリティ 2-776
選択に関するポート プライオリティ 2-765
プライマリまたはセカンダリ 2-776
有効期限 2-776
ルート ポート
UplinkFast 2-774
新しいルート ポート選択の高速化 2-774
指定ポートの制限 2-740
ルート ガード 2-740
ルートとなるポートの制限 2-740
ループ ガード 2-740
STP の拡張システム ID 2-738
SVI、作成 2-203
SVI ステータスの計算 2-804
Switched Port Analyzer（スイッチド ポート アナライザ）
「SPAN」を参照

switchport access コマンド 2-802
switchport autostate exclude コマンド 2-804
switchport backup interface コマンド 2-806
switchport block コマンド 2-810
switchport host コマンド 2-812
switchport mode private-vlan コマンド 2-816
switchport mode コマンド 2-813
switchport nonegotiate コマンド 2-818
switchport port-security aging コマンド 2-825
switchport port-security コマンド 2-820
switchport priority extend コマンド 2-827
switchport private-vlan コマンド 2-829
switchport protected コマンド 2-831
switchport trunk コマンド 2-833
switchport voice vlan コマンド 2-837, 2-838
switchport コマンド 2-800
switch priority コマンド 2-793, 2-795
switch provision コマンド 2-796
switch renumber コマンド 2-798
system env temperature threshold yellow コマンド 2-840
system mtu コマンド 2-842

T

tar ファイル、作成、一覧表示、および抽出 2-15
TDR、実行 2-844
Telnet、クラスタ スイッチへの通信に使用 2-446
test cable-diagnostics tdr コマンド 2-844
traceroute mac ip コマンド 2-848
traceroute mac コマンド 2-845
trunk ports 2-813
type（ブート ローダー）コマンド A-23

U

UDLD
　アグレッシブ モード 2-852, 2-854
　インターフェイスごとのイネーブル化 2-854
　エラー回復タイマー 2-191
　グローバルにイネーブル化 2-852
　シャットダウン インターフェイスのリセット 2-856
　ステータス 2-695
　デバッグ メッセージ、表示 B-101
　ノーマル モード 2-852, 2-854
　メッセージ タイマー 2-852
udld port コマンド 2-854
udld reset コマンド 2-856
udld コマンド 2-852
UniDirectional 2-730
UniDirectional Link Detection（単方向リンク検出）
　「UDLD」を参照
unset（ブート ローダー）コマンド A-24
UplinkFast、STP 用 2-774

V

Version Mismatch モード 2-690, C-38
version（ブート ローダー）コマンド A-26
VLAN
　MAC アドレス
　　数 2-627
　　表示 2-640
　VTP の SNMP トラップ 2-721, 2-724
　ゲスト VLAN のサプリカントのイネーブル化 2-145, 2-156, 2-196
　再起動 2-715
　シャットダウン 2-715
　設定 2-859
　設定の表示 2-700
　中断 2-715
　デバッグ メッセージ、表示
　　ISL B-97
　　VLAN IOS File System エラー テスト B-95
　　VLAN マネージャのアクティビティ B-93
　　VTP B-99
　標準範囲 2-859

プライベート 2-816
設定 2-436
表示 2-700
「プライベート VLAN」も参照
vlan access-map コマンド 2-860
vlan dot1q tag native コマンド 2-863
vlan filter コマンド 2-865
VLAN Query Protocol
「VQP」を参照
VLAN Trunking Protocol
「VTP」を参照
VLAN アクセス マップ
アクション 2-6
表示 2-705
VLAN アクセス マップ コンフィギュレーション モード 2-860
VLAN コンフィギュレーション モード
概要 1-3
コマンド
VLAN 2-859
VTP 2-878
説明 1-5
入力 2-862
VLAN での MLD スヌーピング、イネーブル化 2-296
VLAN フィルタ、表示 2-706
VLAN ベースの QoS 2-378
VLAN マップ
作成 2-860
定義 2-336
適用 2-865
表示 2-705
VMPS
エラー回復タイマー 2-192
サーバの設定 2-870
ダイナミック VLAN 割り当ての再確認 2-867
表示 2-707
vmps reconfirm（グローバル コンフィギュレーション）コマンド 2-868
vmps reconfirm（特権 EXEC）コマンド 2-867
vmps retry コマンド 2-869
vmps server コマンド 2-870
VM モード 2-690, C-38
VQP
クライアント統計情報のクリア 2-106
サーバごとの再試行回数 2-869
再確認間隔 2-868
情報の表示 2-707
ダイナミック VLAN 割り当ての再確認 2-867
ダイナミック アクセス ポート 2-803
VTP
ポート単位でのイネーブル化 2-877
vtp
イネーブル化
トンネリング 2-300
バージョン 2 2-873
プルーニング 2-873
カウンタ表示フィールド 2-710
情報の表示 2-709
ステータス 2-709
ステータス表示フィールド 2-712
設定
ドメイン名 2-872
パスワード 2-873
ファイル名 2-872
モード 2-872
統計情報 2-709
特性の変更 2-872
プルーニング 2-873
プルーニング カウンタのクリア 2-107
モード 2-872
vtp primary コマンド 2-879
vtp（インターフェイス コンフィギュレーション）コマンド 2-877
vtp（グローバル コンフィギュレーション）コマンド 2-872

X

XENPAK モジュール シリアル EERPOM 情報 2-509, 2-549

あ

アクセス グループ
IP 2-205
MAC、表示 2-620
アクセス コントロール エントリ
「ACE」を参照
アクセス コントロール リスト
「ACL」を参照
アクセスマップ コンフィギュレーション モード 2-336
アクセス モード 2-813
アクセス リスト、IPv6 2-275
アップグレード
ソフトウェア イメージ
コピー 2-8
ステータスのモニタリング 2-479
ダウンロード 2-11
アドレスのエイリアス 2-385

い

イーサネット コントローラ、内部レジスタの表示 2-505
イーサネット統計情報、収集 2-456
イメージ
「ソフトウェア イメージ」を参照
インターフェイス
MAC アドレス テーブルの表示 2-631
イーサネット インターフェイスのチャネル グループへの割り当て 2-75
再起動 2-714
設定 2-182
ディセーブル化 2-714
デバッグ メッセージ、表示 B-16
複数の設定 2-201
ポート チャネル論理の作成 2-199
インターフェイス コンフィギュレーション モード 1-3, 1-4
インターフェイスの速度、設定 2-779
インターフェイス範囲マクロ 2-120

え

エラー条件、表示 2-538

お

音声 VLAN
設定 2-837, 2-838
ポート プライオリティの設定 2-827
温度情報、表示 2-532
オンライン診断
グローバル コンフィギュレーション モード
テストベースのテスト スケジュールのクリア 2-138
テストベースのテストの設定 2-138
ヘルス モニタ診断テスト スケジュールのクリア 2-89
ヘルス モニタ診断テスト スケジュールのセットアップ 2-89
ヘルス モニタ診断テストの設定 2-89
スケジューリング
イネーブル化 2-138
削除 2-138
スケジュールされたスイッチオーバー
イネーブル化 2-138
ディセーブル化 2-138
テスト、開始 2-140
テスト間隔、設定 2-138
表示
イベント ログ 2-519
現在スケジュールされているタスク 2-519
サポートされるテスト スイート 2-519
設定されたブートアップ カバレッジ レベル 2-519

テスト ID 2-519
テスト結果 2-519
テスト統計 2-519
ヘルス モニタリング診断テスト、設定 2-135

か

階層ポリシー マップ 2-423
回復メカニズム
原因 2-191
タイマーの間隔 2-192
表示 2-88, 2-491, 2-536, 2-540
拡張検出、候補スイッチの 2-110
拡張範囲 VLAN
許可 VLAN リスト 2-833
プルーニング適格リスト 2-833
環境変数、表示 2-489

き

起動
Cisco IOS イメージ 2-72
環境変数の表示 2-489
手動 2-70
中断 2-63, 2-67
許可 VLAN 2-833
許可ステート、制御ポートの 2-170

く

クエリー時間、MVR 2-384
クラスタ
HSRP グループのクラスタへのバインド 2-117
HSRP スタンバイ グループ 2-117
SNMP トラップ 2-718
拡張検出のホップ カウント制限 2-110
候補の追加 2-113
冗長性 2-117
通信
Telnet を使用したメンバー 2-446
クラスタの外部にある装置 2-115
デバッグ メッセージ、表示 B-8
入力して設定 2-113
表示
候補スイッチ 2-499
ステータス 2-497
デバッグ メッセージ B-8
メンバー スイッチ 2-501
クラス マップ
一致基準の定義 2-338
作成 2-84
表示 2-496
クリティカル VLAN 2-27
グローバル コンフィギュレーション モード 1-2, 1-4

こ

候補スイッチ
「クラスタ」を参照
コマンド スイッチ
「クラスタ」を参照
混合ポート、プライベート VLAN 2-816
コントローラ、ワイヤレス 2-467
コンフィギュレーション ファイル
名前の指定 2-66, 2-71
パスワード回復のディセーブル時の考慮事項 A-1

さ

サービス クラス
「CoS」を参照
再認証
試行間隔 2-178
定期的 2-174
再認証、IEEE 802.1x 対応ポートの 2-172

し

システム メッセージのログ 2-317
システム メッセージのログ、フラッシュへのメッセージの保存 2-318
システム リソース テンプレート 2-457
自動ネゴシエーション、デュプレックス モードの 2-183
シャットダウンしきい値、レイヤ 2 プロトコル トンネリング 2-300
ジャンボ フレーム
　「MTU」を参照
集約ポート ラーナー 2-403
受信、フロー制御パケットの 2-197
冗長性、クラスタ スイッチの 2-117
信頼される境界、QoS の 2-375

す

スイッチポート、表示 2-551
スイッチング、特徴
　インターフェイスに戻る 2-800
　変更 2-800
スケジュールされたスイッチオーバー
　イネーブル化 2-138
　ディセーブル化 2-138
スタック、スイッチ
　MAC アドレス 2-787
　新しいメンバーのプロビジョニング 2-796
　スタック メンバー アクセス 2-467
　スタック メンバーの数 2-689, 2-798
　スタック メンバーのプライオリティ値 2-689, 2-795
　メンバーのイネーブル化 2-793
　メンバーのディセーブル化 2-793
　リロード 2-448
スタック メンバー
　アクセス 2-467
　数 2-689, 2-798
　プライオリティ値 2-795
　プロビジョニング 2-796
　リロード 2-448
スタティック アクセス ポート、設定 2-802
スティッキ ラーニング、イネーブル化 2-820

せ

制限 VLAN
　「dot1x auth-fail vlan」を参照
製品 ID 情報、表示 2-564
セキュア ポート、制限 2-822
設定、複数のインターフェイスの 2-201

そ

送信、フロー制御パケットの 2-197
送信元ポート、MVR 2-387
即時脱退機能、MVR 2-387
即時脱退処理 2-260
即時脱退処理、IPv6 2-296
ソフトウェア イメージ
　アップグレード 2-8, 2-11
　アップロード 2-18
　コピー 2-8
　削除 2-122
　ダウンロード 2-11
ソフトウェア バージョン、表示 2-698

た

ダイナミック ARP 検査
　ARP ACL
　　VLAN に適用 2-213
　　定義 2-20
　　パケットの許可 2-407
　　パケットの拒否 2-124
　　表示 2-480
　clear

統計情報 2-90
log buffer
configure 2-217
VLAN 単位でイネーブル化 2-222
インターフェイスの信頼状態 2-219
エラー回復タイマー 2-191
エラー検出 2-185
記録するパケットのタイプ 2-223
クリア
ログ バッファ 2-89
検証チェック 2-220
着信 ARP パケットのレート制限 2-215
統計情報
クリア 2-90
表示 2-565
表示
ARP ACL 2-480
信頼状態およびレート制限 2-565
設定および動作ステート 2-565
統計情報 2-565
ログ バッファ 2-565
ログ バッファ
クリア 2-89
表示 2-565
ダイナミック アクセス ポート
制限 2-803
設定 2-802
弾力的、認証、順序付け 2-38

て

定義済みのコマンド モード 1-2
ディレクトリ、削除 2-122
電源情報、表示 2-532
転送結果、表示 C-6
テンプレート、システム リソース 2-457

と

統計情報、イーサネット グループ 2-456
特権 EXEC モード 1-2, 1-3
ドメイン名、VTP 2-872
トランキング、VLAN モード 2-813
トランク、DTP をサポートしないデバイス 2-814
トランク モード 2-813, 2-814
ドロップしきい値、レイヤ 2 プロトコル トンネリング 2-301
トンネル ポート、レイヤ 2 プロトコル、表示 2-607

な

内部レジスタ、表示 2-505, 2-515

に

認証失敗 VLAN
「dot1x auth-fail vlan」を参照

ね

ネイティブ VLAN 2-833
ネイティブ VLAN タギング 2-863

は

ハードウェア ACL 統計情報 2-476
パケットの転送、ACL の一致 2-6
パケットのドロップ、ACL の一致 2-6
パスワード、VTP 2-873
パスワード回復メカニズム、イネーブル化およびディセーブル化 2-462
バックアップ、インターフェイス
設定 2-806
表示 2-552

ひ

非 IP トラフィック アクセス リスト 2-324
非 IP トラフィックの転送
許可 2-415
拒否 2-132
非 IP プロトコル
拒否 2-132
転送 2-415
非ネゴシエーション DTP メッセージング 2-818
標準範囲 VLAN 2-859

ふ

ファイル、削除 2-122
ファイル名、VTP 2-872
ファン 2-532
ファン情報、表示 2-532
ブート ローダー
アクセス A-1
環境変数
設定 A-20
設定の表示 A-20
説明 A-20
場所 A-21
リセット A-24
起動
Cisco IOS イメージ A-2
ヘルパー イメージ 2-68
システムのリセット A-18
ディレクトリ
削除 A-19
作成 A-15
リストの表示 A-7
表示
使用可能なコマンド A-12
バージョン A-26
メモリ ヒープ使用率 A-13
ファイル
コピー A-5
削除 A-6
内容の表示 A-4, A-16, A-23
名前変更 A-17
リストの表示 A-7
ファイル システム
一貫性チェックの実行 A-11
フォーマット A-10
フラッシュの初期化 A-9
プロンプト A-1
フォールバック プロファイル、表示 2-545
負荷分散方式、EtherChannel 2-425
物理ポート ラーナー 2-403
不明なマルチキャスト トラフィック、回避 2-810
不明なユニキャスト トラフィック、回避 2-810
プライオリティ値、スタック メンバー 2-689, 2-795
プライベート VLAN
アソシエーション 2-829
混合ポート 2-816
設定 2-436
表示 2-700
ポートの設定 2-816
ホスト ポート 2-816
マッピング
設定 2-829
表示 2-551
プルーニング
VLAN 2-833
VTP
イネーブル化 2-873
インターフェイス情報の表示 2-551
プルーニング適格 VLAN リスト 2-835
フレーム転送情報、表示 C-6
ブロードキャスト ストーム制御 2-790
フロントエンド コントローラ、カウンタおよびステータス情報 C-8

ほ

ポート セキュリティ
- イネーブル化 2-820
- 違反エラーの回復 2-191
- エージング 2-825
- デバッグ メッセージ、表示 B-81

ポート タイプ、MVR 2-387
ポート、デバッグ B-79
ポートの信頼状態、QoS のポート 2-375
ポート範囲、定義 2-120
ポートベース認証
- AAA 方式のリスト 2-3, 2-857
- IEEE 802.1x AAA アカウンティング方式 2-1
- IEEE 802.1x 対応ポートの再認証 2-172
- IEEE 802.1x のイネーブル化
  - インターフェイス単位 2-170
  - グローバル 2-142
- IEEE 802.1x の準備テスト 2-176
- MAC 認証バイパス 2-163
- 違反モードの設定 2-181
- インターフェイスの初期化 2-162, 2-177
- オーセンティケータとしての PAE 2-169
- 許可ステートの手動制御 2-170
- ゲスト VLAN 2-157
- スイッチからクライアントへの再送信時間 2-178
- スイッチから認証サーバへの再送信時間 2-178
- スイッチとクライアント間のフレーム再送信回数 2-167, 2-165
- 設定可能な IEEE 802.1x パラメータのリセット 2-155
- 定期的な再認証
  - イネーブル化 2-174
  - 試行間隔 2-178
- デバッグ メッセージ、表示 B-10
- 認証交換に失敗したあとの待機期間 2-178
- ホスト モード 2-160

ポート、保護 2-831
保護ポート、表示 2-556
ホスト接続、ポート設定 2-812
ホスト ポート、プライベート VLAN 2-816
ホップ カウント制限、クラスタの 2-110
ポリシー マップ
- インターフェイスへの適用 2-464, 2-471
- 階層 2-423
- 作成 2-422
- トラフィックの分類
  - DSCP 値または IP precedence 値の設定 2-469
  - クラスの定義 2-81
  - 信頼状態の定義 2-850
- 表示 2-670
- ポリサー
  - 単一クラス用 2-418
  - 表示 2-643
  - 複数のクラス 2-343, 2-420
  - ポリシング設定 DSCP マップ 2-349

ポリシング設定 DSCP マップ 2-349

ま

マクロ
- インターフェイス範囲 2-120, 2-201

マップ
- QoS
  - 定義 2-349
  - 表示 2-650
- VLAN
  - 作成 2-860
  - 定義 2-336
  - 表示 2-705

マルチキャスト グループ、MVR 2-385
マルチキャスト グループ アドレス、MVR 2-387
マルチキャスト ストーム制御 2-790
マルチキャスト ルータ学習方式 2-261
マルチキャスト ルータ ポート、IPv6 2-296
マルチキャスト ルータ ポート、設定 2-261

む

無効な GBIC
エラー回復タイマー 2-191
エラー検出 2-185

め

メカニズムの検出、原因 2-185
メンバー スイッチ
「クラスタ」を参照

も

モード、MVR 2-384
モード、コマンド 1-2

ゆ

ユーザ EXEC モード 1-2, 1-3
ユニキャスト ストーム制御 2-790

ら

ライン コンフィギュレーション モード 1-3, 1-5

り

リソース テンプレート、表示 2-677
リンク フラップ
エラー回復タイマー 2-191
エラー検出 2-185

る

ルーテッド ポート
IP アドレス 2-209
サポートされる数 2-209
ルート 2-740
ルート ガード、スパニング ツリー用 2-740
ループ ガード、スパニング ツリー用 2-740, 2-744
ループバック エラー
回復タイマー 2-191
検出 2-185

れ

レイヤ 2 traceroute
IP アドレス 2-848
MAC アドレス 2-845
レイヤ 2 プロトコル トンネリング エラー回復 2-302
レイヤ 2 プロトコル トンネル
エラー回復タイマー 2-191
エラー検出 2-185
レイヤ 2 プロトコル トンネル カウンタ 2-95
レイヤ 2 プロトコル トンネル ポート、表示 2-607
レシーバ ポート、MVR 2-387

ろ

論理インターフェイス 2-199

わ

ワイヤレス コントローラ、アクセス 2-467
ワイヤレス コントローラ スイッチ B-104